Carlos Ivorra Castillo

EL CÁLCULO SECUENCIAL DE GENTZEN

El finitismo de Hilbert, con su requisito de ser "intuitivo", tiene una frontera muy poco natural.

KURT GÖDEL

Índice General

Introducción

En [LM] hemos presentado un cálculo deductivo $K_{\mathcal{L}}$ que formaliza el concepto de deducción lógica que usan los matemáticos. Esto significa, por una parte, que

1. Un matemático considera que una fórmula de un lenguaje formal $\mathcal{L}$ es lógicamente deducible a partir de unas premisas —en el sentido vago de que hay un argumento que garantiza que si las premisas son verdaderas la conclusión también tiene que serlo— si y sólo si existe una deducción en $K_{\mathcal{L}}$ de dicha fórmula a partir de las premisas dadas, que es algo definido con total precisión.

Y por otra parte, que

2. El concepto de deducción en $K_{\mathcal{L}}$ es puramente formal, es decir, que no depende para nada del posible significado de las fórmulas consideradas.

Sin embargo, en la práctica, los razonamientos en $K_{\mathcal{L}}$ tienen un aspecto bastante "caótico" si se examinan en términos puramente formales, y sólo se capta su "lógica" cuando uno se para a pensar en ese significado que en teoría debería ser irrelevante.

Por ejemplo, aquí tenemos un ejemplo de razonamiento formal presentado como ejemplo en el capítulo II de [LM]:

$$
\begin{array}{rll}
(1) & \bigwedge xyz((xy)z = x(yz)) & \text{Premisa} \\
(2) & \quad x \mid y \land y \mid z & \text{Hipótesis} \\
(3) & \quad x \mid y & \text{EC 2} \\
(4) & \quad \bigvee u\ y = xu & \text{R 3} \\
(5) & \quad y = xu & \text{EP 4} \\
(6) & \quad y \mid z & \text{EC 2} \\
(7) & \quad \bigvee u\ z = yu & \text{R 6} \\
(8) & \quad z = yv & \text{EP 7} \\
(9) & \quad z = (xu)v & \text{ETI 5, 8} \\
(10) & \quad (xu)v = x(uv) & \text{EG 1} \\
(11) & \quad z = x(uv) & \text{TI 9, 10} \\
(12) & \quad \bigvee u\ z = xu & \text{IP 11} \\
(13) & \quad x \mid z & \text{R 12} \\
(14) & x \mid y \land y \mid z \rightarrow x \mid z & \\
(15) & \bigwedge xyz(x \mid y \land y \mid z \rightarrow x \mid z) & \text{IG 14}
\end{array}
$$

$$\dfrac{\dfrac{\Rightarrow 0+0=0 \qquad \dfrac{0+x=x\Rightarrow (0+x)'=x' \qquad \dfrac{\Rightarrow (0+x)'=0+x' \qquad (0+x)'=0+x',\,(0+x)'=x'\Rightarrow 0+x'=x'}{(0+x)'=x'\Rightarrow 0+x'=x'}}{0+0=0\Rightarrow 0+x=x}}{\Rightarrow 0+x=x}}{\Rightarrow \bigwedge u\, 0+u=u}$$

Si prescindimos completamente de las indicaciones de la derecha y tratamos de captar algún patrón formal mediante una inspección superficial de la sucesión de fórmulas de la izquierda, difícilmente encontraremos nada destacable, y esto pasa con un argumento que no está completamente detallado, en el sentido de que, si incluyéramos todos los pasos intermedios omitidos en virtud de las justificaciones de las reglas de inferencia derivadas, el panorama sería aún más desolador: nos encontraríamos continuamente con fórmulas muy complejas introducidas directamente como axiomas y con otras introducidas siempre con dos únicos criterios (*modus ponens* y generalización), de tal forma que la sucesión "ahora MP 4, 5", "ahora IG 7", "ahora axioma", "ahora MP 8, 9"... no arrojaría luz alguna sobre la estructura lógica del argumento subyacente.

Sin embargo, el cálculo deductivo $K_{\mathfrak{L}}$ está concebido para que —debidamente complementado con suficientes reglas de inferencia y técnicas de deducción derivadas— se corresponda exactamente con el modo en que los matemáticos conciben una demostración en la práctica, de modo que podemos considerar que la única diferencia entre un argumento formalizado en $K_{\mathfrak{L}}$ (en términos de las suficientes reglas de inferencia y técnicas de deducción derivadas) y un argumento expresado informalmente como es habitual en los libros de matemáticas consiste en el grado de detalle que se da del argumento, de modo que si un matemático que no conociera $K_{\mathfrak{L}}$ se esforzara por detallar hasta el más mínimo detalle un argumento, llegaría sin saberlo a una demostración en $K_{\mathfrak{L}}$.

Aquí vamos a estudiar un cálculo deductivo que, en principio cumple exactamente la misma función que $K_{\mathfrak{L}}$, es decir, la de formalizar el concepto matemático de deducción lógica y que, por lo tanto, es equivalente a $K_{\mathfrak{L}}$, pero que difiere sustancialmente de la forma en la que los matemáticos conciben las demostraciones. Así, un matemático considerará que una fórmula es deducible de unas premisas si y sólo si existe una deducción en el cálculo deductivo que vamos a estudiar, a pesar de que un matemático nunca la formularía de tal modo.

Por ejemplo, la "estructura" que vemos a la izquierda de esta página es una demostración de la fórmula $\bigwedge u\, 0+u=u$ a partir de los axiomas de Peano $0+0=0$ y $(0+x)'=0+x'$ y de dos axiomas lógicos, usando además el principio de inducción matemática, que no está expresado en forma de axioma, sino de regla de inferencia. Este cálculo deductivo alternativo es (una de las muchas variantes de) lo que se conoce como el *cálculo secuencial de Gentzen.*

Similarmente, el lector puede comparar la demostración que hemos mostrado en la página vii con la versión secuencial que está en la página 36. Naturalmente, no esperamos que el lector entienda en este momento las demostraciones en términos del cálculo secuencial, sino que el único propósito de estos ejemplos es que el lector se forme una primera idea superficial del aspecto que tienen las demostraciones en el cálculo deductivo que vamos a estudiar.

La pregunta obligada en este punto es qué interés tiene formalizar los argumentos matemáticos con este cálculo deductivo tan "curioso" cuando $K_{\mathcal{L}}$ cumple a la perfección su misión de formalizar la lógica matemática y además de una forma totalmente natural para un matemático.

La respuesta es que, en cierto sentido, podríamos decir que el cálculo de Gentzen es "la forma correcta" de formalizar la lógica para su estudio, la forma que pone de manifiesto las simetrías entre los distintos signos y reglas de inferencia, el papel exacto que desempeña cada signo lógico, cada regla de inferencia, cada axioma, en una deducción, y como consecuencia, sucede que el hecho de que toda demostración matemática pueda formalizarse en términos del cálculo secuencial permite obtener resultados profundos que, con la formalización natural desde el punto de vista del matemático, pero artificiosa desde el punto de vista puramente lógico, sería imposible obtener o, cuanto menos, mucho más complicado.

Por poner un ejemplo del tipo de resultados a los que nos referimos, podemos citar el teorema 3.22, que afirma que si una fórmula de tipo Σ_n es demostrable en $\mathrm{I}\Sigma_n$, es decir, en la aritmética de Peano con el principio de inducción restringido a fórmulas de tipo Σ_n, entonces existe una demostración (secuencial) de dicha fórmula en la que todas las fórmulas que intervienen son de tipo Σ_n. Esto no es trivial en absoluto, y tiene muchas consecuencias. Por ejemplo, permite probar (teorema 5.15) que en $\mathrm{I}\Sigma_{n+1}$ es posible demostrar la consistencia de $\mathrm{I}\Sigma_n$, lo cual, a su vez, implica por ejemplo que la aritmética de Peano no es finitamente axiomatizable.

En este libro mostraremos diversas aplicaciones del cálculo secuencial a la teoría de la demostración de la aritmética de Peano y sus fragmentos,[1] como el hecho de que $\mathrm{I}\Sigma_1$ es una extensión conservativa de la aritmética recursiva primitiva, o la caracterización de las funciones demostrablemente recursivas en $\mathrm{I}\Sigma_1$ y en AP, de donde a su vez obtendremos ejemplos de sentencias indecidibles en AP. Pero el teorema de Gentzen que más ha dado que hablar —y que también veremos aquí— es su demostración de que la aritmética de Peano es consistente. En el punto medio entre quienes consideran que esto es evidente y quienes consideran que es indemostrable, Gentzen publicó una prueba (varias, de hecho) que reducen —mediante argumentos estrictamente finitistas— la consistencia de la aritmética de Peano a una afirmación (la inducción hasta el ordinal ϵ_0, expresada aritméticamente) que puede considerarse finitista si no somos excesivamente estrictos a la hora de especificar qué admitimos como argumento finitista o que,

[1]En el capítulo IX, dedicado a la lógica de segundo orden, no sólo estudiaremos la aritmética de Peano de segundo orden, sino que también interpretaremos la teoría de conjuntos NBG como la extensión predicativa de segundo orden de ZFC.

cuanto menos, está en la frontera misma del finitismo. Discutiremos esto con el debido detalle en los capítulos VI y VII.

En este libro suponemos que el lector está familiarizado con algunas partes de [LM], especialmente con la aritmética de Peano y con la teoría de la recursión.

Capítulo I

El cálculo proposicional

Para familiarizarnos gradualmente con las ideas que subyacen en el cálculo secuencial de Gentzen, vamos a exponerlo en primer lugar en el contexto más simple del cálculo proposicional, y en el capítulo siguiente lo aplicaremos a la lógica de primer orden.

1.1 El lenguaje del cálculo proposicional

Definición 1.1 El *lenguaje del cálculo proposicional* $\mathcal{L}_p$ consta de cinco signos a los que llamaremos *conectores lógicos,* y los representaremos por $\neg$ (negador), $\vee$ (disyuntor), $\wedge$ (conjuntor), $\rightarrow$ (implicador) y $\leftrightarrow$ (coimplicador), además de un conjunto infinito de variables $P_0, P_1, P_2, P_3 \ldots$

En la práctica usaremos letras arbitrarias p, q, r, ... para referirnos a las variables.

Una *cadena de signos* de $\mathcal{L}_p$ es una sucesión finita de signos de $\mathcal{L}_p$, con posibles repeticiones, y en un orden determinado. Por ejemplo, una cadena de signos es $\wedge\, pqr\neg\neg{\rightarrow}rr\, \vee$.

Si Z_1 y Z_2 son dos cadenas de signos de $\mathcal{L}_p$, diremos que son *idénticas* (y lo representaremos por $Z_1 \equiv Z_2$) si constan de los mismos signos situados en el mismo orden.

Si $Z_1, \ldots, Z_n$ son cadenas de signos de $\mathcal{L}_p$, representaremos por $Z_1 \cdots Z_n$ su *yuxtaposición,* es decir, la cadena que empieza con los signos de Z_1, continúa con los de Z_2, etc.

Fórmulas Una cadena de signos A es una *fórmula* de $\mathcal{L}_p$ si existe una sucesión de cadenas de signos $A_1, \ldots, A_n$ de modo que $A_n \equiv A$ y cada A_i es una variable, o bien es de la forma

$$\neg A_j, \qquad \vee A_j A_k \qquad \wedge A_j A_k, \qquad \rightarrow A_j A_k, \qquad \leftrightarrow A_j A_k,$$

para ciertos $j, k < i$.

Por ejemplo, $A \equiv \vee{\to}pq{\to}qr$ es una fórmula de $\mathcal{L}_p$. La sucesión que lo justifica es

$$\begin{aligned}
&A_1 \equiv p\\
&A_2 \equiv q\\
&A_3 \equiv r\\
&A_4 \equiv {\to}pq\\
&A_5 \equiv {\to}qr\\
&A_6 \equiv \vee{\to}pq{\to}qr
\end{aligned}$$

En la práctica, a la hora de nombrar una fórmula, usaremos un criterio más práctico que el de nombrar sus términos en el orden en que aparecen en ella, que consistirá en aplicar los convenios siguientes:

$$(A \vee B) \equiv \vee AB, \quad (A \wedge B) \equiv \wedge AB, \quad (A \to B) \equiv {\to}AB, \quad (A \leftrightarrow B) \equiv {\leftrightarrow}AB.$$

Esta notación requiere usar paréntesis para evitar ambigüedades. Por ejemplo, no es lo mismo

$$(A \vee B) \vee C \equiv \vee\vee ABC, \qquad A \vee (B \vee C) \equiv \vee A \vee BC.$$

No obstante, suprimiremos los paréntesis que podamos evitar sin introducir ambigüedades. Para ello adoptaremos el convenio de que (salvo que los paréntesis indiquen otra cosa) $\neg$ se aplica antes que $\wedge$ y $\vee$, y que éstos se aplican antes que $\to$ y $\leftrightarrow$. Por ejemplo, $\neg p \to q \vee r$ se entiende como $(\neg p) \to (q \vee r)$ y no como $\neg((p \to q) \vee r)$.

De este modo, la fórmula $A \equiv \vee{\to}pq{\to}qr$ la representaremos normalmente como

$$A \equiv (p \to q) \vee (q \to r).$$

De la definición de fórmula se sigue inmediatamente que si A y B son fórmulas de $\mathcal{L}_p$, también lo son

$$\neg A, \quad A \vee B, \quad A \wedge B, \quad A \to B, \quad A \leftrightarrow B.$$

Más aún, toda fórmula de $\mathcal{L}_p$ es una variable o bien se descompone de una de las cinco formas anteriores. Según el caso se dice que es una *negación* o una *disyunción* o una *conjunción* o una *implicación* o una *coimplicación.* Notemos que una misma fórmula no puede ser de dos tipos, pues su primer signo determina a cuál de ellos corresponde. Las fórmulas que constan únicamente de una variable se llaman *fórmulas atómicas.*

Valoraciones Nuestra intención es que las fórmulas de $\mathcal{L}_p$ representen afirmaciones que pueden ser verdaderas o falsas, pero las hemos definido en términos estrictamente formales, es decir, especificando el orden que deben seguir los signos de $\mathcal{L}_p$ para constituir una fórmula, sin aludir en ningún momento a su posible significado.

Nos ocupamos ahora de en qué condiciones una fórmula es verdadera o falsa. La idea básica es que las fórmulas atómicas representan afirmaciones cuya verdad o falsedad tiene que ser establecida externamente a la lógica proposicional, pero que una vez determinado si las variables que aparecen en una fórmula A son verdaderas o falsas, la estructura de A determina completamente si es verdadera o falsa. Para concretar esta idea introducimos el concepto de valoración:

Definición 1.2 Consideremos una fórmula A en la que aparezcan a lo sumo las variables $p_1, \ldots, p_n$. Una *valoración* de A es cualquier criterio v que asigne a cada una de las variables p_i un valor $v(p_i)$ igual a 0 o a 1, si bien en este contexto escribiremos $v(p_i) = F$ (falso) o $v(p_i) = V$ (verdadero), respectivamente.

Una valoración v de una fórmula determina si ésta es verdadera o falsa (siempre con respecto a v) mediante los criterios siguientes:

1. $\neg A$ es verdadera si y sólo si A es falsa.
2. $A \vee B$ es verdadera si y sólo si A es verdadera o B es verdadera.
3. $A \wedge B$ es verdadera si y sólo si A y B son verdaderas.
4. $A \rightarrow B$ es verdadera en todos los casos salvo si A es verdadera y B es falsa.
5. $A \leftrightarrow B$ es verdadera si y sólo si A y B son ambas verdaderas o ambas falsas.

Las tablas siguientes muestran los cinco criterios anteriores de forma explícita:

A	$\neg A$
V	F
F	V

A	B	$A \vee B$
V	V	V
V	F	V
F	V	V
F	F	F

A	B	$A \wedge B$
V	V	V
V	F	F
F	V	F
F	F	F

A	B	$A \rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

A	B	$A \leftrightarrow B$
V	V	V
V	F	F
F	V	F
F	F	V

Escribiremos $v(A) = V$ o $v(A) = F$ según si A es verdadera o falsa respecto de la valoración v.

Técnicamente, las cinco tablas definen otras tantas funciones $v_\neg$, $v_\vee$, $v_\wedge$, $v_\rightarrow$ y $v_\leftrightarrow$, de modo que, por ejemplo, la segunda de las condiciones anteriores afirma que $v(A \vee B) = v_\vee(v(A), v(B))$, etc.

Notemos que una fórmula A con n variables tiene 2^n valoraciones posibles. Las tabla que indican el valor de $v(A)$ para cada una de las 2^n valoraciones de A se llama la *tabla de verdad* de A. Para la fórmula que hemos tomado de ejemplo es:

p	q	r	$p \to q$	$q \to r$	$(p \to q) \lor (q \to r)$
V	V	V	V	V	V
V	V	F	V	F	V
V	F	V	F	V	V
V	F	F	F	V	V
F	V	V	V	V	V
F	V	F	V	F	V
F	F	V	V	V	V
F	F	F	V	V	V

Una *tautología* es una fórmula que resulta verdadera respecto de todas sus valoraciones.

La tabla anterior muestra que la fórmula A es un ejemplo de tautología.

Consecuencias lógicas En términos generales, el propósito de la lógica es extraer consecuencias lógicas de unas premisas dadas, en un sentido que —al menos en el contexto particular de la lógica proposicional— podemos precisar como sigue:

Definición 1.3 Diremos que una fórmula A de $\mathcal{L}_p$ es *consecuencia lógica* de unas *premisas* $A_1, \ldots, A_n$ de $\mathcal{L}_p$ si A es verdadera respecto de toda valoración respecto de la cual todas las premisas sean verdaderas. También se dice que concluir A a partir de dichas premisas es un *razonamiento válido.* Es fácil ver que esto equivale a que la fórmula[1]

$$A_1 \land \cdots \land A_n \to A$$

sea una tautología.

Así pues, siempre es posible determinar si una fórmula es consecuencia lógica de unas premisas dadas construyendo la tabla de verdad con todas las variables que aparecen en ellas. No es necesario agrupar las premisas con una conjunción ni formar la implicación, sino que basta fijarse en las filas en las que todas las premisas toman el valor V y comprobar si el valor de la conclusión en dichas filas también es V en todos los casos.

1.2 El cálculo secuencial

A la hora de determinar si una fórmula es o no consecuencia lógica de unas premisas dadas, el método de las tablas de verdad que acabamos de comentar tiene una limitación fundamental, y es que no es aplicable al contexto de la lógica de primer orden, que es la que realmente se necesita para formalizar el razonamiento matemático.

[1]En principio, cuando escribimos la conjunción de más de dos fórmulas, habría que especificar cómo se asocian, pues, $(A \land B) \land C$ y $A \land (B \land C)$ son fórmulas distintas, pero es inmediato que una es verdadera respecto de una valoración dada si y sólo si lo es la otra, por lo que en realidad los paréntesis resultan irrelevantes.

Una alternativa que sí que puede ser generalizada debidamente es justificar la validez de un razonamiento construyendo una *deducción lógica,* es decir, una sucesión de fórmulas en la que cada una de ellas sea una de las premisas, o bien un axioma lógico (perteneciente a un conjunto prefijado de fórmulas que ya hayamos comprobado que son tautologías, de modo que podamos incluirlos en cualquier deducción con la seguridad de que serán verdaderas) o bien resulte de aplicar una regla de inferencia a fórmulas previas de la deducción (que son criterios para pasar de unas fórmulas a otras que hayamos comprobado que son válidos en el sentido de que siempre dan lugar a fórmulas verdaderas cuando se aplican a premisas verdaderas).

Esta forma de proceder se corresponde con lo que hacen realmente los matemáticos, si bien el cálculo proposicional que ahora nos ocupa es sólo un pálido reflejo de lo que constituye el auténtico razonamiento matemático.

Pensemos por ejemplo en los dos razonamientos siguientes:

$$\begin{array}{l} p \to \neg q \\ r \to q \\ r \lor s \\ \hline \neg p \lor s \end{array} \qquad \begin{array}{l} \\ p \to (q \lor r) \\ r \to \neg s \\ \hline p \to (\neg q \to s) \end{array}$$

Se nos plantea el problema de determinar si son razonamientos válidos, es decir, si la fórmula situada bajo la raya es en cada caso consecuencia lógica de las fórmulas situadas sobre ella. En lugar de calcular tablas de verdad de 16 filas, una forma de justificar la validez del primer razonamiento mediante el cálculo deductivo descrito[2] en el capítulo II de [LM] es construir la deducción siguiente:

$$\begin{array}{rll}
(1) & p \to \neg q & \text{Premisa} \\
(2) & r \to q & \text{Premisa} \\
(3) & r \lor s & \text{Premisa} \\
\vert\ (4) & \neg\neg p & \text{Hipótesis} \\
\vert\ (5) & p & \text{DN 4} \\
\vert\ (6) & \neg q & \text{MP 1, 5} \\
\vert\ (7) & \neg r & \text{MT 2, 6} \\
\vert\ (8) & s & \text{MTP 3, 7} \\
(9) & \neg\neg p \to s & \\
(10) & \neg p \lor s & \text{EDI 9}
\end{array}$$

En cambio, si intentamos hacer algo parecido con el segundo razonamiento estaremos condenados al fracaso, pues el razonamiento no es válido, lo cual

[2]El cálculo deductivo descrito en [LM] corresponde a la lógica de primer orden, pero podemos reinterpretar los axiomas K1, K2 y K3 del sistema $K_{\mathcal{L}}$ introducido en la sección 2.2 como fórmulas de $\mathcal{L}_p$, y tomarlos como axiomas, a los que añadimos la regla de inferencia MP más las necesarias para introducir y eliminar los conectores $\lor$, $\land$ y $\to$, que en [LM] se consideran definidos a partir de $\neg$ y $\to$ (concretamente, necesitamos EDI para el disyuntor, las dos primeras leyes de De Morgan para el conjuntor e IB, EB para el bicondicionador). Sobre esta base, podemos demostrar todas las reglas de inferencia expuestas en [LM] que no tienen que ver con cuantificadores, con las mismas demostraciones, así como el teorema de deducción. No damos detalles de todo esto porque aquí vamos a presentar un cálculo deductivo alternativo.

puede justificarse calculando las 16 filas de su tabla de verdad y comprobando que exactamente en una de ellas las premisas resultan verdaderas y la conclusión falsa, o bien encontrando por tanteo la valoración que falsea el razonamiento.

Respecto a la forma en que hemos encontrado la deducción que justifica la validez del primer razonamiento, es cierto que no es muy difícil llegar hasta ella, pero —en relación a la simplicidad del ejemplo— tanto el establecimiento de la estrategia de la deducción, como la elección de los pasos apropiados para llevarla a cabo requieren una cierta habilidad para fijarse en cada momento en las fórmulas adecuadas.

El cálculo secuencial que vamos a presentar aquí tiene la ventaja de que nos proporciona un algoritmo explícito para determinar si un razonamiento dado es válido o no que no requiere sino comprobaciones rutinarias, exactamente igual que la construcción de tablas de verdad, pero que tiene la ventaja de que todas las ideas que vamos a presentar pueden utilizarse igualmente en el contexto de la lógica de primer orden, que es donde realmente tendrá interés aplicarlas.

Secuentes El cálculo deductivo descrito en [LM] es lo que se conoce como un cálculo deductivo "a la Hilbert", es decir, consistente en construir sucesiones de fórmulas en las que cada una se deduce de algunas de las precedentes por razonamientos elementales cuya validez ha sido comprobada de antemano. Esto se corresponde con la forma en que de hecho conciben los matemáticos las demostraciones lógicas. Sin embargo, el cálculo secuencial de Gentzen tiene un planteamiento sustancialmente distinto, y muy alejado de la forma en que trabajan los matemáticos. Para empezar, las deducciones del cálculo secuencial no son sucesiones de fórmulas, sino de secuentes, en el sentido que introducimos a continuación:

Definición 1.4 Un *secuente* en $\mathcal{L}_p$ es una expresión de la forma $\Gamma \Rightarrow \Delta$, donde Γ y Δ son dos conjuntos finitos de fórmulas de $\mathcal{L}_p$. El conjunto Γ recibe el nombre de *antecedente,* del secuente mientras que Δ es el *consecuente.*

Cuando decimos que Γ y Δ son conjuntos (y no sucesiones) de fórmulas, en ello está implícito que el orden en que escribimos sus elementos es irrelevante, y que las repeticiones son redundantes. Por ejemplo, si α, β, γ, ϵ, δ son fórmulas de $\mathcal{L}$, entonces

$$\alpha, \beta, \gamma \Rightarrow \delta, \epsilon, \qquad \gamma, \beta, \alpha \Rightarrow \epsilon, \delta, \epsilon$$

son el mismo secuente. No excluimos la posibilidad de que Γ o Δ sean vacíos, de modo que

$$\alpha, \beta \Rightarrow, \qquad \Rightarrow \delta, \epsilon, \qquad \Rightarrow$$

son tres ejemplos de secuentes en $\mathcal{L}$. Al último lo llamaremos *secuente vacío.*

Usaremos letras griegas mayúsculas como Γ, Δ, para representar conjuntos finitos de fórmulas, mientras que las letras griegas minúsculas representarán fórmulas. Una expresión como

$$\Gamma_1, \alpha, \Gamma_2 \Rightarrow \Delta, \delta_1, \delta_2$$

debe entenderse como el secuente cuyo antecedente está formado por las fórmulas de Γ_1 y Γ_2 más la fórmula α, y cuyo consecuente está formado por las fórmulas de Δ además de δ_1 y δ_2, siempre entendiendo que las posibles repeticiones son redundantes, de modo que si, por ejemplo, δ_2 ya está en Δ, se trata del mismo secuente que

$$\Gamma_1, \alpha, \Gamma_2 \Rightarrow \Delta, \delta_1.$$

Vamos a definir un cálculo secuencial que nos permitirá trabajar con los secuentes formalmente, es decir, sin atribuirles ningún significado, pero esto no quita para que los secuentes tengan asociado un significado preciso:

Una *valoración* v de un secuente $S \equiv \Gamma \Rightarrow \Delta$ es una valoración definida sobre las variables de todas las fórmulas que aparecen en él. Diremos que S es *verdadero* respecto de v si alguna de las fórmulas de su antecedente es falsa o alguna de las fórmulas de su consecuente es verdadera respecto de v, entendiendo que el secuente vacío $\Rightarrow$ es falso.

Equivalentemente, si el secuente $S \equiv \gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$ no es vacío, entonces es verdadero respecto de v si y sólo si lo es la fórmula

$$\bar{S} \equiv \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n.$$

Si tanto el antecedente como el consecuente de S son no vacíos, esto equivale a que sea verdadera la fórmula

$$\gamma_1 \wedge \cdots \wedge \gamma_m \rightarrow \delta_1 \vee \cdots \vee \delta_n,$$

lo que explica la notación que empleamos para representar los secuentes.

Notemos que en particular un secuente de la forma $\Rightarrow \alpha$ es verdadero respecto de una valoración v si y sólo si α es verdadera mientras que un secuente $\alpha \Rightarrow$ es verdadero si y sólo si α es falsa.

Vemos así que la capacidad expresiva de los secuentes es la misma que la de las fórmulas, pues, para todo secuente S, la fórmula $\bar{S}$ afirma lo mismo que S, en el sentido de que S es verdadero respecto de una valoración si y sólo si lo es $\bar{S}$ y, recíprocamente, para toda fórmula α, el secuente $\Rightarrow \alpha$ afirma lo mismo que α.

Cálculos secuenciales Para razonar formalmente en términos de secuentes necesitamos fijar los mismos elementos que en el caso de un cálculo deductivo "a la Hilbert", es decir, unos axiomas y unas reglas de inferencia:

Definición 1.5 Un *cálculo secuencial* K para la lógica proposicional está determinado por un conjunto de secuentes en $\mathcal{L}_p$ llamados *axiomas* de K y un número finito de *reglas de inferencia primitivas* que determinan cuándo un secuente es *consecuencia inmediata* de uno o varios secuentes (siempre un número finito).

Vamos a considerar un único ejemplo de cálculo secuencial para el cálculo proposicional:

El cálculo secuencial PK Llamaremos PK al cálculo secuencial cuyos axiomas son los secuentes de la forma

$$p \Rightarrow p,$$

donde p es una fórmula atómica de $\mathcal{L}_p$, y cuyas reglas de inferencia primitivas son las siguientes:

$$\textbf{Debilitación izquierda}\ \frac{\Gamma \Rightarrow \Delta}{\alpha, \Gamma \Rightarrow \Delta}, \quad \textbf{Debilitación derecha}\ \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \alpha},$$

$$\textbf{Corte}\quad \frac{\Gamma \Rightarrow \Delta, \alpha \qquad \alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta},$$

$$\begin{array}{c|cc}
\neg & \dfrac{\Gamma \Rightarrow \Delta, \alpha}{\neg\alpha, \Gamma \Rightarrow \Delta}, & \dfrac{\alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\alpha}, \\[2ex]
\vee & \dfrac{\alpha,\, \Gamma \Rightarrow \Delta \qquad \beta,\, \Gamma \Rightarrow \Delta}{\alpha \vee \beta, \Gamma \Rightarrow \Delta}, & \dfrac{\Gamma \Rightarrow \Delta,\, \alpha,\, \beta}{\Gamma \Rightarrow \Delta,\, \alpha \vee \beta}, \\[2ex]
\wedge & \dfrac{\alpha,\, \beta,\, \Gamma \Rightarrow \Delta}{\alpha \wedge \beta,\ \Gamma \Rightarrow \Delta}, & \dfrac{\Gamma \Rightarrow \Delta,\, \alpha \quad \Gamma \Rightarrow \Delta,\, \beta}{\Gamma \Rightarrow \Delta, \alpha \wedge \beta}, \\[2ex]
\to & \dfrac{\Gamma \Rightarrow \Delta, \alpha \qquad \beta, \Gamma \Rightarrow \Delta}{\alpha \to \beta,\ \Gamma \Rightarrow \Delta}, & \dfrac{\alpha, \Gamma \Rightarrow \Delta, \beta}{\Gamma \Rightarrow \Delta, \alpha \to \beta}, \\[2ex]
\leftrightarrow & \dfrac{\alpha,\, \beta,\, \Gamma \Rightarrow \Delta \qquad \Gamma \Rightarrow \Delta,\, \alpha,\, \beta}{\alpha \leftrightarrow \beta,\ \Gamma \Rightarrow \Delta}, & \dfrac{\alpha, \Gamma \Rightarrow \Delta, \beta \qquad \beta, \Gamma \Rightarrow \Delta, \alpha}{\Gamma \Rightarrow \Delta,\, \alpha \leftrightarrow \beta}.
\end{array}$$

Antes de analizar este cálculo secuencial conviene introducir el vocabulario siguiente:

1. Las reglas de debilitación se llaman *reglas débiles,* mientras que las restantes son *reglas fuertes.*

2. Las reglas de debilitación y corte se llaman *reglas estructurales,* mientras que las restantes son *reglas lógicas.*

3. Cada regla de inferencia tiene un *secuente inferior* y uno o dos *secuentes superiores.*

4. La fórmula que aparece en el secuente inferior fuera de los conjuntos Γ y Δ se llama *fórmula principal* de la regla de inferencia (y es la que le da nombre). La única regla sin fórmula principal es la regla de corte.

5. Las fórmulas que aparecen en los secuentes superiores fuera de los conjuntos Γ y Δ se llaman *fórmulas auxiliares.* Las únicas reglas sin fórmulas auxiliares son las reglas de debilitación. La fórmula auxiliar de la regla de corte se llama *fórmula de corte.*

6. Las fórmulas que aparecen en los conjuntos Γ y Δ se llaman *fórmulas colaterales.*

Fórmulas auxiliares

$$\frac{\alpha,\Gamma\Rightarrow\Delta \qquad \beta,\Gamma\Rightarrow\Delta}{\alpha\vee\beta,\Gamma\Rightarrow\Delta}$$

Secuentes superiores

Secuente inferior

Fórmula principal   Fórmulas colaterales

Lo primero que podemos observar para entender el trasfondo del cálculo secuencial PK es lo siguiente:

Teorema 1.6 *Todos los axiomas de* PK *son verdaderos respecto de cualquier valoración. Si los secuentes superiores de una regla de inferencia de* PK *son verdaderos respecto de una valoración dada, el secuente inferior también lo es.*

Demostración: De acuerdo con las definiciones que hemos dado, $\alpha \Rightarrow \alpha$ es verdadero si la fórmula $\neg\alpha \vee \alpha$ es verdadera, lo cual es obviamente cierto. Esto prueba la primera parte del enunciado.

Para probar la segunda revisamos las reglas de inferencia una a una. Fijamos una valoración v y distinguimos dos casos:

1) Si Γ y Δ no son ambos vacíos y la fórmula

$$\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n$$

es verdadera respecto a la valoración fijada, entonces el secuente inferior de cualquiera de las reglas es verdadero por definición.

2) Supongamos en segundo lugar que Γ y Δ son ambos vacíos o que no lo son y la fórmula

$$\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n$$

es falsa. Entonces:

En el caso de las reglas de debilitación, el secuente superior es falso, luego este caso no puede darse.

En la regla de corte, los secuentes superiores dicen que α es verdadera y falsa, luego este caso tampoco puede darse.

La regla izquierda del negador afirma que si α es verdadera, entonces $\neg\alpha$ es falsa, mientras que la regla derecha afirma que si α es falsa entonces $\neg\alpha$ es verdadera.

La regla izquierda del disyuntor afirma que si α y β son falsas, entonces $\alpha \vee \beta$ es falsa, mientras que la regla derecha afirma que si α es verdadera o β es verdadera, entonces $\alpha \vee \beta$ es verdadera.

La regla izquierda del conjuntor afirma que si α es falsa o β es falsa, entonces $\alpha \wedge \beta$ es falsa, mientras que la regla derecha afirma que si α es verdadera y β es verdadera, entonces $\alpha \wedge \beta$ es verdadera.

La regla izquierda del implicador afirma que si α es verdadera y β es falsa, entonces $\alpha \rightarrow \beta$ es verdadera, mientras que la regla derecha afirma que si α es falsa o β es verdadera, entonces $\alpha \rightarrow \beta$ es verdadera.

Finalmente, la regla izquierda del coimplicador afirma que si una de las fórmulas α o β es falsa y una de ellas es verdadera, entonces $\alpha \leftrightarrow \beta$ es falsa, mientras que la regla derecha afirma que si ambas tienen el mismo valor de verdad, entonces $\alpha \leftrightarrow \beta$ es verdadera. ■

Para expresar todo el alcance del teorema anterior introducimos el concepto de deducción formal:

Definición 1.7 Una *deducción* en un cálculo secuencial K a partir de un conjunto de secuentes $\mathfrak{S}$ (llamados *premisas* de la deducción) es un conjunto finito de secuentes dispuestos en forma de árbol, de modo que hay un único secuente en el nivel inferior (llamado *secuente final*) y sobre cada secuente S que no sea una premisa o un axioma de K se encuentran uno o varios secuentes de los cuales S es consecuencia inmediata. Los axiomas y las premisas se llaman *secuentes iniciales* de la deducción.

Una *demostración* en K es una deducción sin premisas.

Usaremos la notación $\mathfrak{S} \underset{K}{\vdash} S$ para indicar que S es el secuente final de una deducción en K con premisas en $\mathfrak{S}$. En particular, $\underset{K}{\vdash} S$ indica que S es un teorema de K.

El teorema siguiente es inmediato a partir del teorema 1.6:

Teorema 1.8 (de corrección) *Si $\mathfrak{S}$ es un conjunto de secuentes verdaderos respecto de una valoración dada y $\mathfrak{S} \underset{\mathrm{PK}}{\vdash} S$, entonces S también es verdadero respecto de dicha valoración.*

En efecto, tenemos que S puede obtenerse aplicando sucesivamente reglas de inferencia de PK a axiomas y premisas, pero las premisas son verdaderas por hipótesis y los axiomas por 1.6, y al aplicar reglas de inferencia obtenemos siempre secuentes verdaderos, luego S tiene que ser verdadero.[3]

En particular, los teoremas de PK son tautológicos, en el sentido de que sonverdaderos respecto de cualquier valoración. Sucede que también se cumple el recíproco:

Teorema 1.9 *Si S es un secuente verdadero respecto de todas sus valoraciones, entonces $\underset{\mathrm{PK}}{\vdash} S$.*

Observemos que , de la propia definición de secuente verdadero se sigue que una fórmula α es consecuencia lógica de unas premisas $\alpha_1, \ldots, \alpha_n$ si y sólo si el secuente $\alpha_1 \ldots, \alpha_n \Rightarrow \alpha$ es verdadero respecto de todas las valoraciones, y por los dos últimos teoremas esto equivale a que $\underset{\mathrm{PK}}{\vdash} \alpha_1, \ldots, \alpha_n \Rightarrow \alpha$.

[3]Más precisamente, la demostración de 1.6 junto con un razonamiento que justifique que las premisas son verdaderas permite obtener a partir de una deducción de S un razonamiento que justifique que S es verdadero.

La prueba de 1.9 se basa en el teorema siguiente:

Teorema 1.10 (de inversión) *Si el secuente inferior de una regla de inferencia de* PK *que no sea de debilitación es verdadero respecto de una valoración, también lo son su secuente o sus secuentes superiores.*

DEMOSTRACIÓN: El argumento es el mismo que el del teorema 1.6: si los conjuntos Γ y Δ no son ambos vacíos y el secuente $\Gamma \Rightarrow \Delta$ es verdadero respecto de la valoración dada, es inmediato que los secuentes superiores de todas las reglas son verdaderos (excepto en el caso de las reglas de debilitación si se trata del secuente vacío).

Podemos suponer, por lo tanto, que Γ y Δ no son ambos vacíos y que el secuente $\Gamma \Rightarrow \Delta$ es falso respecto de la valoración dada. Entonces, considerando cada regla por separado, es inmediato que los secuentes superiores también son verdaderos. ∎

Vamos a dar una prueba constructiva del teorema 1.9. Concretamente, vamos a mostrar un procedimiento que, dado un secuente arbitrario S, o bien nos proporciona una demostración de S no bien nos determina una valoración respecto del que S es falso. Lo ilustraremos primeramente con los ejemplos de la página 5:

Ejemplo 1 *Estudiar la validez del razonamiento*

$$\begin{array}{l} p \to \neg q \\ r \to q \\ r \vee s \\ \hline \neg p \vee s \end{array}$$

Sólo tenemos que determinar si el secuente

$$p \to \neg q,\ r \to q,\ r \vee s \Rightarrow \neg p \vee s$$

es un teorema de PK. Para ello vamos construyendo una demostración "de abajo hacia arriba", eligiendo cualquier fórmula no atómica y aplicando la regla lógica correspondiente a su estructura. Hemos marcado en negrita la fórmula elegida en cada paso como fórmula principal. La elección es arbitraria.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{r \Rightarrow r}{p,\ p \to \neg q,\ r \Rightarrow r,\ s} \qquad \dfrac{\dfrac{p \Rightarrow p}{p,\ q,\ r \Rightarrow p,\ s} \qquad \dfrac{\dfrac{q \Rightarrow q}{p,\ q,\ r \Rightarrow q,\ s}}{p,\ \boldsymbol{\neg q},\ q,\ r \Rightarrow s}}{p,\ \boldsymbol{p \to \neg q},\ q,\ r \Rightarrow s}}{p,\ p \to \neg q,\ \boldsymbol{r \to q},\ r \Rightarrow s} \qquad \dfrac{s \Rightarrow s}{p,\ p \to \neg q,\ r \to q,\ s \Rightarrow s}}{p,\ p \to \neg q,\ r \to q,\ \boldsymbol{r \vee s} \Rightarrow s}}{p \to \neg q,\ r \to q,\ r \vee s \Rightarrow \boldsymbol{\neg p},\ s}}{p \to \neg q,\ r \to q,\ r \vee s \Rightarrow \boldsymbol{\neg p \vee s}}$$

En cuanto llegamos a un secuente con una misma fórmula atómica en el antecedente y en el consecuente, en el paso siguiente ponemos el axioma lógico correspondiente a dicha fórmula. Así obtenemos una demostración y concluimos que el razonamiento es válido. ∎

Ejemplo 2 *Estudiar la validez del razonamiento*

$$\begin{array}{l} p \to (q \lor r) \\ r \to \neg s \\ \hline p \to (\neg q \to s) \end{array}$$

Se trata de determinar si el secuente

$$p \to (q \lor r),\ r \to \neg s \Rightarrow p \to (\neg q \to s)$$

es un teorema de PK. Para ello intentamos aplicar el mismo procedimiento que hemos empleado en el ejemplo anterior:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{p \Rightarrow p}{p,\ r \to \neg s \Rightarrow p,\ q,\ s} \quad \dfrac{\dfrac{q \Rightarrow q}{p,\ q,\ r \to \neg s \Rightarrow q,\ s} \quad \dfrac{\dfrac{r \Rightarrow r}{p,\ r \Rightarrow q,\ r,\ s} \quad \dfrac{p,\ r \Rightarrow q,\ s}{p,\ r,\ \boldsymbol{\neg s} \Rightarrow q,\ s}}{p,\ r,\ \boldsymbol{r \to \neg s} \Rightarrow q,\ s}}{p,\ \boldsymbol{q \lor r},\ r \to \neg s \Rightarrow q,\ s}}{p,\ \boldsymbol{p \to (q \lor r)},\ r \to \neg s \Rightarrow q,\ s}}{\boldsymbol{\neg q},\ p,\ p \to (q \lor r),\ r \to \neg s \Rightarrow s}}{p,\ p \to (q \lor r),\ r \to \neg s \Rightarrow \boldsymbol{\neg q \to s}}}{p \to (q \lor r),\ r \to \neg s \Rightarrow \boldsymbol{p \to (\neg q \to s)}}$$

Sin embargo, ahora el resultado es distinto, porque hemos llegado hasta el secuente $p,\ r \Rightarrow q,\ s$ en el que ya no hay conectores para seguir aplicando reglas de inferencia y no ninguna fórmula atómica en los dos miembros que nos permita llegar a un axioma. Un secuente así es falso necesariamente respecto de la valoración que hace verdaderas las fórmulas de su antecedente y falsas las de su consecuente, que en este caso es la dada por

$$v(p) = v(r) = V, \quad v(q) = v(s) = F.$$

Aunque es fácil comprobarlo directamente, el teorema de inversión nos asegura que el secuente del que hemos partido es falso respecto de v, luego por el teorema de corrección éste no puede ser un teorema de PK y concluimos que el razonamiento no es válido. ■

La prueba del teorema 1.9 se reduce a observar que, cualquiera que sea el secuente de partida, si vamos aplicando a la inversa reglas lógicas a partir de él, tras un número finito de pasos tenemos que llegar a un árbol cuyos secuentes iniciales consten únicamente de fórmulas atómicas (pues en cada paso eliminamos un conector lógico). Si en todos ellos hay una misma fórmula en el antecedente y en el consecuente, podemos pasar al axioma correspondiente mediante reglas de debilitación y concluimos que el secuente de partida es un teorema. Si, por el contrario, hay secuentes iniciales sin fórmulas atómicas comunes en el antecedente y en el consecuente, cada uno de ellos determina una valoración que lo hace falso y, por el teorema de inversión, también hace falso al secuente de partida.

Ahora podemos demostrar el recíproco del teorema de corrección:

Teorema 1.11 (de completitud semántica de PK) *Si $\mathfrak{S}$ es un conjunto de secuentes y S es un secuente verdadero respecto respecto de toda valoración que haga verdaderos a los secuentes de $\mathfrak{S}$, entonces $\mathfrak{S} \underset{\text{PK}}{\vdash} S$.*

Demostración: Podemos suponer que $\mathfrak{S}$ es finito, pues, en caso contrario, para cada valoración v que haga falso a S, elegimos un secuente S_v en $\mathfrak{S}$ que sea falso respecto de una extensión adecuada de v. El conjunto $\mathfrak{S}_0$ formado por estos secuentes S_v es finito, y así si una valoración hace falso a S, se extiende a una valoración que hace falso a un secuente de $\mathfrak{S}_0$, luego S es verdadero respecto de todas las valoraciones que hacen verdaderos a los secuentes de $\mathfrak{S}_0$. Si probamos que S es consecuencia de $\mathfrak{S}_0$, también lo será de $\mathfrak{S}$.

Así pues, podemos suponer que $\mathfrak{S}$ consta de los secuentes $S_1, \ldots, S_k$. Podemos suponer que ninguno de ellos es vacío, pues en tal caso es inmediato que de éste se deduce S por debilitación. Sea $S \equiv \Gamma \Rightarrow \Delta$ y, para cada secuente $S_i \equiv \gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$ de $\mathfrak{S}$, consideramos la fórmula

$$\bar{S}_i \equiv \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n.$$

Entonces, el secuente $S^* \equiv \bar{S}_1, \ldots, \bar{S}_k, \Gamma \Rightarrow \Delta$ es verdadero respecto de toda valoración v pues, o bien v hace falso a alguna fórmula $\bar{S}_i$, o bien las hace verdaderas a todas, en cuyo caso hace verdaderos a todos los secuentes de $\mathfrak{S}$, luego a S y también a S^*. Por el teorema 1.9 concluimos que S^* es un teorema de KP.

Ahora bien, usando la reglas derechas del negador, del disyuntor y de debilitación vemos que $S_i \underset{\text{KP}}{\vdash} \Gamma \Rightarrow \Delta, \bar{S}_i$, luego aplicando la regla de corte llegamos a que $\mathfrak{S} \underset{\text{PK}}{\vdash} S$. ■

De la prueba que hemos dado del teorema 1.9 se deduce el hecho siguiente:

Teorema 1.12 (de eliminación de cortes) *Si S es un secuente demostrable en* PK, *existe una demostración de S que no utiliza la regla de corte.*

De hecho, en la prueba de 1.9 hemos visto cómo construir una demostración de S usando las reglas de inferencia lógicas y las de debilitación, pero sin recurrir en ningún momento a la regla de corte.

Esto puede parecer anecdótico, pero la eliminación de cortes resulta ser una poderosa herramienta de la teoría de la demostración, y uno de los motivos por los que el cálculo secuencial es mejor opción que otras alternativas a la hora de estudiar el razonamiento formal.

Por otra parte, esto no debe interpretarse como que la regla de corte es redundante. El teorema anterior sólo se aplica a demostraciones (sin premisas) en PK, pero no es necesariamente cierto para deducciones a partir de unas premisas dadas. Por ejemplo, es fácil ver que $\Rightarrow \neg\neg\alpha \underset{\text{KP}}{\vdash} \Rightarrow \alpha$, pero toda deducción tiene que tener al menos un corte, ya que todas las consecuencias que podamos extraer de $\Rightarrow \neg\neg\alpha$ sin la regla de corte contendrán al menos una subfórmula igual a $\neg\neg\alpha$, luego ninguna de ellas será $\Rightarrow \alpha$.

1.3 Reglas derivadas de inferencia

Veamos algunas reglas de inferencia adicionales que pueden usarse para abreviar deducciones:

Variantes Algunas reglas admiten variantes equivalentes de interés. Por ejemplo, la regla derecha del disyuntor es equivalente a las reglas

$$\frac{\Gamma \Rightarrow \Delta,\, \alpha}{\Gamma \Rightarrow \Delta,\, \alpha \lor \beta}, \qquad \frac{\Gamma \Rightarrow \Delta,\, \beta}{\Gamma \Rightarrow \Delta,\, \alpha \lor \beta},$$

en el sentido de que estas dos reglas pueden ser demostradas y, recíprocamente, si tomamos éstas como reglas primitivas, podemos demostrar la regla derecha del disyuntor.

En efecto, estas variantes se prueban trivialmente sin más que añadir la fórmula que falta por debilitación y luego aplicar la regla del disyuntor. Recíprocamente, si tomamos las dos variantes como primitivas, podemos probar así la regla del disyuntor:

$$\cfrac{\cfrac{\Gamma \Rightarrow \Delta,\, \alpha,\, \beta}{\Gamma \Rightarrow \Delta,\, \alpha \lor \beta,\, \beta}}{\Gamma \Rightarrow \Delta,\, \alpha \lor \beta}$$

donde en el último paso hemos aplicado la regla del disyuntor que transforma β en $\alpha \lor \beta$, pero, como la disyunción ya está en el consecuente, no necesitamos volverla a escribir.

Similarmente, la regla izquierda del conjuntor es equivalente a las reglas[4]

$$\frac{\alpha,\, \Gamma \Rightarrow \Delta}{\alpha \land \beta,\ \Gamma \Rightarrow \Delta}, \qquad \frac{\beta,\, \Gamma \Rightarrow \Delta}{\alpha \land \beta,\ \Gamma \Rightarrow \Delta}.$$

Por otra parte, la regla izquierda del disyuntor es equivalente a

$$\frac{\alpha,\, \Gamma \Rightarrow \Delta \qquad \beta,\, \Gamma' \Rightarrow \Delta'}{\alpha \lor \beta,\, \Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'},$$

y la regla derecha del disyuntor es equivalente a

$$\frac{\Gamma \Rightarrow \Delta,\, \alpha \qquad \Gamma' \Rightarrow \Delta',\, \beta}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha \land \beta},$$

Y la regla de corte es equivalente a esta variante:

$$\frac{\Gamma \Rightarrow \Delta,\, \alpha \qquad \alpha,\, \Gamma' \Rightarrow \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}.$$

Estas variantes incluyen a la regla original como caso particular, recíprocamente, pueden probarse a partir de la regla original sin más que cambiar primero los conjuntos de fórmulas colaterales por Γ, Γ' y Δ, Δ' por debilitación. ■

[4]Pero observemos que con estas versiones alternativas de las reglas del disyuntor y del conjuntor ya no es cierto el teorema de inversión.

Reglas inversas Las reglas siguientes nos permiten eliminar signos lógicos, en vez de introducirlos:

$$\frac{\neg\alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta,\ \alpha}, \quad \frac{\Gamma \Rightarrow \Delta,\ \neg\alpha}{\alpha,\ \Gamma \Rightarrow \Delta}, \quad \frac{\alpha \vee \beta,\ \Gamma \Rightarrow \Delta}{\alpha,\ \Gamma \Rightarrow \Delta}, \quad \frac{\alpha \vee \beta,\ \Gamma \Rightarrow \Delta}{\beta,\ \Gamma \Rightarrow \Delta},$$

$$\frac{\Gamma \Rightarrow \Delta,\ \alpha \vee \beta}{\Gamma \Rightarrow \Delta,\ \alpha,\ \beta}, \quad \frac{\alpha \wedge \beta,\ \Gamma \Rightarrow \Delta}{\alpha,\ \beta,\ \Gamma \Rightarrow \Delta}, \quad \frac{\Gamma \Rightarrow \Delta,\ \alpha \wedge \beta}{\Gamma \Rightarrow \Delta,\ \alpha}, \quad \frac{\Gamma \Rightarrow \Delta,\ \alpha \wedge \beta}{\Gamma \Rightarrow \Delta,\ \beta},$$

$$\frac{\alpha \rightarrow \beta,\ \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta,\ \alpha}, \quad \frac{\alpha \rightarrow \beta,\ \Gamma \Rightarrow \Delta}{\beta,\ \Gamma \Rightarrow \Delta}, \quad \frac{\Gamma \Rightarrow \Delta,\ \alpha \rightarrow \beta}{\alpha,\ \Gamma \Rightarrow \Delta,\ \beta}.$$

Todas son consecuencia del teorema de completitud y del de inversión, pero vamos a dar las deducciones correspondientes (omitimos las que se prueban análogamente a la regla que la precede):

$$\frac{\dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha,\ \Gamma \Rightarrow \Delta,\ \alpha}}{\Gamma \Rightarrow \Delta, \alpha, \neg\alpha} \qquad \dfrac{\neg\alpha,\ \Gamma \Rightarrow \Delta}{\neg\alpha,\ \Gamma \Rightarrow \Delta, \alpha}}{\Gamma \Rightarrow \Delta,\ \alpha}$$

$$\frac{\dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha,\ \Gamma \Rightarrow \Delta,\ \alpha,\ \beta}}{\alpha,\ \Gamma \Rightarrow \Delta,\ \alpha \vee \beta} \qquad \dfrac{\alpha \vee \beta,\ \Gamma \Rightarrow \Delta}{\alpha \vee \beta,\ \alpha,\ \Gamma \Rightarrow \Delta}}{\alpha,\ \Gamma \Rightarrow \Delta}$$

$$\frac{\dfrac{\Gamma \Rightarrow \Delta,\ \alpha \vee \beta}{\Gamma \Rightarrow \Delta,\ \alpha,\ \beta,\ \alpha \vee \beta} \qquad \dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha,\ \Gamma \Rightarrow \Delta,\ \alpha,\ \beta} \quad \dfrac{\beta \Rightarrow \beta}{\beta,\ \Gamma \Rightarrow \Delta,\ \alpha,\ \beta}}{\alpha \vee \beta,\ \Gamma \Rightarrow \Delta,\ \alpha,\ \beta}}{\Gamma \Rightarrow \Delta,\ \alpha,\ \beta}$$

$$\frac{\dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha,\ \beta,\ \Gamma \Rightarrow \Delta,\ \alpha} \quad \dfrac{\beta \Rightarrow \beta}{\alpha,\ \beta,\ \Gamma \Rightarrow \Delta,\ \beta}}{\alpha,\ \beta,\ \Gamma \Rightarrow \Delta,\ \alpha \wedge \beta} \qquad \dfrac{\alpha \wedge \beta, \Gamma \Rightarrow \Delta}{\alpha \wedge \beta,\ \alpha,\ \beta,\ \Gamma \Rightarrow \Delta}}{\alpha,\ \beta,\ \Gamma \Rightarrow \Delta}$$

$$\frac{\dfrac{\Gamma \Rightarrow \Delta,\ \alpha \wedge \beta}{\Gamma \Rightarrow \Delta,\ \alpha,\ \alpha \wedge \beta} \qquad \dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha,\ \beta,\ \Gamma \Rightarrow \Delta,\ \alpha}}{\alpha \wedge \beta,\ \Gamma \Rightarrow \Delta,\ \alpha}}{\Gamma \Rightarrow \Delta,\ \alpha}$$

$$\frac{\dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha,\ \Gamma \Rightarrow \Delta,\ \alpha,\ \beta}}{\Gamma \Rightarrow \Delta,\ \alpha,\ \alpha \rightarrow \beta} \qquad \dfrac{\alpha \rightarrow \beta,\ \Gamma \Rightarrow \Delta}{\alpha \rightarrow \beta,\ \Gamma \Rightarrow \Delta,\ \alpha}}{\Gamma \Rightarrow \Delta,\ \alpha}$$

La siguiente es similar, partiendo esta vez de $\beta \Rightarrow \beta$.

$$\frac{\dfrac{\Gamma \Rightarrow \Delta,\ \alpha \rightarrow \beta}{\alpha,\ \Gamma \Rightarrow \beta,\ \alpha \rightarrow \beta} \qquad \dfrac{\dfrac{\alpha \Rightarrow \alpha}{\alpha,\ \Gamma \Rightarrow \Delta, \beta, \alpha} \quad \dfrac{\beta \Rightarrow \beta}{\beta,\ \alpha,\ \Gamma \Rightarrow \Delta,\ \beta}}{\alpha \rightarrow \beta,\ \alpha,\ \Gamma \Rightarrow \Delta,\ \beta}}{\alpha,\ \Gamma \Rightarrow \Delta,\ \beta}$$

■

Capítulo II

El cálculo secuencial para la lógica de primer orden

En el capítulo I de [LM] introdujimos los conceptos fundamentales sobre lenguajes formales de primer orden y sus modelos, y al hacerlo adoptamos una serie de convenios arbitrarios que eran los más adecuados para presentar en el capítulo siguiente el cálculo deductivo "a la Hilbert" que subyace en todos los resultados posteriores.

Por ejemplo, adoptamos el convenio de que los conectores $\vee$, $\wedge$, $\leftrightarrow$ y el particularizador $\bigvee$ no eran propiamente signos de los lenguajes formales, sino que se definían a partir de $\neg$, $\rightarrow$ y $\bigwedge$. Esto era conveniente porque los axiomas y las reglas de inferencia del cálculo deductivo expuesto allí pueden enunciarse exclusivamente en términos de estos signos, de modo que introducir los demás como signos primitivos obligaría a introducir nuevos axiomas o nuevas reglas de inferencia, que complicarían a su vez el análisis del sistema deductivo obligando a considerar más casos concernientes a los nuevos signos primitivos, que en el fondo son redundantes.

Sin embargo, el cálculo secuencial está pensado para explotar al máximo el aspecto formal de las demostraciones matemáticas, y para ello no podemos pasar por alto la estructura concreta de las fórmulas que resulta de los convenios concretos que hayamos fijado. Por ejemplo, al tratar con fórmulas de tipo

$$\bigvee x \bigwedge y \bigvee z\, \alpha,$$

donde α es una fórmula sin cuantificadores, o una fórmula de tipo Δ_0 en un sistema aritmético, no es lo mismo tener realmente tres cuantificadores alternados, cuyo uso está regulado por reglas de inferencia totalmente análogas para uno y otro, que tener realmente una fórmula

$$\neg\bigwedge x \neg\bigwedge y \neg\bigwedge z \neg\alpha,$$

donde la alternancia real es entre generalizadores y negadores, entre los cuales no existe ninguna clase de analogía. Esto puede dificultar o, cuanto menos, oscurecer, muchos argumentos.

Por este motivo, aquí vamos a considerar los dos cuantificadores $\bigwedge$ y $\bigvee$ como signos primitivos de todo lenguaje formal. Esto dará lugar a casos adicionales en algunos argumentos, que podrían evitarse si sólo consideráramos como signo primitivo a uno de los cuantificadores, pero la analogía entre el caso correspondiente a cada cuantificador será tan estrecha, que la molestia será mínima.

Similarmente, sucede que $\neg$ y $\rightarrow$ no serán en nuestro contexto los conectores lógicos más adecuados para definir en términos de ellos todos los demás, sino que será mucho más conveniente adoptar $\neg$ y $\vee$, pues las reglas de inferencia válidas para el disyuntor (que serán las mismas que hemos visto en el capítulo anterior para la lógica proposicional) gozan de una perfecta simetría que no se da en las reglas del implicador, esencialmente porque en $\alpha \vee \beta$ las fórmulas α y β son intercambiables, mientras que en $\alpha \rightarrow \beta$ no lo son. Los argumentos propios del cálculo secuencial nos obligarían a recordar en todo momento que en $\alpha \rightarrow \beta$ se esconde un negador, en la forma $\neg\alpha \vee \beta$, de modo que las manipulaciones con implicaciones sólo se entienden plenamente cuando se conciben como combinaciones de manipulaciones de negaciones y disyunciones. Así pues, en la primera sección revisaremos las definiciones dadas en el capítulo I de [LM] enfatizando las diferencias.

2.1 Lenguajes formales de primer orden

Como acabamos de explicar, vamos a definir el concepto de lenguaje formal tomando como signos primitivos $\neg$, $\vee$, $\bigwedge$ y $\bigvee$, lo cual dotará a la teoría de una valiosa simetría. Ésta podría ser aún mayor si añadiéramos el conjuntor $\wedge$ a los signos primitivos, pero no ganaríamos nada en la práctica y, por otra parte, precisamente por la simetría entre el conjuntor y el disyuntor, las modificaciones necesarias en todos los argumentos para añadir el conjuntor son triviales.

Otro signo lógico destacado es el igualador $=$. Aunque sólo nos van a interesar lenguajes formales con igualador, algunos resultados básicos del cálculo secuencial se enuncian más claramente para lenguajes sin igualador, por lo que en la definición no exigiremos que los lenguajes lo tengan, si bien a largo plazo sólo nos interesarán los lenguajes con igualador.

Otro convenio que resultará útil para simplificar el enunciado de algunos teoremas es el de dividir a las variables de un lenguaje formal en dos grupos disjuntos: el de las variables libres y el de las variables ligadas, de modo que, al construir fórmulas, como por ejemplo

$$\bigwedge u(u \in x \rightarrow u \in y),$$

tendremos la precaución de elegir las variables x e y —que están libres en la fórmula— en el conjunto de las variables libres de $\mathcal{L}$, y la variable u —que está ligada en la fórmula— en el conjunto de las variables ligadas de $\mathcal{L}$. Esto en la práctica no supone ninguna limitación, pues siempre es irrelevante usar una variable u otra en un momento dado, por lo que no perdemos nada por escogerla en un conjunto u otro según si la vamos a dejar libre o ligada en una fórmula determinada.

Por último, en [LM] consideramos lenguajes formales con descriptor, lo cual es muy útil a la hora de tratar teóricamente las definiciones matemáticas que introducen nuevas constantes o funtores a una teoría. No obstante, en [LM] se prueba desde un punto de vista teórico el descriptor es prescindible, y como aquí estamos interesados en el uso teórico del cálculo secuencial, vamos a prescindir del descriptor desde el primer momento.

Teniendo esto en cuenta, modificamos como sigue la definición [LM 1.1] de lenguaje formal:

Definición 2.1 Un *lenguaje formal de primer orden* $\mathcal{L}$ sin igualador es una colección de signos divididos en las categorías siguientes y de modo que cumplan las propiedades que se indican:

Variables libres Un lenguaje $\mathcal{L}$ debe tener infinitas variables libres. Cada variable libre debe tener asociado un número natural distinto al que llamaremos su *índice,* de tal forma que todo natural es índice de una variable libre de $\mathcal{L}$. Llamaremos x_i a la variable libre de índice i de $\mathcal{L}$.

Variables ligadas Un lenguaje $\mathcal{L}$ debe tener infinitas variables ligadas. Cada variable ligada debe tener asociado un número natural distinto al que llamaremos su *índice,* de tal forma que todo natural es índice de una variable ligada de $\mathcal{L}$. Llamaremos u_i a la variable ligada de índice i de $\mathcal{L}$.

Constantes Un lenguaje $\mathcal{L}$ puede tener cualquier cantidad de constantes, desde ninguna hasta infinitas. En cualquier caso, cada constante debe tener asociado un *índice* natural. Llamaremos c_i a la constante de $\mathcal{L}$ de índice i (si existe) de modo que si $\mathcal{L}$ tiene $m+1$ constantes éstas serán $c_0, c_1, \ldots, c_m$, mientras que si $\mathcal{L}$ tiene infinitas constantes, los índices recorrerán todos los números naturales.

Relatores Cada relator debe tener asociado un número natural no nulo al que llamaremos su *rango.* Llamaremos relatores n-ádicos a los relatores de rango n. El número de relatores n-ádicos de $\mathcal{L}$ puede variar entre ninguno e infinitos.

Funtores Cada funtor ha de llevar asociado un *rango* en las mismas condiciones que los relatores.

Negador Llamaremos $\neg$ al negador de $\mathcal{L}$.

Disyuntor Llamaremos $\vee$ al disyuntor de $\mathcal{L}$.

Cuantificador universal Llamaremos $\bigwedge$ al cuantificador universal (o generalizador) de $\mathcal{L}$.

Cuantificador existencial Llamaremos $\bigvee$ al cuantificador existencial (o particularizador) de $\mathcal{L}$.

Cada signo de $\mathcal{L}$ debe pertenecer a una de estas categorías y sólo a una. Las constantes, los funtores y los relatores se llaman *signos eventuales* de $\mathcal{L}$, mientras que los restantes son *signos obligatorios.*

Un *lenguaje formal* de primer orden *con igualador* es un lenguaje formal que incluye un relator diádico distinguido al que llamaremos *igualador,* o simplemente $=$, y al que consideraremos también como signo obligatorio de $\mathcal{L}$.

Definición 2.2 Sea $\mathcal{L}$ un lenguaje formal. Una *cadena de signos* de $\mathcal{L}$ es una sucesión finita de signos de $\mathcal{L}$ repetidos o no y en un cierto orden. Si $\zeta_1, \ldots, \zeta_n$ son cadenas de signos de $\mathcal{L}$ llamaremos $\zeta_1 \cdots \zeta_n$ a la cadena que resulta de yuxtaponer las cadenas $\zeta_1, \ldots, \zeta_n$ en este orden. En particular podemos nombrar una cadena nombrando a cada uno de sus signos en el orden en que aparecen.

Dos cadenas de signos ζ_1 y ζ_2 son *idénticas* si constan de los mismos signos en el mismo orden. Lo indicaremos así: $\zeta_1 \equiv \zeta_2$ (y en caso contrario escribiremos $\zeta_1 \not\equiv \zeta_2$). Así pues, $\zeta_1 \equiv \zeta_2$ significa que "ζ_1" y "ζ_2" son dos nombres para la misma cadena de signos.

Semiexpresiones En ausencia del descriptor, la definición de expresión dada en [LM 1.5] puede desdoblarse en dos definiciones independientes de "término" y "fórmula", si bien la división que hemos hecho entre variables libres y ligadas nos obliga a definir en primer lugar los conceptos de "semitérminos" y "semifórmulas" para definir posteriormente los términos y las fórmulas como los semitérminos y semifórmulas cuyas variables que están de hecho libres y ligadas en ella pertenecen al conjunto adecuado.

Definición 2.3 Una cadena de signos t de un lenguaje formal $\mathcal{L}$ es un *semitérmino* si existe una sucesión finita $t_0, \ldots, t_m$ de cadenas de signos de $\mathcal{L}$ de modo que $t_m \equiv t$ y cada t_k cumple una de las condiciones siguientes:

1. t_k es una variable.
2. t_k es una constante.
3. $t_k \equiv ft_1 \cdots t_n$, donde f es un funtor n-ádico de $\mathcal{L}$ y los t_i son cadenas anteriores de la sucesión.

Un *término* es un semitérmino que no contiene variables ligadas.

Una cadena de signos α de un lenguaje formal $\mathcal{L}$ es una *semifórmula* si existe una sucesión finita $\alpha_0, \ldots, \alpha_m$ de cadenas de signos de $\mathcal{L}$ de modo que $\alpha_m \equiv \alpha$ y cada α_k cumple una de las condiciones siguientes:

1. $\alpha_k \equiv Rt_1 \cdots t_n$, donde R es un relator n-ádico de $\mathcal{L}$ y los t_i son semitérminos de $\mathcal{L}$.
2. $\alpha_k \equiv \neg\alpha$, donde α es una cadena anterior de la sucesión.
3. $\alpha_k \equiv \vee\alpha\beta$, donde α y β son cadenas anteriores de la sucesión.
4. $\alpha_k \equiv \bigwedge u\, \alpha$, donde u es una variable ligada y α es una cadena anterior de la sucesión.
5. $\alpha_k \equiv \bigvee u\, \alpha$, donde u es una variable ligada y α es una cadena anterior de la sucesión.

Una cadena de signos θ es una *semiexpresión* de $\mathcal{L}$ si es un semitérmino o una semifórmula de $\mathcal{L}$.

Un poco más adelante definiremos las fórmulas como las semifórmulas en las que las variables que aparecen libres son variables libres de $\mathcal{L}$, pero para ello todavía tenemos que definir el concepto de aparición libre o ligada de una variable en una fórmula.

Convenios de notación En la definición de lenguaje formal hemos indicado que llamaremos x_i a la variable libre de índice i de un lenguaje formal y u_i a su variable ligada de índice i. En lo sucesivo (salvo que indiquemos lo contrario) entenderemos tácitamente que x, y, z nombran a variables libres cualesquiera (no necesariamente distintas entre sí), mientras que u, v, w nombrarán siempre a variables ligadas cualesquiera.

A su vez c nombrará a una constante, R^n a un relator n-ádico y f^n a un funtor n-ádico. Similarmente, convenimos en que t, t_1, t_2, etc. nombrarán a semitérminos arbitrarios, mientras que α, β, γ representarán semifórmulas arbitrarias.

Por otra parte, en lugar de nombrar cada semiexpresión nombrando los términos que aparecen en ella en el orden en que lo hacen, normalmente emplearemos otros convenios de notación alternativos (los dos últimos valen para lenguajes con igualador):

1. $(\alpha \vee \beta) \equiv \vee \alpha\beta$
2. $(\alpha \wedge \beta) \equiv \neg(\neg\alpha \vee \neg\beta)$,
3. $(\alpha \rightarrow \beta) \equiv (\neg\alpha \vee \beta)$,
4. $(\alpha \leftrightarrow \beta) \equiv \big((\alpha \wedge \beta) \vee (\neg\alpha \wedge \neg\beta)\big)$,
5. $\overset{1}{\bigvee} u\, \alpha \equiv \bigvee v \bigwedge u(\alpha \leftrightarrow v = u)$,
6. $(t_1 = t_2) \equiv {=}\, t_1 t_2$,
7. $(t_1 \neq t_2) \equiv \neg(t_1 = t_2)$.

Además, cuando haya que escribir varios cuantificadores seguidos del mismo tipo, como $\bigvee u \bigvee v \bigvee w$ escribiremos más brevemente $\bigvee uvw$.

Al tratar con lenguajes formales particulares adoptaremos tácitamente convenios de notación similares. Por ejemplo, en un lenguaje con un funtor diádico $+$, escribiremos normalmente $(t_1 + t_2) \equiv +t_1t_2$.

Los paréntesis son necesarios en principio para evitar ambigüedades en la aplicación de estos convenios, pero los omitiremos cuando no haya ambigüedades posibles.

Con estos convenios, en la práctica podemos tratar con el *conjuntor* $\wedge$, el *implicador* $\rightarrow$ y el *coimplicador* $\leftrightarrow$ como si fueran signos de $\mathcal{L}$ en pie de igualdad con el negador o el disyuntor, si bien en teoría “no existen”, lo que nos permitirá reducir las definiciones y las demostraciones que obliguen a distinguir casos en función de los signos de un lenguaje formal dado. ■

De acuerdo con las definiciones y convenios de notación que hemos dado, podemos decir que todo semitérmino es una variable, una constante o bien de la forma $f^n t_1, \ldots, t_n$, así como que una semifórmula es de la forma $R^n t_1 \cdots t_n$, o bien $\neg\alpha$, o bien $\alpha \vee \beta$, o bien $\bigwedge u\, \alpha$, o bien $\bigvee u\, \alpha$. Las semifórmulas del primer tipo se llaman *semifórmulas atómicas.*

Variables libres y ligadas Una cosa es que una variable de un lenguaje formal $\mathcal{L}$ sea libre o ligada en el sentido de que la hayamos clasificado como tal al definir $\mathcal{L}$ y otra muy distinta que aparezca libre o ligada en una semifórmula. Nuestra intención es definir las fórmulas como las semifórmulas en las que las variables que aparecen libres sean libres, pero para eso en primer lugar tenemos que definir el concepto de aparición libre:

Definición 2.4 Sea $\mathcal{L}$ un lenguaje formal. Definimos como sigue el conjunto de variables que *aparecen libres* en una semifórmula de $\mathcal{L}$:

1. Las variables que aparecen libres en $R^n t_1 \cdots t_n$ son todas las variables que aparecen en la semifórmula (tanto si son variables libres como ligadas).
2. Las variables que aparecen libres en $\neg\alpha$ son las mismas que aparecen libres en α.
3. Las variables que aparecen libres en $\alpha \vee \beta$ son las que aparecen libres en α y las que aparecen libres en β.
4. Las variables que aparecen libres en $\bigwedge u\, \alpha$ o $\bigvee u\, \alpha$ son las que aparecen libres en α y son distintas de u.

Similarmente definimos el conjunto de las variables que aparecen ligadas en una semifórmula de $\mathcal{L}$:

1. En una semifórmula atómica $R^n t_1 \cdots t_n$ ninguna variable aparece ligada.
2. Las variables que aparecen ligadas en $\neg\alpha$ son las mismas que aparecen ligadas en α.
3. Las variables que aparecen ligadas en $\alpha \vee \beta$ son las que aparecen ligadas en α y las que aparecen ligadas en β.
4. Las variables que aparecen ligadas en $\bigwedge u\, \alpha$ o $\bigvee u\alpha$ son u y las que aparecen ligadas en α.

De acuerdo con estas definiciones, las variables que aparecen ligadas en una semifórmula son siempre variables ligadas, pero las variables que aparecen libres pueden ser libres o ligadas.

Llamaremos *fórmulas* de $\mathcal{L}$ a las semifórmulas en las que ninguna variable ligada aparece libre o, equivalentemente, son las semifórmulas en las que las variables que aparecen libres son libres y las que aparecen ligadas son ligadas.

Si entendemos que las variables que aparecen libres en un semitérmino son todas las que aparecen en él (y que ninguna variable aparece ligada en un semitérmino), entonces también se cumple que los términos (que hemos definido como semitérminos sin variables ligadas) son los semitérminos en los que ninguna variable ligada aparece libre.

Notemos que una variable está libre o ligada en $\alpha \wedge \beta$, $\alpha \rightarrow \beta$ o $\alpha \leftrightarrow \beta$ si y sólo si lo está en α o en β.

Llamaremos *expresiones* a los términos y a las fórmulas de $\mathcal{L}$. Equivalentemente, las expresiones son las semiexpresiones en las que las variables que aparecen libres son libres y las que aparecen ligadas son ligadas.

Una expresión es *abierta* si tiene variables libres. En caso contrario es cerrada. Un *designador* es un término cerrado. Una *sentencia* es una fórmula cerrada.

Nota Con esto hemos presentado con rigor la idea subyacente a la distinción entre variables libres y ligadas en un lenguaje formal. Por ejemplo, en un lenguaje dotado de igualador y de un relator $\in$, tenemos que

$$\bigwedge u(u \in x \rightarrow u \in y)$$

es una fórmula sin más requisito que haber tomado las variables x, y de entre las variables libres de $\mathcal{L}$ y la variable u entre las variables ligadas. En cambio, las semifórmulas

$$u \in x \rightarrow u \in y, \qquad u \in x, \qquad u \in y,$$

necesarias para construir recurrentemente la fórmula indicada, son ejemplos de semifórmulas que no son fórmulas, pues tienen libre la variable ligada u.

De este modo, para construir una fórmula, partimos de semitérminos con variables libres y ligadas y los vamos combinando con relatores y otros signos lógicos, pero sólo acabamos teniendo una fórmula cuando hemos ligado efectivamente con cuantificadores todas las variables ligadas que aparecen en los semitérminos. ■

Sustitución de variables por términos Entre las ventajas más inmediatas de haber establecido la distinción entre variables libres y ligadas de un lenguaje formal está la simplificación de la definición se sustitución de una variable libre por un término en una expresión (compárese con la definición [LM 1.11] y la discusión previa):

Definición 2.5 Sea $\mathcal{L}$ un lenguaje formal. Definimos la *sustitución* de una variable x (libre o ligada) por un término t en una semiexpresión θ de $\mathcal{L}$ como la semiexpresión $\mathtt{S}_x^t\theta$ determinada por las reglas siguientes:

1. $\mathtt{S}_x^t x_0 \equiv \begin{cases} t & \text{si } x \equiv x_0, \\ x_0 & \text{si } x \not\equiv x_0. \end{cases}$
2. $\mathtt{S}_x^t c \equiv c$.
3. $\mathtt{S}_x^t f^n t_1 \cdots t_n \equiv f^n S_x^t t_1 \cdots S_x^t t_n$.
4. $\mathtt{S}_x^t R^n t_1 \cdots t_n \equiv R^n S_x^t t_1 \cdots S_x^t t_n$.
5. $\mathtt{S}_x^t \neg\alpha \equiv \neg \mathtt{S}_x^t \alpha$.

6. $\mathtt{S}_x^t(\alpha \lor \beta) \equiv \mathtt{S}_x^t\alpha \lor \mathtt{S}_x^t\beta$.

7. $\mathtt{S}_x^t \bigwedge u\, \alpha \equiv \begin{cases} \bigwedge u\, \alpha & \text{si } x \equiv u, \\ \bigwedge u\, \mathtt{S}_x^t\, \alpha & \text{si } x \not\equiv u. \end{cases}$

8. $\mathtt{S}_x^t \bigvee u\, \alpha \equiv \begin{cases} \bigvee u\, \alpha & \text{si } x \equiv u, \\ \bigvee u\, \mathtt{S}_x^t\, \alpha & \text{si } x \not\equiv u. \end{cases}$

Más simplemente, $\mathtt{S}_x^t\theta$ no es sino la semiexpresión que resulta quitar cada aparición en θ de la variable x y poner en su lugar todo el término t. Puesto que las variables de t son todas libres, no cabe la posibilidad de que ninguna de ellas quede ligada por un cuantificador al introducirla en θ, ya que los cuantificadores sólo ligan variables ligadas. Es claro que $\mathtt{S}_x^t\theta$ es una expresión si θ lo es.

A partir de la definición del conjuntor, etc. se obtiene fácilmente que

$$\mathtt{S}_x^t(\alpha \land \beta) \equiv \mathtt{S}_x^t\alpha \land \mathtt{S}_x^t\beta, \quad \mathtt{S}_x^t(\alpha \to \beta) \equiv \mathtt{S}_x^t\alpha \to \mathtt{S}_x^t\beta,$$

$$\mathtt{S}_x^t(\alpha \leftrightarrow \beta) \equiv \mathtt{S}_x^t\alpha \leftrightarrow \mathtt{S}_x^t\beta.$$

A menudo escribiremos $\theta(x_1, \ldots, x_n)$ para indicar que

$$\theta(t_1, \ldots, t_n) \equiv \mathtt{S}_{z_1}^{t_1} \cdots \mathtt{S}_{z_n}^{t_n} \mathtt{S}_{x_1}^{z_1} \cdots \mathtt{S}_{x_n}^{z_n} \theta,$$

donde $z_1, \ldots, z_n$ son variables que no estén ni en $t_1, \ldots, t_n$ ni en θ. De este modo $\theta(t_1, \ldots, t_n)$ no es más que la expresión que resulta de sustituir cada variable x_i libre en θ por el término t_i. En particular, la elección de las variables auxiliares z_i es irrelevante. Sólo las consideramos para evitar que si, por ejemplo, en t_n aparece la variable x_{n-1}, ésta sea sustituida por t_{n-1} dentro de t_n cuando se efectúa la sustitución de x_{n-1} en θ tras haber sustituido x_n por t_n, pero todas las variables auxiliares acaban desapareciendo.

No hay que entender, salvo que se diga explícitamente, que las variables libres $x_1, \ldots, x_n$ aparezcan en θ, ni que no puedan aparecer en θ otras variables libres distintas de las indicadas. Escribir $\theta(x_1, \ldots, x_n)$ simplemente nos indica qué variables hay que sustituir por $t_1, \ldots, t_n$ para calcular $\theta(t_1, \ldots, t_n)$.

La definición de modelo de un lenguaje formal dada en [LM 1.2] vale igualmente sin cambio alguno, si bien la definición de denotación y satisfacción dada en [LM 1.7] requiere modificaciones mínimas debido a que ahora los signos primitivos no son los mismos. Terminamos esta sección con los enunciados correspondientes en nuestro contexto a los teoremas [LM 1.9] y [LM 1.12], cuyas demostraciones son esencialmente las mismas:

Teorema 2.6 *Si v y w son valoraciones de un lenguaje formal $\mathcal{L}$ en un modelo M que coinciden sobre las variables libres de una semiexpresión θ, entonces si θ es un semitérmino, $M(\theta)[v] \equiv M(\theta)[w]$ y si θ es una semifórmula, $M \vDash \theta[v]$ syss $M \vDash \theta[w]$.*

Teorema 2.7 *Sea v una valoración de un lenguaje formal $\mathcal{L}$ en un modelo M. Sea t un término de $\mathcal{L}$, sea θ una semiexpresión y x una variable (libre o ligada). Entonces si θ es un semitérmino*

$$M(\mathtt{S}_x^t\theta)[v] \equiv M(\theta)[v_x^{M(t)[v]}]$$

y si θ es una semifórmula

$$M \vDash \mathtt{S}_x^t\theta[v] \quad syss \quad M \vDash \theta[v_x^{M(t)[v]}].$$

El primero afirma que la interpretación de una expresión en un modelo respecto de una valoración depende únicamente de los objetos que la valoración asigna a las variables libres en la expresión. La primera parte del segundo dice que el objeto denotado por $\mathtt{S}_x^t\theta$ es el objeto denotado por θ cuando la variable x se interpreta como el objeto denotado por t, mientras que la segunda parte dice que $\mathtt{S}_x^t\theta$ es satisfecha si y sólo si θ es satisfecha cuando la variable x se interpreta como el objeto denotado por t.

2.2 El cálculo secuencial de primer orden

La definición de secuente que hemos dado en el capítulo anterior para la lógica proposicional se generaliza literalmente para lenguajes formales de primer orden:

Definición 2.8 Si $\mathcal{L}$ es un lenguaje formal, un *secuente* en $\mathcal{L}$ es una expresión de la forma $\Gamma \Rightarrow \Delta$, donde Γ y Δ son dos conjuntos finitos de fórmulas de $\mathcal{L}$. El conjunto Γ recibe el nombre de *antecedente,* del secuente mientras que Δ es el *consecuente.*

Todas las consideraciones que hemos hecho tras la definición 1.4 son válidas en el contexto actual.

A cada secuente $S \equiv \gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$ no vacío le asociamos la fórmula

$$\bar{S} \equiv \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n.$$

Diremos que un modelo M de $\mathcal{L}$ *satisface* un secuente S respecto de una valoración v, y lo representaremos por $M \vDash S[v]$, si se cumple $M \vDash \bar{S}[v]$.

Diremos que S es *verdadero* en M (y lo representaremos por $M \vDash S$) si es satisfecho por toda valoración, y que es *falso* si no es satisfecho por ninguna valoración. Convenimos en que el secuente vacío no es satisfecho por ninguna valoración en ningún modelo, por lo que es falso en todos los modelos.

Observemos que esta definición es correcta en el sentido de que no depende del orden en que las fórmulas aparecen en el antecedente y el consecuente de S, pues las fórmulas $\bar{S}$ que resultan de cambiar dicho orden (o incluso de introducir repeticiones) son equivalentes en el sentido de que una es verdadera en un modelo si y sólo si lo es cualquier otra.

Así pues, si Γ y Δ son conjuntos no vacíos, tenemos que:

1. El secuente $\Gamma \Rightarrow \Delta$ es verdadero en un modelo M si el hecho de que *todas* las fórmulas de su antecedente sean satisfechas respecto de una valoración en M implica que *alguna* de las fórmulas de su consecuente es satisfecha también.
2. El secuente $\Rightarrow \Delta$ es verdadero en un modelo M si toda valoración satisface *alguna* de las fórmulas de su consecuente.
3. El secuente $\Gamma \Rightarrow$ es verdadero si ninguna valoración en M satisface *todas* las fórmulas de su antecedente.
4. El secuente $\Rightarrow$ nunca es verdadero en M.

En particular
$$M \vDash \Rightarrow \alpha \quad \text{si y sólo si} \quad M \vDash \alpha$$
y
$$M \vDash \ \alpha \Rightarrow \quad \text{si y sólo si} \quad M \vDash \neg\alpha.$$

La interpretación de un secuente $\gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$ con antecedente y consecuente no vacíos es la misma que la de la fórmula
$$\gamma_1 \wedge \cdots \wedge \gamma_m \rightarrow \delta_1 \vee \cdots \vee \delta_n.$$

Las definiciones 1.5 (cálculo secuencial) y 1.7 ("deducción" y "demostración"), que hemos dado en el capítulo anterior para el cálculo proposicional, se aplican literalmente al caso de lenguajes de primer orden:

Definición 2.9 Un *cálculo secuencial* K sobre un lenguaje formal $\mathcal{L}$ está determinado por un conjunto de secuentes llamados *axiomas* de K y un número finito de *reglas de inferencia primitivas* que determinan cuándo un secuente es *consecuencia inmediata* de uno o varios secuentes (siempre un número finito).

Una *deducción* en un cálculo secuencial K a partir de un conjunto de secuentes $\mathfrak{S}$ (llamados *premisas* de la deducción) es un conjunto finito de secuentes dispuestos en forma de árbol, de modo que hay un único secuente en el nivel inferior (llamado *secuente final*) y sobre cada secuente S que no sea una premisa o un axioma de K se encuentran uno o varios secuentes de los cuales S sea consecuencia inmediata. Los axiomas y las premisas se llaman *secuentes iniciales* de la deducción.

Una *demostración* en K es una deducción sin premisas.

Usaremos la notación $\mathfrak{S} \underset{K}{\vdash} S$ para indicar que S es el secuente final de una deducción en K con premisas en $\mathfrak{S}$. En particular, $\underset{K}{\vdash} S$ indica que S es un teorema de K.

Veamos ahora un ejemplo de cálculo secuencial que "captura" el razonamiento matemático en el mismo sentido en que lo hace el sistema deductivo formal $K_{\mathcal{L}}$ introducido en [LM] (salvo que, de momento, consideramos el caso de un lenguaje formal sin igualador). Sus axiomas y reglas de inferencia son análogos a los de PK, salvo que ahora incluimos dos pares de reglas adicionales para los cuantificadores y hemos suprimido las reglas correspondientes a los conectores definidos $\wedge$, $\rightarrow$ y $\leftrightarrow$:

El cálculo secuencial LK Dado un lenguaje formal $\mathcal{L}$ (sin igualador), llamaremos $\mathrm{LK}_{\mathcal{L}}$, o simplemente[1] LK al cálculo secuencias cuyos axiomas son los secuentes de la forma $\alpha \Rightarrow \alpha$, donde α es una fórmula atómica de $\mathcal{L}$, y cuyas reglas de inferencia primitivas son las siguientes:

$$\textbf{Debilitación izquierda}\ \frac{\Gamma \Rightarrow \Delta}{\alpha, \Gamma \Rightarrow \Delta}, \qquad \textbf{Debilitación derecha}\ \frac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \alpha},$$

$$\textbf{Corte}\quad \frac{\Gamma \Rightarrow \Delta, \alpha \qquad \alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta},$$

$$\neg\ \textbf{izquierda}\quad \frac{\Gamma \Rightarrow \Delta, \alpha}{\neg\alpha, \Gamma \Rightarrow \Delta}, \qquad \neg\ \textbf{derecha}\quad \frac{\alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\alpha},$$

$$\vee\ \textbf{izquierda}\quad \frac{\alpha,\, \Gamma \Rightarrow \Delta \qquad \beta,\, \Gamma \Rightarrow \Delta}{\alpha \vee \beta,\, \Gamma \Rightarrow \Delta}, \qquad \vee\ \textbf{derecha}\quad \frac{\Gamma \Rightarrow \Delta,\, \alpha,\, \beta}{\Gamma \Rightarrow \Delta,\, \alpha \vee \beta},$$

$$\bigwedge\ \textbf{izquierda}\quad \frac{\alpha(t),\, \Gamma \Rightarrow \Delta}{\bigwedge u\, \alpha(u),\, \Gamma \Rightarrow \Delta}, \qquad \bigwedge\ \textbf{derecha}\quad \frac{\Gamma \Rightarrow \Delta, \alpha(y)}{\Gamma \Rightarrow \Delta, \bigwedge u\, \alpha(u)},$$

$$\bigvee\ \textbf{izquierda}\quad \frac{\alpha(y),\, \Gamma \Rightarrow \Delta}{\bigvee u\, \alpha(u),\, \Gamma \Rightarrow \Delta}, \qquad \bigvee\ \textbf{derecha}\quad \frac{\Gamma \Rightarrow \Delta,\, \alpha(t)}{\Gamma \Rightarrow \Delta,\, \bigvee u\, \alpha(u)},$$

con la condición de que, en la regla derecha del generalizador y en la regla izquierda del particularizador, la variable libre y no aparezca en las fórmulas de Γ y Δ ni en[2] $\bigwedge u\, \alpha(u)$ o $\bigvee u\, \alpha(u)$.

Usaremos los mismos conceptos de "fórmula principal", "fórmula auxiliar", "fórmula colateral", etc. que hemos introducido en el capítulo anterior. Las reglas del generalizador y del particularizador se incluyen entre las reglas lógicas.

A la variable y de la regla derecha del generalizador y de la regla izquierda del particularizador, a la que se exige no estar libre salvo en la fórmula auxiliar, se la llama *variable propia* de la regla.

Reglas de inferencia para los conectores definidos Las reglas de inferencia de los conectores que faltan se pueden demostrar a partir de sus definiciones. Para facilitar la consulta, en la página siguiente las incluimos junto con las reglas de inferencia primitivas. He aquí las deducciones correspondientes:

La conjunción la hemos definido como $\alpha \wedge \beta \equiv \neg(\neg\alpha \vee \neg\beta)$. Por lo tanto:

$$\cfrac{\cfrac{\cfrac{\cfrac{\alpha,\, \beta,\, \Gamma \Rightarrow \Delta}{\beta,\, \Gamma \Rightarrow \Delta,\, \neg\alpha}}{\Gamma \Rightarrow \Delta,\, \neg\alpha,\, \neg\beta}}{\Gamma \Rightarrow \Delta,\, \neg\alpha \vee \neg\beta}}{\neg(\neg\alpha \vee \neg\beta),\, \Gamma \Rightarrow \Delta} \qquad \cfrac{\cfrac{\cfrac{\Gamma \Rightarrow \Delta,\, \alpha}{\neg\alpha,\, \Gamma \Rightarrow \Delta} \qquad \cfrac{\Gamma \Rightarrow \Delta,\, \beta}{\neg\beta,\, \Gamma \Rightarrow \Delta}}{\neg\alpha \vee \neg\beta,\, \Gamma \Rightarrow \Delta}}{\Gamma \Rightarrow \Delta,\, \neg(\neg\alpha \vee \neg\beta)}$$

[1]Las iniciales LK corresponden a "lógica clásica" en alemán.

[2]Aquí hay que entender que $\alpha(y) \equiv \mathrm{S}_u^y \alpha(u)$, por lo que, en principio, y podría estar libre en la fórmula $\alpha(u)$.

Reglas de inferencia de LK

$$\textbf{Debilitación izquierda}\ \frac{\Gamma\Rightarrow\Delta}{\alpha,\Gamma\Rightarrow\Delta},\qquad \textbf{Debilitación derecha}\ \frac{\Gamma\Rightarrow\Delta}{\Gamma\Rightarrow\Delta,\alpha},$$

$$\textbf{Corte}\quad \frac{\Gamma\Rightarrow\Delta,\alpha\qquad \alpha,\Gamma\Rightarrow\Delta}{\Gamma\Rightarrow\Delta},$$

$$
\begin{array}{c|cc}
\neg & \dfrac{\Gamma\Rightarrow\Delta,\alpha}{\neg\alpha,\Gamma\Rightarrow\Delta}, & \dfrac{\alpha,\Gamma\Rightarrow\Delta}{\Gamma\Rightarrow\Delta,\neg\alpha}, \\[2ex]
\lor & \dfrac{\alpha,\,\Gamma\Rightarrow\Delta\qquad \beta,\,\Gamma\Rightarrow\Delta}{\alpha\lor\beta,\,\Gamma\Rightarrow\Delta}, & \dfrac{\Gamma\Rightarrow\Delta,\,\alpha,\,\beta}{\Gamma\Rightarrow\Delta,\,\alpha\lor\beta}, \\[2ex]
\land & \dfrac{\alpha,\,\beta,\,\Gamma\Rightarrow\Delta}{\alpha\land\beta,\ \Gamma\Rightarrow\Delta}, & \dfrac{\Gamma\Rightarrow\Delta,\,\alpha\quad \Gamma\Rightarrow\Delta,\,\beta}{\Gamma\Rightarrow\Delta,\alpha\land\beta}, \\[2ex]
\rightarrow & \dfrac{\Gamma\Rightarrow\Delta,\alpha\qquad \beta,\Gamma\Rightarrow\Delta}{\alpha\rightarrow\beta,\ \Gamma\Rightarrow\Delta}, & \dfrac{\alpha,\Gamma\Rightarrow\Delta,\beta}{\Gamma\Rightarrow\Delta,\alpha\rightarrow\beta}, \\[2ex]
\leftrightarrow & \dfrac{\alpha,\,\beta,\,\Gamma\Rightarrow\Delta\qquad \Gamma\Rightarrow\Delta,\,\alpha,\,\beta}{\alpha\leftrightarrow\beta,\ \Gamma\Rightarrow\Delta}, & \dfrac{\alpha,\Gamma\Rightarrow\Delta,\beta\qquad \beta,\Gamma\Rightarrow\Delta,\alpha}{\Gamma\Rightarrow\Delta,\alpha\leftrightarrow\beta}, \\[2ex]
\bigwedge & \dfrac{\alpha(t),\,\Gamma\Rightarrow\Delta}{\bigwedge u\,\alpha(u),\,\Gamma\Rightarrow\Delta}, & \dfrac{\Gamma\Rightarrow\Delta,\alpha(y)}{\Gamma\Rightarrow\Delta,\bigwedge u\,\alpha(u)}, \\[2ex]
\bigvee & \dfrac{\alpha(y),\,\Gamma\Rightarrow\Delta}{\bigvee u\,\alpha(u),\,\Gamma\Rightarrow\Delta}, & \dfrac{\Gamma\Rightarrow\Delta,\,\alpha(t)}{\Gamma\Rightarrow\Delta,\,\bigvee u\,\alpha(u)},
\end{array}
$$

con la condición de que, en la regla derecha del generalizador y en la izquierda del particularizador, la variable propia y no aparezca fuera de la fórmula auxiliar.

La implicación la hemos definido como $\alpha\rightarrow\beta\equiv\neg\alpha\lor\beta$, luego

$$\cfrac{\cfrac{\Gamma\Rightarrow\Delta,\,\alpha}{\neg\alpha,\,\Gamma\Rightarrow\Delta}\qquad \beta,\,\Gamma\Rightarrow\Delta}{\neg\alpha\lor\beta,\,\Gamma\Rightarrow\Delta}\qquad \cfrac{\cfrac{\alpha,\,\Gamma\Rightarrow\Delta,\,\beta}{\Gamma\Rightarrow\Delta,\,\neg\alpha,\,\beta}}{\Gamma\Rightarrow\Delta,\,\neg\alpha\lor\beta}$$

La coimplicación es, por definición, $\alpha\leftrightarrow\beta\equiv(\alpha\land\beta)\lor(\neg\alpha\land\neg\beta)$, luego

$$\cfrac{\cfrac{\alpha,\,\beta,\,\Gamma\Rightarrow\Delta}{\alpha\land\beta,\,\Gamma\Rightarrow\Delta}\qquad \cfrac{\cfrac{\Gamma\Rightarrow\Delta,\,\alpha,\,\beta}{\neg\alpha,\,\neg\beta,\,\Gamma\Rightarrow\Delta}}{\neg\alpha\land\neg\beta,\,\Gamma\Rightarrow\Delta}}{(\alpha\land\beta)\lor(\neg\alpha\land\neg\beta),\,\Gamma\Rightarrow\Delta}$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\alpha\Rightarrow\alpha}{\alpha,\,\Gamma\Rightarrow\Delta,\,\alpha}}{\Gamma\Rightarrow\Delta,\,\alpha,\,\neg\alpha}\quad \cfrac{\beta,\,\Gamma\Rightarrow\Delta,\,\alpha}{\Gamma\Rightarrow\Delta,\,\alpha,\,\neg\beta}}{\Gamma\Rightarrow\Delta,\,\alpha,\,\neg\alpha\land\neg\beta}\quad \cfrac{\cfrac{\alpha,\,\Gamma\Rightarrow\Delta,\,\beta}{\Gamma\Rightarrow\Delta,\,\beta,\,\neg\alpha}\quad \cfrac{\cfrac{\beta\Rightarrow\beta}{\beta,\,\Gamma\Rightarrow\Delta,\,\beta}}{\Gamma\Rightarrow\Delta,\,\beta,\,\neg\beta}}{\Gamma\Rightarrow\Delta,\,\beta,\,\neg\alpha\land\neg\beta}}{\Gamma\Rightarrow\Delta,\,\alpha\land\beta,\,\neg\alpha\land\neg\beta}}{\Gamma\Rightarrow\Delta,\,(\alpha\land\beta)\lor(\neg\alpha\land\neg\beta)}\qquad\blacksquare$$

Por supuesto, las reglas de inferencia de LK no son arbitrarias, sino que están elegidas de modo que se cumpla la versión correspondiente del teorema de corrección:

Teorema 2.10 (de corrección) *Si M es un modelo de un lenguaje formal $\mathcal{L}$, $\mathfrak{S}$ es un conjunto de secuentes verdaderos en M y $\mathfrak{S} \underset{\mathrm{LK}}{\vdash} S$, entonces S también es verdadero en M.*

DEMOSTRACIÓN: Es obvio que todos los axiomas de LK son verdaderos en cualquier modelo M, luego basta comprobar que si los secuentes superiores de una regla de inferencia de LK son verdaderos en M, el secuente inferior también lo es. La prueba para todas las reglas de inferencia distintas de las de los cuantificadores es prácticamente la misma que la dada en la prueba del teorema 1.6. Vamos a ver que el resultado también es cierto para las cuatro reglas de los cuantificadores.

Pongamos que Γ consta de $\gamma_1, \ldots, \gamma_m$ y Δ de $\delta_1, \ldots, \delta_n$ (sin excluir que puedan ser conjuntos vacíos). Fijemos una valoración v en M.

Para la regla izquierda del particularizador, si el secuente superior es verdadero en M, tenemos que

$$M \vDash (\neg\alpha(t) \vee \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[v],$$

luego, o bien $M \vDash \neg\alpha(t)[v]$, o bien

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[v].$$

El primer caso, por el teorema 2.7, equivale a $M \vDash \neg\alpha(u)[v_u^{M(t)[v]}]$, o también a que no se cumple $M \vDash \alpha(u)[v_u^{M(t)[v]}]$. Esto implica a su vez que no se cumple $M \vDash \bigwedge u\, \alpha(u)[v_u^{M(t)[v]}]$, o también a que se cumpla $M \vDash \neg\bigwedge u\, \alpha(u)[v_u^{M(t)[v]}]$, que por 2.6 equivale a $M \vDash \bigwedge u\, \alpha(u)[v]$. Por consiguiente, se cumple

$$M \vDash (\neg\bigwedge u\, \alpha(u) \vee \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[v],$$

luego el secuente inferior es verdadero en M.

Si el secuente superior de la regla derecha es verdadero en M, tenemos que, para toda valoración w,

$$M \vDash (\vee \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n \vee \alpha(y))[w].$$

Si $M \vDash \neg\bigwedge u\, \alpha(u)[v]$, entonces existe un a en M tal que $M \vDash \neg\alpha(u)[v_u^a]$ y, llamando $w = v_{uy}^{aa}$, el teorema 2.7 nos da que

$$M \vDash \neg\alpha(y)[w] \quad \text{syss} \quad M \vDash \neg\alpha(u)[w_u^{w(y)}],$$

pero $w_u^{w(y)} = w$ que coincide con v_u^a salvo a lo sumo en y, que no está en $\alpha(u)$, luego por el teorema 2.6 tenemos que se cumple $M \vDash \neg\alpha(y)[w]$, luego, por la hipótesis sobre el secuente superior, tiene que ser

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[w].$$

Pero w coincide con v salvo a lo sumo en las variables u, y, ninguna de las cuales está libre en las fórmulas de Γ y Δ (la variable u porque es ligada, y la variable y por la hipótesis de la regla). Aplicando de nuevo 2.6 llegamos a que

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[v],$$

y esto bajo la hipótesis de que $M \vDash \neg\bigwedge u\,\alpha(u)[v]$, luego en general,

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n \vee \bigwedge u\,\alpha(u))[v],$$

luego el secuente inferior es verdadero en M.

En el caso del generalizador, si el secuente superior de la regla izquierda es verdadero en M, tenemos que, para toda valoración w,

$$M \vDash (\neg\alpha(y) \vee \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[w].$$

Si $M \vDash \bigvee u\,\alpha(u)[v]$, entonces existe un a en M tal que $M \vDash \alpha(u)[v_u^a]$ y, llamando $w = v_{uy}^{aa}$, el teorema 2.7 nos da que

$$M \vDash \alpha(y)[w] \quad \text{syss} \quad M \vDash \alpha(u)[w_u^{w(y)}],$$

pero $w_u^{w(y)} = w$ que coincide con v_u^a salvo a lo sumo en y, que no está en $\alpha(u)$, luego por el teorema 2.6 tenemos que se cumple $M \vDash \alpha(y)[w]$, luego, por la hipótesis sobre el secuente superior, tiene que ser

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[w].$$

Pero w coincide con v salvo a lo sumo en las variables u, y, ninguna de las cuales está libre en las fórmulas de Γ y Δ (la variable u porque es ligada, y la variable y por la hipótesis de la regla). Aplicando de nuevo 2.6 llegamos a que

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[v],$$

y esto bajo la hipótesis $M \vDash \bigvee u\,\alpha(u)[v]$, luego en general,

$$M \vDash (\neg\bigvee u\,\alpha(u) \vee \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[v],$$

luego el secuente inferior es verdadero en M.

Si el secuente superior de la regla derecha es verdadero en M, tenemos que

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n \vee \alpha(t))[v],$$

que por 2.7 equivale a

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n \vee \alpha(u))[v_u^{M(t)[v]}].$$

A su vez, esto implica que

$$M \vDash (\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n \vee \bigvee u\,\alpha(u))[v],$$

luego el secuente inferior es verdadero en M. ■

Nota Observemos que la regla izquierda del particularizador no cumpliría el teorema anterior si no exigiéramos que la variable propia no esté libre en Γ y Δ ni en $\bigvee u\,\alpha(u)$. Por ejemplo, si tomamos $\alpha(u) \equiv u \neq y$, con lo que $\alpha(y) \equiv y \neq y$, el secuente

$$y \neq y \Rightarrow y \neq y$$

es verdadero en cualquier modelo, pero al aplicar la "regla" obtenemos

$$\bigvee u\, u \neq y \Rightarrow y \neq y,$$

que es falso en cualquier modelo en que el igualador se interprete como la identidad y haya más de un objeto en su universo. El "fallo" está en que la variable propia y está libre en $\alpha(u)$.

Similarmente, si tomamos $\alpha(u) \equiv u = z$, con lo que $\alpha(y) \equiv y = z$, el secuente

$$y = z \Rightarrow y = z$$

es verdadero en cualquier modelo, pero al aplicar la "regla" resulta

$$\bigvee u\, u = z \Rightarrow y = z,$$

que no es verdadero en modelos en los que el igualador se interprete como la identidad y haya más de un objeto en su universo, y ahora el "fallo" es que la variable propia y está libre en el consecuente. Es fácil poner ejemplos similares para la regla derecha del generalizador. ■

Aunque hemos tomado únicamente como axiomas los secuentes de la forma $\alpha \Rightarrow \alpha$ donde α es una fórmula atómica, en realidad todos los secuentes de esta forma son teoremas, aunque α no sea atómica:

Teorema 2.11 *Si α es cualquier fórmula de un lenguaje formal $\mathcal{L}$, entonces $\alpha \Rightarrow \alpha$ es un teorema de* LK.

DEMOSTRACIÓN: Razonamos por inducción sobre la longitud de α. Si α es una fórmula atómica entonces $\alpha \Rightarrow \alpha$ es un axioma de LK, luego es su propia demostración. Si $\alpha \equiv \neg\beta$ y el resultado es cierto para β, entonces basta aplicar las reglas del negador:

$$\dfrac{\dfrac{\beta \Rightarrow \beta}{\neg\beta,\, \beta \Rightarrow}}{\neg\beta \Rightarrow \neg\beta}$$

y encadenar esta sucesión con una demostración de $\beta \Rightarrow \beta$.

Si $\alpha \equiv \beta \vee \gamma$ y el resultado es cierto para β y γ, razonamos así:

$$\dfrac{\dfrac{\dfrac{\beta \Rightarrow \beta}{\beta \Rightarrow \beta,\, \gamma} \qquad \dfrac{\gamma \Rightarrow \gamma}{\gamma \Rightarrow \beta,\, \gamma}}{\beta \vee \gamma \Rightarrow \beta,\, \gamma}}{\beta \vee \gamma \Rightarrow \beta \vee \gamma}$$

donde hemos usado (de abajo hacia arriba) las dos reglas del disyuntor y luego las de debilitación. Luego la demostración se prolonga con demostraciones respectivas de los dos secuentes indicados, que existen por hipótesis de inducción.

Si $\alpha \equiv \bigwedge u\,\beta(u)$ e y es una variable libre que no esté en β, podemos aplicar la hipótesis de inducción a la fórmula $\beta(y)$, cuya longitud es la misma que la de la semifórmula $\beta(u)$, que a su vez es menor que la de α. Por lo tanto, podemos razonar así:

$$\begin{array}{c} \beta(y) \Rightarrow \beta(y) \\ \hline \bigwedge u\,\beta(u) \Rightarrow \beta(y) \\ \hline \bigwedge u\,\beta(u) \Rightarrow \bigwedge u\,\beta(u) \end{array}$$

Si $\alpha \equiv \bigvee u\,\beta(u)$ e y es una variable libre que no esté en β, entonces podemos aplicar la hipótesis de inducción a la fórmula $\beta(y)$, cuya longitud es la misma que la de la semifórmula $\beta(u)$, que a su vez es menor que la de α. Por lo tanto, podemos razonar así:

$$\begin{array}{c} \beta(y) \Rightarrow \beta(y) \\ \hline \beta(y) \Rightarrow \bigvee u\,\beta(u) \\ \hline \bigvee u\,\beta(u) \Rightarrow \bigvee u\,\beta(u) \end{array}$$

■

Ejemplo Veamos una demostración del secuente:

$$\Rightarrow \bigvee u(Ru \to \bigwedge v\,Rv),$$

que puede interpretarse como que existe alguien que, si vivirá hasta los 100 años, entonces todos viviremos hasta los 100 años. La idea de la prueba es distinguir dos casos, correspondientes a los secuentes

$$\neg\bigvee v\,\neg Rv \Rightarrow \bigvee u(Ru \to \bigwedge v\,Rv), \qquad \bigvee v\,\neg Rv \Rightarrow \bigvee u(Ru \to \bigwedge v\,Rv),$$

es decir, o bien todos vamos a vivir hasta los 100 años o existe alguien que no va a vivir hasta los 100 años. El primero de estos dos secuentes es equivalente al que resulta de pasar el antecedente al consecuente eliminando el negador. Así tenemos los dos secuentes del penúltimo paso de la demostración, con lo que la regla de corte nos da la conclusión.

$$\begin{array}{cc} \begin{array}{c} Ry \Rightarrow Ry \\ \hline Rx,\, Ry \Rightarrow Ry \\ \hline Rx \Rightarrow Ry,\, \neg Ry \\ \hline Rx \Rightarrow Ry,\, \bigvee v\,\neg Rv \\ \hline Rx \Rightarrow \bigwedge v\,Rv,\, \bigvee v\,\neg Rv \\ \hline \Rightarrow Rx \to \bigwedge v\,Rv,\, \bigvee v\,\neg Rv \\ \hline \Rightarrow \bigvee u(Ru \to \bigwedge v\,Rv),\, \bigvee v\,\neg Rv \end{array} & \begin{array}{c} Ry \Rightarrow Ry \\ \hline Ry \Rightarrow Ry,\, \bigwedge v\,Rv \\ \hline \neg Ry,\, Ry \Rightarrow \bigwedge v\,Rv \\ \hline \neg Ry \Rightarrow Ry \to \bigwedge v\,Rv \\ \hline \neg Ry \Rightarrow \bigvee u(Ru \to \bigwedge v\,Rv) \\ \hline \bigvee v\,\neg Rv \Rightarrow \bigvee u(Ru \to \bigwedge v\,Rv) \end{array} \\ \hline \multicolumn{2}{c}{\Rightarrow \bigvee u(Ru \to \bigwedge v\,Rv)} \end{array}$$

A partir de estos dos secuentes, la prueba se construye mecánicamente “de abajo hacia arriba”. En la rama izquierda eliminamos el particularizador con la regla derecha del particularizador, luego eliminamos el implicador con su regla izquierda, luego eliminamos el generalizador, a continuación el particularizador, luego el negador y así llegamos a un secuente con una fórmula repetida, luego por debilitación lo reducimos a un axioma. Notemos que es esencial eliminar primero el generalizador y luego el particularizador, pues la regla derecha del generalizador requiere que la variable propia y no esté libre en ninguna otra fórmula. La rama derecha se construye análogamente. ■

Variantes Exactamente igual que en el caso del cálculo proposicional, podemos ver que las reglas del disyuntor[3] y la de corte pueden sustituirse por las variantes siguientes en la definición de LK:

$$\frac{\alpha,\,\Gamma\Rightarrow\Delta\qquad\beta,\,\Gamma'\Rightarrow\Delta'}{\alpha\vee\beta,\,\Gamma,\,\Gamma'\Rightarrow\Delta,\,\Delta'},\qquad\frac{\Gamma\Rightarrow\Delta,\,\alpha}{\Gamma\Rightarrow\Delta,\,\alpha\vee\beta},\qquad\frac{\Gamma\Rightarrow\Delta,\,\beta}{\Gamma\Rightarrow\Delta,\,\alpha\vee\beta},$$

$$\frac{\Gamma\Rightarrow\Delta,\,\alpha\qquad\alpha,\,\Gamma'\Rightarrow\Delta'}{\Gamma,\,\Gamma'\Rightarrow\Delta,\,\Delta'}.$$

■

2.3 El cálculo secuencial con igualador

Para tratar con el igualador sólo necesitamos añadir algunos axiomas al cálculo secuencial:

Definición 2.12 Si $\mathcal{L}$ es un lenguaje formal con igualador, llamaremos LK_i al cálculo secuencial que resulta de añadir a LK los *axiomas del igualador,* que son todos los secuentes de la forma:

I1. $\Rightarrow t = t$.

I2. $t_1 = t_1', \ldots, t_n = t_n' \Rightarrow f^n t_1 \cdots t_n = f^n t_1' \cdots t_n'$.

I3. $t_1 = t_1', \ldots, t_n = t_n', R^n t_1 \cdots t_n \Rightarrow R^n t_1' \cdots t_n'$.

Es claro que estos secuentes son verdaderos en todo modelo de $\mathcal{L}$, por lo que el teorema de corrección 2.10 es válido también para LK_i (considerando ahora modelos de $\mathcal{L}$ en los que el igualador se interpreta necesariamente como la identidad).

Veamos unas consecuencias inmediatas de estos axiomas:

Teorema 2.13 *Si $\mathcal{L}$ es un lenguaje formal con igualador, los secuentes siguientes son teoremas de* LK_i*:*

Reflexividad de =	$\Rightarrow t = t$
Simetría de =	$t_1 = t_2 \Rightarrow t_2 = t_1$
Transitividad de =	$t_1 = t_2,\, t_2 = t_3 \Rightarrow t_1 = t_3$

[3] También podemos probar las variantes siguientes de las reglas del conjuntor, aunque tienen menos interés en este contexto, porque las reglas del conjuntor no forman parte de la definición de LK:

$$\frac{\alpha,\,\Gamma\Rightarrow\Delta}{\alpha\wedge\beta,\;\Gamma\Rightarrow\Delta},\qquad\frac{\beta,\,\Gamma\Rightarrow\Delta}{\alpha\wedge\beta,\;\Gamma\Rightarrow\Delta},\qquad\frac{\Gamma\Rightarrow\Delta,\,\alpha\qquad\Gamma'\Rightarrow\Delta',\,\beta}{\Gamma,\,\Gamma'\Rightarrow\Delta,\,\Delta',\,\alpha\wedge\beta}.$$

Demostración: Los secuentes que expresan la reflexividad son axiomas. Para la simetría observamos que el secuente

$$t_1 = t_2,\, t_1 = t_1,\, t_1 = t_1 \Rightarrow t_2 = t_1$$

es un axioma de tipo I3, por lo que

$$\dfrac{\dfrac{\Rightarrow t_1 = t_1}{t_1 = t_2 \Rightarrow t_1 = t_1,\, t_2 = t_1} \qquad t_1 = t_1,\, t_1 = t_2 \Rightarrow t_2 = t_1}{t_1 = t_2 \Rightarrow t_2 = t_1}$$

La transitividad se prueba de forma similar, considerando el axioma

$$t_1 = t_1,\, t_2 = t_3,\, t_1 = t_2 \Rightarrow t_1 = t_3.$$

■

Como en el caso del teorema 2.11, a partir de estos axiomas pueden probarse versiones más generales:

Teorema 2.14 *Si $\alpha(x_1,\ldots,x_k)$ es una fórmula de $\mathcal{L}$ y $t(x_1,\ldots,x_k)$, $s_1,\ldots,s_k$, $t_1,\ldots,t_k$ son términos, los secuentes siguientes son teoremas de* LK_i*:*

I1. $\Rightarrow t = t$.

I2. $s_1 = t_1,\ldots,s_k = t_k \Rightarrow t(s_1,\ldots,s_k) = t(t_1,\ldots,t_k)$.

I3. $s_1 = t_1,\ldots,s_k = t_k,\, \alpha(s_1,\ldots,s_k) \Rightarrow \alpha(t_1,\ldots,t_k)$.

Demostración: Los secuentes de tipo I1. son axiomas de LK_i. Demostramos I2. por inducción sobre la longitud del término t. Si es una variable x_i el secuente es

$$s_1 = t_1,\ldots,s_k = t_k \Rightarrow s_i = t_i,$$

que se demuestra a partir del axioma $s_i = t_i \Rightarrow s_i = t_i$ mediante las reglas de debilitación. Si t es una constante c, entonces el secuente es

$$s_1 = t_1,\ldots,s_k = t_k \Rightarrow c = c,$$

y se demuestra por debilitación a partir del axioma $\Rightarrow c = c$. Si $t \equiv fT_1\cdots T_n$ por hipótesis de inducción podemos probar los secuentes

$$s_1 = t_1,\ldots,s_k = t_k \Rightarrow T_i(s_1,\ldots,s_k) = T_i(t_1,\ldots,t_k).$$

Por otra parte, el secuente siguiente es un axioma de tipo I2:

$$T_1(s_j) = T_1(t_j),\ldots,T_n(s_j) = T_n(t_j) \Rightarrow t(s_j) = t(t_j),$$

donde abreviamos $T_i(s_j) \equiv T_1(s_1,\ldots,s_k)$. Cortando este secuente con el precedente para $i = 1$ (usando la variante más general de la regla de corte) obtenemos

$$s_1 = t_1,\ldots,s_k = t_k,\, T_2(s_j) = T_2(t_j),\ldots,T_n(s_j) = T_n(t_j) \Rightarrow t(s_j) = t(t_j).$$

Similarmente, vamos cortando con los secuentes que tenemos por hipótesis de inducción para $i = 2, \ldots, n$ y llegamos a

$$s_1 = t_1, \ldots, s_k = t_k \Rightarrow t(s_j) = t(t_j).$$

Similarmente, probamos I3. por inducción sobre la longitud de α. En el caso en que $\alpha \equiv RT_1 \cdots T_n$, el secuente siguiente es un axioma:

$$T_1(s_j) = T_1(t_j), \ldots, T_n(s_j) = T_n(t_j),\ \alpha(s_j) \Rightarrow \alpha(t_j)$$

y, por el apartado anterior, los secuentes siguientes son teoremas:

$$s_1 = t_1, \ldots, s_k = t_k \Rightarrow T_i(s_j) = T_i(t_j).$$

Como en el apartado anterior, podemos ir cortando las fórmulas $T_i(s_j) = T_i(t_j)$ hasta obtener el secuente

$$s_1 = t_1, \ldots, s_k = t_k,\ \alpha(s_j) \Rightarrow \alpha(t_j).$$

Si $\alpha \equiv \neg\beta$, razonamos como sigue:

$$\cfrac{\cfrac{t_1 = s_1, \ldots, t_n = s_k,\ \beta(t_i) \Rightarrow \beta(s_i)}{s_1 = t_1, \ldots, s_n = t_k,\ \beta(t_i) \Rightarrow \beta(s_i)}}{s_1 = t_1, \ldots, s_n = t_k,\ \alpha(s_i) \Rightarrow \alpha(t_i)}$$

donde en el primer paso hemos cortado con los teoremas $s_i = t_i \Rightarrow t_i = s_i$ y en el segundo hemos usado las reglas del negador.

Supongamos ahora que $\alpha \equiv \beta \vee \gamma$ y que β y γ cumplen el teorema. Concluimos así:

$$\cfrac{\cfrac{\cfrac{s_i = t_i,\ \beta(s_i) \Rightarrow \beta(t_i)}{s_i = t_i,\ \beta(s_i) \Rightarrow \beta(t_i),\ \gamma(t_i)} \qquad \cfrac{s_i = t_i,\ \gamma(s_i) \Rightarrow \gamma(t_i)}{s_i = t_i,\ \gamma(s_i) \Rightarrow \beta(t_i),\ \gamma(t_i)}}{s_1 = t_1, \ldots, s_k = t_k,\ \beta(s_i) \vee \gamma(s_i) \Rightarrow \beta(t_i),\ \gamma(t_i)}}{s_1 = t_1, \ldots, s_k = t_k,\ \beta(s_i) \vee \gamma(s_i) \Rightarrow \beta(t_i) \vee \gamma(t_i)}$$

Si $\alpha \equiv \bigwedge u\, \beta(u, x_1, \ldots, x_k)$, tomamos una variable libre y que no esté en α ni en ninguno de los términos s_i, t_i. Aplicamos la hipótesis de inducción a la fórmula $\beta(y, x_1, \ldots, x_k)$

$$\cfrac{\cfrac{s_1 = t_1, \ldots, s_k = t_k,\ \beta(y, s_i) \Rightarrow \beta(y, t_i)}{s_1 = t_1, \ldots, s_k = t_k,\ \bigwedge u\, \beta(u, s_i) \Rightarrow \beta(y, t_i)}}{s_1 = t_1, \ldots, s_k = t_k,\ \bigwedge u\, \beta(u, s_i) \Rightarrow \bigwedge u\, \beta(u, t_i)}$$

Observemos que para pasar del segundo secuente al tercero necesitamos que u no esté libre fuera de la fórmula auxiliar, como es el caso.

Si $\alpha \equiv \bigvee u\, \beta(u, x_1, \ldots, x_k)$ razonamos análogamente, sólo que en este caso tenemos que aplicar primero la regla derecha del particularizador y en segundo lugar la regla izquieerda. ∎

Ejemplo Como ilustración vamos a demostrar el secuente

$$\bigwedge uvw((uv)w = u(vw)) \Rightarrow \bigwedge uvw(u \mid v \land v \mid w \rightarrow u \mid w),$$

que se corresponde con la demostración que en la página vii hemos formalizado en el sistema deductivo formal $K_{\mathcal{L}}$ descrito en [LM]. Aquí hay que entender que $x \mid y \equiv \bigvee u\, y = xu$.

Notemos que hemos cambiado los nombres a las variables para distinguir entre variables libres y ligadas.[4]

$$
\begin{array}{c}
\bigwedge uvw((uv)w = u(vw)) \Rightarrow (xx')y' = x(x'y') \qquad y = xx',\, z = yy' \Rightarrow z = (xx')y' \\
\hline
\bigwedge uvw((uv)w = u(vw)),\, y = xx',\, z = yy' \Rightarrow z = (xx')y',\, (xx')y' = x(x'y') \\
\hline
\bigwedge uvw((uv)w = u(vw)),\, y = xx',\, z = yy' \Rightarrow z = x(x'y') \\
\hline
\bigwedge uvw((uv)w = u(vw)),\, y = xx',\, z = yy' \Rightarrow \bigvee u\, z = xu \\
\hline
\bigwedge uvw((uv)w = u(vw)),\, \bigvee u\, y = xu,\, \bigvee u\, z = yu \Rightarrow \bigvee u\, z = xu \\
\hline
\bigwedge uvw((uv)w = u(vw)),\, x \mid y \land y \mid z \Rightarrow x \mid z \\
\hline
\bigwedge uvw((uv)w = u(vw)) \Rightarrow x \mid y \land y \mid z \rightarrow x \mid z \\
\hline
\bigwedge uvw((uv)w = u(vw)) \Rightarrow \bigwedge uvw(u \mid v \land v \mid w \rightarrow u \mid w)
\end{array}
$$

En general, en ejemplos sencillos como éste, en los que podemos permitirnos el lujo de razonar "formalmente", es decir, sin considerar el significado de las fórmulas involucradas, las demostraciones hay que planearlas "de abajo hacia arriba". Así, lo primero que hacemos es quitar los cuantificadores de la conclusión, lo cual es legítimo porque en el penúltimo secuente es posible aplicar tres veces la regla derecha del generalizador, ya que las variables propias que se cuantifican no están libres en ninguna otra fórmula.

A continuación pasamos la hipótesis de la implicación al antecedente del secuente, lo cual puede considerarse como lo análogo a tomarla como premisa.

A continuación eliminamos el conjuntor y aprovechamos para sustituir cada fórmula de divisibilidad por su definición, lo cual técnicamente no es ningún cambio. Estamos aludiendo a las mismas fórmulas con otros nombres.

A continuación eliminamos los particularizadores del antecedente. Notemos que las normas de LK nos obligan a dejar dos variables libres distintas x' e y', pues de lo contrario no sería lícito usar la regla izquierda del particularizador, ya que la variable x' estaría libre en otra fórmula.

A continuación eliminamos el particularizador del consecuente. Podríamos haber puesto cualquier variable, pero si queremos dejar un término que estemos en condiciones de probar que cumple la fórmula correspondiente, ese término tiene que ser $x'y'$ (en este punto no tenemos más remedio que olvidar el formalismo y pararnos a entender qué estamos haciendo realmente).

Ahora observamos que, en realidad, las dos igualdades del antecedente nos permitirán probar la igualdad $z = (xx')y'$, y necesitaremos la propiedad asociativa que estamos tomando como premisa para probar que esta expresión coincide

[4]Para incluir esta distinción en $K_{\mathcal{L}}$ basta modificar la regla de introducción del generalizador, que en lugar de establecer que de α se deduce $\bigwedge x\, \alpha$, debe establecer que de $\alpha(x)$ se deduce $\bigwedge u\, \alpha(u)$.

con la que necesitamos. Por ello descomponemos la igualdad en las dos igualdades correspondientes. El paso del segundo al tercer secuente está justificado por la transitividad de la igualdad.

Por último, el segundo secuente se puede obtener mezclando los dos secuentes de la primera línea. El primero se justifica por tres eliminaciones del generalizador y el segundo por el tercer apartado del teorema 2.14, tomando $\alpha(y) \equiv z = yy'$. ■

2.4 El teorema de completitud

En esta sección demostraremos la versión para la lógica de primer orden del teorema de completitud 1.11. Hemos visto que el cálculo secuencial es correcto, es decir, que todos los secuentes deducibles de un conjunto de premisas dadas serán verdaderos en todos los modelos en los que sean verdaderas las premisas, y ahora tenemos que probar que LK y LK_i son completos, lo que significa que si un secuente S no puede deducirse de unas premisas, ello no puede atribuirse a que falten axiomas o reglas de inferencia, sino que en tal caso necesariamente hay un modelo en el que las premisas son verdaderas pero S no lo es, por lo que S no debe poder deducirse.

La conclusión es que la capacidad deductiva de LK_i es exactamente la misma que la de un matemático: un matemático puede deducir algo de unos axiomas si y sólo si dicha deducción puede formalizarse en LK_i. Como esto también vale para el cálculo deductivo $K_{\mathcal{L}}$ estudiado en [LM], indirectamente concluimos que una fórmula α es deducible de unas premisas en $K_{\mathcal{L}}$ si y sólo si el secuente $\Rightarrow \alpha$ es deducible en LK_i de los secuentes correspondientes a las premisas. La prueba de este hecho a través del teorema de completitud no es constructiva, así que en la sección 2.7 lo probaremos explícitamente.

Deduciremos el teorema de completitud semántica para LK de la versión siguiente del teorema de compacidad:

Teorema 2.15 *Sea* Π *un conjunto tal vez infinito de sentencias de un lenguaje formal* $\mathcal{L}$ *sin igualador y sea* $\Gamma \Rightarrow \Delta$ *un secuente en* $\mathcal{L}$ *que es verdadero en todos los modelos de* Π. *Entonces existe un conjunto finito* Π_0 *de sentencias de* Π *tal que el secuente* $\Pi_0, \Gamma \Rightarrow \Delta$ *es demostrable en* LK *con una demostración que no usa la regla de corte.*

En particular, tomando Π como el conjunto vacío, obtenemos una forma débil del teorema de completitud de LK:

Teorema 2.16 *Si* $\Gamma \Rightarrow \Delta$ *es un secuente verdadero en todos los modelos de un lenguaje formal sin igualador, entonces admite una demostración en* LK *en la que no se usa la regla de corte.*

Esto no es suficiente, pues no nos asegura que en LK sea posible extraer todas las consecuencias lógicas de un conjunto de premisas dado. Esto lo probamos en el teorema siguiente:

Teorema 2.17 (de completitud semántica de LK) *Si $\mathfrak{S}$ es un conjunto de secuentes de un lenguaje $\mathcal{L}$ sin igualador y $\Gamma \Rightarrow \Delta$ es un secuente verdadero en todo modelo de $\mathcal{L}$ en el que sean verdaderos los secuentes de $\mathfrak{S}$, entonces* $\mathfrak{S} \underset{\mathrm{LK}}{\vdash} \Gamma \Rightarrow \Delta$.

DEMOSTRACIÓN: Recordemos que a cada secuente no vacío

$$S \equiv \gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$$

le hemos asociado la fórmula

$$\bar{S} \equiv \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n.$$

Llamaremos $\bigwedge\bar{S}$ a su clausura universal, es decir, la sentencia que resulta de ligar todas las variables libres en $\bar{S}$ mediante cuantificadores universales. Así, un secuente S es válido en un modelo M si y sólo si $M \vDash \bar{S}$, si y sólo si $M \vDash \bigwedge\bar{S}$.

Aplicamos el teorema 2.15 tomando como Π el conjunto de las sentencias $\bigwedge\bar{S}$, donde S recorre los secuentes de $\mathfrak{S}$. Es claro que se cumplen las hipótesis, luego existe un conjunto finito $S_1, \ldots, S_n$ de secuentes en $\mathfrak{S}$ de modo que

$$\underset{\mathrm{LK}}{\vdash} \bigwedge\bar{S}_1, \ldots, \bigwedge\bar{S}_k, \Gamma \Rightarrow \Delta.$$

Aplicando la regla izquierda del conjuntor obtenemos

$$\underset{\mathrm{LK}}{\vdash} \bigwedge\bar{S}_1 \wedge \cdots \wedge \bigwedge\bar{S}_k,\ \Gamma \Rightarrow \Delta.$$

Por otra parte, aplicando repetidamente las reglas derechas del negador y del disyuntor obtenemos que $S_i \underset{\mathrm{LK}}{\vdash} \Rightarrow \bar{S}_i$, aplicando la regla derecha del generalizador $S_i \underset{\mathrm{LK}}{\vdash} \Rightarrow \bigwedge\bar{S}_i$ y, a su vez, por la regla derecha del conjuntor,

$$\mathfrak{S} \underset{\mathrm{LK}}{\vdash} \Rightarrow \bigwedge\bar{S}_1 \wedge \cdots \wedge \bigwedge\bar{S}_k.$$

Debilitamos este secuente añadiendo Γ y Δ y finalmente la regla de corte nos da que $\mathfrak{S} \underset{\mathrm{LK}}{\vdash} \Gamma \Rightarrow \Delta$. ■

De aquí deducimos a su vez la completitud de LK_i:

Teorema 2.18 (de completitud del cálculo secuencial) *Si $\mathfrak{S}$ es un conjunto de secuentes de un lenguaje $\mathcal{L}$ con igualador y $\Gamma \Rightarrow \Delta$ es un secuente verdadero en todo modelo de $\mathcal{L}$ en el que sean verdaderos los secuentes de $\mathfrak{S}$, entonces* $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} \Gamma \Rightarrow \Delta$.

DEMOSTRACIÓN: Sea M un modelo de $\mathcal{L}$ considerado como modelo de un lenguaje sin igualador (es decir, sin exigir que el igualador se interprete como la relación de identidad) en el que sean verdaderos los secuentes de $\mathfrak{S} \cup \mathfrak{S}_i$ (recordemos que $\mathfrak{S}_i$ es el conjunto de los axiomas del igualador).

El teorema 2.13 nos da que en LK_i se demuestran los secuentes siguientes:

$$\Rightarrow x = x, \qquad \Rightarrow x = y \to y = x, \qquad \Rightarrow y = x \land y = z \to x = z.$$

Equivalentemente, estos secuentes se deducen de $\mathfrak{S}_i$ en LK, luego son verdaderos en M, lo cual equivale a que los consecuentes son verdaderos en M, lo que nos da que la relación $M(=)$ es una relación de equivalencia en el universo de M. La representaremos por $\sim$. Sea $\overline{M}$ el conjunto de las clases de equivalencia.

Si f es un funtor n-ádico de $\mathcal{L}$, el secuente

$$x_1 = y_1, \ldots, x_n = y_n \Rightarrow fx_1 \cdots x_n = fy_1 \cdots y_n$$

está en el conjunto $\mathfrak{S}_i$, luego es verdadero en M, y esto se traduce en que si $a_1, \ldots, a_n, b_1, \ldots, b_n$ son objetos de M con $a_i \sim b_i$, entonces

$$M(f)(a_1, \ldots, a_n) \sim M(f)(b_1, \ldots, b_n),$$

luego podemos definir en $\overline{M}$ la función

$$\overline{M}(f)([a_1], \ldots, [a_n]) \equiv [M(f)(a_1, \ldots, a_n))]$$

sin que dependa de la elección de los representantes de las clases de equivalencia. Igualmente, si R es un relator n-ádico, el secuente

$$x_1 = y_1 \land \cdots \land x_n = y_n,\ Rx_1 \cdots x_n \Rightarrow Ry_1 \cdots y_n$$

está en $\mathfrak{S}_i$, luego es verdadero en M, y esto implica que

$$M(R)(a_1, \ldots, a_n) \quad \text{si y sólo si} \quad M(R)(b_1, \ldots, b_n),$$

por lo que podemos definir la relación en $\overline{M}$ dada por

$$\overline{M}(R)([a_1], \ldots, [a_n]) \quad \text{si y sólo si} \quad M(R)(a_1, \ldots, a_n),$$

sin que importe tampoco la elección de los representantes de las clases de equivalencia.

Si además, para cada constante c de $\mathcal{L}$, definimos $\overline{M}(c) = [M(c)]$, tenemos que $\overline{M}$ es un modelo de $\mathcal{L}$ en el que el igualador se interpreta como la identidad.

Si v es una valoración en M y $\bar{v}(x) = [v(x)]$, una simple inducción sobre la longitud de un semitérmino t prueba que

$$\overline{M}(t)[\bar{v}] = [M(t)[v]],$$

y a su vez, una inducción sobre la longitud de una semifórmula α prueba que

$$\overline{M} \vDash \alpha[\bar{v}] \quad \text{si y sólo si} \quad M \vDash \alpha[v].$$

De aquí se sigue a su vez que $\overline{M} \vDash \alpha$ syss $M \vDash \alpha$. Esto implica que un secuente es verdadero en M si y sólo si lo es en $\overline{M}$.

Por lo tanto, $\overline{M}$ es un modelo de $\mathcal{L}$ (como lenguaje con igualador) en el que son verdaderos todos los secuentes de $\mathfrak{S}$, luego por hipótesis $\Gamma \Rightarrow \Delta$ es verdadero en $\overline{M}$, luego también en M.

Con esto hemos probado que este secuente es verdadero en todos los modelos de $\mathcal{L}$ (como lenguaje sin igualador) en los que son verdaderos los secuentes de $\mathfrak{S} \cup \mathfrak{S}_i$, luego el teorema anterior nos permite concluir que $\Gamma \Rightarrow \Delta$ es deducible en LK tomando como premisas los secuentes de $\mathfrak{S} \cup \mathfrak{S}_i$, y esto es tanto como decir que es deducible en LK$_i$ tomando como premisas los secuentes de $\mathfrak{S}$. ■

La prueba del teorema 2.15 se basa en la misma idea que hemos empleado para demostrar el teorema 1.9. En ella partíamos del secuente que queríamos demostrar e íbamos construyendo un árbol aplicando las reglas de inferencia lógicas a las fórmulas no atómicas y así, cuando ya todas las fórmulas eran atómicas, o bien habíamos completado una demostración, cualquiera de sus nodos terminales que no fuera un axioma nos daba una valoración respecto a la que las premisas eran verdaderas, pero la pretendida conclusión era falsa.

Ahora haremos algo parecido, pero, si fallamos en nuestro intento de construir una demostración, lo que obtendremos será un árbol infinito y una de sus ramas determinará un modelo en el que las premisas son verdaderas y la pretendida conclusión es falsa.

Demostración (de 2.15): Es fácil construir explícitamente una enumeración (α_n, t_n) de todos los pares formados por una fórmula y un término de $\mathcal{L}$, de modo que cada par (α, t) aparezca infinitas veces en la sucesión.

Vamos a construir una sucesión D_n de aproximaciones a una demostración del secuente $\Gamma \Rightarrow \Delta$, de modo que cada D_n será un árbol de secuentes que cumpla la definición de demostración (sin admitir la regla de corte) salvo por el hecho de que los secuentes iniciales no tienen por qué ser axiomas, y cuyo secuente final será de la forma $\Pi_n, \Gamma \Rightarrow \Delta$, donde Π_n es un subconjunto finito de Π.

En cada árbol D_n, llamaremos *secuentes activos* a los secuentes iniciales en los que no haya una misma fórmula tanto en el antecedente como en el consecuente. Es claro que si llegamos a un árbol D_n sin secuentes activos, todos sus secuentes iniciales pueden prolongarse hasta secuentes $\alpha \Rightarrow \alpha$ mediante las reglas de debilitación, y éstos hasta axiomas en virtud del teorema 2.11 (en cuya prueba no se usa la regla de corte), luego podremos afirmar que el secuente $\Pi_n, \Gamma \Rightarrow \Delta$ es demostrable sin cortes.

Nuestra estrategia consistirá en ir construyendo la demostración "de abajo hacia arriba", así que tomamos como D_0 el árbol formado únicamente por el secuente $\Gamma \Rightarrow \Delta$. Supuesto construido D_n, si tiene al menos un secuente activo, obtenemos el árbol D_{n+1} aplicando el proceso siguiente:

1. Si α_n está en Π, cambiamos cada secuente $\Gamma' \Rightarrow \Delta'$ del árbol D_n por $\alpha_n, \Gamma' \Rightarrow \Delta'$. Es inmediato que si en D_n cada secuente era consecuencia inmediata (sin cortes) de los secuentes inmediatamente superiores, esto sigue siendo cierto tras añadir α_n, pues es claro que todas las reglas de inferencia primitivas siguen siéndolo cuando se añade una misma sentencia

colateral a todos sus secuentes. (Notemos que si añadiéramos una fórmula con variables libres podrían invalidarse las aplicaciones de la regla izquierda del particularizador o de la regla derecha del generalizador a causa de la restricción sobre la variable propia.)

2. Si α_n es una fórmula atómica o no aparece en ningún secuente activo, el proceso termina y el árbol (tal vez modificado en el paso anterior) es por definición D_{n+1}. A partir de aquí suponemos, pues, que α_n no es atómica y que aparece en algún secuente activo de D_n. Esto nos lleva a distinguir cuatro casos:

   (a) Si $\alpha_n \equiv \neg\beta$ prolongamos los secuentes activos que la contienen mediante las reglas de negación:

$$\frac{\neg\beta,\, \Gamma' \Rightarrow \Delta',\, \beta}{\neg\beta,\, \Gamma' \Rightarrow \Delta'} \qquad \frac{\beta,\, \Gamma' \Rightarrow \Delta',\, \neg\beta}{\Gamma' \Rightarrow \Delta',\, \neg\beta}$$

   Notemos que las reglas de negación no impiden que la fórmula que se pasa al miembro opuesto esté ya en dicho miembro como fórmula colateral, y ése es el caso que estamos considerando aquí.

   (b) Si $\alpha_n \equiv \beta \vee \gamma$ prolongamos como sigue los secuentes activos que la contienen:

$$\frac{\beta,\, \beta\vee\gamma,\, \Gamma' \Rightarrow \Delta' \qquad \gamma,\, \beta\vee\gamma,\, \Gamma' \Rightarrow \Delta'}{\beta\vee\gamma,\, \Gamma' \Rightarrow \Delta'} \qquad \frac{\Gamma' \Rightarrow \Delta',\, \beta\vee\gamma,\, \beta,\, \gamma}{\Gamma' \Rightarrow \Delta',\, \beta\vee\gamma}$$

   (c) Si $\alpha_n \equiv \bigwedge u\, \beta(u)$ prolongamos así los secuentes activos que la contienen:

$$\frac{\bigwedge u\, \beta(u),\, \beta(t_n),\, \Gamma' \Rightarrow \Delta'}{\bigwedge u\, \beta(u),\, \Gamma' \Rightarrow \Delta'} \qquad \frac{\Gamma' \Rightarrow \Delta',\, \beta(y),\, \bigwedge u\, \beta(u)}{\Gamma' \Rightarrow \Delta',\, \bigwedge u\, \beta(u)}$$

   donde y es cualquier variable libre que no haya aparecido hasta el momento en el árbol de secuentes, lo que la convierte en una variable propia aceptable para la regla.

   (d) Si $\alpha_n \equiv \bigvee u\, \beta(u)$ prolongamos así los secuentes activos que la contienen:

$$\frac{\bigvee u\, \beta(u),\, \beta(y),\, \Gamma' \Rightarrow \Delta'}{\bigvee u\, \beta(u),\, \Gamma' \Rightarrow \Delta'} \qquad \frac{\Gamma' \Rightarrow \Delta',\, \beta(t_n),\, \bigvee u\, \beta(u)}{\Gamma' \Rightarrow \Delta',\, \bigvee u\, \beta(u)}$$

   donde y es cualquier variable libre que no haya aparecido hasta el momento en el árbol de secuentes.

Como ya hemos explicado, si llegamos a un árbol D_n sin secuentes activos, podemos concluir que el secuente $\Pi_n,\, \Gamma \Rightarrow \Delta$ es demostrable. Ahora suponemos que el proceso no concluye nunca y vamos a construir un modelo de Π en el que $\Gamma \Rightarrow \Delta$ no sea verdadero.

En este punto conviene precisar el concepto de árbol que venimos manejando, puesto que vamos a pasar de considerar árboles finitos a considerar árboles infinitos. Llamaremos *árbol* a un conjunto parcialmente ordenado, a cuyos elementos llamaremos *nodos,* que tiene un mínimo elemento (llamado *raíz*) y de modo que los nodos anteriores a uno dado son un conjunto finito totalmente ordenado. El árbol es *finitamente ramificado* si cada nodo tiene un número finito de nodos inmediatamente posteriores. El número de nodos menores que un nodo dado es su *altura.* Si el árbol tiene un número finito de nodos, podemos definir su *altura* como la mayor altura de uno de sus nodos.

Los árboles D_n que hemos construido son árboles en este sentido general cuyos nodos son secuentes. Más concretamente, son árboles finitos y finitamente ramificados (cada nodo tiene a lo sumo dos nodos inmediatamente posteriores).

Observemos que, según el proceso de construcción, cada árbol D_{n+1} se obtiene de D_n o bien dejándolo invariante, o bien añadiendo una sentencia a todos los antecedentes de sus secuentes y/o prolongando algunos secuentes activos.

Hay un caso excepcional, a saber, cuando Π es vacío y el secuente $\Gamma \Rightarrow \Delta$ sólo contiene fórmulas atómicas. Es claro que entonces el árbol inicial D_0 nunca sufre modificaciones y todos los árboles D_n son iguales a $\Gamma \Rightarrow \Delta$.

Si el secuente de partida contiene fórmulas no atómicas, puesto que ninguno de los pasos del procedimiento elimina fórmulas de los secuentes, resulta que los secuentes iniciales de cada árbol D_n siempre contienen fórmulas no atómicas y, si son activos, tarde o temprano son prolongados. Lo mismo sucede si Π no es vacío, pues cualquiera de sus sentencias acaba figurando en todos los antecedentes de todos los secuentes de algún árbol D_n y, como las sentencias no pueden ser atómicas, cada secuente activo termina también siendo prolongado.

En definitiva, salvo en el caso excepcional, todo secuente activo de cada árbol D_n acaba siendo prolongado, luego en el proceso de construcción de los árboles D_n nunca dejan de producirse prolongaciones. Es claro entonces que la altura de los árboles D_n crece indefinidamente, pues, dado un D_n, sólo es posible realizar un número finito de prolongaciones sin aumentar la altura del árbol y, como el número de prolongaciones es infinito, tarde o temprano se pasa a otro árbol de altura mayor.

Así pues, siempre salvo en el caso excepcional, a partir de la sucesión de árboles D_n podemos construir un árbol D formado por expresiones de la forma $\Pi, \Gamma' \Rightarrow \Delta'$, que no serán secuentes si Π es infinito (porque los antecedentes contendrán infinitas fórmulas, pero podemos referirnos a ellos como *secuentes generalizados*). Claramente D seguirá siendo finitamente ramificado (cada nodo seguirá teniendo a lo sumo dos extensiones inmediatas), pero su altura será infinita, en el sentido de que tendrá nodos de altura arbitrariamente grande.

En este punto de la prueba recurrimos a un ingrediente esencial:

Teorema de König *Un árbol finitamente ramificado de altura infinita tiene necesariamente una rama infinita, es decir, una sucesión infinita de nodos del árbol cada uno de los cuales está inmediatamente por encima del anterior.*

El teorema de König es elemental: Para cada nodo a de un árbol finitamente ramificado A, el conjunto A_a de los nodos mayores o iguales que a es también un árbol finitamente ramificado.

Ahora observamos que si $b_1, \ldots, b_n$ son los sucesores inmediatos de un nodo a y el árbol A_a tiene altura infinita, entonces algún A_{b_i} tiene altura infinita, pues si todos tuvieran altura finita, entonces la altura de A_a sería una unidad mayor que la mayor de sus alturas.

Así pues, si a_0 es la raíz de A, como el árbol A_{a_0} tiene altura infinita, existe una prolongación inmediata a_1 de a_0 tal que el árbol A_{a_1} también tiene altura infinita, luego existe una prolongación inmediata a_2 de a_1 tal que A_{a_2} también tiene altura infinita, y de este modo construimos una rama $a_0, a_1, a_2, \ldots$

Volviendo a nuestra prueba, salvo en el caso excepcional, tenemos una sucesión infinita de secuentes generalizados que forman una rama en el árbol D.

Más precisamente, cada D_n tiene un único secuente activo $S_n \equiv \Gamma_n \Rightarrow \Delta_n$ tal que el secuente generalizado $S_n^* \equiv \Pi, \Gamma_n \Rightarrow \Delta_n$ es uno de los que forman la rama. Con esta notación la sucesión $S_0^*, S_1^*, \ldots$ es creciente y enumera la rama,[5] pero no tiene por qué ser estrictamente creciente, pues puede tener varios términos consecutivos iguales (más concretamente, si en el paso de D_n a D_{n+1} no se añade ninguna fórmula de Π y S_n no está entre los nodos que se prolongan, tendremos que $S_{n+1}^* \equiv S_n^*$). En el caso excepcional tomamos $S_n^* \equiv \Gamma \Rightarrow \Delta$ para todo n.

Definimos un modelo M de $\mathcal{L}$ tomando como universo los términos de $\mathcal{L}$. La interpretación de una constante es ella misma, es decir, $M(c) \equiv c$, la interpretación de un funtor f es la función dada por $M(f)(t_1, \ldots, t_n) \equiv ft_1 \cdots t_n$ y la interpretación de un relator R es la relación según la cual se cumple $M(R)(t_1, \ldots, t_n)$ si y sólo si la fórmula $Rt_1 \cdots t_n$ está en el antecedente de uno de los secuentes generalizados S_n^*. En el caso excepcional esto se reduce a que $Rt_1 \cdots t_n$ esté en Γ. Fijamos la valoración en M dada por $v(x) \equiv x$. Esto implica claramente que $M(t)[v] \equiv t$ para todo término t.

Basta probar que si una fórmula α figura en un antecedente (resp. consecuente) de uno de los secuentes generalizados S_n^*, entonces $M \vDash \alpha[v]$ (resp. $M \vDash \neg\alpha[v]$). Esto implica que $M \vDash \Pi$ (puesto que las fórmulas de Π no tienen variables libres, luego si son satisfechas respecto de v es que son verdaderas) y que $S \equiv \Gamma \Rightarrow \Delta$ no es verdadero en M, pues no $M \vDash \bar{S}[v]$, luego no $M \vDash \bar{S}$.

[5] Conviene observar que tanto el árbol D como la rama infinita que tomamos pueden ser definidos sin ambigüedad alguna, aunque en general no pueden ser calculados en la práctica. En efecto, podemos definir explícitamente las enumeraciones que hemos usado para construir la sucesión de pares (α_n, t_n) que usamos en la construcción, lo cual determina completamente los árboles D_n, todos los cuales pueden ser construidos en la práctica. Éstos determinan completamente al árbol D y la definición de la rama de secuentes generalizados puede precisarse especificando que, cuando un secuente tiene dos prolongaciones inmediatas (lo cual significa que se ha obtenido mediante la regla izquierda del disyuntor) y ambas son la base de un árbol de altura infinita, entonces tomamos concretamente la prolongación de la izquierda. Esto determina unívocamente la rama, aunque no podemos calcularla en la práctica porque para ello necesitaríamos saber si los dos secuentes generalizados que están por encima se van a ramificar infinitamente o no.

Razonamos por inducción sobre el número de signos lógicos de α. Si α es atómica y figura en el antecedente de un S_m^*, entonces $M \vDash \alpha[v]$ por la propia construcción de M. Si figura en el consecuente de S_m^* no puede figurar en un antecedente de ningún S_k^*, pues entonces podríamos tomar un n suficientemente grande de modo que α estuviera en el antecedente y en el consecuente de S_n, en contradicción con que se trata de un secuente activo. Por tanto $M \vDash \neg\alpha[v]$. (Observemos que este argumento vale en el caso excepcional y termina la prueba en dicho caso.)

Supongamos ahora que $\alpha \equiv \neg\beta$ y que aparece en un S_k^*. Entonces existe un $n > k$ tal que $\alpha \equiv \alpha_n$ está en S_n, y el proceso de construcción implica que S_{n+1} prolonga a S_n mediante una regla de negación, de modo que S_{n+1} tiene a β en el miembro opuesto al que contiene a $\alpha \equiv \neg\beta$. Por lo tanto, teniendo en cuenta la hipótesis de inducción, $M \vDash \alpha[v]$ si y sólo si no $M \vDash \beta[v]$ si y sólo si β aparece en el consecuente, si y sólo si α aparece en el antecedente.

Si $\alpha \equiv \beta \vee \gamma$, razonando como antes podemos tomar un n tal que $\alpha \equiv \alpha_n$ aparece en el secuente S_n, con lo que S_{n+1} es una prolongación de S_n a través de un regla del disyuntor. Si α está en el antecedente de S_n, entonces S_{n+1} contiene a β o a γ en su antecedente, luego, por hipótesis de inducción $M \vDash \beta[v]$ o bien $M \vDash \gamma[v]$, y en ambos casos $M \vDash \alpha[v]$.

Si, por el contrario, α aparece en el consecuente de S_n, entonces β y γ aparecen en el consecuente de S_{n+1}, y por hipótesis de inducción $M \vDash \neg\beta[v]$ y $M \vDash \neg\gamma[v]$, luego $M \vDash \neg\alpha[v]$.

Si $\alpha \equiv \bigwedge u\,\beta(u)$ y está en el antecedente de un S_k^*, dado cualquier término t de $\mathcal{L}$ (es decir, cualquier objeto del universo de M), podemos encontrar un $n > k$ tal que $\alpha_n \equiv \alpha$ y $t_n \equiv t$ y α_n está en S_n. Entonces, en el antecedente de S_{n+1} figura $\beta(t)$, lo que, por hipótesis de inducción, se traduce en que $M \vDash \beta(t)[v]$ o, lo que es lo mismo, $M \vDash \beta(u)[v_u^t]$, y esto para todo t del universo de M, luego $M \vDash \alpha[v]$.

Si α está en el consecuente de un S_k^*, entonces existe un $n > k$ tal que $\alpha_n \equiv \alpha$ está en el consecuente de S_n, y entonces S_{n+1} contiene en su consecuente a $\beta(y)$, para cierta variable y, lo que se traduce en que $M \vDash \neg\beta(y)[v]$ o, lo que es lo mismo, $M \vDash \neg\beta(u)[v_u^y]$. Esto equivale a que no $M \vDash \beta(u)[v_u^y]$, luego no $M \vDash \alpha[v]$, luego $M \vDash \neg\alpha[v]$.

Si $\alpha \equiv \bigvee u\,\beta(u)$ y está en el antecedente de un S_k^*, entonces existe un $n > k$ tal que $\alpha_n \equiv \alpha$ está en el antecedente de S_n y entonces S_{n+1} contiene en su antecedente a $\beta(y)$, para cierta variable y, lo que se traduce en que $M \vDash \beta(y)[v]$ o, lo que es lo mismo, $M \vDash \beta(u)[v_u^y]$, luego $M \vDash \alpha[v]$.

Si α está en el consecuente de un S_k^*, dado cualquier término t de $\mathcal{L}$ (es decir, cualquier objeto del universo de M), podemos encontrar un $n > k$ tal que $\alpha_n \equiv \alpha$ y $t_n \equiv t$ y α_n está en S_n. Entonces, en el consecuente de S_{n+1} figura $\beta(t)$, lo que, por hipótesis de inducción, se traduce en que $M \vDash \neg\beta(t)[v]$ o, lo que es lo mismo no $M \vDash \beta(u)[v_u^t]$, y esto para todo t del universo de M, luego no $M \vDash \alpha[v]$ y $M \vDash \neg\alpha[v]$. ■

Nota La demostración precedente —y, con ella, la del teorema de completitud— está en la frontera del finitismo más "generoso". Desde luego, no es finitista en sentido estricto, pues involucra la construcción de un árbol infinito del que a su vez obtenemos un modelo (también infinito) por un proceso que podemos considerar completamente determinado, pero no efectivo, en el sentido de que, en un caso concreto, no estamos en condiciones de determinar qué sentencias son verdaderas o falsas en dicho modelo. Aun así, no es descabellado considerar que la demostración determina un objeto "real", en el sentido de que podemos hablar objetivamente de él sin remitirnos a ninguna teoría formal para eludir toda cuestión sobre el posible significado de los términos empleados.

Así, con independencia de que podemos considerar el teorema de completitud como un teorema formalizable en cualquier teoría de conjuntos suficientemente rica, desde un finitismo suficientemente laxo podemos considerar que el teorema de completitud es "verdadero", es decir, que nos permite afirmar que si un secuente S no se deduce de un conjunto de secuentes $\mathfrak{S}$, existe objetivamente un modelo en el que los secuentes de $\mathfrak{S}$ son verdaderos y S no lo es.

En particular, esto nos permite definir que un secuente S es una consecuencia lógica de un conjunto $\mathfrak{S}$ de secuentes ($\mathfrak{S} \vDash S$) si S es verdadero en todos los modelos en los que son verdaderos los secuentes de $\mathfrak{S}$. En principio, esto sería inaceptable como definición informal (es decir, fuera del contexto de una teoría formal adecuada) porque "la totalidad de los modelos de un lenguaje formal" no puede ser considerada como un concepto finitista, pero la prueba del teorema de completitud muestra que $\mathfrak{S} \vDash S$ es lo mismo que $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} S$, y esto último es un concepto finitista en el sentido más estricto.

Explícitamente, o bien $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} S$ o bien no $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} S$. En el primer caso, a partir de una deducción de S, la demostración del teorema de corrección nos permite obtener un argumento que justifica que S será verdadero en cualquier modelo bien definido en el que los secuentes de $\mathfrak{S}$ sean verdaderos, y en el segundo caso la demostración del teorema de completitud nos asegura la existencia objetiva de un modelo bien definido en el que los secuentes de $\mathfrak{S}$ son verdaderos y S no lo es. ■

2.5 Consistencia

Ahora que tenemos probado que el cálculo secuencial captura completamente la capacidad de razonamiento lógico, podemos presentar una definición general de teoría axiomática análoga a [LM 3.1]:

Definición 2.19 Una *teoría axiomática* (con igualador) sobre un lenguaje formal $\mathcal{L}$ (con igualasor) es un cálculo deductivo secuencial K cuyos axiomas contengan a los de LK (resp. LK_i) y cuyas reglas de inferencia sean las de LK.

A los axiomas de LK los llamaremos *axiomas lógicos,* a los axiomas adicionales de LK_i los llamaremos *axiomas del igualador* y a los axiomas de K que no sean de los tipos anteriores los llamaremos *axiomas propios* de la teoría K.

Es claro entonces que una demostración en K es lo mismo que una deducción en KL (o LK_i) cuyas premisas sean los axiomas propios de K.

Las teorías axiomáticas más simples son LK y LK_i, cuyos teoremas son precisamente los secuentes *lógicamente válidos,* es decir, los secuentes verdaderos en todos los modelos (en los que el igualador se interpreta como la identidad en el caso de LK_i).

Teorema 2.20 *Sea K una teoría axiomática secuencial sobre un lenguaje formal $\mathcal{L}$. Las afirmaciones siguientes son equivalentes:*

1. *Todos los secuentes de $\mathcal{L}$ son teoremas de K.*
2. *Existe una fórmula α tal que los secuentes $\Rightarrow \alpha$ y $\Rightarrow \neg\alpha$ son demostrables en K.*
3. *El secuente vacío $\Rightarrow$ es un teorema de K.*

DEMOSTRACIÓN: 1) $\Rightarrow$ 2) es trivial. Si se cumple 2), por la regla del negador podemos demostrar los secuentes $\Rightarrow \alpha$ y $\alpha \Rightarrow$, y por la regla de corte podemos demostrar el secuente vacío, luego tenemos 3). Si se cumple 3), las reglas de debilitación nos permiten demostrar cualquier secuente. ■

Definición 2.21 Una teoría axiomática es *contradictoria* si cumple cualquiera de las condiciones del teorema anterior. En caso contrario es *consistente.*

Obviamente una teoría contradictoria no tiene interés alguno, pero el problema es que en general no es fácil asegurar la consistencia de una teoría axiomática dada. A este respecto tenemos lo siguiente:

Definición 2.22 Si M es un modelo de un lenguaje formal $\mathcal{L}$, diremos que M es un *modelo* de un conjunto $\mathfrak{S}$ de secuentes (y lo representaremos por $M \vDash \mathfrak{S}$) si todos los secuentes de $\mathfrak{S}$ son verdaderos en M. Diremos que M es un *modelo* de una teoría axiomática K si lo es del conjunto de sus axiomas propios.

Notemos que si una teoría axiomática K tiene un modelo M, entonces todos sus axiomas son verdaderos en M, porque los axiomas lógicos, y también los del igualador, si $\mathcal{L}$ tiene igualador) son verdaderos en todo modelo. El teorema de corrección 2.10 nos da entonces que, de hecho, todos los teoremas de K son verdaderos en M. Esto nos da la mitad del teorema siguiente:

Teorema 2.23 *Una teoría axiomática es consistente si y sólo si tiene un modelo.*

DEMOSTRACIÓN: Si una teoría axiomática K tiene un modelo M, todos sus teoremas son verdaderos en M, luego el secuente vacío no puede ser un teorema. Este argumento es esencialmente el teorema de corrección, y el teorema de completitud nos da la implicación contraria, pues si el secuente vacío no es un teorema de K, nos da que existe un modelo de K en el que el secuente vacío es falso. Esto último es trivial, pero lo importante es que nos da la existencia de un modelo de K. ■

2.6 Eliminación de cortes

Hemos visto que el cálculo secuencial LK_i es completo, lo cual significa que es capaz de extraer todas las consecuencias lógicas de unas premisas dadas (todas las fórmulas que son necesariamente verdaderas bajo el supuesto de que lo sean las premisas), por lo que, a la hora de estudiar qué puede demostrar un matemático y qué no a partir de unos axiomas dados, es equivalente considerar deducciones en LK_i o en un cálculo deductivo "a la Hilbert" como el cálculo $K_{\mathcal{L}}$ estudiado en [LM]. Sin embargo, todavía no hemos visto ningún hecho que haga preferible el uso del cálculo secuencial, cuya forma de plasmar las demostraciones es sustancialmente diferente a la forma habitual de razonar de los matemáticos.

El interés del cálculo secuencial se debe esencialmente a que permite poner de manifiesto las características puramente formales de los razonamientos matemáticos, es decir, las que no dependen para nada del posible significado de las fórmulas involucradas, sino meramente de su forma. En esta sección veremos algunos primeros ejemplos de argumentos "puramente formales" sobre demostraciones en el cálculo secuencial, en los que nos encontraremos con técnicas e ideas que explotaremos más a fondo en capítulos posteriores. El teorema siguiente es una consecuencia inmediata del teorema 2.16:

Teorema 2.24 (de eliminación de cortes) *Si un secuente puede probarse en* LK*, entonces puede probarse sin usar la regla de corte.*

En efecto, si S es un teorema de LK, por el teorema de corrección 2.10, tenemos que S es verdadero en todos los modelos de $\mathcal{L}$, luego 2.16 nos da que es demostrable sin la regla de corte.

La prueba que hemos visto no es constructiva. Nos asegura que existe una demostración sin cortes, pero no nos dice cómo obtenerla. En esta sección vamos a mostrar una forma explícita de transformar una demostración en LK en otra demostración del mismo secuente en la que no se use la regla de corte.

Para probar 2.24 necesitamos unos hechos elementales sobre demostraciones en LK (que también valen para LK_i):

Teorema 2.25 *Sea D una demostración en* LK *(o en* LK_i*), sea x una variable libre que no sea usada en D como variable propia y sea t un término que no contenga ninguna variable propia de ninguna inferencia en D. Entonces, si sustituimos todas las apariciones de x en D por el término t, obtenemos una demostración en* LK *(o en* LK_i*) del secuente que resulta de sustituir x por t en el secuente final de D).*

DEMOSTRACIÓN: Basta observar que si sustituimos x por t en un axioma, obtenemos un axioma, y que si sustituimos x por t en los secuentes de una regla de inferencia, obtenemos otra regla de inferencia. Lo segundo es inmediato para todas las reglas salvo a lo sumo para la regla izquierda del particularizador, pero en ésta tenemos en cuenta que la variable x no es la variable propia, y que, como t no contiene tampoco a la variable propia, al sustituir x por t ésta sigue sin aparecer en ninguna fórmula donde la regla requiere que no aparezca, luego la regla sigue siendo válida. ■

Con un argumento similar podemos imponer ciertas condiciones a las variables propias de una demostración. Las recogemos en la definición siguiente:

Definición 2.26 Una demostración en LK (o LK_i) es *regular* si una misma variable no aparece como variable propia de dos aplicaciones de la regla derecha del generalizador o de la regla izquierda del particularizador, y además, la variable propia de una aplicación de una de estas reglas sólo aparece en los secuentes situados por encima de (los secuentes superiores de) la regla.

Teorema 2.27 *Toda demostración en* LK *(o* LK_i*) puede transformarse en una demostración regular del mismo secuente sin más que cambiar unas variables propias por otras.*

Demostración: Por 2.25, si en una demostración D cambiamos todas las apariciones de una variable libre x por otra y que no aparezca en D, el resultado es una nueva demostración. Así pues, dada una demostración D, para cada secuente S que resulte de una aplicación de una regla derecha del generalizador o izquierda del particularizador, consideramos la subdemostración D' formada por los secuentes de D situados sobre S, que es en sí misma una demostración de S.

Si en D' cambiamos la variable propia por otra que no aparezca en D, obtenemos una nueva demostración D_1' de S (pues la variable propia no está en S). Al cambiar D' por D_1' en D obtenemos otra demostración D_1 con el mismo secuente final en la que la aplicación de la regla considerada cumple ya la definición de regularidad. Ahora pasamos de D_1 a otra demostración D_2 considerando la variable propia de otra regla, y así hasta que todas las variables propias cumplan lo requerido por la definición de regularidad. ■

Definición 2.28 Un *hilo* en una demostración en LK (o LK_i) es una sucesión de secuentes que empieza en un secuente inicial y termina en el secuente final, de modo que cada secuente distinto del inicial sea el secuente inferior de una regla de inferencia de la demostración que tiene al secuente anterior como uno de sus secuentes superiores.

Así pues, cada demostración en LK tiene tantos hilos como secuentes iniciales. En el ejemplo de la página 32 tenemos una demostración en LK con dos hilos.

Cuando decimos que un secuente está por debajo de otro en una demostración nos referimos a que ambos están en un mismo hilo, y en él uno es posterior al otro.

Llamaremos *grado* de una fórmula α (y lo abreviaremos $g(\alpha)$) al número de signos lógicos que contiene ($\neg$, $\vee$, $\bigwedge$ o $\bigvee$). El *grado* de un corte en una demostración es el grado de la fórmula de corte.

El teorema 2.24 es una consecuencia inmediata del teorema siguiente:

Teorema 2.29 *Si un secuente es demostrable en* LK *con una prueba que contiene un único corte como última inferencia, entonces es demostrable sin cortes.*

Admitiendo este resultado, el teorema 2.24 se prueba por inducción sobre el número de cortes de una demostración de un secuente dado S. Si el resultado es cierto para demostraciones con n cortes y S se demuestra con $n+1$ cortes, consideramos un corte que no tenga otro por encima y, si S' es su secuente inferior, reemplazamos toda la parte de la prueba situada sobre S' por otra prueba alternativa sin cortes, y así conseguimos una prueba de S con n cortes, que por hipótesis de inducción puede reducirse a otra demostración sin cortes.

Demostración: Por conveniencia vamos a considerar la variante general de la regla de corte, de modo que tenemos una demostración D que termina así:

$$\frac{\Gamma \Rightarrow \Delta,\, \alpha \qquad \alpha,\, \Gamma' \Rightarrow \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}.$$

Llamamos S al secuente inferior y S_1 y S_2 a los dos secuentes superiores. Llamaremos hilos izquierdos de D a los hilos que contengan a S_1 e hilos derechos a los que contengan a S_2.

Definimos el *rango* de un hilo izquierdo (derecho) H como el número de secuentes consecutivos, contados a partir de S_1 (o S_2) que contienen a α en su consecuente (antecedente). Lo representaremos por $\operatorname{rang} H$. Como α está en S_1 y en S_2, el rango de un hilo es siempre ≥ 1.

Definimos el *rango izquierdo (derecho)* de la demostración D como el máximo de los rangos de los hilos izquierdos (derechos) de D. Representaremos por $\operatorname{rang}_i(D)$ y $\operatorname{rang}_d(D)$ a los rangos izquierdo y derecho de D. El *rango* de D lo definimos como

$$\operatorname{rang} D = \operatorname{rang}_i(D) + \operatorname{rang}_d(D) \geq 2.$$

Así, la demostración del ejemplo de la página 32 tiene rango izquierdo igual a 4 y rango derecho igual a 1, luego su rango es 5.

Vamos a probar el teorema por inducción sobre el grado g del corte de D, es decir, suponemos que es cierto para demostraciones con corte final de grado menor que g.

A su vez, ahora razonamos por inducción sobre el rango r de D, con lo que suponemos que el resultado es cierto para demostraciones de grado g y rango menor que r.

Caso 1: $\operatorname{rang} D = 2$, es decir, $\operatorname{rang}_i(D) = \operatorname{rang}_d(D) = 1$.

Subcaso 1.1: Uno de los secuentes S_1 o S_2 es un secuente inicial, necesariamente $\alpha \Rightarrow \alpha$, donde α es la fórmula de corte.

Supongamos que S_1 es $\alpha \Rightarrow \alpha$ (el caso de S_2 es análogo). Entonces la demostración D termina así:

$$\frac{\alpha \Rightarrow \alpha \qquad \begin{array}{c}\vdots\\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{array}}{\alpha, \Gamma' \Rightarrow \Delta'}$$

con lo que el corte puede suprimirse, obviamente. A partir de aquí suponemos que ninguno de los secuentes S_1 o S_2 es inicial.

Subcaso 1.2: Uno de los secuentes S_1 o S_2 se obtiene por debilitación.

Pongamos que S_1 se obtiene por debilitación (el caso de S_2 es análogo). Como estamos suponiendo que $\operatorname{rang}_i(D) = 1$, la fórmula de corte no puede aparecer en el consecuente del secuente anterior a S_1, luego tiene que ser la fórmula principal de la regla de debilitación, y la demostración D termina así:

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \Rightarrow \Delta}}{\Gamma \Rightarrow \Delta, \alpha} \qquad \dfrac{\vdots}{\alpha, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

Vemos entonces que podemos pasar de $\Gamma \Rightarrow \Delta$ al secuente final sin más que aplicar la regla de debilitación.

Subcaso 1.3: Tanto S_1 como S_2 se obtienen mediante reglas de inferencia lógicas.

Nuevamente, debido a que $\operatorname{rang}_i(D) = \operatorname{rang}_d(D) = 1$, la fórmula de corte α tiene que ser la fórmula principal de ambas reglas de inferencia.

Si $\alpha \equiv \neg\beta$, entonces la demostración D acaba así:

$$\dfrac{\dfrac{\dfrac{\vdots}{\beta, \Gamma \Rightarrow \Delta}}{\Gamma \Rightarrow \Delta, \neg\beta} \qquad \dfrac{\dfrac{\vdots}{\Gamma' \Rightarrow \Delta', \beta}}{\neg\beta, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

y una demostración alternativa es

$$\dfrac{\dfrac{\vdots}{\Gamma' \Rightarrow \Delta', \beta} \qquad \dfrac{\vdots}{\beta, \Gamma \Rightarrow \Delta}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

donde ahora el corte tiene grado una unidad menor y podemos aplicar la hipótesis de inducción.

Si $\alpha \equiv \beta \vee \gamma$, tenemos:

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma \Rightarrow \Delta, \beta, \gamma}}{\Gamma \Rightarrow \Delta, \beta \vee \gamma} \qquad \dfrac{\dfrac{\vdots}{\beta, \Gamma' \Rightarrow \Delta'} \qquad \dfrac{\vdots}{\gamma, \Gamma' \Rightarrow \Delta'}}{\beta \vee \gamma, \Gamma' \Rightarrow \Delta'}}{\Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

La alternativa es:

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta,\, \gamma\end{matrix} \qquad \begin{matrix}\vdots\\ \beta,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \gamma} \qquad \begin{matrix}\vdots\\ \gamma,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

El corte de β tiene grado menor que el de D, por lo que por hipótesis de inducción podemos demostrar sin cortes el secuente $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \gamma$ y obtenemos así una demostración de S con un único corte cuya fórmula de corte es γ y, de nuevo por hipótesis de inducción, llegamos a una prueba sin cortes.

Si $\alpha \equiv \bigwedge u\, \beta(u)$, tenemos:

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(y)\end{matrix}}{\Gamma \Rightarrow \Delta,\, \bigwedge u\, \beta(u)} \qquad \dfrac{\begin{matrix}\vdots\\ \beta(t),\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\bigwedge u\, \beta(u),\, \Gamma' \Rightarrow \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

Por 2.27 podemos suponer que la demostración del secuente $\Gamma \Rightarrow \Delta,\, \beta(y)$ es regular (y sin cortes), lo que en particular implica que la variable y no es la variable propia de ninguna aplicación de la regla derecha del generalizador o izquierda del particularizador (anterior a la que lleva a S_2). Más aún, la prueba muestra que podemos elegir todas las variables propias de la demostración, por lo que podemos exigir que ninguna esté en t. Por lo tanto, el teorema 2.25 nos da una demostración sin cortes del secuente $\Gamma \Rightarrow \Delta,\, \beta(t)$ (aquí usamos que y no está en Γ o Δ). Por consiguiente, una demostración alternativa es

$$\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t)\end{matrix} \qquad \begin{matrix}\vdots\\ \beta(t),\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

cuyo corte tiene grado menor que el de D, luego por hipótesis de inducción existe otra demostración sin cortes.

Por último, si $\alpha \equiv \bigvee u\, \beta(u)$, tenemos:

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t)\end{matrix}}{\Gamma \Rightarrow \Delta,\, \bigvee u\, \beta(u)} \qquad \dfrac{\begin{matrix}\vdots\\ \beta(y),\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\bigvee u\, \beta(u),\, \Gamma' \Rightarrow \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

y en perfecta analogía con el caso anterior podemos llegar a una demostración:

$$\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t)\end{matrix} \qquad \begin{matrix}\vdots\\ \beta(t),\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

cuyo corte tiene grado menor que el de D, luego por hipótesis de inducción existe otra demostración sin cortes.

Caso 2: $\operatorname{rang}(D) > 2$, luego $\operatorname{rang}_i(D) > 1$ o bien $\operatorname{rang}_d(D) > 1$.

Supongamos concretamente que $\operatorname{rang}_i(D) > 1$. El otro caso se trata análogamente. Notemos que esto implica que S_1 no es un secuente inicial.

Subcaso 2.1: S_2 contiene a α en su consecuente.

Entonces tenemos:

$$\frac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \alpha\end{matrix} \qquad \begin{matrix}\vdots\\ \alpha,\, \Gamma' \Rightarrow \Delta',\, \alpha\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha}$$

y el secuente inferior puede obtenerse del superior izquierdo por debilitación, sin necesidad del corte. A partir de aquí suponemos que α no está en el consecuente de S_2.

Subcaso 2.2 El secuente S_1 se obtiene por debilitación o bien por una regla lógica cuya fórmula principal no es α.

Entonces tenemos

$$\frac{\dfrac{\begin{matrix}\vdots\\ \Gamma'' \Rightarrow \Delta'',\, \alpha\end{matrix} \qquad \begin{matrix}\vdots\\ \Gamma''' \Rightarrow \Delta''',\, \alpha\end{matrix}}{\Gamma \Rightarrow \Delta,\, \alpha} \qquad \begin{matrix}\vdots\\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

si es que la regla que proporciona S_1 tiene dos secuentes superiores. El caso en que sólo haya uno es más simple. Adelantamos el corte:

$$\frac{\begin{matrix}\vdots\\ \Gamma'' \Rightarrow \Delta'',\, \alpha\end{matrix} \qquad \begin{matrix}\vdots\\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma'',\, \Gamma' \Rightarrow \Delta'',\, \Delta'} \qquad \frac{\begin{matrix}\vdots\\ \Gamma''' \Rightarrow \Delta''',\, \alpha\end{matrix} \qquad \begin{matrix}\vdots\\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma''',\, \Gamma' \Rightarrow \Delta''',\, \Delta'}$$

Estas demostraciones tienen el mismo grado, pero el rango es una unidad menor, luego por hipótesis de inducción existen demostraciones sin cortes de los secuentes finales, y usando la misma regla que proporcionaba S_1 en la prueba original (ahora con más fórmulas colaterales), podemos probar sin cortes

$$\frac{\begin{matrix}\vdots\\ \Gamma'',\, \Gamma' \Rightarrow \Delta''\, \Delta'\end{matrix} \qquad \begin{matrix}\vdots\\ \Gamma''',\, \Gamma' \Rightarrow \Delta'''\, \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

Subcaso 2.3 El secuente S_1 se obtiene de una regla lógica cuya fórmula principal es α.

Tenemos cuatro posibilidades. Si $\alpha \equiv \neg\beta$, la situación es

$$\frac{\dfrac{\begin{matrix}\vdots\\ \beta,\, \Gamma \Rightarrow \Delta\end{matrix}}{\Gamma \Rightarrow \Delta,\, \neg\beta} \qquad \begin{matrix}\vdots\\ \neg\beta,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

pero $\neg\beta$ tiene que estar en Δ, por la hipótesis sobre el rango izquierdo. Esto nos permite adelantar el corte:

$$\dfrac{\begin{array}{c}\vdots\\ \beta,\,\Gamma \Rightarrow \Delta,\,\neg\beta\end{array} \qquad \begin{array}{c}\vdots\\ \neg\beta,\,\Gamma' \Rightarrow \Delta'\end{array}}{\beta,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}$$

Esta demostración tiene rango una unidad menor, luego por hipótesis de inducción el secuente inferior puede demostrarse sin cortes y, como Δ contiene a $\neg\beta$, podemos eliminar β del antecedente mediante la regla del negador.

Si $\alpha \equiv \beta \vee \gamma$, la situación es

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta,\,\gamma\end{array}}{\Gamma \Rightarrow \Delta,\,\beta\vee\gamma} \qquad \begin{array}{c}\vdots\\ \beta\vee\gamma,\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}$$

y de nuevo $\beta \vee \gamma$ tiene que estar en Δ y podemos adelantar el corte:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta,\,\gamma,\,\beta\vee\gamma\end{array} \qquad \begin{array}{c}\vdots\\ \beta\vee\gamma,\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta',\,\beta,\,\gamma}$$

Por hipótesis de inducción el secuente inferior puede probarse sin cortes y aplicando a continuación la regla del disyuntor[6] eliminamos β y γ.

Si $\alpha \equiv \bigwedge u\,\beta(u)$, tenemos

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta(y)\end{array}}{\Gamma \Rightarrow \Delta,\,\bigwedge u\,\beta(u)} \qquad \begin{array}{c}\vdots\\ \bigwedge u\,\beta(u),\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}$$

para cierta variable propia y que, según se ve en la prueba de 2.27, podemos sustituirla por otra para asegurar que no esté en Γ' ni en Δ'. Como Δ contiene $\bigwedge u\,\beta(u)$, también podemos adelantar el corte:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta(y),\,\bigwedge u\,\beta(u)\end{array} \qquad \begin{array}{c}\vdots\\ \bigwedge u\,\beta(u),\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta',\,\beta(y)}$$

Por hipótesis de inducción existe una prueba sin cortes del secuente final, y aplicando la regla derecha del generalizador eliminamos $\beta(y)$.

[6]En el caso análogo en que el rango derecho es mayor que 1 estaríamos aplicando la regla izquierda del disyuntor, que tiene dos secuentes superiores, y la hipótesis de inducción nos da demostraciones sin cortes de los secuentes $\beta,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'$ y $\gamma,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'$, y a continuación podemos aplicar la regla izquierda del disyuntor.

Si $\alpha \equiv \bigvee u\,\beta(u)$, tenemos

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t)\end{array}}{\Gamma \Rightarrow \Delta,\, \bigvee u\,\beta(u)} \qquad \begin{array}{c}\vdots\\ \bigvee u\,\beta(u),\, \Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

pero Δ contiene $\bigvee u\,\beta(u)$, con lo que también podemos adelantar el corte:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t),\, \bigvee u\,\beta(u)\end{array} \qquad \begin{array}{c}\vdots\\ \bigvee u\,\beta(u),\, \Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \beta(t)}$$

Por hipótesis de inducción existe una prueba sin cortes del secuente final, y aplicando la regla derecha del particularizador eliminamos $\beta(t)$. ■

La demostración del teorema anterior es constructiva, y puede ser reformulada como un algoritmo para obtener una demostración sin cortes a partir de una demostración dada. La idea básica es ir adelantando los cortes. Aunque en cada paso de la prueba sólo se adelanta una posición, esto es por simplicidad en la exposición teórica. En la práctica se llega antes a la demostración requerida si adelantamos cada corte todo lo posible.

Ejemplo Vamos a eliminar el corte de la demostración considerada en el ejemplo de la página 32. Como el rango izquierdo es 4, podemos adelantar el corte cuatro posiciones, y el resultado es:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{Ry \Rightarrow Ry}{Rx,\, Ry \Rightarrow Ry}}{Rx \Rightarrow Ry,\, \neg Ry}}{Rx \Rightarrow Ry,\, \bigvee v\, \neg Rv} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{Ry \Rightarrow Ry}{Ry \Rightarrow Ry,\, \bigwedge v\, Rv}}{\neg Ry,\, Ry \Rightarrow \bigwedge v\, Rv}}{\neg Ry \Rightarrow Ry \rightarrow \bigwedge v\, Rv}}{\neg Ry \Rightarrow \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{\bigvee v\, \neg Rv \Rightarrow \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{Rx \Rightarrow Ry,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{Rx \Rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{\Rightarrow Rx \rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{\bigvee u(Ru \rightarrow \bigwedge v\, Rv)}$$

Ahora observamos que en lugar de cortar $\bigvee v\, Rv$ podemos cortar $\neg Ry$ en el paso anterior, pero dicho corte tiene rango derecho igual a 3, luego a su vez podemos adelantarlo dos lugares y el resultado es:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{Ry \Rightarrow Ry}{Rx,\, Ry \Rightarrow Ry}}{Rx \Rightarrow Ry,\, \neg Ry} \qquad \dfrac{\dfrac{Ry \Rightarrow Ry}{Ry \Rightarrow Ry,\, \bigwedge v\, Rv}}{\neg Ry,\, Ry \Rightarrow \bigwedge v\, Rv}}{Rx,\, Ry \Rightarrow Ry,\, \bigwedge v\, Rv}}{Rx \Rightarrow Ry,\, Ry \rightarrow \bigwedge v\, Rv}}{Rx \Rightarrow Ry,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{Rx \Rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{\Rightarrow Rx \rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv)}}{\bigvee u(Ru \rightarrow \bigwedge v\, Rv)}$$

Seguidamente vemos que en lugar de cortar $\neg Ry$ podemos cortar Ry en el paso anterior:

$$\begin{array}{c}
\dfrac{Ry \Rightarrow Ry}{Rx,\, Ry \Rightarrow \bigwedge v\, Rv,\, Ry} \qquad Ry \Rightarrow Ry \\ \hline
Rx,\, Ry \Rightarrow Ry,\, \bigwedge v\, Rv \\ \hline
Rx \Rightarrow Ry,\, Ry \rightarrow \bigwedge v\, Rv \\ \hline
Rx \Rightarrow Ry,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv) \\ \hline
Rx \Rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv) \\ \hline
\Rightarrow Rx \rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv) \\ \hline
\bigvee u(Ru \rightarrow \bigwedge v\, Rv)
\end{array}$$

y finalmente eliminamos el corte:

$$\begin{array}{c}
Ry \Rightarrow Ry \\ \hline
Rx,\, Ry \Rightarrow Ry,\, \bigwedge v\, Rv \\ \hline
\Rightarrow Ry,\, Ry \rightarrow \bigwedge v\, Rv \\ \hline
Rx \Rightarrow Ry,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv) \\ \hline
Rx \Rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv) \\ \hline
\Rightarrow Rx \rightarrow \bigwedge v\, Rv,\, \bigvee u(Ru \rightarrow \bigwedge v\, Rv) \\ \hline
\bigvee u(Ru \rightarrow \bigwedge v\, Rv)
\end{array}$$

En este caso la demostración sin cortes ha resultado ser más corta que la original, pero en general el proceso de eliminación de cortes puede aumentar drásticamente la longitud de una demostración. ■

Ejemplo Ahora podemos entender el interés de la distinción que hemos establecido entre variables libres y ligadas. Supongamos que prescindimos de ella y consideramos las definiciones de "fórmula" y "sustitución" dadas en [LM]. Entonces esto es una demostración en LK:

$$\dfrac{\begin{array}{c}
Rxy \Rightarrow Rxy \\ \hline
Rxy \Rightarrow \bigvee v\, Rxv \\ \hline
Rxy \Rightarrow \bigvee uv\, Ruv
\end{array} \qquad \begin{array}{c}
Rzw \Rightarrow Rzw \\ \hline
Rzw \Rightarrow \bigvee x\, Rzx \\ \hline
Rzw \Rightarrow \bigvee yx\, Ryx \\ \hline
\bigvee v\, Rzv \Rightarrow \bigvee yx\, Ryx \\ \hline
\bigvee uv\, Ruv \Rightarrow \bigvee yx\, Ryx
\end{array}}{Rxy \Rightarrow \bigvee yx\, Ryx}$$

Si intentamos aplicar la demostración del teorema 2.29 para eliminar el corte, vemos que no es posible. En efecto, nos encontramos en el subcaso 1.3, con $\alpha \equiv \bigvee u\, \beta(u)$ y $\beta(u) \equiv \bigvee v\, Ruv$. El término t considerado en la prueba es $t \equiv x$ y la variable propia y considerada en la demostración de 2.29 es en este caso la variable z.

Según dicha demostración, lo que procede hacer en este caso es sustituir z por x en el hilo derecho de la demostración para obtener una demostración del secuente

$$\bigvee v\, Rxv \Rightarrow \bigvee yx\, Ryx,$$

pero no podemos hacer tal cosa. Al llevar a cabo la sustitución, o bien nos quedaría el secuente

$$Rxw \Rightarrow \bigvee x\, Rxx,$$

que no es lógicamente válido, o bien, aplicando la definición de sustitución dada en [LM] tendríamos que poner

$$Rxw \Rightarrow \bigvee t\, Rxt,$$

lo que nos obligaría a realizar sustituciones hacia abajo y el secuente final sería

$$\bigvee v\, Rxv \Rightarrow \bigvee yt\, Ryt,$$

que no es el que necesitamos. Vemos así que el teorema 2.25 no es válido sin la distinción entre variables libres y ligadas que hemos establecido, ni tampoco el teorema de eliminación de cortes, cuyo enunciado tendría que modificarse para exigir que en el secuente final de la deducción no aparezca ninguna variable libre y ligada al mismo tiempo. ■

El teorema de eliminación de cortes no es válido para LK_i, pero se cumple una versión ligeramente más débil:

Definición 2.30 Un corte en LK_i es *inesencial* si la fórmula de corte es de la forma $t_1 = t_2$. En caso contrario se dice que es *esencial.*

Teorema 2.31 (de eliminación de cortes) *Si un secuente puede probarse en* LK_i, *entonces puede probarse sin cortes esenciales.*

Demostración: El resultado se sigue inmediatamente de la versión para LK_i del teorema 2.29:

> *Si un secuente es demostrable en* LK_i *con una prueba que contiene un único corte como última inferencia, entonces es demostrable sin cortes esenciales.*

La prueba es exactamente la misma, salvo que hay que considerar más posibilidades en el subcaso 1.1. Ya tenemos contemplada la posibilidad de que alguno de los secuentes S_1 o S_2 sea un axioma lógico. Si ambos secuentes son axiomas del igualador y la fórmula de corte no es una igualdad, necesariamente

$$S_1 \equiv s_1 = t_1, \ldots, s_n = t_n,\ Rs_1 \cdots s_n \Rightarrow Rt_1 \cdots t_n,$$

$$S_2 \equiv t_1 = r_1, \ldots, t_n = r_n,\ Rt_1 \cdots t_n \Rightarrow Rr_1 \cdots r_n,$$

y la conclusión es

$$s_1 = t_1,\ t_1 = r_1,\ \ldots s_n = t_n,\ t_n = r_n,\ Rs_1 \cdots s_n \Rightarrow Rr_1 \cdots r_n.$$

Pero este secuente puede probarse a partir del axioma

$$s_1 = r_1,\ \ldots s_n = r_n,\ Rs_1 \cdots s_n \Rightarrow Rr_1 \cdots r_n.$$

mediante cortes inesenciales con los axiomas

$$s_i = t_i,\ t_i = r_i \Rightarrow s_i = r_i.$$

Otra posibilidad es que α aparezca en S_2 por debilitación, con lo que tenemos:

$$\dfrac{s_1 = t_1, \ldots, s_n = t_n,\, Rs_1 \cdots s_n \Rightarrow Rt_1 \cdots t_n \qquad \dfrac{\Gamma' \Rightarrow \Delta'}{Rt_1 \cdots t_n,\, \Gamma' \Rightarrow \Delta'}}{s_1 = t_1, \ldots, s_n = t_n,\, Rs_1 \cdots s_n,\, \Gamma' \Rightarrow \Delta'}$$

pero obviamente el secuente final se sigue de $\Gamma' \Rightarrow \Delta'$ por debilitación. El caso en que S_2 es un axioma del igualador y α aparece en S_1 por debilitación es análogo. ■

2.7 Apéndice: Conexión con $K_{\mathcal{L}}$

En este capítulo hemos probado que el cálculo secuencial LK_i formaliza perfectamente la lógica matemática, en el sentido de que permite extraer todas las consecuencias lógicas de cualquier conjunto de premisas. Esto lo convierte en una alternativa válida al cálculo deductivo $K_{\mathcal{L}}$ estudiado en [LM]. Sin embargo, la equivalencia entre ambos la proporciona el teorema de completitud, cuya prueba no es constructiva, así que en esta sección vamos a probar explícitamente que las deducciones de LK_i se corresponden con las de $K_{\mathcal{L}}$. Por una parte tenemos lo siguiente:

Teorema 2.32 *Sea $\mathcal{L}$ un lenguaje formal con igualador, sea $\mathfrak{S}$ un conjunto de secuentes en $\mathcal{L}$ y sea Θ el conjunto de las fórmulas $\bar{S}$ asociadas*[7] *a los secuentes S de $\mathfrak{S}$. Entonces, para todo secuente T, si $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} T$, entonces $\Theta \underset{K_{\mathcal{L}}}{\vdash} \bar{T}$.*

Aquí hay que tener en cuenta que $\bar{T}$ es, en principio, una fórmula de $\mathcal{L}$ construida a partir de $\neg$, $\vee$, $\bigwedge$, $\bigvee$, pero para situarnos en el contexto de [LM] tenemos que "traducirla" cambiando $\alpha \vee \beta$ por $\neg\alpha \to \beta$ y $\bigvee u\, \alpha(u)$ por $\neg \bigwedge u\, \neg\alpha(u)$.

DEMOSTRACIÓN: Tenemos una deducción de T en LK_i con premisas en $\mathfrak{S}$. Basta probar que si el secuente S aparece en la deducción, entonces $\Theta \vdash \bar{S}$. Esto es trivial si S es una premisa. Por definición de Γ, se cumple trivialmente para los axiomas lógicos $S \equiv \delta \Rightarrow \delta$, pues $\bar{S} \equiv \neg\delta \vee \delta$ es un teorema lógico, y se comprueba sin dificultad para los axiomas del igualador.

Es claro que ahora basta probar que la fórmula asociada al secuente inferior de una regla de inferencia de LK es consecuencia lógica de las fórmulas asociadas a sus secuentes superiores.

Para todos los casos siguientes fijamos $\Gamma \equiv \{\gamma_1, \ldots, \gamma_m\}$, $\Delta \equiv \{\delta_1, \ldots, \delta_n\}$, que pueden ser vacíos. Si no lo son, llamamos

$$\zeta \equiv \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n.$$

[7] No hemos definido $\bar{S}$ cuando S es el secuente vacío, pero en tal caso podemos considerar que $\bar{S}$ es cualquier fórmula de tipo $\epsilon \wedge \neg\epsilon$.

Debilitación Si el secuente superior no es vacío, la premisa es ζ, y a partir de ella tenemos que probar $\neg\alpha \vee \zeta$ o bien $\zeta \vee \alpha$. En ambos casos se obtiene la conclusión por la regla de introducción del disyuntor. Si el secuente superior es vacío tenemos que probar α o $\neg\alpha$ a partir de una contradicción, lo cual también es posible.

Corte Las premisas son $\zeta \vee \alpha$ y $\neg\alpha \vee \zeta$, que se reducen a α y $\neg\alpha$ si Γ y Δ son ambos vacíos. En este caso tenemos que probar una contradicción a partir de premisas contradictorias, lo cual es posible sin duda. Descartado este caso, tenemos que probar ζ. Basta razonar por reducción al absurdo: si negamos ζ, las premisas nos dan $\alpha \wedge \neg\alpha$.

Negador Es inmediato que las fórmulas asociadas a los secuentes superior e inferior de las dos reglas del negador son lógicamente equivalentes.

Disyuntor Para la regla izquierda las premisas son $\neg\alpha \vee \zeta$ y $\neg\beta \vee \zeta$. Si Γ y Δ son ambos vacíos, tenemos que probar $\neg(\alpha \vee \beta)$ a partir de $\neg\alpha$ y $\neg\beta$, lo cual ciertamente es posible. En caso contrario tenemos que probar $\neg(\alpha \vee \beta) \vee \zeta$, pero las premisas nos dan que $\alpha \rightarrow \zeta$ y $\beta \rightarrow \zeta$, de donde se sigue $\alpha \vee \beta \rightarrow \zeta$, que equivale a la fórmula requerida.

Para la regla derecha partimos de $\zeta \vee \alpha \vee \beta$ y tenemos que probar esto mismo.

Generalizador Para la regla izquierda, suponiendo que Γ y Δ no son ambos vacíos, tenemos $\neg\alpha(t) \vee \zeta$, de donde se sigue $\neg\bigwedge u\, \alpha(u) \vee \zeta$. En efecto, si suponemos $\bigwedge u\, \alpha(u)$, de ahí deducimos $\alpha(t)$ y, de la premisa, deducimos ζ, con lo que tenemos probado que $\bigwedge u\, \alpha(u) \rightarrow \zeta$, lo cual equivale a $\neg\bigwedge u\, \alpha(u) \vee \zeta$. Si Γ y Δ son vacíos el argumento se simplifica.

Para la regla derecha la premisa es $\zeta \vee \alpha(y)$, con la condición adicional de que y no está libre en ζ ni en $\alpha(u)$, y queremos concluir $\zeta \vee \bigwedge u\, \alpha(u)$.

Si Γ y Δ no son ambos vacíos suponemos $\neg\zeta$ y la premisa nos da $\alpha(y)$, de donde se sigue $\bigwedge y\, \alpha(y)$, por la regla de introducción del generalizador. De aquí podemos deducir $\alpha(u)$ (aquí se usa que y no está libre en $\alpha(u)$) y a su vez $\bigwedge u\, \alpha(u)$. Como y no está libre en ζ (ni u tampoco), el teorema de deducción nos da que $\neg\zeta \rightarrow \bigwedge u\, \alpha(u)$, que es equivalente a $\zeta \vee \bigwedge u\, \alpha(u)$. Si Γ y Δ son ambos vacíos el razonamiento se simplifica.

Particularizador Para la regla izquierda la premisa es $\neg\alpha(y) \vee \zeta$, con la condición adicional de que y no está libre en ζ ni en $\alpha(u)$, y queremos concluir $\neg\bigvee u\alpha(u) \vee \zeta$.

Si Γ y Δ no son ambos vacíos suponemos $\neg\zeta$ y la premisa nos da $\neg\alpha(y)$, de donde se sigue $\bigwedge y\neg\alpha(y)$, por la regla de introducción del generalizador, y $\neg\bigvee y\, \alpha(y)$ por la negación del particularizador. Como la variable y no está libre en ζ, podemos aplicar el teorema de deducción y concluir que $\neg\zeta \rightarrow \neg\bigvee y\, \alpha(y)$. De aquí se sigue a su vez $\bigvee y\, \alpha(y) \rightarrow \zeta$. Por otro lado es claro que $\bigvee u\, \alpha(u) \rightarrow \bigvee y\, \alpha(y)$ (se demuestra también con el teorema de deducción, usando que y no está libre en $\alpha(u)$, eliminando el particularizador y volviéndolo a introducir), luego concluimos que $\bigvee u\,\alpha(u) \to \zeta$, de donde finalmente llegamos a $\neg\bigvee u\,\alpha(u) \vee \zeta$ por la regla de introducción del disyuntor. Si Γ y Δ son ambos vacíos el razonamiento se simplifica.

Para la regla derecha, suponiendo que Γ y Δ no son ambos vacíos, tenemos $\zeta \vee \alpha(t)$, de donde se sigue $\zeta \vee \bigvee u\,\alpha(u)$. En efecto, basta suponer $\neg\zeta$, con lo que obtenemos $\alpha(t)$, y de ahí podemos pasar a $\bigvee u\,\alpha(u)$, por la regla de introducción del particularizador. Esto prueba $\neg\zeta \to \bigvee u\,\alpha(u)$, que equivale a la fórmula requerida. Si Γ y Δ son vacíos el argumento se simplifica. ■

Notemos que la demostración del teorema anterior, debidamente desarrollada, nos permite construir explícitamente una deducción de $\bar{T}$ con premisas en Θ a partir de una deducción de T con premisas en $\mathfrak{S}$.

Para enunciar un recíproco al teorema anterior, aparte de la necesidad de traducir de forma obvia las fórmulas construidas a partir de $\neg$, $\to$, $\bigwedge$ a fórmulas construidas a partir de $\neg$, $\vee$, $\bigwedge$, nos encontramos con la necesidad de que las fórmulas respeten la distinción que hemos hecho en el capítulo anterior entre variables libres y ligadas.

Para ello introducimos una variante de $K_{\mathcal{L}}$ consistente en sustituir la regla de introducción del generalizador, que en principio es

$$\frac{\alpha(x)}{\bigwedge x\,\alpha(x)}$$

por la versión más general

$$\frac{\alpha(x)}{\bigwedge u\,\alpha(u)}$$

donde x y u son variables arbitrarias, de modo que permitimos sustituir la variable que generalizamos por otra (que puede ser la misma). La regla original es un caso particular de ésta, luego todas las deducciones en $K_{\mathcal{L}}$ siguen siéndolo con la nueva regla y, recíprocamente, toda aplicación de la nueva regla puede reducirse a la original así:

(1)	$\alpha(x)$	
(2)	$\bigwedge x\,\alpha(x)$	IG 1
(3)	$\bigwedge x\,\alpha(x) \to \alpha(u)$	K4
(4)	$\alpha(u)$	MP 2, 3
(5)	$\bigwedge u\,\alpha(u)$	IG 4

Por consiguiente, con la versión original de $K_{\mathcal{L}}$ y con la variante se pueden deducir exactamente las mismas fórmulas de las mismas premisas.

Sin embargo, con la nueva versión, si dividimos las variables de $\mathcal{L}$ en libres y ligadas y una fórmula α (en el sentido introducido en el capítulo anterior, es decir, no una mera semifórmula) es deducible de un conjunto de fórmulas Θ (no meras semifórmulas), es posible obtener una deducción en la que sólo aparezcan fórmulas.

En efecto, dada una deducción cualquiera de α a partir de Θ, podemos enumerar sin repeticiones todas las variables $x_1, \ldots, x_m$ que aparecen libres en ella y todas las variables $u_1, \ldots, u_n$ que aparecen ligadas (de modo que en principio alguna x_i podría coincidir con alguna u_j). A estas variables les asignamos variables distintas $\bar{x}_1, \ldots, \bar{x}_m$ (del grupo de variables libres) y $\bar{u}_1, \ldots, \bar{u}_n$ (del grupo de variables ligadas), de modo que si x_i ya era una variable libre, entonces $\bar{x}_i \equiv x_i$ y si u_j ya era una variable ligada, entonces $\bar{u}_j \equiv u_j$.

Para cada semifórmula γ, llamamos $\bar{\gamma}$ a la fórmula que resulta de sustituir cada variable x_i que aparezca libre en ella por la variable libre $\bar{x}_i$ y cada variable u_j que aparezca ligada en ella por la variable ligada $\bar{u}_j$. De este modo, si γ es una fórmula, tenemos que $\bar{\gamma} \equiv \gamma$.

Ahora basta observar que si, en la deducción dada, sustituimos cada semifórmula γ por la fórmula $\bar{\gamma}$, obtenemos una nueva deducción de α a partir de Θ formada exclusivamente por fórmulas.

Basta comprobar que si γ es un axioma lógico, entonces $\bar{\gamma}$ también lo es y que las reglas de inferencia siguen siendo válidas cuando cambiamos las semifórmulas por sus fórmulas asociadas. (Esto no sería cierto con la versión original de la regla de introducción del generalizador, pero sí con la nueva.)

Por otro lado, es fácil ver que, para cada semifórmula γ, en $K_{\mathfrak{L}}$ podemos demostrar que $\gamma \leftrightarrow \bar{\gamma}$, por lo que restringirnos a trabajar exclusivamente con fórmulas no supone ninguna restricción en la práctica. Ahora ya podemos enunciar el recíproco del teorema anterior:

Teorema 2.33 *Sea $\mathfrak{L}$ un lenguaje formal con igualador (en el que hemos dividido las variables en libres y ligadas), sea Θ un conjunto de fórmulas de $\mathfrak{L}$ y sea $\mathfrak{S}$ el conjunto de los secuentes de la forma $\Rightarrow \zeta$, para cada fórmula ζ de Θ. Entonces, para toda fórmula α, se cumple $\Theta \underset{K_{\mathfrak{L}}}{\vdash} \alpha$ si y sólo si $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} \Rightarrow \alpha$.*

Demostración: Supongamos que $\Theta \underset{K_{\mathfrak{L}}}{\vdash} \alpha$. Según hemos razonado, podemos tomar una deducción $\alpha_1, \ldots, \alpha_m \equiv \alpha$ formada exclusivamente por fórmulas (en la que se use la versión general de la regla de introducción del particularizador). Basta probar (por inducción sobre i) que los secuentes $\Rightarrow \alpha_i$ son deducibles en LK_i a partir de $\mathfrak{S}$. Por definición de $\mathfrak{S}$, esto es trivial si α_i está en Θ.

Si α_i es un axioma de $K_{\mathfrak{L}}$ basta comprobar que $\Rightarrow \alpha_i$ es un teorema de LK_i, para lo cual tenemos que distinguir los seis tipos de axiomas lógicos. Consideraremos únicamente los tipos K5, K6, pues los otros cuatro son más sencillos.

Para K5 tenemos la deducción siguiente, en la que y es una variable libre que no aparezca en las fórmulas consideradas. Recordemos que K5 exige que la variable u no esté libre en α, lo cual se usa en la deducción siguiente, pues en caso contrario no estaría bien aplicada la regla izquierda del generalizador:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\alpha\Rightarrow\alpha}{\alpha\Rightarrow\beta(y),\,\alpha}\qquad\dfrac{\beta(y)\Rightarrow\beta(y)}{\beta(y),\,\alpha\Rightarrow\beta(y)}}{\alpha\to\beta(y),\,\alpha\Rightarrow\beta(y)}}{\bigwedge u(\alpha\to\beta(u)),\,\alpha\Rightarrow\beta(y)}}{\bigwedge u(\alpha\to\beta(u)),\,\alpha\Rightarrow\bigwedge u\,\beta(u)}}{\bigwedge u(\alpha\to\beta(u))\Rightarrow\alpha\to\bigwedge u\,\beta(u)}}{\Rightarrow\bigwedge u(\alpha\to\beta(u))\to(\alpha\to\bigwedge u\,\beta(u))}$$

Por otra parte, el axioma K6 se deduce así:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Rightarrow t=t}{\Rightarrow\alpha(t),\,t=t}\qquad\alpha(t)\Rightarrow\alpha(t)}{t=t\to\alpha(t)\Rightarrow\alpha(t)}}{\bigwedge u(u=t\to\alpha(u))\Rightarrow\alpha(t)}}{\Rightarrow\bigwedge u(u=t\to\alpha(u))\to\alpha(t)}\qquad\dfrac{\dfrac{\dfrac{\begin{array}{c}t=y,\,\alpha(t)\Rightarrow\alpha(y)\\ \vdots\\ y=t,\,\alpha(t)\Rightarrow\alpha(y)\end{array}}{\alpha(t)\Rightarrow y=t\to\alpha(y)}}{\alpha(t)\Rightarrow\bigwedge u(u=t\to\alpha(u))}}{\Rightarrow\alpha(t)\to\bigwedge u(u=t\to\alpha(u))}}{\Rightarrow\bigwedge u(u=t\to\alpha(u))\leftrightarrow\alpha(t)}$$

donde hay que suponer que u no está libre en t. Los puntos suspensivos hacen referencia a una deducción de $y=t$ a partir de $t=y$.

Si α_i se deduce por modus ponens de fórmulas anteriores α_j, $\alpha_j\to\alpha_i$, basta considerar la deducción siguiente:

$$\dfrac{\Rightarrow\alpha\qquad\dfrac{\Rightarrow\alpha\to\beta}{\alpha\Rightarrow\beta}}{\Rightarrow\beta}$$

de la que se sigue que si los secuentes $\Rightarrow\alpha_j$ y $\Rightarrow\alpha_j\to\alpha_i$ son deducibles a partir de $\mathfrak{S}$, también lo es $\Rightarrow\alpha_i$.

Por último, si α_i se deduce por generalización, observamos que la regla derecha del generalizador nos da

$$\dfrac{\Rightarrow\alpha(y)}{\Rightarrow\bigwedge u\,\alpha(u).}$$

El recíproco es consecuencia del teorema anterior, pues si suponemos que $\mathfrak{S}\underset{\mathrm{LK_i}}{\vdash}\Rightarrow\alpha$, el conjunto Θ asociado a $\mathfrak{S}$ en el teorema anterior no es sino el conjunto Θ de la hipótesis del teorema, y la fórmula $\bar{T}$ no es sino α, luego la conclusión es que $\Theta\underset{K_\mathcal{L}}{\vdash}\alpha$. ■

Así pues, si nos restringimos a trabajar con fórmulas respecto a una división de las variables en un grupo de variables libres y otro grupo de variables ligadas, tenemos que $K_\mathcal{L}$ y LK_i son equivalentes, pues tenemos un procedimiento explícito para obtener una deducción en LK_i del secuente $\Rightarrow\alpha$ a partir de una deducción de α en $K_\mathcal{L}$ y viceversa. Y ya hemos señalado que tal restricción no supone ninguna limitación en la práctica.

Capítulo III

La aritmética de Peano

Recordemos que el lenguaje $\mathcal{L}_a$ de la aritmética de Peano es el que tiene como signos eventuales una constante 0, un funtor monádico S (aunque escribiremos $t' \equiv St$) y dos funtores diádicos $+$ y $\cdot$.

La *aritmética de Peano* (AP) es la teoría axiomática cuyos axiomas propios son las fórmulas

AP1 $\bigwedge u\, u' \neq 0$,

AP2 $\bigwedge uv(u' = v' \rightarrow u = v)$,

AP3 $\bigwedge u\, u + 0 = u$,

AP4 $\bigwedge uv(u + v' = (u + v)')$,

AP5 $\bigwedge u(u \cdot 0 = 0)$,

AP6 $\bigwedge uv(uv' = uv + u)$,

AP7 $\alpha(0) \wedge \bigwedge u(\alpha(u) \rightarrow \alpha(u')) \rightarrow \bigwedge u\, \alpha(u)$,

donde AP7 —el principio de inducción— es en realidad un esquema axiomático, que consta de infinitas fórmulas, una para cada semifórmula $\alpha(u)$, con u como única variable ligada sin cuantificar.[1] A veces tiene interés considerar subteorías resultantes de restringir el principio de inducción exigiendo que α pertenezca a una determinada clase de fórmulas Φ. Llamaremos $\mathrm{AP}(\Phi)$ a la teoría correspondiente.

Un caso de especial interés se da cuando Φ es el conjunto de las fórmulas de tipo Σ_n, en cuyo caso la teoría $\mathrm{AP}(\Phi)$ recibe el nombre de $\mathrm{I}\Sigma_n$. En este punto vamos a modificar ligeramente la definición de la jerarquía de Kleene dada en [LM].

[1]Técnicamente no hemos definido $\alpha(u')$, es decir, la sustitución de una variable ligada por un semitérmino, pero teniendo en cuenta que u' tiene a u como única variable, la definición dada para términos es aceptable en este contexto. No obstante, aquí vamos a trabajar con una reformulación de AP que presentaremos enseguida en la que no se presenta esta situación.

Recordemos la definición $x \leq y \equiv \bigvee u\, x + u = y$, que a su vez nos permite definir los cuantificadores acotados como

$$\bigwedge u \leq y\, \alpha \equiv \bigwedge u(u \leq y \rightarrow \alpha), \qquad \bigvee u \leq y\, \alpha \equiv \bigvee u(u \leq y \wedge \alpha).$$

Ahora definimos las semifórmulas Δ_0 de $\mathcal{L}_a$ como las semifórmulas construidas con el criterio siguiente:

1. Las semifórmulas $s \leq t$ y $s = t$ son Δ_0, para semitérminos s y t arbitrarios.
2. Si α y β son Δ_0, también lo son $\neg\alpha$, $\alpha \vee \beta$, $\bigwedge u \leq t\, \alpha$ y $\bigvee u \leq t\, \alpha$, donde t es un semitérmino en el que no esté la variable u.

Al margen del hecho de que ahora estamos considerando al disyuntor en vez de al implicador como conector lógico primitivo, la diferencia principal con la definición dada en [LM 5.5] es que allí las cotas de los cuantificadores tenían que ser variables, mientras que ahora permitimos que sean semitérminos cualesquiera.

Esto amplía esencialmente el conjunto de las fórmulas Δ_0, pero observemos que si α es una semifórmula de tipo Δ_0 en el sentido amplio, es decir, que contiene cuantificadores acotados en la forma $u_1 \leq t_1, \ldots, u_m \leq t_m$, es claro que

$$\bigvee u\, \alpha \leftrightarrow \bigvee u v_1 \cdots v_m(v_1 = t_1 \wedge \cdots \wedge v_m = t_m \wedge \alpha^*),$$
$$\bigwedge u\, \alpha \leftrightarrow \bigwedge u v_1 \cdots v_m(v_1 = t_1 \wedge \cdots \wedge v_m = t_m \rightarrow \alpha^*),$$

donde α^* es la semifórmula que resulta de sustituir cada acotación $u_i \leq t_i$ por $u_i \leq v_i$. Las subsemifórmulas situadas tras los cuantificadores son de tipo Δ_0 en el sentido estricto de [LM 5.5] y al añadir los cuantificadores resulta una fórmula de tipo Σ_1 o Π_1, respectivamente, en virtud de [LM 5.18]. Esto prueba que las fórmulas Σ_1 o Π_1 construidas a partir de fórmulas Δ_0 en sentido amplio son equivalentes a fórmulas del tipo correspondiente en sentido estricto.

A su vez, esto implica trivialmente que lo mismo sucede para fórmulas de tipo Σ_n o Π_n, pero en este punto también conviene modificar ligeramente la definición dada en [LM 5.17]. Ahora consideraremos como fórmulas Σ_n las de la forma

$$\bigvee u_1 \bigwedge u_2 \cdots \alpha \quad \text{o} \quad \bigwedge u_1 \bigvee u_2 \cdots \alpha,$$

donde α es una semifórmula de tipo Δ_0 y el número de cuantificadores alternados es $\leq n$ en el primer caso y $< n$ en el segundo. Las fórmulas de tipo Π_n serán las de esta misma forma, salvo que ahora exigimos que el número de cuantificadores sea $< n$ en el primer caso y $\leq n$ en el segundo.

La diferencia esencial con [LM 5.17] es que allí exigíamos que hubiera exactamente n cuantificadores alternados, mientras que ahora permitimos que haya menos y, cuando hay estrictamente menos, permitimos que el primero sea indistintamente un generalizador o un particularizador. No obstante, cualquier fórmula de tipo Σ_n o Π_n en este sentido puede completarse a otra con exactamente n cuantificadores (y que empiece por un particularizador o un generalizador según el tipo considerado) sin más que añadir cuantificadores con variables nuevas, que dan lugar a fórmulas equivalentes.

Por consiguiente, todas las fórmulas de tipo Σ_n o Π_n según la definición de [LM 5.17] serían del tipo correspondiente según la nueva definición si no fuera porque hemos cambiado la definición de las fórmulas de tipo Δ_0, pero en cualquier caso son equivalentes[2] a fórmulas del tipo correspondiente según la definición que acabamos de dar. Recíprocamente, toda fórmula de tipo Σ_n o Π_n en el sentido que acabamos de introducir es equivalente a una del mismo tipo según [LM 5.17], concretamente a la que se obtiene haciendo las transformaciones que requiere el cambio de la definición de las fórmulas Δ_0 y añadiendo en su caso cuantificadores con variables nuevas.

Esto hace que las teorías $\mathrm{I}\Sigma_n$ tengan exactamente los mismos teoremas con cualquiera de las dos definiciones de la jerarquía de Kleene. En los resultados demostrados en [LM] nunca ha sido relevante que una fórmula fuera de tipo Σ_n o Π_n en sentido estricto de acuerdo con la definición dada, sino únicamente que fuera equivalente a una fórmula del tipo correspondiente, por lo que todos los resultados demostrados allí siguen siendo válidos con la definición nueva. Sin embargo, en el contexto del cálculo secuencial sí que será relevante la estructura de las fórmulas de tipo Σ_n o Π_n en sentido estricto, y hemos introducido estos cambios para asegurar que el conjunto de las fórmulas Σ_n (o Π_n) es cerrado para subfórmulas y para sustitución, es decir, que si α es del tipo correspondiente, lo mismo sucede con todas sus subfórmulas y con las sustituciones $\mathtt{S}_x^t\alpha$.

3.1 Una axiomática secuencial para AP

Según hemos visto en el capítulo precedente, las consecuencias lógicas de estos axiomas pueden obtenerse indistintamente con el cálculo deductivo considerado en [LM], que captura la forma en que razonan los matemáticos en la práctica, o con el cálculo secuencial LK_i. La versión secuencial de la aritmética de Peano sería, en principio, el cálculo secuencial siguiente:

Definición 3.1 Llamaremos $\mathrm{AP}^*(\Phi)$ al cálculo secuencial sobre el lenguaje $\mathcal{L}_a$ cuyas reglas de inferencia son las de LK_i y cuyos axiomas son los de LK_i más los secuentes:

$$\begin{array}{llll}
(\mathrm{AP1}) & x' = 0 \Rightarrow & (\mathrm{AP4}) & \Rightarrow x + y' = (x+y)' \\
(\mathrm{AP2}) & x' = y' \Rightarrow x = y & (\mathrm{AP5}) & \Rightarrow x \cdot 0 = 0 \\
(\mathrm{AP3}) & \Rightarrow x + 0 = x & (\mathrm{AP6}) & \Rightarrow xy' = xy + x
\end{array}$$

$$(\mathrm{AP7}) \quad \alpha(0), \bigwedge u(\alpha(u) \to \alpha(u')) \Rightarrow \bigwedge u\, \alpha(u),$$

para toda fórmula $\alpha(y)$ de la clase Φ. (Cuando Φ es la clase de todas las fórmulas de $\mathcal{L}_a$ tenemos la aritmética de Peano AP^*).

Notemos que, por simplicidad en los axiomas hemos eliminado los cuantificadores universales, que son redundantes tanto en el cálculo secuencial como en el cálculo $K_{\mathcal{L}}$ descrito en [LM], y hemos pasado algunas fórmulas al antecedente para eliminar signos lógicos.

[2]Sobreentendemos en todo momento la necesidad de "traducir" las fórmulas para hacer comparaciones debido a que hemos cambiado los conectores lógicos primitivos.

Tenemos que un secuente $\Rightarrow \alpha$ es demostrable en $\mathrm{AP}^*(\Phi)$ si y sólo si α es demostrable a partir de los axiomas de Peano con la inducción restringida a Φ en el sistema deductivo $K_{\mathcal{L}}$ descrito en [LM].

Sin embargo, a continuación definimos una versión equivalente de la aritmética de Peano en la que el principio de inducción no se expresa mediante un esquema axiomático, sino mediante una nueva regla de inferencia:

Definición 3.2 Sea Φ una clase de fórmulas del lenguaje de la aritmética $\mathcal{L}_a$. Llamaremos *Aritmética de Peano* ($\mathrm{AP}(\Phi)$) al cálculo secuencial sobre el lenguaje $\mathcal{L}_a$ cuyos axiomas son los de LK_i más los secuentes:

$$\begin{array}{llll}
(\mathrm{AP1}) & x' = 0 \Rightarrow & (\mathrm{AP4}) & \Rightarrow x + y' = (x+y)' \\
(\mathrm{AP2}) & x' = y' \Rightarrow x = y & (\mathrm{AP5}) & \Rightarrow x \cdot 0 = 0 \\
(\mathrm{AP3}) & \Rightarrow x + 0 = x & (\mathrm{AP6}) & \Rightarrow xy' = xy + x
\end{array}$$

y cuyas reglas de inferencia son las de LK más la *regla de inducción* (que tiene dos fórmulas auxiliares y dos principales):

$$\frac{\alpha(y),\, \Gamma \Rightarrow \Delta,\, \alpha(y')}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t)},$$

en la que t es un término arbitrario, $\alpha(y)$ es una fórmula de Φ y la variable propia y no puede aparecer libre en ninguna fórmula colateral (ni obviamente en $\alpha(0)$), pero sí que puede estar en t.

Esta teoría es equivalente a $\mathrm{AP}^*(\Phi)$ en el sentido de que ambas tienen exactamente los mismos teoremas. Para probarlo basta ver que suponiendo la regla de inducción (para fórmulas de Φ) podemos probar todos los axiomas AP7 (para fórmulas de Φ) y viceversa. En efecto, suponiendo la regla de inducción, razonando "de abajo hacia arriba" obtenemos fácilmente la demostración siguiente, en la que la regla de inducción se aplica en el tercer paso:

$$\begin{array}{c}
\alpha(y) \to \alpha(y') \Rightarrow \alpha(y) \to \alpha(y') \\ \hline
\alpha(y),\, \alpha(y) \to \alpha(y') \Rightarrow \alpha(y') \\ \hline
\alpha(y),\, \bigwedge u(\alpha(u) \to \alpha(u')) \Rightarrow \alpha(y') \\ \hline
\alpha(0),\, \bigwedge u(\alpha(u) \to \alpha(u')) \Rightarrow \alpha(x) \\ \hline
\alpha(0) \land \bigwedge u(\alpha(u) \to \alpha(u')) \Rightarrow \alpha(x) \\ \hline
\alpha(0) \land \bigwedge u(\alpha(u) \to \alpha(u')) \Rightarrow \bigwedge u\, \alpha(u) \\ \hline
\Rightarrow \alpha(0) \land \bigwedge u(\alpha(u) \to \alpha(u')) \to \bigwedge u\, \alpha(u)
\end{array}$$

Recíprocamente, si tomamos como axiomas los secuentes AP7 (para fórmulas de Φ), podemos demostrar como sigue la regla de inducción. Por razones tipográficas partimos la prueba en tres bloques:

$$\begin{array}{c}
\alpha(y),\, \Gamma \Rightarrow \Delta,\, \alpha(y') \\ \hline
\Gamma \to \Delta,\, \alpha(y) \to \alpha(y') \\ \hline
\Gamma \Rightarrow \Delta,\, \bigwedge u(\alpha(u) \to \alpha(u')) \\ \hline
\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t),\, \bigwedge u(\alpha(u) \to \alpha(u'))
\end{array}$$

$$\begin{array}{c}
\Rightarrow \alpha(0)\wedge \bigwedge u(\alpha(u)\rightarrow \alpha(u'))\rightarrow \bigwedge u\,\alpha(u)\\ \hline
\Gamma \Rightarrow \Delta,\ \alpha(0)\wedge \bigwedge u(\alpha(u)\rightarrow \alpha(u'))\rightarrow \bigwedge u\alpha(u)\\ \hline
\alpha(0)\wedge \bigwedge u(\alpha(u)\rightarrow \alpha(u')),\, \Gamma \Rightarrow \Delta,\ \bigwedge u\,\alpha(u)\\ \hline
\alpha(0),\ \bigwedge u(\alpha(u)\rightarrow \alpha(u')),\, \Gamma \Rightarrow \Delta,\ \bigwedge u\,\alpha(u)\\ \hline
\alpha(0),\ \bigwedge u(\alpha(u)\rightarrow \alpha(u')),\, \Gamma \Rightarrow \Delta,\ \alpha(t),\ \bigwedge u\,\alpha(u)
\end{array}$$

$$\begin{array}{c}
\alpha(t)\Rightarrow \alpha(t)\\ \hline
\alpha(t),\Gamma \Rightarrow \Delta,\ \alpha(t)\\ \hline
\bigwedge u\,\alpha(u),\,\Gamma \Rightarrow \Delta,\ \alpha(t)\\ \hline
\bigwedge u\,\alpha(u),\ \alpha(0),\ \bigwedge u(\alpha(u)\rightarrow \alpha(u')),\,\Gamma \Rightarrow \Delta,\ \alpha(t)
\end{array}$$

los dos últimos bloques se unen mediante la regla de corte y dan el secuente

$$\bigwedge u(\alpha(u)\rightarrow \alpha(u')),\ \alpha(0),\ \Gamma \Rightarrow \Delta,\ \alpha(t),$$

el cual se une con el primer bloque también con la regla de corte, lo que nos da la conclusión $\alpha(0),\,\Gamma \Rightarrow \Delta,\,\alpha(t)$. ■

Ejemplo Veamos un ejemplo elemental de demostración por inducción. Concretamente, vamos a demostrar que todo número natural no nulo es el siguiente de otro número natural, es decir:

$$\Rightarrow x=0,\ \bigvee u\, x=u'.$$

DEMOSTRACIÓN: Lo probamos por inducción respecto de la fórmula

$$\alpha(x)=x=0\vee \bigvee u\, x=u'.$$

$$\begin{array}{cc}
 & \Rightarrow x'=x'\\ \cline{2-2}
 & \Rightarrow \bigvee u\, x'=u'\\ \cline{2-2}
\Rightarrow 0=0 & x=0\vee \bigvee u\,x=u' \Rightarrow x'=0,\ \bigvee u\, x'=u'\\ \cline{1-1}\cline{2-2}
\Rightarrow 0=0,\ \bigvee u\, 0=u' & x=0\vee \bigvee u\,x=u' \Rightarrow x'=0\vee \bigvee u\, x'=u'\\ \cline{1-1}\cline{2-2}
\Rightarrow 0=0\vee \bigvee u\, 0=u' & 0=0\vee \bigvee u\,0=u' \Rightarrow x=0\vee \bigvee u\, x=u'\\ \hline
\multicolumn{2}{c}{\Rightarrow x=0\vee \bigvee u\, x=u'}\\ \hline
\multicolumn{2}{c}{\Rightarrow x=0,\ \bigvee u\, x=u'}
\end{array}$$

■

Veremos que la formalización del principio de inducción en forma de regla de inferencia es mucho más conveniente a efectos teóricos, pero todavía conviene hacer algunos retoques más al cálculo secuencial de la Aritmética de Peano que no alteren el conjunto de sus teoremas. En primer lugar demostramos lo siguiente:

Teorema 3.3 *Si s y t son términos cualesquiera de $\mathcal{L}_a$, los secuentes siguientes son teoremas de* AP($\varnothing$), *es decir, que pueden demostrarse sin usar la regla de inducción:*

$$\begin{array}{llll}
(\mathrm{AP1}) & s'=0\Rightarrow & (\mathrm{AP4}) & \Rightarrow s+t'=(s+t)'\\
(\mathrm{AP2}) & s'=t'\Rightarrow s=t & (\mathrm{AP5}) & \Rightarrow s\cdot 0=0\\
(\mathrm{AP3}) & \Rightarrow s+0=s & (\mathrm{AP6}) & \Rightarrow st'=st+s
\end{array}$$

Demostración: Todos ellos se demuestran introduciendo generalizadores en el axioma correspondiente y luego eliminándolos con la regla inversa del generalizador. Por ejemplo:

$$\begin{array}{c}
x' = y' \Rightarrow x = y \\ \hline
\Rightarrow x' = y' \to x = y \\ \hline
\Rightarrow \bigwedge uv(u' = v' \to u = v) \\ \hline
\Rightarrow s' = t' \to s = t \\ \hline
s' = t' \Rightarrow s = t
\end{array}$$

■

Nota *En lo sucesivo vamos a tomar como axiomas de* AP(Φ) *todos los secuentes considerados en el teorema anterior.* ■

Obviamente, los teoremas de esta versión de AP(Φ) con más axiomas son exactamente los mismos que los de la versión que hemos definido inicialmente, pues una demostración que use los axiomas adicionales puede prolongarse con la demostración de cada uno de estos axiomas a partir de los axiomas originales. El interés de añadirlos como axiomas es doble. Por una parte, la demostración de los axiomas generalizados requiere usos no triviales de la regla de corte, con lo que al tomarlos como axiomas podemos evitar dichos usos en las demostraciones. Por otra parte, ahora los axiomas de AP tienen claramente la propiedad de que si en uno de ellos sustituimos una variable libre por un término, el secuente resultante es también un axioma.

Ejemplo Veamos ahora un ejemplo más sofisticado, concretamente, una demostración del secuente

$$\Rightarrow \bigvee u(x = 2u \vee x = 2u + 1),$$

que expresa que todo número natural x es par o impar. (Se entiende que $2 = 1'$, donde a su vez $1 = 0'$.) Añadiendo una aplicación de la regla del generalizador derecha podríamos pasar a su vez al secuente (semánticamente) equivalente

$$\Rightarrow \bigwedge v \bigvee u(v = 2u \vee v = 2u + 1).$$

Por razones tipográficas hemos descompuesto la prueba en tres bloques, hemos sustituido cada fórmula por un nombre y hemos recogido en una tabla a qué fórmula corresponde cada nombre:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overset{\text{AM}}{\Rightarrow \eta} \qquad \overset{\text{AI}}{\eta,\, \beta_6 \Rightarrow \zeta}}{\beta_6 \Rightarrow \zeta} \qquad \overset{\text{AI}}{\zeta \Rightarrow \epsilon}}{\beta_6 \Rightarrow \epsilon} \qquad \dfrac{\overset{\text{AM}}{\Rightarrow \theta} \qquad \overset{\text{AI}}{\theta,\, \epsilon \Rightarrow \alpha_4}}{\epsilon \Rightarrow \alpha_4}}{\beta_6 \Rightarrow \alpha_4}}{\beta_6 \Rightarrow \alpha_3,\, \alpha_4 \quad (\vee)}}{\beta_6 \Rightarrow \alpha_2}$$

$$(*)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\overset{\text{AI}}{\beta_7\Rightarrow\lambda}\qquad \dfrac{\dfrac{\overset{\text{AM}}{\Rightarrow\nu}\quad\dfrac{\overset{\text{AI}}{\Rightarrow\xi}\quad\overset{\text{AI}}{\xi,\,\nu\Rightarrow\mu}}{\nu\Rightarrow\mu}}{\Rightarrow\mu}\quad\overset{\text{AI}}{\mu,\,\lambda\Rightarrow\kappa}}{\lambda\Rightarrow\kappa}}{\beta_7\Rightarrow\kappa}\qquad\dfrac{\dfrac{\overset{\text{AM}}{\Rightarrow\rho}\quad\dfrac{\overset{\text{AI}}{\Rightarrow\sigma}\quad\overset{\text{AI}}{\sigma,\,\rho\Rightarrow\pi}}{\rho\Rightarrow\pi}}{\Rightarrow\pi}\quad\overset{\text{AI}}{\pi,\,\kappa\Rightarrow\alpha_6}}{\kappa\Rightarrow\alpha_6}}{\beta_7\Rightarrow\alpha_6}}{\beta_7\Rightarrow\alpha_6,\,\alpha_7\quad(\vee)}}{\beta_7\Rightarrow\alpha_5}$$

$$(**)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overset{\text{AI}}{\Rightarrow\gamma}\qquad\dfrac{\overset{\text{AM}}{\Rightarrow\delta,}\qquad\overset{\text{AI}}{\delta,\,\gamma\Rightarrow\beta_2}}{\gamma\Rightarrow\beta_2}}{\Rightarrow\beta_2}}{\Rightarrow\beta_2,\,\beta_3\quad(\vee)}}{\Rightarrow\beta_1}}{\Rightarrow\beta}\qquad\dfrac{\dfrac{\dfrac{\dfrac{(*)}{\beta_6\Rightarrow\alpha_1}\quad(\vee)\quad\dfrac{(**)}{\beta_7\Rightarrow\alpha_1}}{\beta_5\Rightarrow\alpha_1}}{\beta_4\Rightarrow\alpha_1}}{\beta\Rightarrow\alpha}}{\Rightarrow\alpha}$$

α	$\phi(x)$	$\bigvee u(x = 2u \vee x = 2u+1)$	β_7	$x = 2y+1$
α_1	$\phi(x')$	$\bigvee u(x' = 2u \vee x' = 2u+1)$	γ	$2\cdot 0 = 2\cdot 0$
α_2		$x' = 2y \vee x' = 2y+1$	δ	$2\cdot 0 = 0$
α_3		$x' = 2y$	ϵ	$x' = (2y+0)'$
α_4		$x' = 2y+1$	ζ	$x = 2y+0$
α_5		$x' = 2y' \vee x' = 2y'+1$	η	$2y = 2y+0$
α_6		$x' = 2y'$	θ	$2y+1 = (2y+0)'$
α_7		$x' = 2y'+1$	κ	$x' = 2y+2$
β	$\phi(0)$	$\bigvee u(0 = 2u \vee 0 = 2u+1)$	λ	$x' = (2y+1)'$
β_1		$0 = 2\cdot 0 \vee 0 = 2\cdot 0+1$	μ	$(2y+1)' = 2y+2$
β_2		$0 = 2\cdot 0$	ν	$2y+2 = (2y+1)'$
β_3		$0 = 2\cdot 0+1$	ξ	$2y+2 = 2y+2$
β_4	$\phi(x)$	$\bigvee u(x = 2u \vee x = 2u+1)$	π	$2y+2 = 2y'$
β_5		$x = 2y \vee x = 2y+1$	ρ	$2y' = 2y+2$
β_6		$x = 2y$	σ	$2y' = 2y'$

Para analizar la demostración con más detalle escribimos explícitamente algunas de las fórmulas del último bloque de la prueba:

$$\dfrac{\dfrac{\dfrac{\dfrac{\overset{\text{AI}}{\Rightarrow\gamma}\qquad\dfrac{\overset{\text{AM}}{\Rightarrow 2\cdot 0=0}\qquad\overset{\text{AI}}{\delta,\,\gamma\Rightarrow\beta_2}}{\gamma\Rightarrow 0=2\cdot 0}}{\Rightarrow 0=2\cdot 0}}{\Rightarrow 0=2\cdot 0,\ 0=2\cdot 0+1}}{\dfrac{\Rightarrow 0=2\cdot 0\vee 0=2\cdot 0+1}{\Rightarrow\phi(0)}}\qquad\dfrac{\dfrac{\dfrac{\dfrac{(*)}{x=2y\Rightarrow\phi(x')}\qquad\dfrac{(**)}{x=2y+1\Rightarrow\phi(x')}}{x=2y\vee x=2y+1\Rightarrow\phi(x')}}{\phi(x)\Rightarrow\phi(x')}}{\phi(0)\Rightarrow\phi(x)}}{\Rightarrow\phi(x)}$$

Vemos así que el núcleo del argumento es una inducción respecto de la fórmula

$$\alpha \equiv \phi(x) \equiv \bigvee u(x = 2u \vee x = 2u+1).$$

La parte derecha del árbol contiene la prueba del secuente $\phi(x) \Rightarrow \phi(x')$ y la aplicación de la regla de inducción, que nos da el secuente $\phi(0) \Rightarrow \phi(x)$. La parte izquierda del árbol contiene la demostración del secuente $\Rightarrow \phi(0)$, que al cortarlo con la parte derecha nos da la conclusión.

La prueba de $\Rightarrow \phi(0)$ se reduce inmediatamente a la de $0 = 2 \cdot 0$, lo que a su vez requiere algunas manipulaciones técnicas, porque lo que nos dan los axiomas de Peano es, en realidad, que $2 \cdot 0 = 0$.

Por su parte, la prueba del paso inductivo se reduce a probar $\phi(x')$ descomponiendo $\phi(x)$ en dos casos, según si x es par o impar. El caso en que x es par se prueba en el bloque que conecta con $(*)$, mientras que el caso en que x es impar se prueba en el bloque que conecta con $(**)$. Aquí vemos el primero con algo más de detalle:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\overset{\text{AM}}{\Rightarrow 2y = 2y + 0} \qquad \overset{\text{AI}}{\eta,\, \beta_6 \Rightarrow \zeta}}{x = 2y \Rightarrow x = 2y + 0} \qquad \overset{\text{AI}}{\zeta \Rightarrow \epsilon}}{x = 2y \Rightarrow x' = (2y + 0)'} \qquad \cfrac{\overset{\text{AM}}{\Rightarrow 2y + 1 = (2y + 0)'} \qquad \overset{\text{AI}}{\theta,\, \epsilon \Rightarrow \alpha_4}}{x' = (2y + 0)' \Rightarrow x' = 2y + 1}}{x = 2y \Rightarrow x' = 2y + 1}}{x = 2y \Rightarrow x' = 2y,\, x' = 2y + 1}}{\underset{(*)}{x = 2y \Rightarrow x' = 2y \lor x' = 2y + 1}}$$

Esencialmente, consiste en probar que si $x = 2y = 2y + 0$, entonces también $x' = (2y + 0)' = 2y + 1$. El argumento detallado requiere, además de los dos axiomas de Peano concernientes a la suma, varias aplicaciones de los axiomas del igualador. ■

Todavía conviene hacer un retoque adicional a la axiomática de AP:

Definición 3.4 Llamaremos $\mathcal{L}_a^+$ al lenguaje formal que consta de los signos de $\mathcal{L}_a$ más un relator diádico que representaremos por $\leq$. Abreviaremos:

$$\bigwedge u \leq y\, \alpha \equiv \bigwedge u(u \leq y \rightarrow \alpha), \qquad \bigvee u \leq y\, \alpha \equiv \bigvee u(u \leq y \land \alpha).$$

Definimos las semifórmulas Δ_0 de $\mathcal{L}_a^+$ como las semifórmulas construidas con el criterio siguiente:

1. Las semifórmulas atómicas son Δ_0.
2. Si α y β son Δ_0, también lo son $\neg\alpha$, $\alpha \lor \beta$, $\bigwedge u \leq t\, \alpha$ y $\bigvee u \leq t\, \alpha$, donde t es un semitérmino en el que no esté la variable u.

Una fórmula de $\mathcal{L}_a^+$ es de tipo Σ_n si es de la forma

$$\bigvee u_1 \bigwedge u_2 \cdots \alpha \quad \text{o} \quad \bigwedge u_1 \bigvee u_2 \cdots \alpha,$$

donde α es una semifórmula de tipo Δ_0 y el número de cuantificadores alternados es $\leq n$ en el primer caso y $< n$ en el segundo. Las fórmulas de tipo Π_n son las de esta misma forma, salvo que ahora exigimos que el número de cuantificadores sea $< n$ en el primer caso y $\leq n$ en el segundo.

Si α es una fórmula de $\mathcal{L}_a^+$, llamamos α^* a la fórmula de $\mathcal{L}_a$ que resulta de sustituir cada subsemifórmula atómica $s \leq t$ por $\bigvee u\, u + s \leq t$ (donde u es una variable que no aparezca en s o en t). Es claro entonces que α es una fórmula de tipo Δ_0, Σ_n o Π_n en $\mathcal{L}_a^+$ si y sólo si α^* lo es en $\mathcal{L}_a$.

Definimos $\mathrm{AP}^+(\Phi)$ como el cálculo secuencial sobre $\mathcal{L}_a$ cuyas reglas de inferencia son las de LK más la regla de inducción restringida a fórmulas de Φ y cuyos axiomas son los de AP más los secuentes siguientes:

1)	$\Rightarrow t \leq t$	5)	$\Rightarrow 0 \leq t$
2)	$t_1 \leq t_2,\, t_2 \leq t_1 \Rightarrow t_1 = t_2$	6)	$\Rightarrow t \leq t'$
3)	$t_1 \leq t_2,\, t_2 \leq t_3 \Rightarrow t_1 \leq t_3$	7)	$t_1 \leq t_2' \Rightarrow t_1 \leq t_2,\, t_1 = t_2'$
4)	$\Rightarrow t_1 \leq t_2,\, t_2 \leq t_1$		

donde t, t_1, t_2, t_3 son términos cualesquiera de $\mathcal{L}_a$.

Es fácil ver que si S es uno de estos secuentes, entonces el secuente S^* de $\mathcal{L}_a$ que resulta de sustituir cada fórmula α por α^*, es decir, de sustituir cada semifórmula atómica $s \leq t$ por $\bigvee u\, u + s = t$, es un teorema de $\mathrm{I}\Sigma_1$.

Todos estos teoremas son consecuencias de las propiedades básicas de la suma, todas ellas demostrables en $\mathrm{I}\Sigma_1$. Por ejemplo, el último secuente equivale a que la fórmula

$$t_1 \leq t_2' \rightarrow t_1 \leq t_2 \lor t_1 = t_2'$$

es un teorema de $\mathrm{I}\Sigma_1$, y un esbozo de una demostración es como sigue:

Si $t_1 \leq t_2'$, existe un z tal que $z + t_1 = t_2'$, con lo que caben dos posibilidades, o bien $z = 0$, en cuyo caso $t_1 = t_2'$, o bien $z \neq 0$, en cuyo caso $z = w + 1$, para cierto w, con lo que $w + 1 + t_1 = t_2 + 1$, luego $w + t_1 = t_2$, luego $t_1 \leq t_2$.

Llamamos $\mathrm{I}\Sigma_n^+$ al cálculo secuencial $\mathrm{AP}^+(\Phi)$, donde Φ es el conjunto de las fórmulas de tipo Σ_n. Notemos que [LM 5.21] junto con la equivalencia que hemos probado entre axiomas de inducción y la regla de inducción, prueban que en $\mathrm{I}\Sigma_n$ también es válida la regla de inducción para fórmulas de tipo Π_n.

Ahora es inmediato que si un secuente S es demostrable en $\mathrm{I}\Sigma_n^+$, entonces el secuente S^* es demostrable en $\mathrm{I}\Sigma_n$, ya que al cambiar cada secuente S' de una demostración D de S por el secuente S'^*, todas las reglas de inferencia siguen siendo válidas, y los secuentes iniciales de D se convierten en teoremas de $\mathrm{I}\Sigma_n$, luego añadiendo sus demostraciones obtenemos una demostración D^* de S^* en $\mathrm{I}\Sigma_n$.

En particular, si S es un secuente de $\mathcal{L}_a$, entonces S es demostrable en $\mathrm{I}\Sigma_n$ si y sólo si lo es en $\mathrm{I}\Sigma_n^+$, pues una implicación es un caso particular de lo que acabamos de razonar (ya que en este caso S y S^* son el mismo secuente), y si S es demostrable en $\mathrm{I}\Sigma_n$, trivialmente lo es en $\mathrm{I}\Sigma_n^+$, exactamente con la misma demostración. Igualmente concluimos que S es demostrable en AP si y sólo si lo es en AP^+.

En particular, AP (o $\mathrm{I}\Sigma_n$) es consistente si y sólo si lo es AP^+ (o $\mathrm{I}\Sigma_n^+$).

Más aún, en $\mathrm{I}\Sigma_1^+$ podemos demostrar el secuente

$$\Rightarrow x \leq y \leftrightarrow \bigvee u\, u + x = y.$$

Un esbozo de demostración es el siguiente:

La implicación $x \leq y \rightarrow \bigvee u\, u + x = y$ (que es una fórmula Σ_1) se prueba en AP^+ por inducción sobre x. Si $x = 0$ tenemos que $y + 0 = y$ y, supuesto cierto para x, si suponemos $x' \leq y$, entonces $x \leq x' \leq y$, luego por hipótesis de inducción existe un z tal que $z + x = y$. Si $z = 0$ entonces $x = y$, luego $x' \leq x \leq x'$, luego $x = x'$, pero en AP se demuestra que $\bigwedge u\, u \neq u'$. Por lo tanto $z \neq 0$, luego $z = w + 1$, para cierto w, y entonces $w + 1 + x = y$, luego $w + x' = y$, luego $\bigvee u\, u + x' = y$.

La implicación $\bigvee u\, u + x = y \rightarrow x \leq y$ (que es una fórmula Π_1) la probamos también por inducción sobre x. Si $x = 0$ tenemos que $0 \leq y$ como axioma de AP^+. Supongamos $\bigvee u\, u + x' = y$ y veamos que $x' \leq y$. Si $z + x' = y$, entonces $z' + x = y$, luego $\bigvee u\, u + x = y$, luego por hipótesis de inducción $x \leq y$. Si no se cumpliera $x' \leq y$ sería $y \leq x'$, $y \neq x'$, luego $y \leq x$ (por el axioma 7), luego $x = y$, luego $z + x + 1 = x$, luego $z + 1 = 0$, contradicción.

A partir de aquí una comprobación rutinaria muestra que si α es cualquier fórmula de $\mathcal{L}_a^+$, entonces en $\mathrm{I}\Sigma_1^+$ se demuestra $\Rightarrow \alpha \leftrightarrow \alpha^*$, de donde se sigue a su vez que un secuente S de $\mathcal{L}_a^+$ es demostrable en $\mathrm{I}\Sigma_n^+$ (o en AP^+) si y sólo si S^* es demostrable en $\mathrm{I}\Sigma_n$ (o AP).

En efecto, una implicación ya la tenemos probada y, si S^* es demostrable en $\mathrm{I}\Sigma_n$ (o AP), entonces es demostrable en $\mathrm{I}\Sigma_n^+$ (o AP^+) con la misma prueba, pero S^* es equivalente a S, luego lo mismo vale para S.

Todas estas consideraciones hacen que, a efectos, prácticos, los teoremas de AP y AP^+ (o de $\mathrm{I}\Sigma_n$ e $\mathrm{I}\Sigma_n^+$) son esencialmente los mismos, de modo que es irrelevante considerar una u otra teoría. Sin embargo, a efectos teóricos AP^+ será mucho más conveniente.

Nota *A partir de este momento, llamaremos* $\mathcal{L}_a$, AP *o* $\mathrm{I}\Sigma_n$ *a* $\mathcal{L}_a^+$, AP^+ *e* $\mathrm{I}\Sigma_n^+$, *respectivamente. Siempre que escribamos* $s \leq t$ *se entenderá que se trata de una fórmula atómica y no de* $\bigvee u\, u + s = t$.

3.2 Sentencias Δ_0 en AP($\varnothing$)

Al permitir que los cuantificadores de las fórmulas Δ_0 estén acotados por términos arbitrarios y no necesariamente por variables hace que haya más fórmulas Δ_0 en este sentido que no en el considerado en [LM 5.5]. Por ejemplo, una sentencia Δ_0 en el sentido considerado en [LM 5.5] no puede tener cuantificadores, mientras que en el sentido actual sí que puede tenerlos. En esta sección demostraremos que toda sentencia Δ_0 es demostrable o refutable en AP($\varnothing$), es decir, sin usar la regla de inducción.

En varios enunciados será conveniente distinguir entre un número natural n y el numeral $\bar{n}$ que lo representa en $\mathcal{L}_a$:

$$\bar{0} \equiv 0, \quad \bar{1} \equiv 0', \quad \bar{2} = 0'', \quad \bar{3} \equiv 0''', \ldots$$

Teorema 3.5 *Para todo par de números naturales m y n,*

1. *Si $m = n$, en* AP($\varnothing$) *se puede probar $\Rightarrow \bar{m} = \bar{n}$.*
2. *Si $m \neq n$, en* AP($\varnothing$) *se puede probar $\bar{m} = \bar{n} \Rightarrow$.*
3. *Si $m \leq n$, en* AP($\varnothing$) *se puede probar $\Rightarrow \bar{m} \leq \bar{n}$.*
4. *Si $m > n$, en* AP($\varnothing$) *se puede probar $\bar{m} \leq \bar{n} \Rightarrow$.*
5. *En* AP($\varnothing$) *se puede probar*

$$\Rightarrow \bar{m} + \bar{n} = \overline{m+n}, \qquad \Rightarrow \bar{m}\bar{n} = \overline{mn}$$

y todas estas demostraciones pueden hacerse sin cortes esenciales (entendiendo por cortes no esenciales aquellos cuya fórmula de corte es atómica).

Demostración: 1) Si $m = n$ entonces $\bar{m} \equiv \bar{n}$, por lo que $\Rightarrow \bar{m} = \bar{n}$ es un axioma del igualador.

2) Supongamos que $m < n$. El caso $m > n$ se trata de forma similar. Tenemos que

$$\overline{n-m} = \bar{0} \Rightarrow$$

es un axioma de Peano. La prueba dada en 2.13 del secuente

$$\bar{0} = \overline{n-m} \Rightarrow \overline{n-m} = \bar{0}$$

no usa cortes esenciales. Cortando estos dos secuentes obtenemos una prueba de

$$\bar{0} = \overline{n-m} \Rightarrow .$$

Vamos a ver que, para todo k, podemos demostrar el secuente

$$\bar{k} = \overline{n-m+k} \Rightarrow .$$

Lo tenemos probado para $k = 0$ y, si vale para k, basta cortar con el axioma de Peano

$$\overline{k+1} = \overline{n-m+k+1} \Rightarrow \bar{k} = \overline{n-m-k}.$$

El caso particular $k = m$ nos da una demostración de $\bar{m} = \bar{n} \Rightarrow$.

3) Lo probamos por inducción sobre n. Si $n = 0$ necesariamente $m = n = 0$, y $\Rightarrow \bar{0} \leq \bar{0}$ es un axioma.

Si vale para n y se cumple $m \leq n+1$, o bien $m = n+1$, en cuyo caso $\bar{m} \equiv \overline{n+1}$ y $\Rightarrow \bar{m} \leq \overline{n+1}$ es un axioma, o bien $m \leq n$, en cuyo caso, por hipótesis de inducción, podemos probar $\Rightarrow \bar{m} \leq \bar{n}$ y cortando este secuente y el axioma $\Rightarrow \bar{n} \leq \overline{n+1}$, con el axioma

$$\bar{m} \leq \bar{n},\, \bar{n} \leq \overline{n+1} \Rightarrow \bar{m} \leq \overline{n+1},$$

obtenemos como teorema $\Rightarrow \bar{m} \leq \overline{n+1}$.

4) Si $m > n$, entonces $n \leq m$ y $n \neq m$, luego, por los casos ya probados, en AP($\varnothing$) podemos demostrar $\Rightarrow \bar{n} \leq \bar{m}$ y $\bar{m} = \bar{n} \Rightarrow$. Cortando con el axioma

$$\bar{m} \leq \bar{n}, \bar{n} \leq \bar{m} \Rightarrow \bar{m} = \bar{n}$$

obtenemos $\bar{m} \leq \bar{n} \Rightarrow$.

5) Probamos el caso de la suma por inducción sobre n. Para $n = 0$ el secuente $\Rightarrow \bar{m} + \bar{0} = \bar{m}$ es un axioma.

Supongamos que tenemos una demostración de $\Rightarrow \bar{m}+\bar{n} = \overline{m+n}$. Cortando con el axioma del igualador

$$\bar{m} + \bar{n} = \overline{m+n} \Rightarrow (\bar{m} + \bar{n})' = \overline{m+n+1}$$

obtenemos $\Rightarrow (\bar{m} + \bar{n})' = \overline{m+n+1}$. A su vez, cortando con el axioma del igualador

$$(\bar{m} + \bar{n})' = \bar{m} + \overline{n+1}, (\bar{m} + \bar{n})' = \overline{m+n+1} \Rightarrow \bar{m} + \overline{n+1} = \overline{m+n+1}$$

obtenemos $(\bar{m} + \bar{n})' = \overline{m+n+1} \Rightarrow \bar{m} + \overline{n+1} = \overline{m+n+1}$, pero a su vez $\Rightarrow (\bar{m} + \bar{n})' = \bar{m} + \overline{n+1}$ es un axioma de Peano, y cortando con él llegamos a $\Rightarrow \bar{m} + \overline{n+1} = \overline{m+n+1}$.

En el caso del producto, de nuevo $\Rightarrow \bar{m} \cdot \bar{0} = \bar{0}$ es un axioma. Supongamos que podemos probar $\Rightarrow \bar{m}\bar{n} = \overline{mn}$. Consideramos entonces el axioma del igualador

$$\bar{m} \cdot \overline{n+1} = \bar{m}\bar{n} + \bar{m}, \bar{m}\bar{n} = \overline{mn} \Rightarrow \bar{m} \cdot \overline{n+1} = \overline{mn} + \bar{m}$$

y lo cortamos con $\Rightarrow \bar{m}\bar{n} = \overline{mn}$ y con el axioma

$$\Rightarrow \bar{m} \cdot \overline{n+1} = \bar{m}\bar{n} + \bar{m},$$

lo que nos da una demostración de $\Rightarrow \bar{m} \cdot \overline{n+1} = \overline{mn} + \bar{m}$. Por el caso de la suma, ya probado, podemos demostrar

$$\Rightarrow \overline{mn} + \bar{m} = \overline{m(n+1)},$$

y mediante cortes entre los dos últimos secuentes y el axioma del igualador

$$\bar{m} \cdot \overline{n+1} = \overline{mn} + \bar{m}, \overline{mn} + \bar{m} = \overline{m(n+1)} \Rightarrow \bar{m} \cdot \overline{n+1} = \overline{m(n+1)},$$

obtenemos una demostración de $\Rightarrow \bar{m} \cdot \overline{n+1} = \overline{m(n+1)}$. ■

Definición 3.6 A cada designador t de $\mathcal{L}_a$ le asignamos un número natural $d(t)$ mediante el criterio siguiente:

1. $d(\bar{0}) = 0$,
2. $d(t') = d(t) + 1$,
3. $d(s + t) = d(s) + d(t)$,
4. $d(s \cdot t) = d(s)d(t)$.

Notemos que $d(t)$ no es sino el número natural denotado por t en el modelo natural de $\mathcal{L}_a$, pero vemos que puede ser definido sin hacer referencia alguna a modelos.

Teorema 3.7 *Sean s y t designadores de $\mathcal{L}_a$.*

1. *Si $n = d(t)$, en* AP($\varnothing$) *se demuestra $\Rightarrow \bar{n} = s$. Además la prueba no requiere cortes esenciales.*
2. *Si $\Rightarrow s = t$ es demostrable en* AP($\varnothing$) *sin cortes esenciales y $S(x)$, $T(x)$ son términos arbitrarios, entonces $S(s) = T(s) \Rightarrow S(t) = T(t)$ es demostrable en las mismas condiciones.*
3. *En las mismas condiciones del apartado anterior, para toda fórmula $\alpha(x)$, el secuente $s = t$, $\alpha(s) \Rightarrow \alpha(t)$ es demostrable en* AP($\varnothing$) *sin cortes esenciales.*

Demostración: 1) Razonamos por inducción sobre la longitud de s. Si tiene longitud 1, necesariamente $s \equiv \bar{0}$, y $n = d(\bar{0}) = 0$. Ciertamente $\Rightarrow \bar{0} = \bar{0}$ es demostrable porque es un axioma.

Si $s = t'$ y $n = d(t)$, por hipótesis de inducción podemos probar $\Rightarrow \bar{n} = t$ sin cortes esenciales. Pero entonces $d(s) = n + 1$ y tenemos

$$\frac{\Rightarrow \bar{n} = t \qquad \bar{n} = t \Rightarrow \overline{n+1} = s}{\Rightarrow \overline{n+1} = s}$$

donde el corte es inesencial y el secuente superior derecho es un axioma.

Si $s \equiv t_1 + t_2$, $d(t_1) = m$ y $d(t_2) = n$, entonces $d(s) = m + n$ y podemos probar:

$$\frac{\Rightarrow \bar{m} = t_1 \qquad \bar{m} = t_1, \bar{n} = t_2 \Rightarrow \bar{m} + \bar{n} = s}{\bar{n} = t_2 \Rightarrow \bar{m} + \bar{n} = s}$$

donde el secuente superior izquierdo es demostrable por hipótesis de inducción y el superior derecho es un axioma del igualador. Cortando con $\Rightarrow \bar{n} = t_2$ (que también es demostrable por hipótesis de inducción) obtenemos una demostración del secuente $\Rightarrow \bar{m} + \bar{n} = s$. Por el teorema anterior tenemos también que $\Rightarrow \bar{m} + \bar{n} = \overline{m+n}$. Mediante cortes con los secuentes que expresan la simetría y la transitividad de la igualdad (que se demuestran sin cortes esenciales) obtenemos $\Rightarrow \overline{m+n} = s$.

Si $s = t_1 \cdot t_2$ se razona análogamente.

2) y 3) se obtienen trivialmente mediante cortes inesenciales a partir de los teoremas dados por 2.14 (que se demuestran sin cortes esenciales y, obviamente, sin la regla de inducción). ■

Definición 3.8 Si α es una sentencia de tipo Δ_0, diremos que es *verdadera* (y lo representaremos por $\vDash_0 \alpha$), si se puede probar que lo es a partir de los criterios siguientes:

1. $\vDash_0 s = t$ syss $d(s) = d(t)$,
2. $\vDash_0 s \leq t$ syss $d(s) \leq d(t)$,
3. $\vDash_0 \neg\alpha$ syss no $\vDash_0 \alpha$,
4. $\vDash_0 \alpha \lor \beta$ syss $\vDash_0 \alpha$ o $\vDash_0 \beta$,
5. $\vDash_0 \bigwedge u \leq t\, \alpha(u)$ syss para todo $m \leq d(t)$ se cumple $\vDash_0 \alpha(\bar{m})$.
6. $\vDash_0 \bigvee u \leq t\, \alpha(u)$ syss existe un $m \leq d(t)$ tal que $\vDash_0 \alpha(\bar{m})$.

Es claro que $\vDash_0 \alpha$ equivale a que α sea verdadera en la interpretación natural de $\mathcal{L}_a$, pero aquí es fundamental que $\vDash_0 \alpha$ está definido en términos puramente sintácticos, finitistas, sin hacer referencia a modelos. Siempre podemos comprobar en un número finito de pasos si una sentencia Δ_0 dada es verdadera o falsa.

Teorema 3.9 *Si α es una sentencia de tipo Δ_0, entonces en* AP($\varnothing$) *puede probarse el secuente $\Rightarrow \alpha$ o bien $\alpha \Rightarrow$ según si α es verdadera o falsa. Además la prueba no requiere cortes esenciales.*

DEMOSTRACIÓN: Lo probamos por inducción sobre el número de signos lógicos (conectores y cuantificadores) de α.

Si $\alpha \equiv s = t$ o $\alpha \equiv s \leq t$, sean $m = d(s)$, $n = d(t)$. Según el teorema 3.7 podemos probar $\Rightarrow \bar{m} = s$, $\Rightarrow \bar{n} = t$. Según 3.5 podemos probar $\Rightarrow \bar{m} = \bar{n}$ (resp. $\Rightarrow \bar{m} \leq \bar{n}$) o bien $\bar{m} = \bar{n} \Rightarrow$ (resp. $\bar{m} \leq \bar{n} \Rightarrow$) según si α es verdadera o falsa. A partir de aquí podemos demostrar $\Rightarrow \alpha$ o $\alpha \Rightarrow$ mediante cortes inesenciales con axiomas del igualador. Por ejemplo, en el caso en que se cumpla $\Rightarrow \bar{m} \leq \bar{n}$ basta considerar el axioma

$$\bar{m} = s,\, \bar{n} = t,\, \bar{m} \leq \bar{n} \Rightarrow s \leq t.$$

Si $\alpha \equiv \neg\beta$, por hipótesis de inducción podemos demostrar $\Rightarrow \beta$ o $\beta \Rightarrow$ según si β es verdadera o falsa, y las reglas del negador nos dan una demostración de $\alpha \Rightarrow$ o $\Rightarrow \alpha$ según si α es falsa o verdadera.

Si $\alpha \equiv \beta \lor \gamma$ y $\vDash_0 \alpha$, entonces β o γ es verdadera. Si, por ejemplo, es verdadera β, por hipótesis de inducción podemos demostrar $\Rightarrow \beta$, y la regla derecha del disyuntor nos da $\Rightarrow \alpha$. Si es verdadera γ el razonamiento es análogo.

Si, por el contrario α es falsa, entonces son falsas β y γ, luego por hipótesis de inducción podemos demostrar $\beta \Rightarrow$ y $\gamma \Rightarrow$, y la regla izquierda del disyuntor nos da $\alpha \Rightarrow$.

Si $\alpha \equiv \bigwedge u \leq t\, \beta(u)$, sea $n = d(t)$. Si α es verdadera es que, para todo $m \leq n$, se cumple que $\beta(\bar{m})$ es verdadera, luego por hipótesis de inducción[3] podemos demostrar $\Rightarrow \beta(\bar{m})$.

[3]Notemos que $\beta(\bar{m})$ puede tener mayor longitud que α, pero tiene menos signos lógicos.

Veamos que, para todo $m \leq n$, podemos probar $y \leq \bar{m} \Rightarrow \beta(y)$.

Cortando los axiomas

$$y \leq \bar{0},\, \bar{0} \leq y \Rightarrow y = \bar{0}, \qquad \Rightarrow \bar{0} \leq y$$

obtenemos $y \leq \bar{0} \Rightarrow y = \bar{0}$. Por otra parte, 3.7 nos da

$$\bar{0} = y,\, \beta(\bar{0}) \Rightarrow \beta(y).$$

Cortando estos secuentes con $y = \bar{0} \Rightarrow 0 = \bar{y}$, obtenemos $y \leq \bar{0} \Rightarrow \beta(y)$.

Si podemos probar $y \leq \bar{m} \Rightarrow \beta(y)$ y $m + 1 \leq n$ consideramos el axioma

$$y \leq \bar{m}' \Rightarrow y \leq \bar{m},\, y = \bar{m}'.$$

También tenemos

$$\Rightarrow \beta(\bar{m}'), \qquad \bar{m}' = y,\, \beta(\bar{m}') \Rightarrow \beta(y), \qquad y = \bar{m}' \Rightarrow \bar{m}' = y.$$

Mediante cortes inesenciales llegamos a $y \leq \bar{m}' \Rightarrow \beta(y)$.

En particular, para $m = n$ tenemos una demostración de $y \leq \bar{n} \Rightarrow \beta(y)$. Cortando con $\Rightarrow \bar{n} = t$ y con axiomas del igualador llegamos a $y \leq t \Rightarrow \beta(y)$, desde donde ya podemos concluir:

$$\cfrac{\cfrac{y \leq t \Rightarrow \beta(y)}{\Rightarrow y \leq t \rightarrow \beta(y)}}{\bigwedge u \leq t\, \beta(u)}$$

Si α es falsa, entonces existe un $m \leq n$ tal que $\beta(\bar{m})$ es falsa, luego por hipótesis de inducción podemos demostrar $\beta(\bar{m}) \Rightarrow$. Como $\bar{m} \leq t$ es verdadera, por la parte ya probada podemos demostrar $\Rightarrow \bar{m} \leq t$. La regla izquierda del implicador nos da

$$\bar{m} \leq t \rightarrow \beta(\bar{m}) \Rightarrow$$

y la regla izquierda del generalizador nos da $\bigwedge u \leq t\, \beta(u) \Rightarrow$.

Supongamos, por último, que $\alpha \equiv \bigvee u \leq t\, \beta(u)$ y sea $n = d(t)$. Si α es verdadera es que existe un $m \leq n$ tal que $\beta(\bar{m})$ es verdadera, luego por hipótesis de inducción podemos demostrar $\Rightarrow \beta(\bar{m})$.

Como en el caso anterior, también podemos probar $\Rightarrow \bar{m} \leq t$, y por la regla derecha del conjuntor llegamos a $\Rightarrow \bar{m} \leq t \wedge \beta(\bar{m})$. Finalmente, la regla derecha del particularizador nos da $\Rightarrow \bigvee u \leq t\, \beta(u)$.

Si α es falsa, entonces para todo $m \leq n$ se cumple que $\beta(\bar{m})$ es falsa, luego por hipótesis de inducción podemos demostrar $\beta(\bar{m}) \Rightarrow$. Ahora probamos por inducción sobre m que podemos demostrar $y \leq \bar{m},\, \beta(y) \Rightarrow$.

Para $m = 0$ usamos como antes que $y \leq \bar{0} \Rightarrow y = \bar{0}$, lo cual, combinado con

$$\beta(\bar{0}) \Rightarrow, \qquad \bar{0} = y,\, \beta(\bar{0}) \Rightarrow \beta(y), \qquad y = \bar{0} \Rightarrow \bar{0} = y,$$

nos da $y \leq \bar{0},\, \beta(y) \Rightarrow$.

Si podemos probar $y \leq \bar{m}$, $\beta(y) \Rightarrow$ y $m+1 \leq n$, cortamos con el axioma

$$y \leq \overline{m+1} \Rightarrow y \leq \bar{m},\ y = \overline{m+1}$$

y con

$$\beta(\overline{m+1}) \Rightarrow, \qquad y = \overline{m+1},\ \beta(y) \Rightarrow \beta(\overline{m+1})$$

obtenemos $y \leq \overline{m+1}$, $\beta(y) \Rightarrow$.

En particular podemos probar $y \leq \bar{n}$, $\beta(y) \Rightarrow$, y usando $\Rightarrow \bar{n} = t$ podemos llegar a $y \leq t$, $\beta(y) \Rightarrow$. Aplicando las reglas izquierdas del conjuntor y del particularizador llegamos finalmente a $\bigvee u \leq t\, \beta(u) \Rightarrow$. ■

El hecho de que en el teorema anterior no sea necesaria la regla de inducción depende esencialmente de que hemos introducido axiomáticamente la relación de orden, pues si quisiéramos usar la definición $x \leq y \equiv \bigvee u\, u{+}x = y$ necesitaríamos usar propiedades de la suma que se demuestran por inducción.

3.3 Eliminación de cortes

En esta sección demostraremos una versión para AP del teorema de eliminación de cortes, del que extraeremos varias consecuencias de interés. En realidad vamos a probar un teorema general aplicable a otras teorías axiomáticas distintas de AP:

Definición 3.10 Si $\mathfrak{S}$ es un conjunto de secuentes en un lenguaje formal $\mathcal{L}$, llamaremos LK($\mathfrak{S}$) al cálculo secuencial cuyos axiomas son los de LK más los de $\mathfrak{S}$, mientras que LK$_i$($\mathfrak{S}$) será el cálculo secuencial que además cuenta con los axiomas del igualador $\mathfrak{S}_i$ de LK$_i$. Observemos que una demostración en LK$_i$($\mathfrak{S}$) es lo mismo que una deducción en LK con premisas en $\mathfrak{S}_i \cup \mathfrak{S}$.

Diremos que $\mathfrak{S}$ es *cerrado para sustitución* si al sustituir una variable libre por un término en todas las fórmulas de uno de sus secuentes, el secuente resultante está también en $\mathfrak{S}$.

Observemos que $\mathfrak{S}_i$ cumple claramente esta propiedad, al igual que lo cumple el conjunto de los axiomas lógicos $\alpha \Rightarrow \alpha$, por lo que si $\mathfrak{S}$ es cerrado para sustitución, la sustitución de una variable libre por un término en un axioma de LK($\mathfrak{S}$) es de nuevo un axioma de LK($\mathfrak{S}$).

Vamos a trabajar simultáneamente en dos contextos diferentes: o bien en un sistema LK($\mathfrak{S}$) sobre un lenguaje formal arbitrario (lo que incluye en particular a los sistemas LK$_i$($\mathfrak{S}$)) o bien en un sistema LK($\mathfrak{S}$) + Φ-IND, donde $\mathfrak{S}$ es un conjunto de secuentes en el lenguaje $\mathcal{L}_a$ de la aritmética de primer orden (o una extensión suya) y el sistema indicado es el que resulta de añadir a LK($\mathfrak{S}$) la regla de inducción restringida a fórmulas de una cierta clase Φ. En particular, esto incluye a la aritmética de Peano[4] AP(Φ) con la inducción restringida a Φ.

[4]Y podemos considerar tanto el caso en que $\mathcal{L}_a$ tiene el relator $\leq$ como el caso en que la relación de orden se define a partir de la suma.

Así pues, podemos distinguir entre *axiomas lógicos* (los de LK), *axiomas del igualador* (los axiomas adicionales de LK_i) y *axiomas propios* (los de $\mathfrak{S}$ que no sean axiomas del igualador).

Por otra parte, las reglas de inferencia se clasifican en *estructurales* (debilitación y corte), *lógicas* (las de LK) y, en el caso aritmético, tenemos además una *regla de inferencia propia* (la de inducción).

Supondremos que $\mathfrak{S}$ es cerrado para sustitución, lo cual se cumple en particular en el caso aritmético cuando $\mathfrak{S}$ es el conjunto de los axiomas del igualador y los axiomas de Peano considerados en el teorema 3.3. En el caso aritmético supondremos también que Φ es cerrado para sustitución (lo cual se cumple cuando Φ es el conjunto de todas las fórmulas de $\mathcal{L}_a$, y también cuando es el conjunto de las fórmulas Σ_n, para un cierto n).

En este contexto se cumple la variante siguiente del teorema 2.25:

Teorema 3.11 *Sea $\mathfrak{S}$ un conjunto de secuentes cerrado para sustitución y sea D una demostración en* $\mathrm{LK}(\mathfrak{S})(+\Phi\text{-IND}$, *con Φ cerrado para sustitución). Sea x una variable libre que no sea usada en D como variable propia y t un término que no contenga ninguna variable propia de ninguna inferencia en D. Entonces, al sustituir todas las apariciones de x en D por t queda una demostración del secuente que resulta de sustituir x por t en el secuente final de D.*

Demostración: La prueba es la misma que la de 2.25, sin más que observar que sigue siendo cierto que al sustituir x por t en un axioma seguimos teniendo un axioma, y que las consideraciones hechas en 2.25 para la regla izquierda del particularizador valen igualmente para la regla de inducción. ■

La definición 2.26 de demostración regular se extiende de forma obvia al contexto general que estamos considerando aquí:

Definición 3.12 Una demostración en $\mathrm{LK}(\mathfrak{S})(+\Phi\text{-IND})$ es *regular* si una misma variable no aparece como variable propia de dos aplicaciones de la regla derecha del generalizador, o de la regla izquierda del particularizador o de la regla de inducción, y además, la variable propia de una aplicación de cualquiera de estas reglas sólo aparece en los secuentes situados por encima de la regla.

Teorema 3.13 *Si $\mathfrak{S}$ es un conjunto de secuentes cerrado para sustitución, toda demostración en* $\mathrm{LK}(\mathfrak{S})(+\Phi\text{-IND}$, *con Φ cerrado para sustitución) puede transformarse en una demostración regular del mismo secuente sin más que cambiar unas variables propias por otras.*

Demostración: La prueba es la misma que la de 2.27, sin más que añadir algunas consideraciones adicionales. Por simplicidad repetimos aquí el argumento completo:

Basta tener en cuenta que si en una demostración D cambiamos todas las apariciones de una variable libre x por otra y que no aparezca en D, el resultado es una nueva demostración. En efecto, basta observar que cada regla de inferencia sigue siendo válida cuando una variable libre es sustituida por otra nueva, y que si cambiamos una variable por otra en un axioma obtenemos otro axioma.

Así pues, dada una demostración D, para cada secuente S que resulte de una aplicación de una regla derecha del generalizador, o de una regla izquierda del particularizador o de inducción, consideramos la subdemostración D' formada por los secuentes de D situados sobre S, que es en sí misma una demostración de S.

Si la regla es una regla de un cuantificador y en D' cambiamos la variable propia por otra que no aparezca en D, obtenemos una nueva demostración D'_1 de S (pues la variable propia no está en S), mientras que si se trata de una regla de inducción

$$\frac{\alpha(y),\,\Gamma \Rightarrow \Delta,\,\alpha(y')}{\alpha(0),\,\Gamma \Rightarrow \Delta,\,\alpha(t)},$$

en principio la variable y puede estar en t, pero no en $\alpha(0)$, Γ o Δ, luego, si llamamos z a la variable nueva, sucede que la inferencia

$$\frac{\alpha(z),\,\Gamma \Rightarrow \Delta,\,\alpha(z')}{\alpha(0),\,\Gamma \Rightarrow \Delta,\,\alpha(t)},$$

donde no hemos modificado t, sigue siendo válida, por lo que igualmente obtenemos una demostración D'_1 del mismo secuente S.

Al cambiar D' por D'_1 en D obtenemos otra demostración D_1 con el mismo secuente final en la que la aplicación de la regla considerada cumple ya la definición de regularidad. Ahora pasamos de D_1 a otra demostración D_2 considerando la variable propia de otra regla, y así hasta que todas las variables propias cumplan lo requerido por la definición de regularidad. ■

El concepto de *hilo* de una demostración, definido en 2.28, vale obviamente en este contexto, pero podemos afinar más y seguir la evolución en una demostración de cada fórmula concreta. Para ello introducimos los conceptos siguientes:

Definición 3.14 Diremos que una fórmula α de un secuente superior de una regla de inferencia es un *ascendiente inmediato* de una fórmula β del secuente inferior (o que β es un *descendiente inmediato* de α) si se da alguno de los casos siguientes:

1. Si α es una fórmula colateral de la regla, su único descendiente es la fórmula colateral idéntica en el secuente inferior.

2. Si α es una fórmula auxiliar de una regla distinta de la de corte o inducción, su único descendiente inmediato es la fórmula principal. En el caso de la regla de inducción, el descendiente de la fórmula auxiliar izquierda (derecha) es la fórmula principal izquierda (derecha).

Así, las fórmulas de corte son las únicas fórmulas en los secuentes superiores de una regla de inferencia que no tienen descendiente inmediato, y las fórmulas principales de las reglas de debilitación son las únicas fórmulas en el secuente inferior de una regla que no tienen ascendiente inmediato.

Un poco más en general: las fórmulas de una demostración que no tienen ascendiente inmediato son las de los secuentes iniciales y las fórmulas principales de una regla de debilitación, mientras que las fórmulas que no tienen descendiente inmediato son las del secuente final y las fórmulas de corte. Salvo estos casos, toda fórmula tiene un único descendiente inmediato y uno o varios ascendientes inmediatos.

En la demostración del ejemplo de la página 68, cada descendiente de una fórmula se nombra con la misma letra y otro subíndice, si no se trata de la misma fórmula.

Una *fibra* en una demostración es una sucesión de fórmulas de la demostración, cada una de las cuales es descendiente inmediato de la anterior, de modo que la primera no tenga ascendiente inmediato y la última no tenga descendiente inmediato.

Una fórmula α es un *ascendiente* de otra fórmula β en una deducción[5] si ambas forman parte de una misma fibra, y α aparece en ella antes que β. Diremos que α es un *ascendiente directo* de β (o que β es un *descendiente directo* de α) si además son la misma fórmula.

Notemos que las únicas fórmulas con ascendientes directos son las fórmulas colaterales de las reglas de inferencia.

Para determinar los cortes que pueden ser eliminados de una demostración introducimos el concepto de profundidad de una fórmula:

Definición 3.15 La *profundidad* de una fórmula α en una demostración D, que representaremos por $p(\alpha; D)$, o simplemente por $p(\alpha)$, es un número natural o bien $-\infty$, y está determinada inductivamente por las reglas siguientes (en las que adoptamos el convenio de que $-\infty$ es menor que todo número natural y que $-\infty + 1 = -\infty$):

1. Si α está en un axioma de de $\mathfrak{S}$ o es una fórmula principal de una regla de inducción, entonces $p(\alpha) = 0$.
2. Si α está en un axioma lógico entonces $p(\alpha) = 1$.
3. Si α es la fórmula principal de una regla de debilitación, $p(\alpha) = -\infty$.
4. Si α es la fórmula principal de una regla de inferencia lógica, $p(\alpha)$ es una unidad mayor que el máximo de las profundidades de las fórmulas auxiliares de la regla.
5. Si α es una fórmula colateral[6] del secuente inferior de una regla de inferencia, $p(\alpha)$ es el máximo de las profundidades de sus ascendientes inmediatos.

[5] Notemos que estos conceptos no dependen únicamente de las fórmulas, sino de su posición en la demostración.

[6] Notemos que una fórmula colateral del secuente superior de una regla de inferencia puede coincidir con la fórmula principal. En tal caso, su descendiente en el secuente inferior se considera como fórmula principal y su profundidad se calcula según el caso precedente.

En particular es claro que una fórmula tiene profundidad $-\infty$ si y sólo si todas las fibras a las que pertenece empiezan en fórmulas principales de reglas de debilitación, y la profundidad es 0 si y sólo si todas empiezan en fórmulas principales reglas de debilitación o en un ascendiente directo que está en un axioma propio o del igualador o es una fórmula principal de una regla de inducción (y uno de los dos últimos casos se da al menos una vez).

Por otra parte, la profundidad de una fórmula atómica no puede ser mayor que 1, pues no puede tener ascendientes en el caso 4), y es 1 si y sólo si pertenece a alguna fibra que empieza en un axioma lógico.

La *profundidad* de un corte es el mínimo de las profundidades de las dos fórmulas de corte.

Es fácil ver que todos los cortes de la demostración del ejemplo de la página 68 tienen profundidad 0. En el caso del corte inferior, cuya fórmula de corte es β, ello se debe a que la fórmula de corte derecha tiene profundidad 0 porque es una fórmula principal de la regla de inducción.

Diremos que un corte *está fijo* en una demostración si se cumple una de las dos condiciones siguientes:

1. La fórmula de corte no es atómica y el corte tiene profundidad 0.
2. La fórmula de corte es atómica y tiene profundidad 0 en los dos secuentes superiores del corte.

Los cortes que no están fijos se llaman *libres.* Explícitamente, un corte está libre en una demostración si cumple una de las dos condiciones siguientes:

1. La profundidad del corte es distinta de 0.
2. La fórmula de corte es atómica y en uno de los dos secuentes superiores tiene profundidad 1.

Vamos a probar que todo secuente demostrable admite una demostración sin cortes libres. La demostración del ejemplo de la página 68 no tiene cortes libres.

Observación Un hecho que usaremos a menudo será el siguiente: Supongamos que tenemos dos cortes A y B en dos demostraciones respectivas con la misma fórmula de corte, de modo que la profundidad de ésta en cada secuente superior de A sea mayor o igual que en el secuente correspondiente de B. Entonces, si el corte A está fijo, la única posibilidad para que B esté libre es que tenga profundidad $-\infty$.

En efecto, sabemos que el corte A tiene profundidad 0, y la profundidad de B es claramente menor o igual. Si no es $-\infty$, entonces sigue siendo cero, pero la única posibilidad para que un corte de profundidad 0 sea libre es que la fórmula de corte sea atómica y en uno de los secuentes tenga profundidad 1, pero, siendo atómica, la fórmula de corte tiene profundidad 0 en los dos secuentes superiores de A, luego no puede tener profundidad 1 en ningún secuente de B. ■

Veamos ahora un primer caso sencillo de eliminación de cortes:

Teorema 3.16 *Sea D una demostración de un secuente S y sea S' un secuente obtenido a partir del anterior eliminando (tal vez) algunas fórmulas, pero todas en su caso de profundidad $-\infty$ en D. Entonces existe una demostración D' de S' tal que:*

1. *D' no tiene cortes de profundidad $-\infty$,*

2. *Para cada corte que pueda haber en D' hay otro en D de profundidad mayor o igual. Y si el primero está libre el segundo también lo está.*

3. *La profundidad de cada fórmula de S' en D' es menor o igual que su profundidad en D.*

DEMOSTRACIÓN: Razonamos por inducción sobre el número de reglas de inferencia de D y probamos además que dicho número es menor o igual en D' que en D. Si D consta de un único secuente (inicial), entonces todas sus fórmulas tienen profundidad 0 o 1, luego no hay ninguna fórmula eliminable y el resultado es trivial. Suponemos, pues, que D tiene inferencias, y vamos a distinguir casos según cuál sea la última regla usada.

Supongamos que la última regla es de debilitación, por ejemplo la regla derecha, aunque el caso de la regla izquierda es totalmente análogo. Pongamos:

$$\begin{array}{c} D_0 \\ \vdots \\ \Gamma \Rightarrow \Delta \\ \hline \Gamma \Rightarrow \Delta,\, \alpha \end{array}$$

donde D_0 es la demostración del secuente $\Gamma \Rightarrow \Delta$ que resulta de eliminar la última inferencia. Entonces α tiene profundidad $-\infty$ en el secuente final S, luego puede estar en S' o no. Por hipótesis de inducción existe una demostración D_0' de $\Gamma' \Rightarrow \Delta'$ sin cortes de profundidad $-\infty$, con a lo sumo tantas inferencias como D_0, etc. Si α no está en S' basta tomar $D' \equiv D_0'$, y está en S' obtenemos D' a partir de D_0' introduciendo α por debilitación. Es claro que el número de inferencias de D' es menor o igual que el de D y cumple todo lo requerido.

Supongamos ahora que la última regla es la regla izquierda del disyuntor:

$$\begin{array}{cc} D_1 & D_2 \\ \vdots & \vdots \\ \alpha,\, \Gamma \Rightarrow \Delta & \beta, \Gamma \Rightarrow \Delta \\ \hline \multicolumn{2}{c}{\alpha \vee \beta,\; \Gamma \Rightarrow \Delta} \end{array}$$

Distinguimos dos casos:

a) Si $\alpha \vee \beta$ es una de las fórmulas eliminadas, entonces su profundidad tiene que ser $-\infty$, luego también lo es la de α y β en los secuentes superiores. Por hipótesis de inducción, de cualquiera de las demostraciones D_1 y D_2 se puede extraer una demostración de $\Gamma' \Rightarrow \Delta'$ que claramente cumple lo requerido. (Notemos que al quedarnos solamente con una de las dos ramas de ascendientes de Γ y Δ, es posible que la profundidad de sus fórmulas disminuya, porque éstas pierden antecedentes.)

b) Si $\alpha \lor \beta$ no tiene que ser eliminada, por hipótesis de inducción podemos conseguir pruebas D_1' y D_2' de los secuentes $\alpha, \Gamma' \Rightarrow \Delta'$ y $\beta, \Gamma' \Rightarrow \Delta'$ respectivamente, que a su vez se combinan mediante la regla izquierda del disyuntor para obtener la prueba requerida. Observemos que como cada D_i' tiene a lo sumo tantas reglas de inferencia como D_i, lo mismo vale para D' y D. Las demás propiedades requeridas se cumplen también trivialmente.

Si la última inferencia es cualquiera de las otras reglas de inferencia lógicas, el razonamiento es totalmente análogo.

Supongamos ahora que la última inferencia es un corte:

$$\dfrac{\begin{array}{c} D_1 \\ \vdots \\ \Gamma \Rightarrow \Delta, \alpha \end{array} \qquad \begin{array}{c} D_2 \\ \vdots \\ \alpha, \Gamma \Rightarrow \Delta \end{array}}{\Gamma \Rightarrow \Delta}$$

Por hipótesis de inducción existen demostraciones D_1' y D_2' de los secuentes reducidos $\Gamma' \Rightarrow \Delta', \alpha$ y $\alpha, \Gamma' \Rightarrow \Delta'$ en las condiciones del enunciado. Si α no tiene profundidad $-\infty$ en ninguna de estas dos demostraciones, podemos combinarlas mediante la regla de corte y obtenemos una prueba de $\Gamma' \Rightarrow \Delta'$ en las condiciones requeridas. Aquí tenemos en cuenta la observación precedente al teorema, pues la profundidad de α en cada secuente del corte final de D' es menor o igual que la que tenía en D, luego si el corte estaba fijo en D, sigue fijo en D'.

Si α tiene profundidad $-\infty$ en una de las demostraciones D_i', no podemos hacer esto, porque la prueba final tendría entonces un corte de profundidad $-\infty$ en contra de lo requerido, pero como el número de inferencias de D_i' es menor que el de D, podemos usar por segunda vez la hipótesis de inducción para obtener una prueba de $\Gamma' \Rightarrow \Delta'$ en las condiciones requeridas. (Nuevamente, la profundidad de cada fórmula en el secuente final puede disminuir al haber eliminado todos sus ascendientes en una de las dos ramas.)

Falta considerar la posibilidad de que la última inferencia sea la regla de inducción en el caso aritmético, pero este caso no ofrece ninguna dificultad, pues las dos fórmulas principales tienen profundidad 0, luego no son eliminables. Basta aplicar la hipótesis de inducción al secuente superior y luego completar la demostración obtenida con la regla de inducción. ■

El núcleo de la prueba del teorema de eliminación de cortes libres es el resultado siguiente:

Teorema 3.17 *Sea $\mathfrak{S}$ un conjunto de secuentes cerrado para sustitución y sea D una demostración en* LK($\mathfrak{S}$)(+Φ-IND, *con Φ también cerrado para sustitución) cuya última inferencia sea un corte libre de profundidad $\leq p$, con $p \geq 0$ y de modo que cualquier otro corte libre en D tenga profundidad $< p$. Entonces existe una demostración D^* del mismo secuente final cuyos cortes libres tienen todos profundidad $< p$ y de modo que la profundidad de cada fórmula en el secuente final de D^* es menor o igual que su profundidad en D.*

DEMOSTRACIÓN: Por el teorema 3.13, cambiando unas variables propias por otras podemos pasar a una demostración regular. Es claro que con ello no alteramos la profundidad de las fórmulas, luego podemos suponer que la prueba D de la que partimos es regular. En particular, las variables libres del secuente final no se usan nunca como variables propias.

La demostración D tiene la forma

$$\dfrac{\begin{array}{c} D_1 \\ \vdots \\ \Gamma \Rightarrow \Delta, \epsilon \end{array} \qquad \begin{array}{c} D_2 \\ \vdots \\ \epsilon, \Gamma \Rightarrow \Delta \end{array}}{\Gamma \Rightarrow \Delta}$$

donde D_1 y D_2 representan las demostraciones de los dos secuentes superiores del corte. Si las dos fórmulas de corte tienen profundidad $< p$, no hay nada que probar, así que suponemos que una de ellas tiene profundidad p y que la otra tiene profundidad $\geq p$. Además tenemos que todos los cortes de las demostraciones D_1 y D_2 tienen profundidad menor que p.

Distinguimos casos según la estructura lógica de la fórmula ϵ. Dejamos para el final el caso en que sea atómica. Si ϵ no es atómica, no puede ser $p = 0$ (o el corte sería fijo), luego $p \geq 1$.

Supongamos que $\epsilon \equiv \neg\alpha$. Consideremos los ascendientes directos de $\neg\alpha$ en la demostración D_1. Los que no tienen a su vez un ascendiente directo pueden ser de los tipos siguientes:

1. Fórmulas principales de reglas derechas de debilitación (que tienen profundidad $-\infty$).

2. Fórmulas de secuentes de axiomas de $\mathfrak{S}$ o fórmulas principales de una regla de inducción (que tienen profundidad 0).

3. Fórmulas principales de reglas derechas del negador (que pueden tener cualquier profundidad no nula).

Descartamos que $\neg\alpha$ esté en un axioma lógico porque éstos sólo tienen fórmulas atómicas. Como $\neg\alpha$ tiene que tener al final profundidad ≥ 1, se tiene que dar al menos una vez el caso 3).

Cada vez que se da este caso modificamos la inferencia del negador convirtiéndola en

$$\frac{\alpha, \Gamma' \Rightarrow \Delta'}{\alpha, \Gamma' \Rightarrow \Delta', \neg\alpha}$$

es decir, mantenemos α en el antecedente, con lo que sigue siendo una regla válida, pero ahora es una regla derecha de debilitación y $\neg\alpha$ tiene profundidad $-\infty$, mientras que la profundidad de α en el secuente inferior es una unidad inferior a la de $\neg\alpha$ en el secuente final de D_1.

A partir de aquí añadimos α como fórmula colateral en los antecedentes de todos los secuentes posteriores hasta llegar al secuente final de la prueba. Las reglas de inferencia que tengan sólo un secuente superior siguen siendo válidas de este modo, mientras que las que tengan dos secuentes superiores, si a uno de ellos le falta α en el antecedente, tendremos que añadírselo por debilitación para que siga encajando. Por ejemplo, una regla izquierda del disyuntor como

$$\frac{\alpha',\, \Gamma \Rightarrow \Delta,\, \neg\alpha \qquad \beta', \Gamma \Rightarrow \Delta,\, \neg\alpha}{\alpha' \vee \beta',\ \Gamma \Rightarrow \Delta,\, \neg\alpha}$$

cuyo secuente superior derecho (por ejemplo) tenga por encima una regla de introducción del negador, pero no así el izquierdo, se transforma en

$$\frac{\dfrac{\alpha',\, \Gamma \Rightarrow \Delta,\, \neg\alpha}{\alpha,\, \alpha',\, \Gamma \Rightarrow \Delta,\, \neg\alpha} \qquad \alpha,\, \beta', \Gamma \Rightarrow \Delta,\, \neg\alpha}{\alpha,\, \alpha' \vee \beta',\ \Gamma \Rightarrow \Delta,\, \neg\alpha}$$

De este modo obtenemos una demostración válida D_1' de $\alpha,\, \Gamma \Rightarrow \Delta, \neg\alpha$ con las características siguientes:

1. La profundidad de $\neg\alpha$ en el secuente final es ≤ 0, pues ya sólo tiene ascendientes directos procedentes de axiomas de $\mathfrak{S}$ o de fórmulas principales de reglas de inducción o debilitación.

2. La profundidad de las fórmulas de Γ y Δ en D_1' es la misma que su profundidad en D_1, pues no hemos alterado sus ascendientes directos ni las reglas que los originan.

3. La profundidad de los cortes libres de D_1' es $< p$, porque lo es la de D_1 y no hemos modificado la profundidad de ningún corte.

4. La profundidad de α en el secuente final de D_1' es una unidad inferior a la profundidad de $\neg\alpha$ en el secuente inferior de D_1. En particular, si $\neg\alpha$ tiene profundidad p en el secuente final de D_1, entonces α tiene profundidad $< p$ en el secuente final de D_1'.

Si la profundidad de $\neg\alpha$ en el secuente final de D_1' es $-\infty$, el teorema anterior nos da una demostración D_1'' de $\alpha,\, \Gamma \Rightarrow \Delta$. Si la profundidad es 0 construimos D_1'' como sigue:

$$\frac{\begin{matrix} D_1' \\ \vdots \\ \alpha,\, \Gamma \Rightarrow \Delta,\, \neg\alpha \end{matrix} \qquad \dfrac{\begin{matrix} D_2 \\ \vdots \\ \neg\alpha,\, \Gamma \Rightarrow \Delta \end{matrix}}{\neg\alpha,\, \alpha,\, \Gamma \Rightarrow \Delta}}{\alpha,\, \Gamma \Rightarrow \Delta}$$

Como la profundidad de $\neg\alpha$ en el secuente final de D_2 es ≥ 1 (luego no es $-\infty$) y en el secuente final de D_1' es 0, concluimos que el corte es fijo, y todos los cortes libres de la prueba tienen profundidad menor que p. Además, con cualquiera de las dos construcciones alternativas de D_1'', si $\neg\alpha$ tiene profundidad p en el secuente final de D_1, entonces α tiene profundidad $< p$ en el secuente final de D_1''.

Simétricamente podemos construir una prueba D_2'' del secuente $\Gamma \Rightarrow \Delta, \alpha$ con cortes libres de profundidad $< p$ y de modo que si $\neg\alpha$ tiene profundidad p en el secuente final de D_2 entonces α tiene profundidad $< p$ en el secuente final de D_2''. Uniendo D_1'' y D_2'' mediante un corte (que tendrá necesariamente profundidad $< p$, porque $\neg\alpha$ tiene profundidad exactamente p en el secuente final de D_1 o en el de D_2) obtenemos una prueba D^* de $\Gamma \Rightarrow \Delta$ en las condiciones requeridas.

Supongamos ahora que $\epsilon \equiv \alpha \vee \beta$. Los ascendientes directos de ϵ en D_1 que no tienen a su vez ascendientes directos tienen que estar en uno de los mismos tres casos del caso anterior salvo que ahora en 3) hemos de considerar la regla derecha del disyuntor. Como la profundidad de ϵ en el secuente final de D_1 tiene que ser ≥ 1, al menos una vez se emplea esta regla.

Obtenemos una demostración D_1' del secuente $\Gamma \Rightarrow \Delta, \alpha, \beta, \alpha \vee \beta$ cambiando cada regla derecha del disyuntor que introduzca un ascendiente directo de ϵ por

$$\dfrac{\Gamma' \Rightarrow \Delta', \alpha, \beta}{\Gamma' \Rightarrow \Delta', \alpha, \beta, \alpha \vee \beta}$$

lo que la transforma en una regla de debilitación. En las fórmulas posteriores mantenemos el α y el β adicionales y, cuando deban enlazarse con otros secuentes, intercalamos reglas de debilitación para añadir α y β si es preciso.

Es claro que D_1' cumple las propiedades análogas a las propiedades $1-4$ del caso anterior, con los cambios obvios: la profundidad de $\alpha \vee \beta$ en su secuente final es ≤ 0 y, si $\alpha \vee \beta$ tiene profundidad exactamente p en D_1, entonces α y β tienen ambas profundidad $< p$ en el secuente final de D_1'.

Si la profundidad de $\alpha \vee \beta$ en el secuente final de D_1' es $-\infty$ usamos el teorema anterior para obtener una demostración D_1'' de $\Gamma \Rightarrow \Delta, \alpha, \beta$. Si la profundidad es 0 construimos D_1'' como sigue:

$$\dfrac{\begin{array}{c} D_1' \\ \vdots \\ \Gamma \Rightarrow \Delta, \alpha, \beta, \alpha \vee \beta \end{array} \qquad \dfrac{\begin{array}{c} D_2 \\ \vdots \\ \alpha \vee \beta, \Gamma \rightarrow \Delta \end{array}}{\alpha \vee \beta, \Gamma \Rightarrow \Delta, \alpha, \beta}}{\Gamma \Rightarrow \Delta, \alpha, \beta}$$

Como en el caso anterior, el corte es fijo y los cortes libres de D_1'' tienen profundidad menor que p. Además, si $\alpha \vee \beta$ tiene profundidad p en D_1 entonces α y β tienen profundidad $< p$ en D_1'.

En este punto se rompe la simetría del caso anterior. A partir de D_2 podemos construir dos demostraciones D_2^α y D_2^β de los secuentes $\alpha \vee \beta, \alpha, \Gamma \Rightarrow \Delta$ y $\alpha \vee \beta, \beta, \Gamma \Rightarrow \Delta$, respectivamente, reemplazando cada regla izquierda del disyuntor en D_2 por

$$\frac{\alpha, \Gamma' \Rightarrow \Delta'}{\alpha \vee \beta, \alpha, \Gamma' \Rightarrow \Delta'} \quad o \quad \frac{\beta, \Gamma' \Rightarrow \Delta'}{\alpha \vee \beta, \beta, \Gamma' \Rightarrow \Delta'}$$

respectivamente, suprimiendo en cada caso uno de los secuentes superiores de la regla con todos los situados sobre él en la prueba, e introduciendo reglas de debilitación de forma oportuna. Observemos que, al haber suprimido fragmentos de demostración, la profundidad de cada fórmula de Γ' o Δ' en las reglas truncadas del disyuntor puede disminuir, y con ella la de sus descendientes, luego la profundidad de las fórmulas de Γ o Δ en el secuente final de D_2^α o D_2^β puede ser menor o igual que en el secuente final de D_2.

Por el mismo motivo, la profundidad de los cortes puede disminuir, pero, por la observación previa al teorema anterior, si algún corte fijo pasara por ello a ser libre, lo sería de profundidad $-\infty$, luego no dejaría de cumplirse que los cortes libres de D_2^α y D_2^β tienen todos profundidad $< p$.

Como en los casos anteriores, la profundidad de $\alpha \vee \beta$ es ahora ≤ 0 y, si $\alpha \vee \beta$ tiene profundidad p en el secuente final de D_2, entonces α y β tienen profundidad $< p$ en los secuentes finales de D_2^α y D_2^β.

Si la profundidad de $\alpha \vee \beta$ en el secuente final de D_2^α o D_2^β es $-\infty$ el teorema anterior nos da una demostración $D_2'^\alpha$ o $D_2'^\beta$ de $\alpha, \Gamma \Rightarrow \Delta$ o $\beta, \Gamma \Rightarrow \Delta$. Si la profundidad es 0 podemos construir la prueba eliminando $\alpha \vee \beta$ con un corte fijo con D_1. Si la profundidad de $\alpha \vee \beta$ en el secuente final de D_2 es p, entonces la profundidad de α o β en el secuente final de $D_2'^\alpha$ o $D_2'^\beta$ es $< p$. La demostración siguiente cumple todo lo requerido:

$$\dfrac{\dfrac{\begin{array}{c} D_1'' \\ \vdots \\ \Gamma \Rightarrow \Delta, \alpha, \beta \end{array} \qquad \dfrac{\begin{array}{c} D_2'^\beta \\ \vdots \\ \beta, \Gamma \Rightarrow \Delta \end{array}}{\beta, \Gamma \Rightarrow \Delta, \alpha}}{\Gamma \Rightarrow \Delta, \alpha} \qquad \begin{array}{c} D_2'^\alpha \\ \vdots \\ \alpha, \Gamma \Rightarrow \Delta \end{array}}{\Gamma \Rightarrow \Delta}$$

Supongamos ahora que $\epsilon \equiv \bigvee u\, \alpha(u)$. Razonando como en los casos anteriores, transformamos cada aplicación en D_2 de la regla izquierda del particularizador que genera un ascendiente directo de ϵ pasando de

$$\frac{\alpha(y_i), \Gamma' \Rightarrow \Delta'}{\bigvee u\, \alpha(u), \Gamma' \Rightarrow \Delta'}$$

a

$$\frac{\alpha(y), \Gamma' \Rightarrow \Delta'}{\bigvee u\, \alpha(u), \alpha(y), \Gamma' \Rightarrow \Delta'},$$

donde y es una variable que no aparezca en D, con lo que ahora estamos empleando la regla de debilitación, y la variable y ya no es una variable propia de la demostración. Sustituimos todas las variables propias y_i de todas las aplicaciones de la regla (que serán distintas entre sí, pues estamos suponiendo que la demostración D es regular) por la misma variable y.

En los secuentes que están por encima del secuente superior de la regla cambiamos también y_i por y, con lo que obtenemos una demostración del secuente $\alpha(y),\, \Gamma' \Rightarrow \Delta'$ en virtud del teorema 3.11. En los secuentes que están por debajo del secuente inferior añadimos $\alpha(y)$ y, cuando se combinan con otras ramas de la demostración, intercalamos aplicaciones de la regla de debilitación que añadan $\alpha(y)$ en los lugares oportunos.

Con esto obtenemos una demostración D_2' de $\bigvee u\, \alpha(u),\, \alpha(y),\, \Gamma \Rightarrow \Delta$, de la cual obtenemos del modo usual una demostración D_2'' de $\alpha(y),\, \Gamma \Rightarrow \Delta$. Explícitamente:

$$\begin{array}{c}
\begin{array}{cc}
\begin{array}{c} D_1 \\ \vdots \\ \Gamma \Rightarrow \Delta, \bigvee u\, \alpha(u) \\ \hline \alpha(y), \Gamma \Rightarrow \Delta, \bigvee u\, \alpha(u) \end{array} &
\begin{array}{c} D_2' \\ \vdots \\ \bigvee u\, \alpha(u), \alpha(y), \Gamma \Rightarrow \Delta \end{array}
\end{array} \\ \hline
\alpha(y), \Gamma \Rightarrow \Delta
\end{array}$$

Como siempre, la profundidad de los cortes libres de D_2'' es $< p$ y si ϵ tiene profundidad p en el secuente final de D, entonces $\alpha(y)$ tiene profundidad $< p$ en el secuente final de D_2''. Además la profundidad de las fórmulas de Γ y Δ en el secuente final de D_2'' es la misma que en el secuente final de D_2.

Como y no es una variable propia de la demostración, el teorema 3.11 nos da que si t es un término que no contenga ninguna variable propia de D_2'', el árbol $D_2''(t)$ que resulta de sustituir y por t en todos los secuentes de D_2'' es una demostración de $\alpha(t),\, \Gamma \Rightarrow \Delta$ en la que las fórmulas y cortes tienen la misma profundidad que sus correspondientes en D_2''.

Ahora tomamos D_1 y cambiamos cada inferencia de la forma

$$\begin{array}{c} \Gamma' \Rightarrow \Delta',\, \alpha(t_i) \\ \hline \Gamma' \Rightarrow \Delta',\, \bigvee u\, \alpha(u) \end{array}$$

por

$$\begin{array}{c}
\begin{array}{cc}
\begin{array}{c} \vdots \\ \Gamma' \Rightarrow \Delta',\, \alpha(t_i) \\ \hline \Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta,\, \alpha(t_i) \end{array} &
\begin{array}{c} D_2''(t_i) \\ \vdots \\ \alpha(t_i),\, \Gamma \Rightarrow \Delta \\ \hline \alpha(t_i),\, \Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta \end{array}
\end{array} \\ \hline
\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta \\ \hline
\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta,\, \bigvee u\, \alpha(u)
\end{array}$$

En los secuentes inferiores añadimos las fórmulas de Γ y Δ y $\bigvee u\, \alpha(u)$ y, para enlazar con otras ramas, intercalamos reglas de debilitación cuando es preciso.

El resultado es una demostración D_1' del secuente $\Gamma \Rightarrow \Delta, \bigvee u\, \alpha(u)$ en la que $\bigvee u\, \alpha(u)$ tiene profundidad ≤ 0 y donde la profundidad de las fórmulas de Γ y Δ es menor o igual que su profundidad en el secuente final de D_1. Como en el caso del disyuntor, aunque algún corte fijo pasara a ser libre, su profundidad sería $-\infty$, por lo que no alteraría que la profundidad de los cortes libres en D_1' es $< p$ por serlo en D_1. De esta demostración obtenemos D^*, bien por aplicación del teorema anterior, o bien eliminando $\bigvee u\, \alpha(u)$ con un corte fijo con D_2.

El caso en que $\alpha \equiv \bigwedge u\, \beta(u)$ es completamente análogo al precedente.

Ahora suponemos que la fórmula ϵ es atómica, con lo que su profundidad no puede ser mayor que 1. Como el corte final es libre, $p = 0, 1$, luego los ascendientes directos de ϵ en D_1 o D_2 que no tienen a su vez ascendientes directos pueden estar en axiomas $\epsilon \Rightarrow \epsilon$, en axiomas de $\mathfrak{S}$, o bien ser fórmulas principales de reglas de debilitación o inducción. Transformamos D_1 como sigue:

Cada axioma lógico $\epsilon \Rightarrow \epsilon$ lo reemplazamos por

$$\frac{\begin{array}{c} D_2 \\ \vdots \\ \epsilon,\, \Gamma \Rightarrow \Delta \end{array}}{\epsilon,\, \Gamma \Rightarrow \Delta,\, \epsilon}$$

de modo que la profundidad de ϵ en el consecuente final es $-\infty$. Añadiendo Γ y Δ en los secuentes posteriores e introduciendo reglas de debilitación para enlazar ramas obtenemos una demostración D_1' de $\Gamma \Rightarrow \Delta, \epsilon$ en la que ahora la profundidad de ϵ es ≤ 0, pues ya no tiene ascendientes directos en axiomas lógicos. Como ninguna fórmula pierde ascendientes, las profundidades de fórmulas distintas de ϵ no se ven alteradas, luego los cortes libres de D_1' proceden todos de cortes libres en D_1 y D_2, luego todos tienen profundidad $< p$.

Del mismo modo formamos una demostración D_2' de $\epsilon, \Gamma \Rightarrow \Delta$ en las mismas condiciones. Si en uno de los dos casos la profundidad de ϵ es $-\infty$, el teorema anterior nos da la prueba requerida. En caso contrario, unimos las dos fórmulas con un corte fijo y la prueba concluye igualmente. ■

Aplicando sucesivamente el teorema anterior podemos reducir la profundidad máxima de los cortes libres en una demostración:

Teorema 3.18 *Sea $\mathfrak{S}$ un conjunto de secuentes cerrado para sustitución y sea D una demostración en* LK($\mathfrak{S}$)(+Φ-IND, *con Φ también cerrado para sustitución) cuyos cortes libres tengan todos profundidad $\leq p$, con $p \geq 0$. Entonces existe una demostración D' con el mismo secuente final, cuyos cortes libres tienen todos profundidad $< p$ y la profundidad de cada fórmula en el secuente final de D' es menor o igual que en el secuente final de D.*

Demostración: Por inducción sobre el número de cortes libres de profundidad d que contiene la demostración. Si no hay ninguno no hay nada que probar. En caso contrario tomamos un corte libre de profundidad p que no tenga ningún otro sobre sí. Si llamamos D_0 a la parte de D que queda sobre el secuente inferior del corte, se trata de una prueba en las condiciones del teorema anterior, que nos da una prueba D_0' cuyos cortes libres tienen todos profundidad $< p$. Al sustituir D_0 por D_0' en D obtenemos otra prueba D' del mismo secuente.

Observemos que la profundidad de cualquier fórmula de D' bajo el secuente final de D_0' es menor o igual que su profundidad en D, por lo que la profundidad de los cortes libres (posteriores), en caso de variar, disminuye, luego no puede ser que ninguno pase a tener profundidad $\geq p$. Por el argumento habitual, si algún corte fijo pasara a ser libre por este cambio, lo sería de profundidad $-\infty < p$. Así pues, D' tiene un corte menos de profundidad p, luego por hipótesis de inducción existe la demostración requerida. ■

A su vez, ahora podemos aplicar sucesivamente el teorema anterior para eliminar todos los cortes libres de una demostración:

Teorema 3.19 (De eliminación de cortes libres) *Sea $\mathfrak{S}$ un conjunto de secuentes cerrado para sustitución y S un teorema de* LK($\mathfrak{S}$)(+Φ-IND, *con Φ también cerrado para sustitución). Entonces S admite una demostración sin cortes libres.*

Demostración: Por el teorema anterior podemos conseguir una demostración de S cuyos cortes libres (en caso de tenerlos) tengan todos profundidad $-\infty$. Si los hay, aplicamos 3.16, que nos da una prueba sin cortes libres. ■

Veamos una primera consecuencia no trivial de este resultado, pero antes necesitamos una definición:

Definición 3.20 Un conjunto Φ de fórmulas de un lenguaje formal es *cerrado para subfórmulas* si cuando α es una fórmula de Φ, β es una subsemifórmula de α y β' es una fórmula resultante de sustituir por términos las variables ligadas de β que aparezcan libres en β, entonces β' está en Φ.

Obviamente el conjunto de todas las fórmulas de un lenguaje formal es cerrado para subfórmulas. También lo es el conjunto de las fórmulas Δ_0 de $\mathcal{L}_a$, pues cualquier subsemifórmula de una fórmula Δ_0 es una semifórmula Δ_0, y al sustituir por términos las variables ligadas que aparecen libres en ella obtenemos una fórmula Δ_0. Lo mismo sucede (por el mismo argumento) con el conjunto de las fórmulas Σ_n o Π_n de $\mathcal{L}_a$.

El interés de esta propiedad reside en que si Φ es un conjunto cerrado para subfórmulas y la fórmula principal de una regla de inferencia lógica está en Φ, entonces las fórmulas auxiliares también lo están.

En efecto, en el caso de las reglas del negador o el disyuntor, las fórmulas auxiliares son subfórmulas de la fórmula principal, luego tienen que estar en Φ. En el caso de las reglas de los cuantificadores, las fórmulas auxiliares resultan de eliminar el cuantificador y de sustituir por un término la variable ligada que pasa a estar libre, luego también están en Φ.

Teorema 3.21 *Sea Φ un conjunto de fórmulas de cerrado para sustitución y para subfórmulas y sea $\mathfrak{S}$ un conjunto de secuentes cerrado para sustitución cuyas fórmulas estén todas en Φ. Entonces, todo secuente formado por fórmulas de Φ demostrable en* $\mathrm{LK}(\mathfrak{S})(+\Phi\text{-IND})$*, admite una prueba formada exclusivamente por fórmulas de Φ.*

DEMOSTRACIÓN: Basta considerar una demostración sin cortes libres, según el teorema anterior. Como todos los cortes están fijos, todas las fórmulas de corte tienen profundidad 0, luego cada una de ellas debe tener un ascendiente directo que esté en un axioma de $\mathfrak{S}$ (o sea una fórmula principal de una regla de inducción). Por lo tanto, todas las fórmulas de corte están en Φ.

El hecho de que Φ sea cerrada para sustitución y para subfórmulas implica claramente que todo ascendiente de una fórmula de Φ está en Φ (en el caso de los ascendientes por una regla de inducción es trivial porque, como la inducción está restringida a fórmulas de Φ y Φ es cerrado para sustitución, siempre se cumple que las fórmulas auxiliares y las fórmulas principales de una regla de inducción están en Φ).

Recíprocamente, si en la prueba hubiera una fórmula que no estuviera en Φ, ninguno de sus descendientes estaría en Φ, pero su línea de descendientes tiene que terminar forzosamente en una fórmula de corte o en el secuente final, y ambos casos son imposibles. ■

Todas las consecuencias que vamos a extraer del teorema de eliminación de cortes libres las obtendremos en realidad del caso particular siguiente del teorema anterior:

Teorema 3.22 *Si una fórmula α de tipo Σ_n (con $n \geq 1$) es demostrable en $\mathrm{I}\Sigma_n$, entonces existe una demostración del secuente $\Rightarrow \alpha$ en $\mathrm{I}\Sigma_n$ en la cual sólo intervienen fórmulas de tipo Σ_n.*

Capítulo IV

La aritmética recursiva primitiva I

La aritmética recursiva primitiva (ARP) es una de las teorías axiomáticas formales más débiles en las que se puede formalizar la aritmética básica. Los teoremas formalizables en ARP son los teoremas demostrables mediante argumentos finitistas en el sentido más estricto del término. Vamos a describirla y analizarla con detalle.

4.1 El lenguaje de ARP

Para enfatizar la naturaleza estrictamente finitista de ARP, vamos a construir su lenguaje formal subyacente sobre un alfabeto formado únicamente por dos signos (esto puede hacerse con cualquier lenguaje formal numerable, pero en realidad no tiene trascendencia alguna).

Letras Consideramos un alfabeto formado por dos *letras*: α y β. Una *cadena alfabética* es una sucesión finita de letras, como:

$$\alpha\alpha\beta\alpha\beta\beta, \qquad \beta\alpha\beta\alpha\alpha\beta\beta\beta\beta, \qquad \text{etc.}$$

Si ζ_1 y ζ_2 nombran dos cadenas alfabéticas, escribiremos $\zeta_1 \equiv \zeta_2$ para indicar que son idénticas, es decir, que constan de las mismas letras en el mismo orden.

Si $\zeta_1, \ldots, \zeta_n$ son cadenas alfabéticas, entonces $\zeta_1 \cdots \zeta_n$ denotará su yuxtaposición, es decir, la cadena que empieza con los signos de ζ_1, seguidos de los signos de ζ_2, etc.

Palabras Llamaremos *palabras* a las cadenas alfabéticas siguientes:

$$0 \equiv \beta, \quad S \equiv \beta\alpha, \quad v \equiv \beta\alpha\alpha, \quad P \equiv \beta\alpha\alpha\alpha,$$

$$C \equiv \beta\alpha\alpha\alpha\alpha, \quad \kappa \equiv \beta\alpha\alpha\alpha\alpha\alpha, \quad \rho \equiv \beta\alpha\alpha\alpha\alpha\alpha\alpha, \quad = \equiv \beta\alpha\alpha\alpha\alpha\alpha\alpha\alpha.$$

Una *cadena verbal* es una yuxtaposición de palabras. Por ejemplo,

$$vv\kappa 00S \equiv \beta\alpha\alpha\beta\alpha\alpha\beta\alpha\alpha\alpha\alpha\alpha\beta\beta\beta\alpha.$$

Nota Es fácil diseñar un algoritmo que, dada una cadena alfabética, determine si empieza o no por una palabra[1] y, en tal caso, que determine cuál es y en qué punto de la cadena termina. Es tan simple como que la primera letra debe ser β y a continuación tiene que haber un número de α's entre 0 y 7. Si no es así, no empieza por una palabra y, si es así, la palabra termina donde viene la siguiente β si la hay o es toda la cadena dada si a continuación ya no hay más letras.

Aplicando repetidamente este algoritmo podemos determinar si una cadena alfabética dada es o no una cadena verbal y, en caso afirmativo, determinar la sucesión de palabras que la forman, que está unívocamente determinada. ■

Sintagmas Vamos a llamar *sintagmas* a ciertas cadenas verbales. Concretamente, a las de los tipos siguientes:

Numerales Llamaremos *numerales* a las cadenas verbales siguientes:

$$\bar{0} \equiv 0, \quad \bar{1} \equiv S0, \quad \bar{2} \equiv SS0, \quad \bar{3} \equiv SSS0, \quad \ldots$$

En general, si n es un número natural, escribiremos $\bar{n}$ para referirnos al numeral que consta de n palabras S seguidas de la palabra 0.

Variables Una *variable* es una cadena verbal de la forma vn, donde n es un numeral. Usaremos la notación

$$v_0 \equiv v0, \quad v_1 \equiv vS0, \quad v_2 \equiv vSS0, \quad v_3 \equiv vSSS0, \quad \ldots$$

En la práctica usaremos letras cualesquiera, como x, y, z, x_1, x_2, … para nombrar variables arbitrarias.

Proyecciones Si $1 \leq i \leq r$ son números naturales, llamaremos *proyección de rango r e índice i* a la cadena verbal $P_i^r \equiv P\bar{r}\bar{\imath}$. Por ejemplo,

$$P_2^4 \equiv PSSSS0SS0.$$

Dada una cadena verbal, es fácil diseñar un algoritmo que determine si empieza por un sintagma y, en caso afirmativo, que determine de qué tipo es y en qué punto de la cadena termina. ■

[1] Esto no es exacto. Por ejemplo, la cadena alfabética que acabamos de considerar podría considerarse que empieza por la palabra β, por $\beta\alpha$ o por $\beta\alpha\alpha$, pero para que tal palabra pueda ser la primera de una cadena verbal, es necesario que sea $\beta\alpha\alpha$.

Funtores Definimos una *sucesión de funtores* como una sucesión de pares

$$(F_1, r_1), \ldots, (F_n, r_s),$$

donde cada F_i es una cadena verbal y cada r_i es un número natural no nulo, de modo que cada par (F_i, r_i) cumpla una de las condiciones siguientes:

1. Es de la forma $(S, 1)$, $(C, 1)$ o (P_i^r, r).
2. Es de la forma $(\kappa F_j F_{i_1} \cdots F_{i_m}, n)$, donde $j, i_1, \ldots, i_m < i$, $r_j = m$ y $r_{i_l} = n$, para $l = 1, \ldots, m$.
3. Es de la forma $(\rho F_j F_k, n+1)$, donde $j, k < i$, $r_j = n$, $r_k = n+2$.

Diremos que F es un *funtor de rango* r si existe una sucesión de funtores que termina en el par (F, r).

Notemos que, más en general, si (F_i, r_i) aparece en una sucesión de funtores, entonces F_i es un funtor de rango r_i. De la definición de funtor se sigue inmediatamente que todo funtor F está necesariamente en uno de los casos siguientes:

1. Es $F \equiv S$, y entonces su rango es 1.
2. Es $F \equiv C$, y entonces su rango es 1.
3. Es $F \equiv P_i^r$, y entonces su rango es r.
4. Es $F \equiv \kappa G H_1 \cdots H_m$, donde G es un funtor de rango m y $H_1, \ldots, H_m$ son funtores de rango n, y entonces su rango es n.
5. Es $F \equiv \rho G H$, donde G es un funtor de rango n y H es un funtor de rango $n+2$, y entonces su rango es $n+1$.

Además, no puede estar en dos casos a la vez, pues los funtores de cada caso empiezan por una palabra distinta.

Recíprocamente, cualquier cadena verbal construida según se indica en 4. o en 5. es un funtor. Por ejemplo, s G es un funtor de rango m y $H_1, \ldots, H_m$ son funtores de rango n, entonces $\kappa G H_1 \cdots H_m$ es un funtor de rango n.

Nota Es fácil diseñar un algoritmo que, dada una sucesión de palabras, determine si empieza por un funtor y, en caso afirmativo, determine dónde acaba y cuál es su rango. Por ejemplo, dada la cadena

$$\zeta \equiv \rho P S 0 S 0 \kappa S P S S S 0 S S S 0,$$

observamos que su primera palabra es ρ, luego si empieza por un funtor, detrás de ρ deben venir dos funtores. El primero de estos funtores empieza por P, luego debe ser una proyección. Aplicando el algoritmo de lectura de proyecciones, concluimos que es necesariamente P_1^1 y esto termina la identificación del primer funtor que buscábamos, que tiene rango 1, luego el segundo debe tener rango 3 y el funtor inicial de la sucesión debe tener rango 2.

Vemos que el segundo empieza por κ, luego tras él debe venir una sucesión de $m+1$ funtores. Como el signo siguiente es S, es ya de por sí el primer funtor, que tiene rango $m=1$. Por lo tanto, a continuación debe venir un único funtor de rango 3. Como el signo siguiente es P, éste debe ser una proyección de rango 3. Aplicando el algoritmo de lectura de proyecciones, concluimos que es P_3^3 y esto completa el primer sintagma de la cadena ζ. Como ahí se acaba la cadena, concluimos que $\zeta \equiv \rho P_1^1 \kappa S P_3^3$ consta de un único funtor de rango 2, cuya estructura es necesariamente la que hemos obtenido.

Es fácil ver que esta forma de argumentar se puede concretar en un algoritmo que detecte si algo que debería cumplirse no se cumple (y entonces concluya que la cadena dada no empieza por un funtor) y en caso contrario vaya determinando su estructura y el punto en que termina. ■

Términos Una *sucesión de términos* es una sucesión de cadenas verbales $t_1, \ldots, t_s$ de modo que cada una de ellas t_i cumpla una de las condiciones siguientes:

1. Es una variable.
2. Es 0.
3. Es de la forma $Ft_{i_1} \cdots t_{i_r}$, donde F es un funtor de rango r e $i_1, \ldots, i_r < i$.

Un *término* es una cadena verbal t para la que existe una sucesión de términos que termine en t. Obviamente, todos los elementos de una sucesión de términos son términos, por lo que todo término t está en uno de los casos siguientes:

1. $t \equiv v_i$ es una variable.
2. $t \equiv 0$.
3. $t \equiv Ft_1 \cdots t_r$, donde F es un funtor de rango r y $t_1, \ldots, t_r$ son términos.

Recíprocamente, toda cadena verbal construida de esta forma es un término. Los términos sin variables se llaman *designadores.*

Nota Nuevamente, es fácil diseñar un algoritmo para que, dada una cadena verbal, determine si empieza por un término y, en caso afirmativo, determine dónde termina y cuál es su estructura. Por ejemplo, dada la cadena

$$t \equiv \rho PS0S0\kappa SPSSS0SSS0SSS0SS0,$$

como empieza por ρ, debe empezar por un funtor y, aplicando el algoritmo de lectura de funtores, concluimos que empieza por el funtor de rango 2 dado por $F \equiv \rho P_1^1 \kappa S P_3^3$, tras el cual deben venir dos términos. La palabra siguiente es S, que es un funtor de rango 1, luego el primero de estos dos términos debe constar de S seguida de otro término. Como luego viene otra S, este segundo término debe ser de la forma S seguida de otro término, y lo mismo una vez más, hasta que aparece un 0, que ya es de por sí un término, luego el primero de los dos términos que buscábamos es $\bar{3} \equiv SSS0$. Lo que queda es $SS0$, que necesariamente se identifica como el término $\bar{2} \equiv SS0$. Así pues, la cadena dada es el término

$$t \equiv FSSS0SS0 \equiv F\bar{3}\bar{2}.$$

Aunque la notación que empleamos es inequívoca, para facilitar la lectura podemos añadir paréntesis y escribir, por ejemplo,

$$t \equiv F(SSS0, SS0) \equiv F(\bar{3}, \bar{2}),$$

pero hay que entender que esto no son sino formas alternativas de nombrar la misma cadena verbal. La cadena en sí no la modificamos. ■

Fórmulas Definimos una *fórmula* como una cadena verbal de la forma $=st$, donde s y t son términos. En la práctica escribiremos $s = t$, pero el hecho de que técnicamente el $=$ esté delante simplifica la identificación de las cadenas verbales que son fórmulas. Diremos que s es el *miembro izquierdo* y que t es el *miembro derecho* de la fórmula $s = t$. Las fórmulas sin variables se llaman *sentencias.*

Es fácil diseñar un algoritmo para que, dada una cadena verbal, determine si es o no una fórmula y, en caso afirmativo, determine sus miembros, que están unívocamente determinados. ■

Sustitución Si s, t son términos y x es una variable, definimos la *sustitución* $\mathtt{S}_x^t s$ como el término que se calcula con las reglas siguientes:

1. $\mathtt{S}_x^t 0 \equiv 0$,
2. $\mathtt{S}_x^t y \equiv \begin{cases} t & \text{si } y \equiv x, \\ x & \text{si } y \not\equiv x, \end{cases}$
3. $\mathtt{S}_x^t F(t_1, \ldots, t_n) \equiv F(\mathtt{S}_x^t t_1, \cdots, \mathtt{S}_x^t t_n)$.

Más llanamente, es el término que resulta de cambiar por t cada x que aparezca en s.

Si $\alpha \equiv s_1 = s_2$ es una fórmula, definimos $S_x^t \alpha \equiv \mathtt{S}_x^t s_1 = \mathtt{S}_x^t s_2$.

Si $x_1, \ldots, x_n$ son variables distintas, $t_1, \ldots t_n$ son términos y θ es un término o una fórmula, definimos

$$\mathtt{S}_{x_1 \cdots x_n}^{t_1 \cdots t_n} \theta \equiv \mathtt{S}_{y_1}^{t_1} \cdots \mathtt{S}_{y_n}^{t_n} \mathtt{S}_{x_1}^{y_1} \cdots \mathtt{S}_{x_n}^{y_n} \theta,$$

donde $y_1, \ldots, y_n$ son variables cualesquiera distintas entre sí y distintas de todas las variables que aparecen en $t_1, \ldots, t_n$.

En la práctica, $\mathtt{S}_{x_1 \cdots x_n}^{t_1 \cdots t_n} \theta$ no es sino el término o fórmula que resulta de sustituir por t_i cada x_i que aparezca en θ (pero no las x_i que pudieran aparecer en otros t_j).

Nota Es fácil diseñar un algoritmo que calcule la sustitución de unas variables dadas por unos términos dados en un término o una fórmula dada. ■

En la práctica usaremos la notación habitual para representar las sustituciones, de modo que, si θ es un término o una fórmula, escribiremos $\theta(x_1,\ldots,x_n)$, para unas variables arbitrarias $x_1,\ldots,x_n$, lo cual no significará en sí mismo nada en particular, salvo que si más adelante escribimos $\theta(t_1,\ldots,t_n)$, esto deberá entenderse como la sustitución $\mathsf{S}^{t_1\cdots t_n}_{x_1\cdots x_n}\theta$. ■

4.2 Demostraciones en ARP

Notemos que el lenguaje formal de la aritmética recursiva primitiva es muy peculiar, ya que carece de conectores lógicos y de cuantificadores. Para aproximarlo lo más posible a un lenguaje formal de primer orden podemos definir $\mathcal{L}_{\mathrm{arp}}$ como el lenguaje cuyos signos son las variables, la constante 0, el relator $=$ y los infinitos funtores del lenguaje definido en la sección precedente. Así sigue sin ser un lenguaje de primer orden, pero pasaría a serlo si le añadiéramos los conectores lógicos y los cuantificadores.

Pese a estas carencias, vamos a definir un cálculo deductivo sobre $\mathcal{L}_{\mathrm{arp}}$, con sus axiomas y sus reglas de inferencia, que no puede ser un caso particular de ninguno de los cálculos deductivos que conocemos.

Axiomas Vamos a llamar *axiomas* de ARP a ciertas fórmulas que especificamos a continuación. Hay uno o dos axiomas asociados a cada funtor, salvo en el caso del funtor S, que no tiene ningún axioma asociado.

1. El axioma asociado al funtor C es:
$$C(v_0)=0.$$

2. El axioma asociado al funtor P^r_i es:
$$P^r_i(v_1,\ldots,v_r)=v_i.$$

3. El axioma asociado a un funtor $F\equiv \kappa G H_1\cdots H_m$, donde G tiene rango m y los H_i tienen rango n, es:
$$F(v_1,\ldots,v_n)=G(H_1(v_1,\ldots,v_n),\ldots,H_m(v_1,\ldots,v_n)).$$
Expresaremos esta relación diciendo que el funtor F está definido por *composición* a partir de los funtores G y $H_1,\ldots,H_n$.

4. Los axiomas asociados a un funtor $F\equiv\rho GH$, donde G tiene rango n y H tiene rango $n+2$, son:
$$\begin{aligned} F(v_1,\ldots,v_n,0) &= G(v_1,\ldots,v_n),\\ F(v_1,\ldots,v_n,Sv_{n+1}) &= H(v_1,\ldots,v_n,v_{n+1},F(v_1,\ldots,v_n,v_{n+1})).\end{aligned}$$
Expresaremos esto diciendo que el funtor F está definido por *recursión* a partir de los funtores G y H. ■

Reglas de inferencia Llamaremos *reglas de inferencia* de ARP a los cuatro criterios siguientes, que determinan cuándo una fórmula es *consecuencia inmediata* de otra u otras fórmulas dadas:

$$(S_1)\ \frac{s_1(x) = s_2(x)}{s_1(t) = s_2(t)} \qquad (S_2)\ \frac{t_1 = t_2}{s(t_1) = s(t_2)} \qquad (T)\ \frac{t_1 = t_2 \qquad t_1 = t_3}{t_2 = t_3}$$

$$(I_0)\ \frac{s_1(0) = s_2(0) \qquad s_1(Sx) = h(x, s_1(x)) \qquad s_2(Sx) = h(x, s_2(x))}{s_1(x) = s_2(x)}$$

Aquí $s(x)$, $s_1(x)$, $s_2(x)$, t, t_1, t_2, t_3 y $h(x, y)$ son términos arbitrarios.

Por ejemplo, la regla T afirma que cualquier fórmula $t_2 = t_3$ es consecuencia inmediata de las fórmulas $t_1 = t_2$ y $t_1 = t_3$, e igualmente con las restantes.

Nos referiremos a las dos primeras reglas como *reglas de sustitución,* la tercera será la *regla de transitividad (del igualador)* y a la cuarta la llamaremos *regla de inducción.*

Demostraciones Si Γ es un conjunto de fórmulas, una *deducción* en ARP a partir de un conjunto Γ de premisas es una sucesión de fórmulas $\alpha_1, \ldots, \alpha_n$, de modo que cada una de ellas sea un axioma, una premisa o bien sea consecuencia inmediata de fórmulas anteriores de la sucesión. Una *demostración* en APR es una deducción sin premisas.

Un *teorema* de ARP es una fórmula α tal que existe una demostración cuya última fórmula es α. Escribiremos $\underset{\mathrm{ARP}}{\vdash} \alpha$ para indicar que α es un teorema.

En la práctica, en una demostración podemos incluir cualquier fórmula demostrada previamente, pues siempre podríamos repetir su demostración, así como emplear reglas derivadas de inferencia, es decir, que si hemos probado que de ciertas fórmulas es posible deducir otra en varios pasos, podemos poner directamente la consecuencia deseada sin necesidad de repetir los pasos necesarios cada vez.

Por ejemplo, aplicando varias veces la regla de sustitución S_1 a cada axioma, obtenemos un teorema idéntico al axioma salvo que las variables que aparecen en él no son precisamente $v_1, \ldots, v_n$, sino otras variables cualesquiera. Por lo tanto, cuando usemos un axioma, lo introduciremos con las variables que nos resulten más convenientes según el contexto. Por ejemplo, la fórmula

$$P_2^3(x, y, z) = y$$

no es un axioma salvo que $x \equiv v_1$, $y \equiv v_2$, $z \equiv v_3$, pero se deduce del axioma

$$P_2^3(v_1, v_2, v_3) = v_2$$

aplicando varias veces la regla S_1. En la práctica la contaremos como axioma, aunque realmente es un teorema. ■

El igualador Veamos ahora unos resultados adicionales que nos permitirán manejar las igualdades con fluidez. En primer lugar observamos que, para todo término t, se cumple $\underset{\text{ARP}}{\vdash} t = t$.

En efecto, una demostración es como sigue:

(1)	$p_1^1(x) = x$	Axioma
(2)	$p_1^1(t) = t$	S_1, 1
(3)	$t = t$	T, 2, 2

Notemos que hemos aplicado la regla de inferencia de transitividad T tomando como sus dos premisas la misma línea 2 de la demostración (alternativamente, podríamos haber deducido 2 dos veces a partir de 1).

Un ejemplo de regla derivada de inferencia es la regla de *simetría:*

$$(S)\,\frac{t_1 = t_2}{t_2 = t_1}$$

Esto significa que tomando $t_1 = t_2$ como premisa podemos deducir $t_2 = t_1$. Una deducción es la siguiente:

(1)	$t_1 = t_2$	Premisa
(2)	$t_1 = t_1$	Teorema
(3)	$t_2 = t_1$	T, 1, 2

De aquí deducimos a su vez una variante de la regla de transitividad:

$$\frac{t_1 = t_2 \qquad t_2 = t_3}{t_1 = t_3}$$

La deducción es:

(1)	$t_1 = t_2$	Premisa
(2)	$t_2 = t_1$	S, 1
(3)	$t_2 = t_3$	Premisa
(4)	$t_1 = t_3$	T, 2, 3

■

El funtor sucesor El funtor S no tiene ningún axioma asociado, pero su comportamiento está determinado por la regla de inducción. Conviene probar dos reglas de inferencia relacionadas:

$$(I_1)\,\frac{t(Sx) = t(x)}{t(x) = t(0)} \qquad (I_2)\,\frac{s_1(0) = s_2(0) \qquad s_1(Sx) = s_2(Sx)}{s_1(x) = s_2(x)}$$

Demostración: La regla I_1 afirma que si un término toma el mismo valor en cada número natural y en su siguiente, entonces tiene que ser constante. Para probarlo aplicamos la regla de inducción a los términos $s_1(x) \equiv t(x)$, $s_2(x) \equiv t(0)$, $h(x, y) \equiv y$, con lo que se reduce a:

$$\frac{t(0) = t(0) \qquad t(Sx) = t(x) \qquad t(0) = t(0)}{t(x) = t(0)}$$

Vemos que las premisas primera y tercera son un mismo teorema y la segunda es la premisa de I_1, luego, en efecto, la conclusión se deduce dicha premisa.

La regla I_2 se sigue inmediatamente de I_0, usando $h(x,y) \equiv s_2(Sx)$, pues así I_0 se reduce a:

$$\frac{s_1(0) = s_2(0) \qquad s_1(Sx) = s_2(Sx) \qquad s_2(Sx) = s_2(Sx)}{s_1(x) = s_2(x)}$$

de modo que las dos primeras premisas son las premisas de I_2 y la tercera es un teorema. ■

Definición de funtores por términos Veamos ahora que todo término puede usarse para definir un funtor:

Teorema 4.1 *Si $t(x_1,\ldots,x_n)$ es un término cuyas variables están todas entre $x_1,\ldots,x_n$, entonces existe un funtor F_t de rango n tal que*

$$\underset{\mathrm{ARP}}{\vdash} F_t(x_1,\ldots,x_n) = t(x_1,\ldots,x_n).$$

Demostración: Razonamos por inducción sobre la longitud de t. Si $t \equiv 0$, basta tomar $F_0 \equiv \kappa C P_1^n$, pues la definición de F_0 es:

$$F_0(x_1,\ldots,x_n) = C(P_n^1(x_1,\ldots,x_n)),$$

y por otro lado, la definición de C es $C(x) = 0$, luego aplicando S_1 obtenemos

$$C(P_n^1(x_1,\ldots,x_n)) = 0,$$

y finalmente T nos da la igualdad

$$F_0(x_1,\ldots,x_n) = 0.$$

La alternativa es que $t \equiv Ft_1 \cdots t_m$, para cierto funtor F y ciertos términos t_i para los que, por hipótesis de inducción, existen funtores F_{t_i} tales que

$$\underset{\mathrm{ARP}}{\vdash} F_{t_i}(x_1,\ldots,x_n) = t_i(x_1,\ldots,x_n).$$

Basta tomar $F_t \equiv \kappa F f_{t_1} \cdots F_{t_m}$, pues la definición de F_t es

$$F_t(x_1,\ldots,x_n) = F(F_{t_1}(x_1,\ldots,x_n),\ldots,F_{t_m}(x_1,\ldots,x_n)).$$

Si llamamos $\bar{t}_i \equiv F_{t_i}(x_1, l\ldots,t_n)$, tenemos $F_t(x_1,\ldots,x_n) = F(\bar{t}_1,\ldots,\bar{t}_n)$ así como $\bar{t}_i = t_i$, luego aplicando S_2 sucesivamente obtenemos

$$F(\bar{t}_1,\ldots,\bar{t}_n) = F(t_1,\bar{t}_2,\ldots,\bar{t}_n),$$

$$F(t_1,\bar{t}_2,\ldots,\bar{t}_n) = F(t_1,t_2,\bar{t}_3,\ldots,\bar{t}_n),$$

etc., y aplicando T concluimos

$$F_t(x_1,\ldots,x_n) = Ft_1\cdots t_n \equiv t.$$ ■

En principio, todos los funtores definidos por recursión tienen al menos rango 2, pero, con la ayuda del teorema anterior, vamos a ver ahora que también es posible definir funtores de rango 1 de este modo:

Teorema 4.2 *Si t es un designador y H es un funtor de rango 2, existe un funtor F de rango 1 que cumple*

$$F(0) = t, \qquad F(Sx) = H(x, F(x)).$$

Demostración: Por el teorema anterior existe un funtor para el que se cumple $G(y) = t$. Consideramos el funtor de rango 2 con axiomas

$$\bar{F}(y, 0) = G(y), \qquad \bar{F}(y, Sx) = H(x, \bar{F}(y, x)),$$

y a su vez definimos $F(x) = \kappa \bar{F} C P_1^1$. Así $F(x) = \bar{F}(0, x)$, luego

$$F(0) = \bar{F}(0, 0) = G(0) = t, \quad F(Sx) = \bar{F}(0, Sx) = H(x, \bar{F}(0, x)) = H(x, F(x)).$$

■

Recogemos en el teorema siguiente los resultados que acabamos de demostrar, y que recogen la forma más natural de trabajar con los funtores de ARP:

Teorema 4.3 *Se cumple:*

1. *Si $t(x_1, \ldots, x_n)$ es un término cuyas variables están todas entre $x_1, \ldots, x_n$, entonces existe un funtor F_t de rango n tal que*

$$F_t(x_1, \ldots, x_n) = t(x_1, \ldots, x_n).$$

2. *Si $g(x_1, \ldots, x_n)$, $h(x_1, \ldots, x_n, x, y)$ son términos con a lo sumo las variables indicadas, existe un funtor F de rango $n + 1$ que cumple:*

$$F(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n),$$
$$F(x_1, \ldots, x_n, Sx) = h(x_1, \ldots, x_n, x, F(x_1, \ldots, x_n, x)).$$

3. *Si t es un designador y $h(x, y)$ es un término con a lo sumo las variables indicadas, existe un funtor F de rango 1 que cumple*

$$F(0) = t, \qquad F(Sx) = h(x, F(x)).$$

La única variante en 2) y 3) es que en los miembros derechos ponemos términos arbitrarios en vez de funtores, lo cual es lícito gracias a 1), y ello nos evita toda preocupación sobre que el número de variables sea el exigido por el esquema de recursión.

Notemos también que, en 2) el hecho de que la recursión se haga sobre el último argumento de F es anecdótico. Por ejemplo, si queremos que la recursión se haga sobre el primero basta considerar el funtor:

$$F^*(x_1, \ldots, x_{n+1}) = F(P_2^{n+1}(x_1, \ldots, x_{n+1}), \ldots, P_{n+1}^{n+1}(x_1, \ldots, x_{n+1}), P_1^{n+1}(x_1, \ldots, x_{n+1})),$$

que cumple

$$F^*(0, x_1, \ldots, x_n) = g(x_1, \ldots, x_n),$$
$$F^*(Sx, x_1, \ldots, x_n) = h(x_1, \ldots, x_n, x, F^*(x, x_1, \ldots, x_n)).$$

Suma Para familiarizarnos con el funcionamiento de ARP vamos a analizar la formalización de la suma de números naturales. En realidad, todas las funciones que podemos estudiar en ARP "ya están definidas", pues cada funtor tiene su propio nombre, como es el caso del funtor $\rho P_1^1 \kappa S P_3^3$, que hemos considerado como ejemplo en la sección precedente. Cuando digamos que estamos definiendo una función en ARP lo único que hacemos en realidad es darle un nombre más manejable que "su nombre de fábrica". Así, podemos definir la suma como el funtor $+ \equiv \rho P_1^1 \kappa S P_3^3$, y añadir el convenio de que en la práctica escribiremos[2] $(t_1 + t_2) \equiv +t_1 t_2$.

Sin embargo, en la práctica nunca definiremos un funtor exhibiendo "su nombre de fábrica", que será siempre irrelevante a todos los efectos. Lo que haremos será escribir los axiomas asociados al funtor. Así, lo "usual" es definir la suma como el funtor $+$ que cumple las ecuaciones

$$x + 0 = x, \qquad x + Sy = S(x + y).$$

La existencia del funtor suma está justificada por el hecho de que las dos fórmulas anteriores se ajustan al esquema de recursión: definimos $x + 0$ en términos de un funtor de rango 1 actuando sobre x y, aunque $x + Sy$ debería definirse en términos de un funtor de rango 3 actuando sobre x, y, $x + y$, no hay inconveniente en definirlo en términos del funtor S de rango 1, pues ello sólo exige componerlo con la proyección P_3^3 para que formalmente tenga 3 argumentos, aunque en realidad sólo se tenga en cuenta el tercero. En general, nunca debe preocuparnos el uso de un funtor con menos parámetros de los que *a priori* requeriría, pues el número de parámetros siempre se puede aumentar componiendo con proyecciones.

Veamos algunos teoremas relativos a la suma:[3]

1. $Sx = x + 1$,

2. $(x + y) + z = x + (y + z)$,

3. $x + y = y + x$.

DEMOSTRACIÓN: 1) Claramente[4] $x + 1 = x + S0 = S(x + 0) = Sx$.

---

[2] En lo sucesivo aplicaremos tácitamente convenios de notación similares, destinados a facilitar la lectura o adecuar la notación a la acostumbrada.

[3] Cuando no haya confusión posible, representaremos los numerales como 0, 1, 2, ... en lugar de $\bar{0}$, $\bar{1}$, $\bar{2}$, ...

[4] Como hemos señalado al tratar las reglas de inferencia del igualador, éstas nos permiten formalizar cualquier manipulación razonable de igualdades. Por ejemplo, en este caso la igualdad $x + 1 = x + S0$ es realmente una identidad: $x + 1 \equiv x + S0$, luego podemos escribirla por la reflexividad de la igualdad, la segunda sale de aplicar S_1 al axioma $x + Sy = S(x + y)$, sustituyendo $y = 0$ (que es algo que todo matemático hace instintivamente, sin preocuparse de S_1), y la tercera igualdad sale de aplicar S_2 al axioma $x + 0 = x$ (y es también algo que cualquier matemático hace sin dudar). Además, podemos escribir cadenas de igualdades, pues cualquier igualdad entre dos términos de la cadena se justifica por la regla T. En lo sucesivo no detallaremos estos usos de las reglas de sustitución y del igualador.

2) Consideramos los términos

$$s_1(z) \equiv (x+y)+z, \qquad s_2(z) \equiv x+(y+z).$$

El primer axioma de la suma nos da:

$$(x+y)+0 = x+y = x+(y+0),$$

que es lo mismo que $s_1(0) = s_2(0)$. Por otra parte, el segundo nos da:

$$(x+y)+Sz = S((x+y)+z), \quad x+(y+Sz) = x+S(y+z) = S(x+(y+z)),$$

que es lo mismo que $s_1(Sz) = S(s_1(z))$, $s_2(Sz) = S(s_2(z))$. La regla de inducción[5] nos permite concluir $s_1(z) = s_2(z)$.

3) Veamos en primer lugar que $0+x = x$. Razonamos también por inducción, con $s_1(x) \equiv 0+x$ y $s_2(x) \equiv x$. Tenemos

$$s_1(0) = 0+0 = 0 = s_2(0).$$

Por otra parte, $s_1(Sx) = S(0+x)$ y $s_2(Sx) = Sx$, Así $s_1(Sx) = S(s_1(x))$, $s_2(Sx) = S(s_2(x))$, luego la regla de inducción nos da $s_1(x) = s_2(s)$.

Ahora consideramos $s_1(y) = x+Sy$, $s_2(y) = Sx+y$. Entonces

$$s_1(0) = x+S0 = S(x+0) = Sx = Sx+0 = s_2(0).$$

Por otra parte,

$$s_1(Sy) = x+SSy = S(x+Sy) = S(s_1(y)),$$

$$s_2(Sy) = Sx+Sy = S(Sx+y) = S(s_2(y)).$$

La regla de inducción nos da que $x+Sy = Sx+y$.

Finalmente consideramos $s_1(y) = x+y$, $s_2(y) = y+x$. Tenemos que

$$s_1(0) = x+0 = x = 0+x = s_2(0),$$

donde hemos usado el primer teorema que hemos probado en este apartado. Por otra parte,

$$s_1(Sy) = x+Sy = S(x+y) = S(s_1(y)),$$

$$s_2(Sy) = Sy+x = y+Sx = S(y+x) = S(s_2(y)),$$

donde hemos usado el segundo teorema que hemos probado en este apartado. La regla de inducción nos da $s_1(y) = s_2(y)$. ■

[5] El termino $h(z,y)$ es en este caso $h(z,y) \equiv Sy$.

Producto Llamamos *producto* al funtor $\cdot$ determinado por los axiomas[6]

$$x \cdot 0 = 0, \qquad x \cdot Sy = x \cdot y + x.$$

Los teoremas básicos sobre el producto son:

1. $x \cdot 1 = x$,
2. $x \cdot y = y \cdot x$,
3. $x \cdot (y + z) = x \cdot y + x \cdot z$,
4. $x(yz) = (xy)z$.

Demostración: 1) $x \cdot 1 = x \cdot S0 = x \cdot 0 + x = 0 + x = x$.

2) Veamos en primer lugar que $0 \cdot x = 0$. Razonamos por inducción con $s_1(x) = 0 \cdot x$, $s_2(x) = 0$. Entonces

$$s_1(0) = 0 \cdot 0 = 0 = s_2(0).$$

Por otra parte,

$$s_1(Sx) = 0 \cdot Sx = 0 \cdot x + 0 = 0 \cdot x = s_1(x),$$
$$s_2(Sx) = (Sx) \cdot 0 = 0 = s_2(x),$$

luego la regla de inducción nos da la conclusión.

Ahora tomamos $s_1(y) = (Sx) \cdot y$, $s_2(y) = x \cdot y + y$. Entonces

$$s_1(0) = (Sx) \cdot 0 = 0 = 0 + 0 = x \cdot 0 + 0 = s_2(0).$$

Por otro lado[7]

$$s_1(Sy) = (Sx) \cdot Sy = (Sx) \cdot y + Sx = s_1(y) + Sx,$$
$$s_2(Sy) = x \cdot Sy + Sy = x \cdot y + x + Sy = S(x \cdot y + x + y)$$
$$= S(x \cdot y + y + x) = x \cdot y + y + Sx = s_2(y) + Sx.$$

La regla de inducción nos da que $(Sx) \cdot y = x \cdot y + y$.

Finalmente tomamos $s_1(x) = x \cdot y$, $s_2(x) = y \cdot x$. Entonces

$$s_1(0) = 0 \cdot y = 0 = y \cdot 0 = s_2(y).$$
$$s_1(Sx) = Sx \cdot y = x \cdot y + y = s_1(x) + y,$$
$$s_2(Sx) = y \cdot Sx = y \cdot x + y = s_2(x) + y,$$

luego concluimos que $x \cdot y = y \cdot x$.

[6] Es fácil ver que $\cdot \equiv \rho C\kappa{+}P_3^3 P_1^3$, pero esto es irrelevante. Basta comprobar que la definición se ajusta al esquema de recursión.

[7] Notemos que una vez probada la asociatividad de la suma ya no necesitamos distinguir entre términos como $(x \cdot y + y) + Sx$ y $x \cdot y + (y + Sx)$, pues se puede demostrar que son iguales, luego intercambiables, por lo que no hace falta poner paréntesis en las sumas de varios sumandos. Lo mismo valdrá para el producto en cuanto hayamos probado su asociatividad.

3) Tomamos $s_1(z) = x \cdot (y + z)$, $s_2(z) = x \cdot y + x \cdot z$. Entonces

$$s_1(0) = x \cdot (y + 0) = x \cdot y = x \cdot y + 0 = x \cdot y + x \cdot 0 = s_2(0).$$

Por otra parte

$$s_1(Sz) = x \cdot (y + Sz) = x \cdot S(y + z) = x \cdot (y + z) + x = s_1(z) + x,$$

$$s_2(Sz) = x \cdot y + x \cdot Sz = x \cdot y + x \cdot z + x = s_2(z) + x,$$

luego la regla de inducción nos permite concluir. La prueba de 4) es similar. ■

Ahora ya debería estar claro el sentido de todas las definiciones que hemos dado: la aritmética recursiva primitiva está diseñada de modo que sus funtores representan todas las funciones recursivas primitivas, y ya hemos visto cómo podemos trabajar concretamente con dos de ellas: la suma y el producto.

En principio, ARP sólo permite calcular funciones recursivas primitivas y mostrar algunas relaciones entre ellas. Sin embargo, veremos que el potencial que esto ofrece —siendo relativamente modesto en comparación con otras teorías axiomáticas— es mucho mayor de lo que podría parecer a primera vista.

Cálculos explícitos Ahora que hemos visto el funcionamiento de ARP en algunos casos sencillos, vamos a usar las técnicas que hemos empleado para probar algunos resultados generales. No obstante, consideremos antes un ejemplo de la cuestión que vamos a tratar aquí. La fórmula $2 \cdot 3 = 6$ es un teorema de ARP. La demostración es como sigue:

$$\begin{aligned} 2 \cdot 3 &= 2 \cdot 2 + 2 = (2 \cdot 1 + 2) + 2 = ((2 \cdot 0 + 2) + 2) + 2 = ((0 + 2) + 2) + 2 \\ &= S(((0 + 2) + 2) + 1) = SS(((0 + 2) + 2) + 0) = SS((0 + 2) + 2) \\ &= SS((S(0 + 2) + 1)) = SS(SS((0 + 2) + 0)) = SSSS(0 + 2) \\ &= SSSSS(0 + 1) = SSSSSS(0 + 0) = SSSSSS0 = 6. \end{aligned}$$

Podríamos haber abreviado la demostración usando algunos de los teoremas que hemos demostrado sobre la suma y el producto, pero hemos dado una demostración basada exclusivamente en las definiciones de la suma y del producto (y de los numerales). Como el producto se define a partir de la suma y la suma a partir del funtor S, lo que hemos hecho ha sido reducir el cálculo de un producto al cálculo de varias sumas, y el cálculo de las sumas a aplicar varias veces el operador S.

Es fácil convencerse de que en ARP se puede calcular cualquier suma y cualquier producto, pero en realidad sucede algo mucho más general: todas las funciones expresables mediante funtores de ARP se pueden calcular en la práctica, en el sentido de que el resultado se puede reducir a un numeral (no en vano son las funciones recursivas primitivas).

La idea es muy simple: sabemos calcular los funtores S, C y P_i^r y, si sabemos calcular unos funtores, también podemos calcular otro definido a partir de ellos por composición o por recursión. Como todo funtor se define en términos de los funtores S, C y P_i^r mediante un número finito de composiciones y recursiones, concluimos que podemos calcular cualquier funtor. La formalización de esta idea es el teorema siguiente:

Teorema 4.4 *Para cada designador t podemos calcular explícitamente un número natural $n = d(t)$ de modo que $\underset{\text{ARP}}{\vdash} t = \bar{n}$.*

Demostración: Razonamos por inducción sobre la longitud de t. Si $t \equiv 0$ es claro que basta tomar $d(0) = 0$. En otro caso $t \equiv Ft_1 \cdots t_n$, para cierto funtor F. Por hipótesis de inducción podemos calcular explícitamente los números $d_i = d(t_i)$. Ahora razonamos por inducción sobre la longitud de F.

1. Si $F \equiv S$, basta tomar $d(St_1) = d(t_1) + 1$.

2. Si $F \equiv C$, basta tomar $d(Ct_1) = 0$.

3. Si $F \equiv P_i^n$, basta tomar $d(t) = d(t_i)$.

4. Si $F \equiv \kappa G H_1 \cdots H_m$, por hipótesis de inducción podemos calcular
$$e_i = H_i(t_1, \ldots, t_n),$$
de modo que
$$\underset{\text{ARP}}{\vdash} H_i(t_1, \ldots, t_n) = \bar{e}_i,$$
así como $e = d(G(\bar{e}_1, \ldots, \bar{e}_m))$, de modo que
$$\underset{\text{ARP}}{\vdash} G(\bar{e}_1, \ldots, \bar{e}_m) = \bar{e}.$$
Aplicando la regla S_1 llegamos a que
$$\underset{\text{ARP}}{\vdash} F(t_1, \ldots, t_n) = \bar{e},$$
luego $d(t) = e$ cumple lo requerido.

5. Si $F \equiv \rho G H$, podemos calcular
$$e_0 = d(G(t_1, \ldots, t_{n-1})),$$
de modo que $\underset{\text{ARP}}{\vdash} G(t_1, \ldots, t_{n-1}) = \bar{e}_0$. A partir de aquí, podemos ir calculando
$$e_{i+1} = d(H(t_1, \ldots, t_{n-1}, \bar{\imath}, \bar{e}_i)),$$
de modo que $\underset{\text{ARP}}{\vdash} H(t_1, \ldots, t_{n-1}, \bar{\imath}, \bar{e}_i) = \bar{e}_{i+1}$. Por otro lado, por la definición de F, podemos probar
$$F(t_1, \ldots, t_{n-1}, 0) = G(t_1, \ldots, t_{n-1}),$$
$$F(t_1, \ldots, t_{n-1}, Sx) = H(t_1, \ldots, t_{n-1}, x, F(t_1, \ldots, t_{n-1}, x)).$$

La primera igualdad nos da que $F(t_1, \ldots, t_{n-1}, 0) = \bar{e}_0$, y la segunda aplicada a $x = \bar{0}, \bar{1}, \ldots$ nos va dando sucesivamente $F(t_1, \ldots, t_{n-1}, \bar{\imath}) = \bar{e}_i$.

En particular, si $i = d(t_n)$, tenemos que $t_n = \bar{\imath}$, luego

$$F(t_1, \ldots, t_n) = \bar{e}_i,$$

luego $d(t) = e_{d(t_n)}$ cumple lo requerido. ■

4.3 El cálculo proposicional

La lógica de ARP puede parecer excesivamente débil desde el momento en que carece de conectores y cuantificadores, pero vamos a ver que en realidad podemos definirlos aritméticamente. Para ello necesitamos introducir la resta truncada de números naturales:

Resta truncada Consideramos los funtores cuyos axiomas son

$$\mathrm{pre}(0) = 0, \quad \mathrm{pre}(Sx) = x,$$

$$x \dot{-} 0 = x, \qquad x \dot{-} Sy = \mathrm{pre}(x \dot{-} y).$$

La idea subyacente es que el funtor pre resta una unidad a cada número natural no nulo, mientras que la resta truncada es

$$x \dot{-} y = \begin{cases} x - y & \text{si } y \leq x, \\ 0 & \text{si } y > x. \end{cases}$$

Sin embargo, no estamos en condiciones de enunciar estos hechos en APR. Veamos lo que podemos demostrar de momento sobre estos funtores:

1. $x \dot{-} 1 = \mathrm{pre}\, x$.

   En efecto: $x \dot{-} 1 = \mathrm{pre}(x \dot{-} 0) = \mathrm{pre}\, x$.

2. $Sx \dot{-} Sy = x \dot{-} y$.

   Razonamos por inducción:

   $$Sx \dot{-} S0 = \mathrm{pre}(Sx \dot{-} 0) = \mathrm{pre}\, Sx = x = x \dot{-} 0,$$

   $$Sx \dot{-} SSy = \mathrm{pre}(Sx \dot{-} Sy), \qquad x \dot{-} Sy = \mathrm{pre}(x \dot{-} y),$$

   luego la regla de inducción nos da la igualdad.

3. $x \dot{-} x = 0$.

   Podemos aplicar la variante I_1 a $t(x) = x \dot{-} x$. Como $Sx \dot{-} Sx = x \dot{-} x$, la conclusión es $x \dot{-} x = 0 \dot{-} 0 = 0$.

4. $0 \dot{-} x = 0$.

   Razonamos por inducción con $s_1(x) \equiv 0 \dot{-} x$ y $s_2(x) \equiv 0$. Así

$$s_1(0) = 0 \dot{-} 0 = 0 = s_2(0),$$

$$s_1(Sx) = 0 \dot{-} Sx = \mathrm{pre}(0 \dot{-} x) = \mathrm{pre}\, s_1(x),$$

$$s_2(Sx) = 0 = \mathrm{pre}\, 0 = \mathrm{pre}\, s_2(x).$$

5. $(x+y) \dot{-} y = x$.

   Aplicamos I_1 a $t(y) \equiv (x+y) \dot{-} y$. Se cumple que

$$t(Sy) = (x+Sy) \dot{-} Sy = S(x+y) \dot{-} Sy = (x+y) \dot{-} y = t(y),$$

   luego la conclusión es $(x+y) \dot{-} y = (x+0) \dot{-} 0 = x$.

6. $(x+y) \dot{-} x = y$.

   Esto es consecuencia del resultado precedente y de la conmutatividad de la suma.

7. $(x+z) \dot{-} (y+z) = x \dot{-} y$.

   Aplicamos I_1 a $t(z) \equiv (x+z) \dot{-} (y+z)$.

$$t(Sz) = (x+Sz) \dot{-} (y+Sz) = S(x+z) \dot{-} S(y+z) = (x+z) \dot{-} (y+z),$$

   luego $(x+z) \dot{-} (y+z) = (x+0) \dot{-} (y+0) = x \dot{-} y$.

8. $y \dot{-} (x+y) = 0$.

   En efecto, por 7,

$$y \dot{-} (x+y) = (0+y) \dot{-} (x+y) = 0 \dot{-} x = 0.$$

9. $x(1 \dot{-} x) = 0$.

   Por la regla I_2:

$$0 \cdot (1 \dot{-} 0) = 0, \qquad Sx(1 \dot{-} Sx) = Sx(0 \dot{-} x) = Sx \cdot 0 = 0.$$

10. $(1 \dot{-} x)y = y \dot{-} xy$.

    Por inducción respecto de x:

$$(1 \dot{-} 0)y = y = y \dot{-} 0 = y \dot{-} (0 \cdot y),$$

$$(1 \dot{-} Sx)y = (0 - x)y = 0 \cdot y = 0,$$

$$y \dot{-} (Sx) \cdot y = y \dot{-} (y + xy) = 0,$$

    donde en el último paso hemos usado 8.

Finalmente probamos una ecuación que no es fácil de probar en el contexto en que nos encontramos, pero que es la clave para eliminar todas las restricciones técnicas que de momento encontramos en ARP:

Teorema 4.5 $x + (y \dot{-} x) = y + (x \dot{-} y)$.

DEMOSTRACIÓN: Sea $t_1(x, y) \equiv x + (y \dot{-} x)$, de modo que

$$t_1(x, 0) = x, \quad t_1(0, y) = y, \qquad t_1(Sx, Sy) = St_1(x, y).$$

Igualmente, sea $t_2(x, y) \equiv y + (x \dot{-} y)$, de modo que

$$t_2(x, 0) = x, \quad t_2(0, y) = y, \quad t_2(Sx, Sy) = St_2(x, y).$$

En primer lugar demostramos que

$$(x \dot{-} 1) + (1 \dot{-} (1 \dot{-} x)) = x.$$

Aplicamos la regla I_2. Para $x = 0$ se cumple la igualdad, pues

$$(0 \dot{-} 1) + (1 \dot{-} (1 \dot{-} 0)) = 0 + (1 \dot{-} 1) = 0.$$

Por otro lado, usando 2 de la lista precedente,

$$(Sx \dot{-} 1) + (1 \dot{-} (1 \dot{-} Sx)) = x + (1 \dot{-} (0 \dot{-} x)) = x + 1 = Sx,$$

luego I_2 nos permite concluir.

De aquí deducimos a su vez que

$$t_1(x, y) = t_1(x \dot{-} 1, y \dot{-} 1) + (1 \dot{-} (1 \dot{-} (x + y))). \tag{4.1}$$

Aplicamos de nuevo la regla I_2. El miembro derecho en $y = 0$ es

$$t_1(x \dot{-} 1, 0) + (1 \dot{-} (1 \dot{-} x)) = x \dot{-} 1 + (1 \dot{-} (1 \dot{-} x)) = x = t_1(x, 0),$$

por la igualdad que hemos demostrado previamente. Por otra parte,

$$\begin{gathered} t_1(x \dot{-} 1, Sy \dot{-} 1) + (1 \dot{-} (1 \dot{-} (x + Sy))) = \\ t_1(x \dot{-} 1, \operatorname{pre} Sy) + (1 \dot{-} (1 \dot{-} S(x + y))) = \\ t_1(x \dot{-} 1, y) + (1 \dot{-} (0 \dot{-} (x + y))) = \\ t_1(x \dot{-} 1, y) + 1 = St_1(x \dot{-} 1, y). \end{gathered}$$

Por lo tanto, para aplicar I_2 basta demostrar la igualdad

$$t_1(x, Sy) = St_1(x \dot{-} 1, y).$$

Ésta la probamos a su vez aplicando I_2. Para $x = 0$ se reduce a $Sy = Sy$. Además,

$$t_1(Sx, Sy) = St_1(x, y) = St_1(\operatorname{pre} Sx, y) = St_1(Sx \dot{-} 1, y).$$

Esto termina la prueba de (4.1). Ahora consideramos el funtor dado por las ecuaciones

$$F(x,y,0)=0, \quad F(x,y,Sz)=F(x,y,z)+(1 \dot{-} (1 \dot{-} ((x \dot{-} z)+(y \dot{-} z)))).$$

Vamos a demostrar que

$$t_1(x \dot{-} z, y \dot{-} z)+F(x,y,z)=t_1(x \dot{-} Sz, y \dot{-} Sz)+F(x,y,Sz). \tag{4.2}$$

En efecto, por (4.1) tenemos que

$$t_1(x \dot{-} z, y \dot{-} z)+F(x,y,z)=$$

$$t_1((x \dot{-} z) \dot{-} 1, (y \dot{-} z) \dot{-} 1)+F(x,y,z)+(1 \dot{-} (1 \dot{-} ((x \dot{-} z)+(y \dot{-} z))))=$$

$$t_1(x \dot{-} Sz, y \dot{-} Sz)+F(x,y,Sz).$$

Notemos que el miembro derecho de (4.2) resulta de sustituir z por Sz en el miembro izquierdo, luego la regla I_1 nos da que

$$t_1(x \dot{-} z, y \dot{-} z)+F(x,y,z)=t_1(x \dot{-} 0, y \dot{-} 0)+F(x,y,0)=t_1(x,y).$$

Sustituyendo z por y queda

$$t_1(x \dot{-} y, 0)+F(x,y,y)=t_1(x,y),$$

o también:

$$t_1(x,y)=x \dot{-} y+F(x,y,y).$$

Ahora bien, intercambiando los papeles de x e y el mismo razonamiento vale para t_2, y nos lleva hasta

$$t_2(x \dot{-} z, y \dot{-} z)+F(x,y,z)=t_2(x,y).$$

(Notemos que la definición de F es simétrica.) Nuevamente sustituimos z por y, con lo que obtenemos:

$$t_2(x,y)=x \dot{-} y+F(x,y,y),$$

luego $t_1(x,y)=t_2(x,y)$, que es lo que queríamos probar. ■

El valor absoluto Ahora consideramos el funtor dado por

$$|x-y|=(x \dot{-} y)+(y \dot{-} x),$$

para el que se cumplen las dos reglas de inferencia:

$$\frac{s=t}{|s-t|=0} \qquad \frac{|s-t|=0}{s=t}$$

En efecto, la primera es inmediata, mientras que, si suponemos $|s - t| = 0$, tenemos que

$$|s - t| \dot{-} (t \dot{-} s) = 0$$

(porque $0 \dot{-} x = 0$), pero esto es

$$((s \dot{-} t) + (t \dot{-} s)) - (t \dot{-} s) = 0$$

y el teorema 5 del apartado precedente nos da que $s \dot{-} t = 0$. Análogamente (usando el teorema 6) concluimos que $t \dot{-} s = 0$, y el teorema 4.5 nos da entonces que $s = t$.

Algunas propiedades elementales del valor absoluto son:

1. $|x - y| = |y - x|$,
2. $|x - 0| = x$,
3. $|(x + z) - (y + z)| = |x - y|$,
4. $|zx - zy| = z|x - y|$.

Todas ellas se demuestran sin dificultad a partir de las propiedades que hemos demostrado para la resta truncada.

Si $\alpha \equiv s_1 = s_2$ es una fórmula, definimos $t_\alpha \equiv |s_1 - s_2|$. En estos términos, las reglas anteriores se pueden enunciar así:

$$\frac{\alpha}{t_\alpha = 0} \qquad \frac{t_\alpha = 0}{\alpha} \tag{4.3}$$

Los conectores Ahora ya podemos introducir los conectores lógicos. Si α y β son fórmulas, definimos:

$$\neg\alpha \equiv 1 \dot{-} t_\alpha = 0, \qquad \alpha \rightarrow \beta \equiv (1 \dot{-} t_\alpha) \cdot t_\beta = 0.$$

$$\alpha \vee \beta \equiv t_\alpha \cdot t_\beta = 0, \qquad \alpha \wedge \beta \equiv t_\alpha + t_\beta = 0, \qquad \alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha).$$

Escribiremos también $s \neq t \equiv \neg(s = t)$. En términos de estos conectores podemos probar muchas reglas de inferencia de interés. La más notable es el principio general de inducción:

$$(I)\ \frac{\alpha(0) \qquad \alpha(x) \rightarrow \alpha(Sx)}{\alpha(x)}.$$

Demostración: Pongamos que $\alpha(x) \equiv s(x) = t(x)$ y consideremos el funtor que cumple $F(x) = t_\alpha \equiv |s(x) - t(x)|$. Claramente, basta probar la validez de la regla

$$\frac{F(0) = 0 \qquad (1 \dot{-} F(x)) \cdot F(Sx) = 0}{F(x) = 0}.$$

Para ello consideramos el funtor que cumple las ecuaciones

$$G(0) = 1, \qquad G(Sx) = G(x)(1 \dot{-} F(x)).$$

Así:

$$\begin{aligned} G(SSx)) &= G(Sx)(1 \dot{-} F(Sx)) = G(x)(1 \dot{-} F(x))(1 \dot{-} F(Sx)) \\ &= G(x)((1 \dot{-} F(x)) \dot{-} (1 \dot{-} F(x))F(Sx)) = G(Sx), \end{aligned}$$

pues estamos tomando como premisa que $(1 \dot{-} F(x))F(Sx) = 0$. Por I_1 aplicada al término $G(Sx)$ concluimos que $G(Sx) = G(S0) = G(0)(1 \dot{-} F(0)) = 1$, donde hemos usado la premisa $F(0) = 0$. Así pues, $G(Sx) = G(x)(1 \dot{-} F(x)) = 1$, de donde

$$F(x) = G(x)(1 \dot{-} F(x))F(x) = 0,$$

donde hemos usado que $x(1 \dot{-} x) = 0$. ■

Esta regla de inducción sirve de poco si no sabemos manipular los conectores lógicos. Empezamos probando dos reglas de inferencia sobre ellos (*Modus ponendo ponens* e *Introducción del conjuntor*):

$$\text{(MP)}\ \frac{\alpha \qquad \alpha \rightarrow \beta}{\beta} \qquad\qquad \text{(IC)}\ \frac{\alpha \qquad \beta}{\alpha \wedge \beta}$$

DEMOSTRACIÓN: Si suponemos α y $\alpha \rightarrow \beta$, por (4.3) tenemos $t_\alpha = 0$ y, por definición, tenemos $(1 \dot{-} t_\alpha) \cdot t_\beta = 0$, luego $t_\beta = 0$ y, de nuevo por (4.3), concluimos β.

Si suponemos α y β, por (4.3) tenemos $t_\alpha = 0$ y $t_\beta = 0$, luego también $t_\alpha + t_\beta = 0$, pero esto es $\alpha \wedge \beta$. ■

Veamos a continuación algunos teoremas relativos a los conectores:

1. $((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \gamma)) \rightarrow (\alpha \rightarrow \gamma)$.
2. $\neg\neg\alpha \rightarrow \alpha, \qquad \alpha \rightarrow \neg\neg\alpha$.
3. $((\alpha \rightarrow \beta) \wedge \neg\beta) \rightarrow \neg\alpha$.
4. $\alpha \wedge \neg\alpha \rightarrow \beta$.
5. $\alpha \vee \neg\alpha$.
6. $\alpha \rightarrow (\alpha \vee \beta), \qquad \beta \rightarrow (\alpha \vee \beta)$.
7. $(\alpha \vee \alpha) \rightarrow \alpha$.
8. $((\alpha \rightarrow \gamma) \wedge (\beta \rightarrow \gamma)) \rightarrow ((\alpha \vee \beta) \rightarrow \gamma)$.
9. $(\alpha \wedge \beta) \rightarrow \alpha, \qquad (\alpha \wedge \beta) \rightarrow \beta$.
10. $\neg(\alpha \wedge \neg\alpha)$.
11. $((\alpha \wedge \beta) \rightarrow \gamma) \rightarrow (\alpha \rightarrow (\beta \rightarrow \gamma))$.

Demostración:

1) Por definición se trata de la fórmula

$$(1 \dot{-} ((1 \dot{-} t_\alpha) \cdot t_\beta + (1 \dot{-} t_\beta) \cdot t_\gamma)) \cdot (1 \dot{-} t_\alpha) \cdot t_\gamma = 0.$$

Más en general, vamos a demostrar

$$(1 \dot{-} ((1 \dot{-} x) \cdot y + (1 \dot{-} y) \cdot z)) \cdot (1 \dot{-} x) \cdot z = 0.$$

Aplicamos I_2 a la variable x.

1. Para $x = 0$ tenemos que probar

$$(1 \dot{-} (y + (1 \dot{-} y) \cdot z)) \cdot z = 0.$$

Demostraremos esto mediante I_2 aplicado a la variable y:

(a) Para $y = 0$ tenemos que probar

$$(1 \dot{-} z) \cdot z = 0,$$

lo cual ya lo tenemos demostrado.

(b) Para Sy tenemos que probar

$$(1 \dot{-} (Sy + (1 \dot{-} Sy) \cdot z)) \cdot z = 0,$$

pero el miembro izquierdo es $(1 \dot{-} Sy) \cdot z = 0 \cdot z = 0$.

2. Para Sx tenemos que probar

$$(1 \dot{-} ((1 \dot{-} Sx) \cdot y + (1 \dot{-} y) \cdot z)) \cdot (1 \dot{-} Sx) \cdot z = 0,$$

lo cual se cumple porque $1 \dot{-} Sx = 0$.

2) Sustituyendo t_α por una variable arbitraria, tenemos que probar las fórmulas

$$(1 \dot{-} (1 \dot{-} (1 \dot{-} x))) \cdot x = 0, \qquad (1 \dot{-} x) \cdot (1 \dot{-} (1 \dot{-} x))) = 0.$$

Las dos se prueban trivialmente mediante I_2.

3) Basta probar la fórmula

$$(1 \dot{-} ((1 \dot{-} x) \cdot y + (1 \dot{-} y))) \cdot (1 \dot{-} x) = 0.$$

Es inmediato que al sustituir x por Sx en el miembro izquierdo queda 0, luego, por I_2, basta probar que

$$1 \dot{-} (y + (1 \dot{-} y)) = 0,$$

lo cual se prueba trivialmente mediante I_2.

4) Basta probar la fórmula

$$(1 \dot{-} (x + (1 \dot{-} x))) \cdot y = 0,$$

pero el primer factor es nulo, como ya hemos señalado en el apartado precedente.

5 Es consecuencia de la igualdad $x \cdot (1 \dot{-} x) = 0$, que ya tenemos demostrada.

6) Basta probar $(1 \dot{-} x) \cdot x \cdot y = 0$, pero esto se cumple porque $(1 \dot{-} x) \cdot x = 0$.

7) Basta probar $(1 \dot{-} (x \cdot x)) \cdot x = 0$, lo cual se obtiene fácilmente mediante la regla I_2.

8) Basta probar

$$(1 \dot{-} ((1 \dot{-} x) \cdot z + (1 \dot{-} y) \cdot z)) \cdot (1 \dot{-} xy) \cdot z = 0.$$

Aplicamos I_2 respecto de la variable x:

1. Para $x = 0$ tenemos que probar:

   $$(1 \dot{-} (z + (1 \dot{-} y) \cdot z)) \cdot z = 0.$$

   Aplicamos para ello I_2 respecto de la variable y:

   (a) Para $y = 0$ tenemos que probar:

   $$(1 \dot{-} (z + z)) \cdot z = 0.$$

   Aplicamos I_2 respecto de la variable z:

   i. Es inmediato que el miembro izquierdo vale 0 en $z = 0$.

   ii. Para Sz queda:

   $$(1 \dot{-} (Sz + Sz)) \cdot Sz = 0,$$

   lo cual se cumple porque $Sz + Sz = S(Sz + z)$.

   (b) Para Sy queda:

   $$(1 \dot{-} z) \cdot z = 0,$$

   y esto ya lo tenemos demostrado.

2. Para Sx queda:

   $$(1 \dot{-} (1 \dot{-} y) \cdot z) \cdot (1 \dot{-} (Sx) \cdot y) \cdot z = 0.$$

   Lo probamos mediante I_2 respecto de la variable y:

   (a) Para $y = 0$ la ecuación se reduce a $(1 \dot{-} z) \cdot z = 0$, y ya la hemos demostrado.

   (b) Para Sy queda:

   $$(1 \dot{-} (Sx) \cdot Sy) \cdot z = 0,$$

   y esto se cumple porque $(Sx) \cdot (Sy) = (x+1) \cdot (y+1) = S(xy+x+y)$.

9) Basta probar $(1 \dot{-} (x+y)) \cdot x = 0$, lo cual se obtiene inmediatamente mediante I_2.

10) Basta probar $1 \dot{-} (x + (1 \dot{-} x)) = 0$, pero ésta se obtiene inmediatamente con I_2.

11 Basta probar

$$(1 \dot{-} ((1 \dot{-} (x+y)) \cdot z)) \cdot (1-x) \cdot (1-y) \cdot z = 0.$$

Vamos a aplicar la regla I_2. Es claro que al sustituir x por Sx el miembro izquierdo da 0, luego basta probar:

$$(1 \dot{-} ((1 \dot{-} y) \cdot z)) \cdot (1-y) \cdot z = 0.$$

Probamos esto mediante I_2, y de nuevo es claro que el miembro izquierdo vale 0 si cambiamos y por Sy, y en $y=0$ se reduce a $(1 \dot{-} z) \cdot z = 0$, que ya sabemos que es un teorema. ■

Nota Las implicaciones de los teoremas anteriores dan lugar a su vez a reglas de inferencia usando la regla MP y, si es necesario, IC. Por ejemplo, las siguientes son la regla del *modus tollendo tollens,* la del *silogismo hipotético* y la del *dilema:*

$$\text{(MT)}\ \frac{\alpha \to \beta \qquad \neg\beta}{\neg\alpha}, \quad \text{(SH)}\ \frac{\alpha \to \beta \qquad \beta \to \gamma}{\alpha \to \gamma}, \quad \text{(Dil)}\ \frac{\alpha \to \gamma \qquad \beta \to \gamma}{\alpha \vee \beta \to \gamma}$$

■

La regla que se deriva del teorema siguiente no es sino S_2, pero de momento no es trivial que también sea válida como implicación:

Teorema 4.6 $x = y \to s(x) = s(y)$.

DEMOSTRACIÓN: De la regla I_2 (respecto de z) se sigue inmediatamente la fórmula

$$(1 \dot{-} z)s(y+z) = (1 \dot{-} z)s(y).$$

En particular

$$(1 \dot{-} (x \dot{-} y))s(y + (x \dot{-} y)) = (1 \dot{-} (x \dot{-} y))s(y).$$

Multiplicamos ambos miembros por $1 \dot{-} |x-y|$:

$$(1 \dot{-} |x-y|)(1 \dot{-} (x \dot{-} y))s(y + (x \dot{-} y)) = (1 \dot{-} |x-y|)(1 \dot{-} (x \dot{-} y))s(y).$$

Y ahora observamos que

$$(1 \dot{-} |x-y|)(1 \dot{-} (x \dot{-} y)) = 1 \dot{-} |x-y|. \tag{4.4}$$

En efecto:

$$(1 \dot{-} |x-y|)(1 \dot{-} (x \dot{-} y)) = (1 \dot{-} |x-y|) \dot{-} (1 \dot{-} |x-y|)(x \dot{-} y).$$

La fórmula $(1 \dot{-} w)w = 0$ nos da $(1 \dot{-} |x-y|)|x-y| = 0$, que es lo mismo que

$$(1 - |x-y|)(x \dot{-} y) + (1 - |x-y|)(y \dot{-} x) = 0,$$

pero la fórmula $(x+y) \dot{-} y = x$ implica que si una suma es 0, el primer sumando es 0, luego

$$(1 - |x-y|)(x \dot{-} y) = 0,$$

lo que prueba (4.4), y a su vez esto reduce la fórmula anterior a (4.4) hasta

$$(1 \dot{-} |x-y|)s(y + (x \dot{-} y)) = (1 \dot{-} |x-y|)s(y).$$

Por simetría, también podemos demostrar

$$(1 \dot{-} |x-y|)s(x + (y \dot{-} x)) = (1 \dot{-} |x-y|)s(x),$$

y el teorema 4.5 nos da que ambos miembros izquierdos son iguales, luego

$$(1 \dot{-} |x-y|)s(x) = (1 \dot{-} |x-y|)s(y). \tag{4.5}$$

Por consiguiente:

$$|(1 \dot{-} |x-y|)s(x) - (1 \dot{-} |x-y|)s(y)| = 0,$$

pero esto equivale a

$$(1 \dot{-} |x-y|)|s(x) - s(y)| = 0,$$

y esto es, por definición, $x = y \rightarrow s(x) = s(y)$. ■

Las manipulaciones de los conectores lógicos se simplifican drásticamente gracias al teorema siguiente:

Teorema 4.7 (Teorema de deducción) *Si de unas premisas $\alpha_1, \ldots, \alpha_n, \alpha$ podemos deducir una fórmula β y en la deducción no se usan las reglas S_1 o I_0 respecto de variables que aparecen en α, entonces a partir de $\alpha_1, \ldots, \alpha_n$ podemos deducir $\alpha \rightarrow \beta$.*

DEMOSTRACIÓN: Supongamos que tenemos una deducción $\delta_1, \ldots, \delta_m$ con premisas $\alpha_1, \ldots, \alpha_n, \alpha$ que termina con $\delta_m \equiv \beta$. Sea $R = 1 \dot{-} t_\alpha$, que es un término en el que aparecen las mismas variables que en α.

Pongamos que $\delta_i \equiv s_i = t_i$, y vamos a demostrar que $\delta'_i \equiv R \cdot s_i = R \cdot t_i$ es un teorema, para todo i. En particular, para $i = m$ tendremos probado

$$|R \cdot s_m - R \cdot t_m| = 0,$$

de donde se sigue que $R \cdot |s_m - t_m| = 0$, que es lo mismo que $(1 \dot{-} t_\alpha) \cdot t_\beta = 0$, y esto es, por definición, $\alpha \rightarrow \beta$.

Suponemos que tenemos demostraciones de las fórmulas δ'_j para $j < i$ y veamos cómo demostrar δ'_i.

Si $\delta_i \equiv \alpha$, se trata de probar

$$(1 \dot{-} |s_i - t_i|) \cdot s_i = (1 \dot{-} |s_i - t_i|) \cdot t_i = 0,$$

pero esto es un caso particular de la fórmula (4.5), que hemos demostrado en la prueba del teorema 4.6.

Si $s_i = t_i$ es un axioma o una premisa α_j, podemos incluirlo en la deducción como axioma o premisa y de él se sigue $R \cdot s_i = R \cdot t_i$ aplicando la regla S_2 al término $R \cdot x$.

Ahora basta probar que si δ_i se sigue de fórmulas anteriores de la deducción mediante una de las cuatro reglas de inferencia primitivas, entonces δ_i' puede deducirse de las fórmulas correspondientes de la demostración que estamos construyendo. Equivalentemente, basta probar que cada regla de inferencia sigue siendo válida si sus fórmulas se multiplican por R.

- Para la regla S_1 se trata de ver que

$$\frac{R \cdot s_1(x) = R \cdot s_2(x)}{R \cdot s_1(t) = R \cdot s_2(t)}$$

es una regla de inferencia válida, lo cual es cierto (es un caso particular de S_1) siempre y cuando la variable x no aparezca en R, y esto lo tenemos garantizado por la hipótesis del teorema, ya que las variables de R son las de la premisa α y suponemos que en la demostración nunca se usa S_1 respecto de variables presentes en α.

- Para la regla S_2 tenemos que demostrar que

$$\frac{R \cdot t_1 = R \cdot t_2}{R \cdot s(t_1) = R \cdot s(t_2)}$$

es una regla de inferencia válida. Vamos a probar, de hecho, el teorema

$$R \cdot t_1 = R \cdot t_2 \rightarrow R \cdot s(t_1) = R \cdot s(t_2). \tag{4.6}$$

La regla se sigue, entonces, de aplicar MP. En primer lugar observamos que

$$R \cdot t_1 = R \cdot t_2 \rightarrow (R = 0 \lor t_1 = t_2), \tag{4.7}$$

pues, por definición de la implicación, se trata de la fórmula

$$(1 \dot{-} R \cdot |t_1 - t_2|) \cdot R \cdot |t_1 - t_2| = 0,$$

que es un caso particular de $(1 \dot{-} x) \cdot x = 0$.

Por otra parte,

$$R = 0 \rightarrow R \cdot s(t_1) = R \cdot s(t_2),$$

$$t_1 = t_2 \rightarrow R \cdot s(t_1) = R \cdot s(t_2).$$

La primera implicación se debe a que, por definición, es la fórmula

$$(1 \dot{-} R) \cdot R \cdot |s(t_1) - s(t_2)| = 0$$

y sabemos que $(1 \dot{-} R) \cdot R = 0$. La segunda es un caso particular de 4.6, aplicado al término $R \cdot z$, donde z es cualquier variable que no esté en R. Por la regla del dilema, que ya hemos demostrado, concluimos

$$(R = 0 \vee t_1 = t_2) \to R \cdot s(t_1) = R \cdot s(t_2),$$

y la regla del silogismo hipotético aplicada a (4.7) nos da la conclusión (4.6).

- Para la regla T tenemos que demostrar

$$\frac{R \cdot t_1 = R \cdot t_2 \qquad R \cdot t_1 = R \cdot t_3}{R \cdot t_2 = R \cdot t_3}$$

que no es sino un caso particular de T.

- Para la regla I_0 tenemos que probar:

$$\frac{R \cdot s_1(0) = R \cdot s_2(0) \;\; R \cdot s_1(Sx)) = R \cdot h(x, s_1(x)) \;\; R \cdot s_2(Sx) = R \cdot h(x, s_2(x))}{R \cdot s_1(x) = R \cdot s_2(x)}$$

bajo el supuesto de que la variable x no está en R.

Veamos en primer lugar que la regla de inferencia siguiente es válida:

$$\frac{s_1 = t_1 \qquad s_2 = t_2}{s_1 = s_2 \to t_1 = t_2}$$

En efecto, por la regla S_2, de las premisas obtenemos

$$|s_1 - s_2| = |t_1 - s_2|, \qquad |t_1 - s_2| = |t_1 - t_2|,$$

luego por transitividad concluimos que $|s_1 - s_2| = |t_1 - t_2|$. De aquí, por S_2,

$$(1 \dot{-} |s_1 - s_2|) \cdot |t_1 - t_2| = (1 \dot{-} |s_1 - s_2|) \cdot |s_1 - s_2| = 0,$$

y esta última fórmula es $s_1 = s_2 \to t_1 = t_2$.

Por consiguiente, de las premisas de la regla de inducción deducimos

$$R \cdot h(x, s_1(x)) = R \cdot h(x, s_2(x)) \to R \cdot s_1(Sx) = R \cdot s_2(Sx).$$

Por otra parte, un caso particular de (4.6) es:

$$R \cdot s_1(x) = R \cdot s_2(x) \to R \cdot h(x, s_1(x)) = R \cdot h(x, s_2(x)),$$

y, encadenando las dos implicaciones obtenemos

$$R \cdot s_1(x) = R \cdot s_2(x) \to R \cdot s_1(Sx) = R \cdot s_2(Sx).$$

Como también contamos con la premisa $R \cdot s_1(0) = R \cdot s_2(0)$, la regla de inducción general I nos permite concluir $R \cdot s_1(x) = R \cdot s_2(x)$. ■

Nota La restricción sobre el uso de las variables de la hipótesis en la deducción es necesaria para que el teorema de deducción sea válido. Si no la tenemos en cuenta, podríamos "demostrar" cosas como éstas:

(1)	$x = 0$	Hipótesis
(2)	$1 = 0$	S_1, 1 (no permitida)
(3)	$x = 0 \to 1 = 0$	Falso teorema de deducción
(4)	$0 = 0 \to 1 = 0$	S_1, 3
(5)	$0 = 0$	Teorema
(6)	$1 = 0$	MP, 4, 5

(1)	$x = 1$	Hipótesis
(2)	$Sx = 2$	$S_2, 1$
(3)	$0 \cdot (2 \dot{-} 0) = 0$	Teorema
(4)	$Sx \cdot (2 \dot{-} Sx) = 2 \cdot (2 \dot{-} 2)$	$S_2, 2$
(5)	$2 \cdot (2 \dot{-} 2) = 0$	Teorema
(6)	$Sx \cdot (2 \dot{-} Sx) = 0$	$T, 4, 5$
(7)	$x \cdot (2 \dot{-} x) = 0$	$I_2, 3, 6$ (no permitida)
(8)	$x = 1 \to x \cdot (2 \dot{-} x) = 0$	Falso teorema de deducción
(9)	$1 = 1 \to 1 \cdot (2 \dot{-} 1) = 0$	$S_2, 8$
(10)	$1 = 1$	Teorema
(11)	$1 \cdot (2 \dot{-} 1) = 0$	MP 9, 10
(12)	$1 \cdot (2 \dot{-} 1) = 1$	Teorema
(12)	$1 = 0$	T 11, 12

■

Del teorema de deducción se sigue fácilmente una variante de interés:

Teorema 4.8 (Reducción al absurdo) *Si de unas premisas $\alpha_1, \ldots, \alpha_n, \neg\alpha$ podemos deducir una fórmula $\beta \land \neg\beta$ y en la deducción no se usan las reglas S_1 o I_0 respecto de variables que aparecen en α, entonces a partir de $\alpha_1, \ldots, \alpha_n$ podemos deducir α.*

Demostración: Por el teorema de deducción, de $\alpha_1 \ldots, \alpha_n$ se deduce la implicación $\neg\alpha \to (\beta \land \neg\beta)$, pero $\neg(\beta \land \neg\beta)$ es un teorema, luego podemos deducir $\neg\neg\alpha$ y, por consiguiente, α. ■

Igualmente se justifica la variante consistente en suponer α y concluir $\neg\alpha$.

Una aplicación sencilla de la reducción al absurdo es la validez de la regla

$$\frac{\neg\alpha}{\alpha \to \beta}$$

que expresa que una fórmula falsa implica cualquier otra.

Ahora ya podemos demostrar cualquier teorema lógico o cualquier regla de inferencia lógica mediante argumentos lógicos, sin necesidad de reducirlos a argumentos aritméticos como hemos venido haciendo hasta este momento. Por ejemplo, veamos las demostraciones de las reglas de equivalencia entre el disyuntor y el implicador:

$$\frac{\alpha \lor \beta}{\neg\alpha \to \beta} \qquad \frac{\neg\alpha \to \beta}{\alpha \lor \beta}$$

(1)	$\alpha \lor \beta$	Premisa
(2)	$\neg\alpha$	Hipótesis
(3)	α	Hipótesis
(4)	$\neg\beta$	Hipótesis
(5)	$\alpha \land \neg\alpha$	IC 2, 3
(6)	β	R abs.
(7)	$\alpha \to \beta$	
(8)	$\beta \to \beta$	Teorema
(9)	$\alpha \lor \beta \to \beta$	Dil, 7, 8
(10)	β	MP 1, 9
(11)	$\neg\alpha \to \beta$	

(1)	$\neg\alpha \to \beta$	Premisa
(2)	$\neg(\alpha \lor \beta)$	Hipótesis
(3)	$\alpha \to \alpha \lor \beta$	Teorema
(4)	$\neg\alpha$	MT 2, 3
(5)	$\beta \to \alpha \lor \beta$	Teorema
(6)	$\neg\beta$	MT 2, 5
(7)	β	MP 1, 4
(8)	$\alpha \lor \beta$	R abs.

Similarmente podemos probar las leyes de De Morgan, que expresan la equivalencia entre el conjuntor y el disyuntor:

$$\frac{\alpha \land \beta}{\neg(\neg\alpha \lor \neg\beta)} \qquad \frac{\neg(\neg\alpha \lor \neg\beta)}{\alpha \land \beta}$$

(1)	$\neg\alpha$	Hipótesis
(2)	$\alpha \land \beta$	Hipótesis
(3)	α	EC 1
(4)	$\neg(\alpha \land \beta)$	R abs.
(5)	$\neg\alpha \to \neg(\alpha \land \beta)$	
(6)	$\neg\beta$	Hipótesis
(7)	$\alpha \land \beta$	Hipótesis
(8)	β	EC 7
(9)	$\neg(\alpha \land \beta)$	R abs.
(10)	$\neg\beta \to \neg(\alpha \land \beta)$	
(11)	$\neg\alpha \lor \neg\beta \to \neg(\alpha \land \beta)$	Dil 5, 10
(12)	$\alpha \land \beta$	Premisa
(13)	$\neg\neg(\alpha \land \beta)$	DN 12
(14)	$\neg(\neg\alpha \lor \neg\beta)$	MT 11, 13

(1)	$\neg(\neg\alpha \lor \neg\beta)$	Premisa
(2)	$\neg\alpha$	Hipótesis
(3)	$\neg\alpha \lor \neg\beta$	ID, 2
(4)	α	R abs.
(5)	$\neg\beta$	Hipótesis
(6)	$\neg\alpha \lor \neg\beta$	ID, 5
(7)	β	R abs.
(8)	$\alpha \land \beta$	IC 4, 7

En las demostraciones usamos la regla de eliminación del conjuntor (EC), que hemos demostrado en forma de implicación.

No hemos demostrado ningún teorema o regla sobre el bicondicionador $\leftrightarrow$. En la práctica bastan las que se deducen de su definición y de las reglas de introducción y eliminación del conjuntor:

$$\frac{\alpha \to \beta \qquad \beta \to \alpha}{\alpha \leftrightarrow \beta} \qquad \frac{\alpha \leftrightarrow \beta}{\alpha \to \beta,\ \beta \to \alpha}$$

Tautologías El cálculo deductivo de ARP no es semánticamente completo debido a la ausencia de cuantificadores, pero podemos probar que es suficiente para demostrar todas las fórmulas tautológicas, en el sentido que vamos a precisar a continuación.

Si $A(p_1, \ldots, p_n)$ es una fórmula del lenguane $\mathcal{L}_p$ del cálculo proposicional cuyas variables están entre $p_1, \ldots, p_n$ y $\alpha_1, \ldots, \alpha_n$ son fórmulas del lenguaje $\mathcal{L}_{\text{arp}}$ de ARP, podemos definir una fórmula $A(\alpha_1, \ldots, \alpha_n)$ de $\mathcal{L}_{\text{arp}}$ con el criterio obvio:

1. Si $A \equiv p_i$, entonces $A(p_1, \ldots, p_n) \equiv \alpha_i$,
2. Si $A \equiv \neg B$, entonces $A(p_1, \ldots, p_n) \equiv \neg B(p_1, \ldots, p_n)$,
3. Si $A \equiv B \lor C$, entonces $A(p_1, \ldots, p_n) \equiv B(p_1, \ldots, p_n) \lor C(p_1, \ldots, p_n)$,
4. Si $A \equiv B \land C$, entonces $A(p_1, \ldots, p_n) \equiv B(p_1, \ldots, p_n) \land C(p_1, \ldots, p_n)$,
5. Si $A \equiv B \to C$, entonces $A(p_1, \ldots, p_n) \equiv B(p_1, \ldots, p_n) \to C(p_1, \ldots, p_n)$,
6. Si $A \equiv B \leftrightarrow C$, entonces $A(p_1, \ldots, p_n) \equiv B(p_1, \ldots, p_n) \leftrightarrow C(p_1, \ldots, p_n)$.

Una *tautología* en el lenguaje de ARP es una fórmula obtenida de este modo a partir de una tautología del lenguaje del cálculo proposicional.[8]

Por ejemplo,

$$(x = y \land y = z) \to (x = y \to y = z)$$

es una tautología, pero

$$x = y \land y = z \to x = z$$

no lo es.

Teorema 4.9 *Todas las tautologías son teoremas de* ARP.

Demostración: Sea $A(p_1, \ldots, p_n)$ una tautología en $\mathcal{L}_p$ y sean $\alpha_1, \ldots, \alpha_n$ fórmulas de ARP. Tenemos que probar que $A(\alpha_1, \ldots, \alpha_n)$ es un teorema de ARP.

Por simplificar la notación, si $B \equiv B(p_1, \ldots, p_n)$ es cualquier fórmula de $\mathcal{L}_p$ cuyas variables estén entre $p_1, \ldots, p_n$, llamaremos $\bar{B} \equiv B(\alpha_1, \ldots, \alpha_n)$.

Por el teorema 1.9, el secuente $\Rightarrow \bar{A}$ es demostrable en PK, y la prueba muestra que existe una demostración D en la que no se usa la regla de corte, lo que a su vez implica que en ella no aparecen más variables aparte de $p_1, \ldots, p_n$.

Basta probar que si $S \equiv \gamma_1, \ldots, \gamma_k \Rightarrow \delta_1, \ldots, \delta_r$ es un secuente de D, entonces

$$\underset{\text{ARP}}{\vdash} \neg\bar{\gamma}_1 \lor \cdots \lor \neg\bar{\gamma}_k \lor \bar{\delta}_1 \lor \cdots \lor \bar{\delta}_r,$$

pues esto aplicado al secuente final $\Rightarrow A$ de D, nos da que $\underset{\text{ARP}}{\vdash} \bar{A}$, que es lo que pretendemos probar.

[8]Notemos que del mismo modo se pueden definir las tautologías en cualquier lenguaje formal de primer orden.

Los secuentes iniciales de D son de la forma $p_i \Rightarrow p_i$, y la fórmula correspondiente en $\mathcal{L}_{\rm arp}$ es $\neg\alpha_i \lor \alpha_i$, que ciertamente es demostrable en ARP. Por consiguiente, basta demostrar que si las fórmulas correspondientes a los secuentes superiores de una regla de inferencia de PK son teoremas de ARP, lo mismo vale para la fórmula correspondiente al secuente inferior. Esto se comprueba sin dificultad analizando las reglas una a una. Veamos, a modo de ejemplo, el caso de la regla izquierda del disyuntor. Suponemos que

$$\mathop{\vdash}_{\rm ARP} \neg\bar\alpha \lor \neg\bar\gamma_1 \lor \cdots \lor \neg\bar\gamma_k \lor \bar\delta_1 \lor \cdots \lor \bar\delta_r,$$

$$\mathop{\vdash}_{\rm ARP} \neg\bar\beta \lor \neg\bar\gamma_1 \lor \cdots \lor \neg\bar\gamma_k \lor \bar\delta_1 \lor \cdots \lor \bar\delta_r$$

y distinguimos dos casos: si $\neg\bar\gamma_1 \lor \cdots \lor \neg\bar\gamma_k \lor \bar\delta_1 \lor \cdots \lor \bar\delta_r$, entonces

$$\neg(\bar\alpha \lor \bar\beta) \lor \neg\bar\gamma_1 \lor \cdots \lor \neg\bar\gamma_k \lor \bar\delta_1 \lor \cdots \lor \bar\delta_r.$$

Si, por el contrario, $\neg(\neg\bar\gamma_1 \lor \cdots \lor \neg\bar\gamma_k \lor \bar\delta_1 \lor \cdots \lor \bar\delta_r)$ o bien no hay fórmulas colaterales, entonces $\neg\bar\alpha$ y $\neg\bar\beta$, luego $\neg(\bar\alpha \lor \bar\beta)$, luego llegamos a la misma conclusión que en el primer caso. ■

Esto se traduce en que en lo sucesivo no necesitamos preocuparnos por el modo en que aplicamos reglas de inferencia lógicas en ARP: si nos convencemos de que una fórmula α tiene que ser verdadera si unas premisas $\alpha_1, \ldots, \alpha_n$ lo son, sin tener en cuenta para ello el significado de las fórmulas atómicas que las componen, entonces α es demostrable en ARP a partir de dichas premisas (porque la implicación $\alpha_1 \land \cdots \land \alpha_n \to \alpha$ es una tautología).

4.4 La aritmética básica en ARP

Ahora que contamos con el cálculo proposicional estamos en mejores condiciones para explorar qué resultados pueden formalizarse en ARP. En la sección anterior hemos señalado que en la práctica ya podemos "olvidarnos" de la definición aritmética de los conectores lógicos y trabajar con ellos como conectores propiamente dichos. Sin embargo, todavía necesitamos recurrir a la aritmética subyacente para demostrar dos teoremas aritméticos básicos, a saber, las dos primeras afirmaciones del teorema siguiente:

Teorema 4.10 *Las fórmulas siguientes son teoremas de* ARP:

1. $Sx \neq 0$.
2. $Sx = Sy \to x = y$.
3. $x = 0 \lor x = S(x \dot{-} 1)$.
4. $x + z = y + z \to x = y$.
5. $x + y = 0 \leftrightarrow x = 0 \land y = 0$.
6. $xy = 0 \leftrightarrow x = 0 \lor y = 0$.

Demostración: 1) Por definición del negador, $Sx \neq 0$ no es sino la fórmula $1 \dot{-} Sx = 0$, que ya sabemos que es demostrable.

2) Ahora tenemos la fórmula $(1 \dot{-} |Sx - Sy|) \cdot |x \dot{-} y| = 0$, que es equivalente a $(1 \dot{-} |x - y|) \cdot |x \dot{-} y| = 0$, la cual también es demostrable (es un caso particular de $(1 \dot{-} x) \cdot x = 0$).

3) Por inducción sobre x. Para $x = 0$ es trivial y, supuesto cierto para x, tenemos que $(Sx) \dot{-} 1 = (x + 1) \dot{-} 1 = x$, luego $Sx = S(Sx \dot{-} 1)$.

4) Se prueba fácilmente por inducción sobre z.

5) Es inmediato porque si $y \neq 0$, entonces $y = S(y \dot{-} 1)$, luego

$$0 = x + y = S(x + (y \dot{-} 1),$$

en contra de 1), luego $y = 0$ y, por consiguiente, $x = 0$. La otra implicación es obvia.

6) Si $xy = 0$, pero $y \neq 0$, entonces $xy = x(S(y \dot{-} 1)) = x(y \dot{-} 1) + x = 0$, luego $x = 0$ por el resultado precedente. ■

Nota En ARP no tenemos cuantificadores, pero eso no significa que no podamos expresar y demostrar enunciados que ordinariamente expresaríamos con ellos. Por ejemplo, la segunda afirmación del teorema anterior es lo que, si tuviéramos cuantificadores, escribiríamos como $\bigwedge x(Sx = Sy \to x = y)$, mientras que la tercera es lo que más habitualmente expresaríamos en la forma

$$\bigwedge u(u = 0 \vee \bigvee v\, u = Sv).$$

En ARP no tenemos particularizador, pero eso no significa que no podamos expresar enunciados que ordinariamente expresaríamos con él. Lo que sucede es que si queremos afirmar que existe un u que cumple algo, tenemos que construir una función (recursiva primitiva) que calcule ese u, como en este caso es la función $x \dot{-} 1$. ■

Definición 4.11 $x \leq y \equiv x + (y \dot{-} x) = y$.

Si dispusiéramos de particularizador, habríamos definido

$$x \leq y \equiv \bigvee u\, u + x = y,$$

pero al no disponer de él, hemos tenido que decir explícitamente quién es u. Veamos que se trata de una relación de orden:

1. $x \leq x + y$.

   Por la propiedad (6) de la resta truncada.

2. $x \leq x$.

3. $x \leq y \wedge y \leq x \to x = y$.

   Tenemos que $x + (y \dot{-} x) = y$, $y + (x \dot{-} y) = x$, luego

   $$x + (y \dot{-} x) + (x \dot{-} y) = x,$$

   luego $(y \dot{-} x) + (x \dot{-} y) = 0$, luego $x \dot{-} y = 0 = y \dot{-} x$, luego

   $$x = x + (y \dot{-} x) = y.$$

4. $x \leq y \wedge y \leq z \to x \leq z$.

   Tenemos $x + (y \dot{-} x) = y \wedge y + (z \dot{-} y) = z$, luego

   $$x + (y \dot{-} x) + (z \dot{-} y) = z,$$

   luego $x \leq z$ por (1).

5. $0 \leq x$.

6. $x \leq Sx$.

   Pues $x + Sx \dot{-} x = x + ((x + 1) \dot{-} x) = x + 1 = Sx$.

7. $x \leq y \vee y \leq x$.

   Lo probamos por inducción sobre y. Para $y = 0$ es claro. Si vale para y, en el caso $x \leq y$ tenemos $x \leq y \leq Sy$, mientras que si $y \leq x$, entonces $y + (x \dot{-} y) = x$. Si $x \dot{-} y = 0$, entonces $y = x$ y $x \leq Sy$. Si $x \dot{-} y \neq 0$, entonces $y + S((x \dot{-} y) \dot{-} 1)) = x$, luego $Sy + ((x \dot{-} y) \dot{-} 1) = x$, luego $Sy \leq x$ por (1).

8. $y \leq Sx \leftrightarrow y \leq x \vee y = Sx$.

   Si $y \leq Sx$, entonces $y + (Sx \dot{-} y) = Sx$. Si $Sx \dot{-} y = 0$, queda $y = Sx$ y, en caso contrario, $y + S((Sx \dot{-} y) \dot{-} 1) = Sx$, luego $y + ((Sx \dot{-} y) \dot{-} 1) = x$, luego $y \leq x$, por (1).

   Si $y \leq x \vee y = Sx$, en el segundo caso es claro que $y \leq Sx$, mientras que en el primero $y + (x \dot{-} y) = x$, luego $y + S(x \dot{-} y) = Sx$, luego $y \leq Sx$, de nuevo por (1).

9. $x \leq y \leftrightarrow x + z \leq y + z$.

   Si $x \leq y$, entonces $x + (y \dot{-} x) = y$, luego $x + z + (y \dot{-} x) = y + z$, luego $x + z \leq y + z$ por (1).

   Si $x + z \leq y + z$, entonces $x \leq y \vee y \leq x$, pero si se da el segundo caso, por la parte ya probada, $y + z \leq x + z$, luego $x + z = y + z$, luego $x = y$, luego $x \leq y$.

10. $z \neq 0 \wedge xz = yz \to x = y$.

    Podemos suponer que $x \leq y$. Entonces $x + (y \dot{-} x) = y$, luego $xz = (y \dot{-} x)z + yz = xz$, luego $(y \dot{-} x)z = 0$, luego $y \dot{-} x = 0$, luego $x = y$.

11. $x \leq y \rightarrow xz \leq yz$.

    Pues $x + (y \mathbin{\dot{-}} x) = y$, luego $xz + (y \mathbin{\dot{-}} x)z = yz$, luego $xz \leq yz$.

12. $z \neq 0 \land xz \leq yz \rightarrow x \leq y$.

    Se cumple $x \leq y \lor y \leq x$, pero en el segundo caso $yz \leq xz$, luego $yz = xz$, luego $y = x$, luego $x \leq y$.

Definimos $x < y \equiv x \leq y \land x \neq y$. Las propiedades obvias de esta relación se deducen inmediatamente de las propiedades correspondientes de $\leq$.

Potencias Para completar la aritmética básica de los números naturales introducimos la exponenciación mediante el funtor determinado por las ecuaciones:

$$x^0 = 1, \qquad x^{y+1} = x^y \cdot x.$$

Las propiedades siguientes se prueban fácilmente por inducción:

1. $x^{y+z} = x^y x^z$,
2. $(xy)^z = x^z y^z$
3. $(x^u)^z = x^{yz}$.
4. $x > 0 \rightarrow 0^x = 0$.
5. $1^x = x$.
6. $x \leq y \rightarrow x^z \leq y^z$.
7. $x \geq 1 \land y \leq z \rightarrow x^y \leq x^z$.
8. $x \geq 2 \rightarrow y < x^y$.

Veamos la última como ejemplo. Razonamos por inducción sobre y. Para $y = 0$ es inmediato. Supuesto cierto para y, o bien $y = 0$, en cuyo caso se cumple que $y + 1 = 1 < x = x^1 = x^{y+1}$, o bien $y \geq 1$, en cuyo caso

$$x^{y+1} = x^y \cdot x \geq x^y \cdot 2 > y \cdot 2 = y + y \geq y + 1.$$

4.5 Cuantificadores acotados

Veamos ahora que en ARP también podemos definir cuantificadores de la forma $\bigvee u \leq x$, $\bigwedge u \leq x$.

Definición 4.12 Si $\alpha \equiv s_1 = s_2$ es una fórmula de $\mathcal{L}_{\mathrm{arp}}$ cuyas variables estén entre $x_1, \ldots, x_n$, definimos el funtor $\chi_\alpha(x_1, \ldots, x_n) \equiv \chi[\alpha]$ dado por

$$\chi_\alpha(x_1, \ldots, x_n) = 1 \mathbin{\dot{-}} t_\alpha \equiv 1 \mathbin{\dot{-}} |s_1 - s_2|.$$

Así, teniendo en cuenta las reglas (4.3), se cumple que

$$\chi_\alpha(x_1,\ldots,x_n)=1\leftrightarrow\alpha(x_1,\ldots,x_n),$$

$$\chi_\alpha(x_1,\ldots,x_n)=0\leftrightarrow\neg\alpha(x_1,\ldots,x_n).$$

Dada una fórmula $\alpha(x_1,\ldots,x_n,x)$, consideramos el funtor dado por las ecuaciones

$$M_\alpha(x_1,\ldots,x_n,0)=\chi_\alpha(x_1,\ldots,x_n,0),$$

$$M_\alpha(x_1,\ldots,x_n,Sx)=M_\alpha(x_1,\ldots,x_n,x)+$$

$$\chi[M_\alpha(x_1,\ldots,x_n,x)=0\land\chi_\alpha(x_1,\ldots,x_n,Sx)]\cdot(x+2).$$

Notemos que —abreviando $x_1,\ldots,x_n$ como $\bar{x}$— la sucesión

$$M_\alpha(\bar{x},0),M_\alpha(\bar{x},1),M_\alpha(\bar{x},2),\ldots$$

toma el valor 0 hasta que aparece el primer x que cumple $\alpha(\bar{x},x)$, y a partir de ese momento toma el valor $x+1$. Definimos

$$\begin{array}{rcl}\bigvee u\leq x\,\alpha(x_1,\ldots,x_n,u)&\equiv&M_\alpha(x_1,\ldots,x_n,x)\neq 0,\\ \bigwedge u\leq x\,\alpha(x_1,\ldots,x_n,u)&\equiv&\neg\bigvee u\leq x\,\neg\alpha(x_1,\ldots,x_n,u),\\ \mu u\leq x\,\alpha(x_1,\ldots,x_n,u)&=&M_\alpha(x_1,\ldots,x_n,x)\dot{-}1.\end{array}$$

Vamos a comprobar que estas definiciones se comportan como cabe esperar. En los resultados siguientes escribiremos $\alpha(x)$ en lugar de $\alpha(x_1,\ldots,x_n,x)$, es decir, no supondremos que x es la única variable de α.

1. $\mu u\leq x\,\alpha(u)\leq x$.

   Por inducción sobre x. Para $x=0$ tenemos que

   $$\mu u\leq 0\,\alpha(u)=M_\alpha(0)\dot{-}1=\chi_\alpha(0)\dot{-}1=0\leq 0,$$

   pues $\chi_\alpha(0)$ sólo puede valer 0 o 1.

   Si vale para x, distinguimos dos casos:

   Si $M_\alpha(x)\neq 0$, entonces $M_\alpha(Sx)=M_\alpha(x)$, luego

   $$\mu u\leq Sx\,\alpha(u)=\mu u\leq x\,\alpha(u)\leq x\leq Sx.$$

   Si $M_\alpha(x)=0$, entonces

   $$M_\alpha(Sx)=\chi[M_\alpha(x)=0\land\chi_\alpha(Sx)]\cdot(x+2)\leq x+2,$$

   luego $\mu u\leq Sx\,\alpha(u)=M_\alpha(Sx)\dot{-}1\leq(x+2)\dot{-}1=Sx$.

2. $y \leq x \wedge \alpha(y) \rightarrow (\bigvee u \leq x\, \alpha(u) \wedge \mu u \leq x\, \alpha(u) \leq y)$.

   Por inducción sobre x. Para $x = 0$ tenemos $y = 0$, $\alpha(0)$, luego

   $$M_\alpha(x) = \chi_\alpha(0) = 1 \neq 0.$$

   además, $\mu u \leq 0\, \alpha(u) = M_\alpha(0) \dot{-} 1 = 1 \dot{-} 1 = 0$, luego $\mu u \leq 0\, \alpha(u) \leq y$.

   Supuesto para x, si $y \leq Sx \wedge \alpha(y)$, o bien $y \leq x$ o bien $y = Sx$. En el primer caso, por hipótesis de inducción, $\bigvee u \leq x\, \alpha(u)$, es decir, $M_\alpha(x) \neq 0$, luego $M_\alpha(Sx) \neq 0$, luego también se cumple $\bigvee u \leq Sx\, \alpha(u)$.

   Además, $M_\alpha(Sx) = M_\alpha(x)$, luego $\mu u \leq Sx\, \alpha(u) = \mu u \leq x\, \alpha(u) \leq y$.

   Si $y = Sx$, tenemos $\chi_\alpha(Sx) = 1 \neq 0$ luego, o bien $M_\alpha(x) \neq 0$, o bien

   $$\chi[M_\alpha(x) = 0 \wedge \chi_\alpha(Sx)] \cdot (x + 2) \neq 0,$$

   y en ambos casos $M_\alpha(Sx) \neq 0$, luego $\bigvee u \leq Sx\, \alpha(u)$.

   Si $M_\alpha(x) \neq 0$, entonces $M_\alpha(Sx) = M_\alpha(x)$, luego

   $$\mu u \leq Sx\, \alpha(u) = \mu u \leq x\, \alpha(u) \leq x \leq Sx.$$

   Si $M_\alpha(x) = 0$, entonces

   $$M_\alpha(Sx) = \chi[M_\alpha(x) = 0 \wedge \chi_\alpha(Sx)] \cdot (x + 2) = x + 2,$$

   luego $\mu u \leq Sx = Sx \leq y$.

3. $\bigvee u \leq x\, \alpha(u) \rightarrow \alpha(\mu u \leq x\, \alpha(u))$.

   Por inducción sobre x. Para $x = 0$ tenemos $\chi_\alpha(0) = M_\alpha(0) \neq 0$, luego se cumple $\alpha(0)$ y además $\mu u \leq 0\, \alpha(u) = M_\alpha(0) \dot{-} 1 = 1 \dot{-} 1 = 0$, luego se cumple $\alpha(\mu u \leq 0\, \alpha(u))$.

   Si vale para x y $\bigvee u \leq Sx\, \alpha(u)$, entonces $M_\alpha(Sx) \neq 0$. Distinguimos dos casos:

   Si $M_\alpha(x) \neq 0$, entonces $\bigvee u \leq x\, \alpha(u)$, luego por hipótesis de inducción $\alpha(\mu u \leq x\, \alpha(u))$. Además $\mu u \leq x\, \alpha(u) = M_\alpha(x) \dot{-} 1$. En este caso $M_\alpha(Sx) = M_\alpha(x)$, luego $\mu u \leq Sx\, \alpha(u) = \mu u \leq x\, \alpha(u)$, luego $\alpha(\mu u \leq Sx\, \alpha(u))$.

   Si $M_\alpha(x) = 0$, necesariamente

   $$\chi[M_\alpha(x) = 0 \wedge \chi_\alpha(Sx)] \cdot (x + 2) \neq 0,$$

   luego $\chi_\alpha(Sx) = 1$, luego se cumple $\alpha(Sx)$. Además

   $$M_\alpha(Sx) = \chi[M_\alpha(x) = 0 \wedge \chi_\alpha(Sx)] \cdot (x + 2) = x + 2,$$

   luego $\mu u \leq Sx\, \alpha(u) = (x + 2) \dot{-} 1 = Sx$, luego $\alpha(\mu u \leq Sx\, \alpha(u))$.

4. $y \leq x \wedge \bigwedge u \leq x\, \alpha(u) \to \alpha(y)$.
   Supuesto $y \leq x \wedge \bigwedge u \leq x\, \alpha(u)$ y $\neg\alpha(y)$, entonces $\bigvee u \leq x\, \neg\alpha(u)$, luego $\neg\bigwedge u \leq x\, \alpha(u)$ y tenemos una contradicción.

Podemos considerar también las variantes

$$\bigwedge u < x\, \alpha(u) \equiv \bigwedge u \leq x(u < x \to \alpha(u)),$$

$$\bigvee u < x\, \alpha(u) \equiv \bigvee u \leq x(u < x \wedge \alpha(u)),$$

y es fácil probar que cumplen los resultados obvios que cabe esperar que cumplan.

Ahora es fácil probar la regla de inducción completa:

$$\frac{\bigwedge u < x\, \phi(u) \to \phi(x)}{\phi(x)}$$

Demostración: Probamos por inducción que $\psi(x) \equiv \bigwedge u < x\, \phi(u)$. Se cumple trivialmente para $x = 0$ y, si vale para x, por la premisa, tenemos $\phi(x)$, de donde se deduce obviamente que $\bigwedge u < Sx\, \phi(u)$. En particular se cumple $\psi(Sx) \equiv \bigwedge u < Sx\, \phi(u)$, luego haciendo $u = x$ obtenemos $\phi(x)$. ■

4.6 Sucesiones y conjuntos

Para terminar probaremos que en ARP es posible definir sucesiones finitas y conjuntos finitos. Para ello necesitaremos probar algunos resultados aritméticos adicionales.

División euclídea Empezamos demostrando la existencia y unicidad de la división euclídea:

Definición 4.13 Definimos los funtores determinados por

$$c(D, d) = \mu u \leq D\, D < d(u+1), \qquad r(D, d) = D \dot{-} d \cdot c(D, d).$$

Teorema 4.14 *Se cumple:*

1. $d \neq 0 \to D = d \cdot c(D, d) + r(D, d) \wedge r(D, d) < d$.
2. $d \neq 0 \wedge D = d \cdot c + r \wedge r < d \to c = c(D, d) \wedge r = r(D, d)$.

Demostración: 1) Como $d \neq 0$, tenemos que $1 \leq d$, luego

$$D \leq dD < dD + d = d(D+1),$$

y esto prueba que $\bigvee u \leq D\, D < d(u+1)$, luego $D < d \cdot (c(D, d) + 1)$. Tiene que ser $d \cdot c(D, d) \leq D$, pues si fuera $D < d \cdot c(D, d)$, entonces $c(D, d) \neq 0$, luego, llamando $c' \equiv c(D, d) \dot{-} 1$, se cumpliría $c(D, d) = c' + 1$, luego $c' < c(D, d)$ y $D < d \cdot (c' + 1)$, en contra de la minimalidad de $c(D, d)$. Así pues:

$$d \cdot c(D, d) \leq D < d \cdot (c(D, d) + 1).$$

Por la definición de $\leq$, la primera desigualdad implica que

$$D = d \cdot c(D, d) + r(D, d).$$

Tiene que ser $r(D, d) < d$, pues si $d \leq r(D, d)$, entonces

$$d + (r(D, d) \dot{-} d) = r(D, d)$$

y así

$$D = d \cdot c(D, d) + d + (r(D, d) \dot{-} d) = d \cdot (c(D, d) + 1) + (r(D, d) \dot{-} d),$$

luego $d \cdot (c(D, d) + 1) \leq D$, contradicción.

2) Tenemos que $dc \leq D = dc+r < dc+d = d(c+1)$, luego la minimalidad de $c(D, d)$ implica que $c(D, d) \leq c$. Si la desigualdad fuera estricta, $c(D, d)+1 \leq c$, luego

$$D < d(c(D, d) + 1) \leq dc \leq dc + r = D,$$

y tenemos una contradicción. Por lo tanto, $c = c(D, d)$, y como

$$d \cdot c(D, d) + r(D, d) = D = d \cdot d + r = d \cdot c(D, d) + r,$$

también $r = r(D, d)$. ■

Por ejemplo, ahora podemos clasificar a los números naturales en *pares* e *impares,* según si $r(D, 2) = 0$ o $r(D, 2) = 1$. Equivalentemente, por la unicidad de la división euclídea, los números pares son los de la forma $2n$ y los impares los de la forma $2n + 1$. Es fácil probar que

$$r(ab, 2) = r(a, 2)r(b, 2),$$

de modo que el producto de par por par o par por impar es par, mientras que el producto de impares es impar.

Sucesiones finitas Veamos cómo podemos tratar en APR con sucesiones finitas de números naturales. Empezamos estudiando los pares ordenados:

Definición 4.15 Definimos el funtor

$$\langle x, y\rangle_2 = c((x + y)(x + y + 1), 2) + x,$$

donde $c(D, d)$ es el cociente de la división euclídea de D entre d.

Es fácil ver que la división es exacta,[9] de modo que

$$2\langle x, y\rangle_2 = (x + y)(x + y + 1) + 2x.$$

Observemos ahora que

$$(z + 1)(z + 2) = 2^2 + 3z + 2 \geq 2z + 2 > 2z.$$

Por lo tanto, si definimos el funtor

$$F(z) = \mu u \leq z + 1(2z < u(u + 1)),$$

tenemos que $z + 1$ cumple la propiedad considerada, luego

$$2z < F(z)(F(z) + 1) \qquad \text{y} \qquad F(z) \leq z + 1.$$

No puede ser $F(z) = 0$, luego si definimos $G(z) = F(z) \dot{-} 1$, se cumple que $F(z) = G(z)+1$ y, como $G(z) < F(z)$, no puede cumplir la propiedad que define a F, luego

$$G(z)(G(z) + 1) \leq 2z < (G(z) + 1)(G(z) + 2), \qquad G(z) \leq z.$$

Observemos además que si un r cumple

$$r(r + 1) \leq 2z < (r + 1)(r + 2),$$

necesariamente $r = G(z)$, pues por la minimalidad de F tenemos $F(z) \leq r + 1$, luego $G(z) \leq r$ y, si la desigualdad fuera estricta, $G(z) \leq r$, luego

$$(G(z) + 1)(G(z) + 2) \leq r(r + 1) \leq 2z,$$

y tenemos una contradicción.

Definimos el funtor

$$z_1 = c(2z \dot{-} G(z)(G(z) + 1), 2).$$

Es fácil ver que el argumento de c es par, por lo que

$$2z = G(z)(G(z) + 1) + 2z_1.$$

Además se cumple que $z_1 \leq G(z)$, pues si fuera $G(z) < z_1$, entonces

$$2G(z) < 2z_1 = 2z \dot{-} G(z)(G(z) + 1) = 2z - G(z)^2 - G(z),$$

luego $G(z)^2+3G(z) < 2z$, luego $G(z)^2+3G(z)+1 \leq 2z$. Otra vez, distinguiendo casos según si $G(z)$ es par o impar, se comprueba que el miembro izquierdo siempre es impar, por lo que no puede darse la igualdad, luego

$$(G(z) + 1)(G(z) + 2) = G(z)^2 + 3G(z) + 2 \leq 2z,$$

[9] Porque el dividendo es necesariamente el producto de un número par por un impar, luego es par.

en contradicción con la construcción de G. Por lo tanto, $z_1 \leq G(z)$, luego el funtor

$$z_2 = G(z) \dot{-} z_1$$

cumple $G(z) = z_1 + z_2$ y

$$2z = G(z)(G(z)+1) + 2z_1 = (z_1+z_2)(z_1+z_2+1) + 2z_1 = 2\langle z_1, z_2\rangle_2 \,,$$

luego $z = \langle z_1, z_2\rangle_2$.

El teorema siguiente recoge las propiedades que hemos demostrado de los funtores $\langle x, y\rangle_2$, z_1 y z_2 junto con algunas más:

Teorema 4.16 *Se cumple:*

1. $z = \langle z_1, z_2\rangle_2$,
2. $z_1 + z_2 \leq z$,
3. $z = \langle x, y\rangle_2 \to x = z_1 \land y = z_2$.

Demostración: Ya hemos demostrado la primera afirmación, y también la segunda, pues hemos visto que $z_1 + z_2 = G(z) \leq z$.

Si $z = \langle x, y\rangle_2$, llamando $r = x + y$, tenemos que $2z = r(r+1) + 2x$, con $x \leq r$, luego

$$r(r+1) \leq 2z \leq r^2 + r + 2x \leq r^2 + 3r < r^2 + 3r + 2 = (r+1)(r+2),$$

y antes hemos probado que esto implica $r = G(z) = z_1 + z_2$, luego

$$(z_1+z_2)(z_1+z_2+1) + 2z_1 = 2z = r(r+1) + 2x$$

implica que $2x = 2z_1$, luego $x = x_1$, y entonces $z_1 + z_2 = x + y$ implica que $y = z_2$. ■

Con esto hemos probado que cada número natural z se expresa de forma única como un par $\langle z_1, z_2\rangle_2$ de números naturales. Tanto la función que a cada par de números naturales le asigna el número $\langle z_1, z_2\rangle_2$ como las proyecciones que a cada z le asignan sus coordenadas z_1 y z_2 son funciones recursivas primitivas.

Similarmente podemos considerar el funtor

$$\langle x, y, z\rangle_3 = \langle \langle x, y\rangle_2 \,, z\rangle_2$$

y las proyecciones $z_1^3 = (z_1)_1$, $z_2^3 = (z_1)_2$, $z_z^3 = z_2$, de modo que

$$z = \langle z_1, z_2, z_3\rangle \,, \qquad z = \langle u, v, w\rangle_3 \to u = z_1 \land v = z_2 \land w = z_3.$$

Así, podemos identificar los números naturales con las ternas de números naturales.

En general, podemos definir los funtores

$$\langle x_1,\ldots,x_n\rangle_n = \big\langle \langle x_1,\ldots,x_{n-1}\rangle_{n-1}, x_n\big\rangle_2$$

y las proyecciones[10]

$$\begin{array}{rcll} p_i^n(z) & = & p_i^{n-1}(z_1), & \text{para } i<n \\ p_n^n(z) & = & z_2. & \end{array}$$

Si definimos $\langle x\rangle_1 = x$, estas definiciones coinciden con las que ya teníamos en el caso $n=2$.

Razonando por inducción sobre n, se prueba sin dificultad que

$$z = \langle p_1^n(z),\ldots,p_n^n(z)\rangle_n, \quad z=\langle x_1,\ldots,x_n\rangle_n \to x_1 = z_1 \land \cdots \land x_n = z_n.$$

Ejemplo Un simple cálculo nos da que

$$\langle 3,1\rangle_2 = 13, \quad \langle 3,1,5\rangle_3 = \langle 13,5\rangle_2 = 184,$$

de modo que el número 184 puede verse como él mismo, o como el par $\langle 13,5\rangle_2$ o como la terna $\langle 3,1,5\rangle_3$.

En general, cada número natural n puede verse indistintamente como un número (él mismo), como un par de números, o una terna, o una cuádrupla, etc. Por ejemplo, el número $n = 17\,337\,210$ puede verse como

$$17\,337\,210, \quad (5\,882,5), \quad (104,3,5), \quad (13,0,3,5), \quad (3,1,0,3,5),$$

$$(0,2,1,0,3,5), \quad (0,0,2,1,0,3,5), \quad (0,0,0,2,1,0,3,5),\ldots$$

Para evitar que un mismo número pueda verse como muchas cosas a la vez, podemos definir una nueva familia de infinitos funtores:

$$\langle x_1,\ldots,x_n\rangle_\infty^n = \langle n-1, \langle x_1,\ldots,x_n\rangle_n\rangle_2 + 1.$$

Así, cada número natural no nulo s codifica una única sucesión. Para calcularla, pasamos a $s \dot{-} 1$, intepretamos el resultado como un par y la primera componente $+1$ nos indica la longitud n de la sucesión codificada, y ésta es la segunda componente interpretada precisamente como sucesión de longitud n.

Más precisamente, definimos la *longitud* de un número natural como

$$\ell(s) = (1 \dot{-} (1 \dot{-} s))(s_1+1).$$

Así, $\ell(0)=0$, mientras que si $s\neq 0$, entonces $\ell(s)>0$ y $s_1 = \ell(s)\dot{-}1$.

[10] Notemos que no hemos definido un funtor $\langle x_1,\ldots,x_n\rangle_n$ de rango $n+1$, sino infinitos funtores de rango n. Igualmente, la definición de las proyecciones no es la definición de un único funtor $p_i^n(z)$ de rango 3, sino que estamos definiendo infinitos funtores de rango 1, cada uno con su propia definición.

Para definir las proyecciones definimos primero el funtor

$$R(s,0) = (s \dot{-} 1)_2, \qquad R(s,i+1) = R(s,i)_1.$$

$$p_i^\infty(s) = (1 \dot{-} i)R(s,(s \dot{-} 1)_1) + (1 \dot{-} (1 \dot{-} i))R(s,(s \dot{-} 1)_1 \dot{-} i)_2.$$

Notemos que $p_i^\infty(s)$ es un funtor de rango 2, es decir, que ahora no tenemos infinitos funtores de rango 1, sino que tanto i como s son argumentos de un mismo funtor.

Ejemplo Si $s = \langle 3,2,7\rangle_\infty = \big\langle 2, \langle\langle 3,2\rangle_2, 7\rangle_2\big\rangle_2 + 1$, tenemos que

$$R(s,0) = \langle\langle 3,2\rangle_2, 7\rangle_2, \quad R(s,1) = \langle 3,2\rangle_2, \quad R(s,2) = 3,$$

luego $p_0^\infty(s) = R(s,2) = 3$, $p_1^\infty(s) = R(s,1)_2 = 2$, $p_2^\infty(s) = R(s,0)_2 = 7$. ■

Nota A partir de ahora escribiremos $s_i \equiv p_i^\infty(s)$. ■

Notemos que $\ell(s) \leq s$ y $\bigwedge i < \ell(s)\, s_i \leq s$.

Veamos que todo número natural, visto como sucesión, está unívocamente determinado por sus proyecciones.

Teorema 4.17 $\ell(s) = \ell(t) \land (\bigwedge i < \ell(s)\, s_i = t_i) \to s = t.$

Demostración: Si $\ell(s) = \ell(t) = 0$, entonces $s = t = 0$. Supongamos que $\ell(s) = \ell(t) > 0$. Entonces

$$l = (s \dot{-} 1)_1 = \ell(s) \dot{-} 1 = \ell(t) \dot{-} 1 = (t \dot{-} 1)_1.$$

Veamos por inducción que

$$i \leq l \to R(s, l \dot{-} i) = R(t, l \dot{-} i).$$

Para $i = 0$ tenemos que

$$R(s,l) = s_0 = t_0 = R(t,l).$$

Si es cierto para $i < l$, entonces $i+1 \leq l$, luego $i + 1 + (l \dot{-} (i+1)) = l$, de donde $(l \dot{-} (i+1)) + 1 = l \dot{-} i$. Por lo tanto,

$$R(s,l\dot{-}(i{+}1))_1 = R(s,(l\dot{-}(i{+}1)){+}1) = R(s,l\dot{-}i) = R(t,l\dot{-}i) = R(t,l\dot{-}(i{+}1))_1.$$

Por otra parte,

$$R(s, l \dot{-} (i+1))_1 = s_{i+1} = t_{i+1} = R(t, l \dot{-} (i+1))_1,$$

luego $R(s,l\dot{-}(i{+}1)) = R(t,l\dot{-}(i{+}1))$. Esto completa la inducción y, aplicándolo a $i = l$ obtenemos

$$(s \dot{-} 1)_2 = R(s,0) = R(t,0) = (t \dot{-} 1)_2,$$

pero $(s \dot{-} 1)_1 = l = (t \dot{-} 1)_1$, luego de hecho $s \dot{-} 1 = t \dot{-} 1$, luego $s = t$. ■

Notemos que, aunque aparentemente hemos hecho que el 0 no codifique a ninguna sucesión, en realidad no es así, sino que las definiciones que hemos dado nos permiten considerar que 0 representa a la sucesión vacía, es decir, una sucesión de longitud 0 que no tiene ningún término.

Ejemplo La tabla siguiente muestra la interpretación como sucesiones de los 40 primeros números naturales:

0		10	$0,0,0,0$	20	$0,0,0,0,1$	30	$0,3$
1	0	11	4	21	$0,0,0,0,0,0$	31	$1,0,0$
2	1	12	$0,2$	22	6	32	$0,0,1,1$
3	$0,0$	13	$0,1,0$	23	$2,0$	33	$0,0,0,0,2$
4	2	14	$0,0,0,1$	24	$0,1,1$	34	$0,0,0,0,1,0$
5	$0,1$	15	$0,0,0,0,0$	25	$0,0,0,2$	35	$0,0,0,0,0,0,1$
6	$0,0,0$	16	5	26	$0,0,0,1,0$	36	$0,0,0,0,0,0,0,0$
7	3	17	$1,1$	27	$0,0,0,0,0,1$	37	8
8	$1,0$	18	$0,0,2$	28	$0,0,0,0,0,0,0$	38	$1,2$
9	$0,0,1$	19	$0,0,1,0$	29	7	39	$0,0,3$

Por ejemplo, para calcular la sucesión asociada al número 352 889 465, como no es 0, le restamos 1 y lo interpretamos como par:

$$352\,889\,464 = \langle 3, 26\,563\rangle_2\,,$$

lo que nos indica que debemos interpretar el número 26 563 como una sucesión de longitud 4, la cual resulta ser $3, 2, 2, 1$.

A partir de ahora, cuando hablemos de la sucesión $3, 2, 2, 1$, entenderemos que no es sino una forma de referirnos al número natural 352 889 465. ■

Una comprobación rutinaria muestra que

$$p_i^\infty(\langle x_0, \ldots, x_{n-1}\rangle_\infty^n) = x_i,$$

lo que muestra que toda sucesión finita de números naturales está codificada por un número natural. En la práctica podemos omitir el superíndice n en el funtor $\langle x_0, \ldots, x_{n-1}\rangle_\infty^n$, puesto que éste se deduce del número de argumentos.

No debemos confundir un número natural n con la sucesión de longitud 1 que lo tiene como único término. Ésta viene dada por el funtor

$$\langle n\rangle_\infty = \langle 0, n\rangle_2 + 1.$$

Definición 4.18 Diremos que una sucesión t extiende a otra s si

$$s \sqsubseteq t \equiv \ell(s) \leq \ell(t) \land \bigwedge i < \ell(s)\, s_i = t_i.$$

Es fácil ver que:

1. $s \sqsubseteq s$,

2. $s \sqsubseteq t \wedge t \sqsubseteq s \rightarrow s = t$,

3. $s \sqsubseteq t \wedge t \sqsubseteq u \rightarrow s \sqsubseteq u$,

4. $0 \sqsubseteq s$.

Definimos

$$s^\frown\langle n\rangle = (1 \dot{-} s)\,\langle n\rangle_\infty + (1 \dot{-} (1 \dot{-} s))(\langle \ell(s), \langle (s \dot{-} 1)_2, n\rangle_2\rangle_2 + 1).$$

Una comprobación rutinaria muestra que

$$\ell(s^\frown\langle n\rangle) = \ell(s) + 1, \quad s \sqsubseteq s^\frown\langle n\rangle\,, \quad (s^\frown\langle n\rangle)_{\ell(s)} = n.$$

Vemos así que $s^\frown\langle n\rangle$ no es sino la sucesión que resulta de añadir n como último término a la sucesión representada por s. Más en general, definimos

$$s^\frown t = F(s, t, \ell(t)),$$

donde F es el funtor dado por

$$F(s, t, 0) = s, \qquad F(s, t, n + 1) = F(s, t, n)^\frown \langle t_n\rangle\,.$$

De nuevo una comprobación rutinaria muestra que

$$\ell(s^\frown t) = \ell(s) + \ell(t), \quad \bigwedge i < \ell(s)(s^\frown t)_i = s_i, \quad \bigwedge i < \ell(t)\,(s^\frown t)_{\ell(s)+i} = t_i.$$

En particular, $s \sqsubseteq s^\frown t$.

Definimos la restricción de una sucesión mediante el funtor dado por

$$s|_0 = 0, \qquad s|_{i+1} = s|_i{}^\frown \langle s_i\rangle\,.$$

Es fácil probar que $i \leq \ell(s) \rightarrow \ell(s|_i) = i \wedge s|_i \sqsubseteq s$. Más aún, si $t \sqsubseteq s$, entonces $t = s|_{\ell(t)}$.

Similarmente definimos $s|^i = F(s, i, \ell(s) \dot{-} i)$, donde

$$F(s, i, 0) = s_i, \qquad F(s, i, n + 1) = F(s, i, n)^\frown \langle s_{i+n}\rangle\,.$$

Así, si $i \leq \ell(s)$, se cumple que $\ell(s|^i) = \ell(s) \dot{-} i$ y $s = s|_i{}^\frown s|^i$.

A partir de este momento ya no usaremos más los funtores $\langle x_1, \ldots, x_n\rangle_n$ ni sus proyecciones correspondientes, sino que siempre que hablemos de sucesiones de números naturales consideraremos los funtores $\langle x_1, \ldots, x_n\rangle_\infty$ y las proyecciones dadas por el funtor $p_i^\infty(s)$, de rango 2.

Si $F(x_1, \ldots, x_{n+1})$ es un funtor de rango $n + 1$, podemos definir a partir de él otro funtor igualmente de rango $n + 1$ dado por

$$F|_0(x_1, \ldots, x_n) = 0,\ F|_{x+1}(x_1, \ldots, x_n) = F|_x(x_1, \ldots, x_n)^\frown\langle F(x_1, \ldots, x_n, x)\rangle\,.$$

Es claro que $\ell(F|_x(x_1, \ldots, x_n)) = x$ y

$$\bigwedge i < x\, F|_x(x_1, \ldots, x_n)_i = F(x_1, \ldots, x_n, i).$$

Teorema 4.19 (Recursión completa) *Si G es un funtor de rango $n+2$, existe un funtor F de rango $n+1$ tal que*

$$F(x_1,\ldots,x_n,x) = G(x_1,\ldots,x_n,x,F|_x(x_1,\ldots,x_n)).$$

Demostración: Definimos un funtor H mediante

$$\begin{aligned} H(x_1,\ldots,x_n,0) &= 0,\\ H(x_1,\ldots,x_n,x+1) &= H(x_1,\ldots,x_n,x)^\frown\langle G(x_1,\ldots,x_n,x,H(x_1,\ldots,x_n,x))\rangle\,. \end{aligned}$$

Y a su vez,

$$F(x_1,\ldots,x_n,x) = H(x_1,\ldots,x_n,x+1)_x.$$

Veamos que F cumple lo requerido. Por aligerar la notación escribiremos $\bar{x}$ en lugar de $x_1,\ldots,x_n$. En primer lugar, una simple inducción nos da que $\ell(H(\bar{x},x)) = x$. En segundo lugar, $H(\bar{x},x) = F|_x(\bar{x})$. En efecto, para $x=0$ es

$$H(\bar{x},0) = 0 = F|_0(\bar{x}),$$

y si vale para x, entonces, como $\ell(H(\bar{x},x+1)) = x+1$, la definición de H implica que

$$H(\bar{x},x+1) = H(\bar{x},x)^\frown\langle H(\bar{x},x+1)_x\rangle\,,$$

luego por la hipótesis de inducción y la definición de F:

$$H(\bar{x},x+1) = F|_x(\bar{x})^\frown\langle F(\bar{x},x)\rangle = F|_{x+1}(\bar{x}).$$

Finalmente probamos por inducción que F cumple la propiedad del enunciado:

$$\begin{aligned} F(\bar{x},0) &= H(\bar{x},1)_0 = G(\bar{x},0,0) = G(\bar{x},0,F|_0(\bar{x})),\\ F(\bar{x},x+1) &= H(\bar{x},x+2)_{x+1} = G(\bar{x},x+1,H(\bar{x},x+1)) = G(\bar{x},x+1,F|_{x+1}(\bar{x})). \end{aligned}$$

■

Sumas finitas Ahora que ya sabemos manipular sucesiones finitas en ARP, pasamos a estudiar las sumas finitas:

Definición 4.20 Si $t(x_1,\ldots,x_n)$ es un término cuyas variables estén entre las indicadas, definimos un funtor de rango n mediante las ecuaciones:

$$\begin{aligned} \sum_{i<x} t(x_1,\ldots,x_{n-1},i) &= 0\\ \sum_{i<x+1} t(x_1,\ldots,x_{n-1},i) &= \sum_{i<x} t(x_1,\ldots,x_{n-1},i) + t(x_1,\ldots,x_{n-1},x). \end{aligned}$$

Escribiremos también:

$$\sum_{i\leq x} t(x_1,\ldots,x_{n-1},i) = \sum_{i<x+1} t(x_1,\ldots,x_{n-1},i).$$

Los hechos siguientes se demuestran fácilmente por inducción sobre x (por simplicidad omitimos los parámetros que no son relevantes en el enunciado de las propiedades):

1. $\sum\limits_{i<x} t_1(i) + \sum\limits_{i<x} t_2(i) = \sum\limits_{i<x} (t_1(i) + t_2(i))$.
2. $\sum\limits_{i<x} y \cdot t(i) = y \sum\limits_{i<x} t(i)$.
3. $\sum\limits_{i<y+x} t(i) = \sum\limits_{i<y} t(i) + \sum\limits_{i<x} t(y+i)$.
4. $\bigwedge i < x\, t_1(i) \leq t_2(i) \to \sum\limits_{i<x} t_1(i) \leq \sum\limits_{i<x} t_2(i)$.
5. $\sum\limits_{i<x} t(i) = 0 \to \bigwedge i < x\, t(i) = 0$.

Desarrollos decimales Hasta ahora, cuando hemos escrito números como 184, teníamos que entender que 184 no era más que una forma de abreviar un numeral compuesto por 184 funtores S seguidos de un 0. Sin embargo ahora podemos formalizar en ARP el concepto de desarrollo decimal que nos permite interpretar 184 como lo que expresa realmente. Empezamos introduciendo las definiciones necesarias:

Definición 4.21 Consideremos el funtor dado por

$$s_{(d)} = \sum_{i<\ell(s)} s_i d^i.$$

Un *desarrollo decimal en base* d de un número natural x es una sucesión finita s tal que $\bigwedge i < \ell(s)\, s_i < d$ y $x = s_{(d)}$. Diremos que se trata de un desarrollo *reducido* si $\ell(s) = 0$ (lo cual sólo puede suceder si $x = 0$) o bien $\ell(s) > 0$ y $s_{\ell(s) \dot{-} 1} \neq 0$.

Vamos a demostrar que cada número natural admite un desarrollo decimal en cualquier base $d \geq 2$ y que éste es único si exigimos que sea reducido.

Empezamos considerando el funtor dado por las ecuaciones

$$\begin{aligned} F(x, d, 0) &= \langle c(x, d), r(x, d)\rangle, \\ F(x, d, i+1) &= \langle c(F(x, d, i)_0, d), r(F(x, d, i)_0, d)\rangle. \end{aligned}$$

donde c y r son los funtores que calculan el cociente y el resto de la división euclídea. Definimos $x_i^*[d] = F(x, d, i)_0$, $x_i[d] = F(x, d, i)_1$. Así

$$x = x_0^*[d] \cdot d + x_0[d], \qquad x_i^*[d] = x_{i+1}^*[d] \cdot d + x_{i+1}[d],$$

con $x_i[d] < d$, para todo i. De aquí se sigue que

$$x = x_n^*[d] \cdot d^{n+1} + \sum_{i \leq n} x_i[d] \cdot d^i.$$

En efecto, razonamos por inducción sobre n. Para $n = 0$ es inmediato y, si vale para n,

$$\begin{aligned} x &= x^*_n[d] \cdot d^{n+1} + \sum_{i \leq n} x_i[d] \cdot d^i \\ &= (x^*_{n+1}[d] \cdot d + x_{n+1}[d]) \cdot d^{n+1} + \sum_{i \leq n} x_i[d] \cdot d^i \\ &= x^*_{n+1}[d] \cdot d^{n+2} + x_{n+1}[d] \cdot d^{n+1} + \sum_{i \leq n} x_i[d] \cdot d^i \\ &= x^*_{n+1}[d] \cdot d^{n+2} + \sum_{i \leq n+1} x_i[d] \cdot d^i. \end{aligned}$$

Si $d \geq 2$ tenemos que $x < d^{x+1}$, luego $x^*_x[d] = 0$, pues de lo contrario la expresión que acabamos de probar nos daría que $d^{x+1} \leq x$. Por consiguiente,

$$x = \sum_{i \leq x} x_i[d] \cdot d^i.$$

Con esto ya hemos probado que todo número natural admite un desarrollo decimal en base d. Vamos a afinar un poco la construcción para quedarnos con uno reducido. Definimos

$$N_d(x) = \mu u \leq x + 1\ x = \sum_{i < u} x_i[d] \cdot d^i,$$

de modo que

$$x = \sum_{i < N_d(x)} x_i[d] \cdot d^i.$$

Claramente $N_d(0) = 0$ y si $x \neq 0$, entonces $N_d(x) > 0$ y $n_d(x) = N_d(x) \dot{-} 1$ cumple que $x_{n_d(x)}[d] \neq 0$, o de lo contrario sería

$$x = \sum_{i < n_d(x)} x_i[d] \cdot d^i$$

con $n_d(x) < N_d(x)$, en contra de la minimalidad de $N_d(x)$.

Definimos las *cifras decimales de x en base d* como la sucesión dada por la restricción a $N_d(x)$ del funtor $x_i[d]$, es decir, $x[d] = x|_{N_d(x)}[d]$. El teorema siguiente recoge lo que hemos demostrado y algunos hechos más:

Teorema 4.22 *Si $d \geq 2$, todo número natural $x \neq 0$ admite el desarrollo decimal reducido en base d*

$$x = x[d]_{(d)} = \sum_{i \leq n_d(x)} x_i[d] \cdot d^i,$$

Además, si $x = s_{(d)}$ es otro desarrollo decimal en base d, entonces $\ell(s) > n_d(x)$, y, para todo $i < \ell(s)$, se cumple que

$$s_i = \begin{cases} x_i[d] & si\ i \leq n_d(x), \\ 0 & si\ i > n_d(x). \end{cases}$$

En particular, x admite un único desarrollo decimal reducido.

Demostración: Ya hemos probado que $x[d]_{(d)} = x$, que $x_i[d] < d$ y que $x_{n_d(x)}[d] \neq 0$, por lo que $x[d]$ es un desarrollo decimal reducido de x.

Para probar la unicidad partimos de una sucesión $s > 0$ arbitraria tal que $\bigwedge i < \ell(s)\, s_i < d$ y vamos a probar por inducción que, para todo $k < \ell(s)$, se cumple

$$(s_{(d)})^*_k[d] = \sum_{i<\ell(s) \dot{-} (k+1)} s_{i+k+1} d^i \wedge \bigwedge i \leq k\, (s_{(d)})_i[d] = s_i.$$

Para $k = 0$ tenemos que

$$s_{(d)} = \sum_{i<\ell(s)} s_i \cdot d^i = \sum_{i<\ell(s) \dot{-} 1} s_{i+1} \cdot d^{i+1} + s_0 = d \cdot \sum_{i<\ell(s) \dot{-} 1} s_{i+1} \cdot d^i + s_0,$$

luego por la unicidad de la división euclídea concluimos que $x_0[d] = s_0$ y

$$(s_{(d)})^*_0[d] = \sum_{i<\ell(s) \dot{-} 1} s_{i+1} \cdot d^i.$$

Supuesto cierto para k y $k + 1 < \ell(s)$, tenemos que

$$(s_{(d)})^*_k[d] = d \cdot (s_{(d)})^*_{k+1}[d] + (s_{(d)})_{k+1}[d], \qquad (s_{(d)})_{k+1}[d] < d,$$

$$\sum_{i<\ell(s) \dot{-} (k+1)} s_{i+k+1} d^i = d \cdot \sum_{i<\ell(s) \dot{-} (k+2)} s_{i+k+2} d^i + s_{k+1}, \qquad s_{k+1} < d.$$

Por la unicidad de la división euclídea, tiene que ser

$$(s_{(d)})^*_{k+1}[d] = \sum_{i<\ell(s) \dot{-} (k+2)} s_{i+k+2} d^i, \qquad (s_{(d)})_{k+1}[d] = s_{k+1},$$

lo que completa la inducción. En particular, para $k = \ell(s) \dot{-} 1$ tenemos que

$$\bigwedge i < \ell(s)\, (s_{(d)})_i[d] = s_i.$$

Si suponemos que $s_{(d)} = x$, entonces $x = \sum_{i<\ell(s)} x_i[d] \cdot d^i$, luego por la definición de $N_d(x)$ tiene que ser $n_d(x) < N_d(x) \leq \ell(s)$. Además,

$$x = \sum_{i<\ell(s)} s_i \cdot d^i = \sum_{i<N_d(x)} x_i[d] \cdot d^i + \sum_{i<\ell(s) \dot{-} N_d(x)} s_{N_d(x)+i}\, d^{N_d(x)+i},$$

pero el primero de los últimos dos sumandos también vale x, luego

$$\sum_{i<\ell(s) \dot{-} N_d(x)} s_{N_d(x)+i}\, d^{N_d(x)+i} = 0,$$

luego $\bigwedge i < \ell(s) \dot{-} N_d(x)\ s_{N_d(x)+i} = 0$, luego $s_i = 0$ si $N_d(x) \leq i < \ell(s)$.

De este modo, el desarrollo reducido $x = \sum_{i \leq n_d(x)} x_i[d] \cdot d^i$ es esencialmente único, en cuanto que cualquier otro desarrollo decimal de x resulta de prolongar éste con cifras nulas. ■

Por otro lado, observemos que $0 = 0_{(d)}$ es por definición el único desarrollo decimal reducido de 0.

La unicidad de los desarrollos decimales puede expresarse así:

Teorema 4.23 $d \geq 2 \wedge \bigwedge i < x + y\ x_i[d] = y_i[d] \to x = y$.

Así pues, ahora podemos definir las cifras decimales

$$1 = S0, \quad 2 = S1, \quad 3 = S2, \quad 4 = S3, \quad 5 = S4,$$

$$6 = S5, \quad 7 = S6, \quad 8 = S7, \quad 9 = S8$$

y convenir en que todo numeral como 1 314 ha de interpretarse como

$$\langle 4, 1, 3, 1 \rangle_{S9}.$$

En particular, $S9 = 10$ y $\langle 4, 1, 3, 1 \rangle_{10} = 1 \cdot 10^3 + 3 \cdot 10^2 + 1 \cdot 10 + 4$.

La relación de pertenencia Ahora veremos que, al igual que podemos interpretar los números naturales como sucesiones finitas, también podemos interpretarlos como conjuntos finitos. Para ello basta considerar la relación de pertenencia siguiente:

Definición 4.24 $x \in y \equiv y_x[2] = 1, \qquad x \notin y \equiv \neg x \in y$.

Equivalentemente, un número natural x pertenece a otro y si la cifra de orden x del desarrollo binario de y vale 1.

En particular, si $x \in y$, entonces $x < 2^x \leq y$. Esto hace que podamos considerar cuantificadores acotados en la forma

$$\bigvee u \in y\, \alpha(u) \equiv \bigvee u \leq y(u \in y \wedge \alpha(u)),$$

$$\bigwedge u \in y\, \alpha(u) \equiv \bigwedge u \leq y(u \in y \to \alpha(u)).$$

La unicidad de los desarrollos decimales implica claramente el axioma de extensionalidad:

$$\bigwedge u \in x\, u \in y \wedge \bigwedge u \in y\, u \in x \to x = y.$$

Definimos la inclusión como

$$x \subset y \equiv \bigwedge u \in x\, u \in y,$$

de modo que

1. $x \subset x$,
2. $x \subset y \wedge y \subset x \to x = y$,
3. $x \subset y \wedge y \subset z \to x \subset z$.

Definimos $\varnothing \equiv 0$, y es inmediato que $x \notin \varnothing$, así como que $\varnothing \subset x$.

Una simple inducción prueba la igualdad

$$\sum_{i<k} 2^i = 2^k - 1.$$

Por lo tanto, si definimos $I_k = 2^k - 1$, se cumple que

$$N_2(I_k) = k \quad \text{y} \quad \bigwedge i < k\, (I_k)_i[2] = 1.$$

En términos de la relación de pertenencia:

$$\bigwedge i < k\, i \in I_k \wedge \bigwedge i \in I_k\, i < k.$$

En otras palabras, I_k es el conjunto de todos los números menores que k. Ahora necesitamos un resultado técnico. Definimos:

$$x^-(k) = \sum_{i<k} x_i[2] \cdot 2^i, \quad x^+(k) = \sum_{i<N_2(x) \dot{-} (k+1)} x_{k+1+i}[2] \cdot 2^i.$$

Teorema 4.25 *Se cumple:*

$$x = x^-(k) + x_k[2] \cdot 2^k + x^+(k) \cdot 2^{k+1}, \quad x^-(k) < 2^k.$$

y

$$x = p + q \cdot d^k + r \cdot 2^{k+1} \wedge p < 2^k \rightarrow p = x^-(k) \wedge q = x_k[2] \wedge r = x^-(k).$$

Demostración: Sabemos que

$$x = \sum_{i<N_2(x)} x_i[2] \cdot 2^i = \sum_{i<k+1} x_i[2] \cdot 2^i + \sum_{i<N_2(x) \dot{-} (k+1)} x_{k+1+i}[2] \cdot 2^{k+1+i}.$$

Notemos que esta igualdad es trivial si $N_2(k) \leq k+1$, pues el último sumatorio es nulo, mientras que si $k+1 < N_2(k)$ podemos expresar

$$N_2(k) = k + 1 + (N_2(k) \dot{-} (k+1))$$

y aplicar una de las propiedades de las sumas finitas que hemos enunciado. A su vez

$$x = \sum_{i<k} x_i[2] \cdot 2^i + x_k[2] \cdot 2^k + 2^{k+1} \sum_{i<N_2(x) \dot{-} (k+1)} x_{k+1+i}[2] \cdot 2^i.$$

Además,

$$x^-(k) = \sum_{i<k} x_i[2] \cdot 2^i \leq \sum_{i<k} 2^i = 2^k - 1 < 2^k.$$

Esto prueba la primera parte del teorema. Supongamos ahora que

$$x = p + q \cdot d^k + r \cdot 2^{k+1} \wedge p < 2^k.$$

Entonces

$$p = \sum_{i<N_2(p)} p_i[2] \cdot 2^i.$$

Además, o bien $p = 0$, en cuyo caso $N_2(p) = 0 \leq k$, o bien $p_{N_2(p) \dot{-} q}[2] = 1$, luego $2^{N_2(p) \dot{-} 1} \leq p < 2^k$, luego $N_2(p) \dot{-} q < k$, luego $N_2(p) \leq k$ en cualquier caso. Por lo tanto, podemos escribir

$$p = \sum_{i<k} p_i[2] \cdot 2^i,$$

de donde

$$\begin{aligned} x &= \sum_{i<k} p_i[2] \cdot 2^i + q \cdot d^k + 2^{k+1} \sum_{i<N_2(r)} r_i[2] \cdot 2^i \\ &= \sum_{i<k} p_i[2] \cdot 2^i + q \cdot d^k + \sum_{i<N_2(r)} r_i[2] \cdot 2^{k+1+i}. \end{aligned}$$

Definimos $s = (p|_k[2]^\frown \langle q \rangle)^\frown\, r|_{N_2(r)}[2]$. La definición de la concatenación de sucesiones nos da que

$$\bigwedge i < k\, s_i = p_i[2], \quad s_k = q, \quad \bigwedge i < N_2(r)\, s_{k+1+i} = r|_i[2].$$

Por lo tanto, tenemos que

$$x = \sum_{i<k} s_i \cdot 2^i + s_k \cdot d^k + \sum_{i<N_2(r)} s_{k+1+i} \cdot 2^{k+1+i} = \sum_{i<k+1+N_2(r)} s_i \cdot 2^i.$$

Por la unicidad del desarrollo binario concluimos que

$$\bigwedge i < k + 1 + N_2(r)\, s_i = x_i[2],$$

luego $p = x^-(k)$, $q = x_2[k]$ y $r = x^+(k)$. ■

De aquí deducimos lo siguiente:

Teorema 4.26 $k \notin x \to (y \in x + 2^k \leftrightarrow y \in x \vee y = k)$.

Demostración: En efecto, si $k \notin x$, entonces $x_k[2] = 0$, luego

$$x = x^-(k) + 0 \cdot 2^k + x^+(k) \cdot 2^{k+1},$$

con lo que

$$x + 2^k = x^-(k) + 1 \cdot 2^k + x^+(k) \cdot 2^{k+1},$$

y, en virtud del teorema anterior,

$$(x + 2^k)^-(k) = x^-(k), \quad (x + 2^k)_k[2] = 1, \quad (x + 2^k)^+(k) = x^+(k).$$

De aquí se sigue fácilmente que

$$i \neq k \to (x + 2^k)_i[2] = x_i[2],$$

de donde llegamos a la conclusión. ■

En particular, para $x = 0$ tenemos que, si definimos $\{k\} = 2^k$, se cumple

$$k \in \{k\} \wedge (y \in \{k\} \to y = k).$$

Fijemos ahora una fórmula cualquiera $\alpha(x, x_1, \ldots, x_n)$, cuyas variables estén entre las indicadas. Definimos los funtores

$$\begin{aligned} F_\alpha(x_1, \ldots, x_n, 0) &= 0, \\ F_\alpha(x_1, \ldots, x_n, x+1) &= F_\alpha(x_1, \ldots, x_n, x+1) + 2^x \chi_\alpha(x, x_1, \ldots, x_n), \end{aligned}$$

y a su vez

$$\{u < k \mid \alpha(u, x_1, \ldots, x_n)\} = F_\alpha(x_1, \ldots, x_n, k).$$

Teorema 4.27 *Si $\alpha(x, x_1, \ldots, x_n)$ es una fórmula cualquiera, en* ARP *se demuestra:*

$$x \in \{u < k \mid \alpha(u, x_1, \ldots, x_n)\} \leftrightarrow x < k \wedge \alpha(x, x_1, \ldots, x_n).$$

Demostración: Lo probamos por inducción sobre k. Por abreviar omitimos los parámetros $x_1, \ldots, x_n$. Para $k = 0$ es trivial. Supongamos que vale para k. Entonces

$$\{u < k+1 \mid \alpha(u)\} = \{u < k \mid \alpha(u)\} + 2^k \chi_\alpha(k).$$

Además, por hipótesis de inducción, $k \notin \{u < k \mid \alpha(u)\}$. Distinguiendo dos casos según si se cumple o no $\alpha(k)$ y aplicando el teorema anterior en el primero, llegamos a que, en ambos casos,

$$x \in \{u < k+1 \mid \alpha(u)\} \leftrightarrow x \in \{u < k \mid \alpha(u)\} \vee (\alpha(k) \wedge x = k).$$

Por hipótesis de inducción, esto sucede si y sólo si

$$(x < k \wedge \alpha(x)) \vee (x = k \wedge \alpha(x)),$$

lo cual equivale a $x < k+1 \wedge \alpha(x)$. ■

Notemos que en el teorema anterior podemos cambiar $u < k$ por $u \in k$, entendiendo que

$$\{u \in k \mid \alpha(u)\} = \{u < k \mid u \in k \wedge \alpha(u)\}.$$

A partir de aquí ya podemos definir fácilmente todos los conceptos conjuntistas básicos:

$$\begin{aligned} x \cup y &= \{u < x+y \mid u \in x \vee u \in y\}, \\ x \cap y &= \{u < x+y \mid u \in x \wedge u \in y\}, \\ x \setminus y &= \{u < x \mid u \in x \wedge u \notin y\}, \\ \mathcal{P}x &= \{u < x+1 \mid u \subset x\}, \\ \bigcup x &= \{u < x \mid \bigvee v \in x\, u \in v\}, \\ \bigcap x &= \{u < x \mid \bigwedge v \in x\, u \in v\}, \\ x \times y &= \{w < \langle x, y\rangle \mid \bigvee u \in x \bigvee v \in y\, w = \langle u, v\rangle\}. \end{aligned}$$

En la definición de $\mathcal{P}x$, notemos que $y \subset x \to y_i[2] \leq x_i[2]$, de donde $y \leq x$.

También podemos definir $\{x_1, \ldots, x_n\} = \{x_1\} \cup \cdots \cup \{x_n\}$.

El mínimo y el máximo de un conjunto pueden definirse así:

$$\min x = \mu u \leq x (u \in x), \qquad \max x = x - \mu u \leq x (x - u \in x),$$

de modo que

$$x \neq \varnothing \rightarrow (\min x \in x \land \bigwedge u \in x \; \min x \leq u),$$
$$x \neq \varnothing \rightarrow (\max x \in x \land \bigwedge u \in x \; u \leq \max x).$$

Ahora no ofrece ninguna dificultad definir los conceptos conjuntistas de relación y función,[11] junto con todos sus conceptos relacionados (relación de orden, de equivalencia, etc., aplicaciones inyectivas, suprayectivas, biyectivas, etc.)

Teniendo en cuenta que $\langle a, b \rangle < a + b$, resulta que toda $f : x \longrightarrow y$ cumple $f \subset I_{x+y}$, luego podemos definir

$$y^x = \{f \in \mathcal{P}(I_{x+y}) \mid f : x \longrightarrow y\}.$$

Para cualquier conjunto x, podemos definir su dominio y su rango como

$$\mathcal{D}x = \{u \leq x \mid \bigvee v \leq x \; \langle u, v \rangle \in x\}, \quad \mathcal{R}x = \{u \leq x \mid \bigvee v \leq x \; \langle v, u \rangle \in x\}.$$

Si fijamos un término $t(x, x_1, \ldots, x_n)$, podemos definir el funtor

$$\begin{aligned} F_t(x_1, \ldots, x_n, y, 0) &= 0, \\ F_t(x_1, \ldots, x_n, y, x+1) &= F_\alpha(x_1, \ldots, x_n, x+1) \cup \{t(x, x_1, \ldots, x_n)\} \cdot \chi[x \in y], \end{aligned}$$

y a su vez

$$\{t(u, x_1, \ldots, x_n) \mid u \in y\} = F_t(x_1, \ldots, x_n, y, y).$$

Teorema 4.28 *Si $t(x, x_1, \ldots, x_n)$ es un término cualquiera, en* ARP *se demuestra:*

$$z \in \{t(u, x_1, \ldots, x_n) \mid u \in y\} \leftrightarrow \bigvee u \in y \; z = t(u, x_1, \ldots, x_n).$$

DEMOSTRACIÓN: Omitiendo los parámetros, supongamos que

$$z \in \{t(u) \mid u \in y\} = F_t(y, y).$$

Podemos tomar entonces $w \equiv \mu u \leq y \, z \in F_t(y, u)$. No puede ser $w = 0$, luego, llamando $x = w \dot{-} 1$, se cumple que $w = x + 1$ y así

$$z \in F_t(y, x+1) = F_t(y, x) \cup \{t(x)\} \cdot \chi(x \in y).$$

Por la minimalidad de w, tenemos que $z \notin F_t(y, x)$, luego se tiene que cumplir que $z = t(x)$ y $\chi[x \in y] = 1$, que es lo mismo que $x \in y$. Por lo tanto, $\bigvee u \in y \; z = t(u)$.

[11] Las funciones pueden definirse como conjuntos de pares ordenados en el sentido conjuntista $(x, y) = \{\{x\}, \{x, y\}\}$, aunque en nuestro contexto es más práctico usar los pares $\langle x, y \rangle$ que ya tenemos definidos. No hay ninguna diferencia esencial entre una y otra opción.

Recíprocamente, supongamos que $\bigvee u \in y\, z = t(u)$ y tomemos

$$x = \mu u \in y\, z = t(u).$$

Entonces $x \in y$, luego $x < y$, luego $x + 1 \leq y$.

$$z \in F_t(y, x) \cup \{t(x)\} \cdot \chi[x \in y] = F_t(y, x + 1).$$

Ahora bien, una simple inducción demuestra que

$$x_1 \leq x_1 \to F_t(y, x_1) \subset F_t(y, x_2),$$

luego podemos concluir que $z \in F_t(y, y) = \{t(u) \mid u \in y\}$. ■

Por ejemplo, con este teorema podemos definir el rango de una sucesión como

$$\mathcal{R}s = \{s_i \mid i < \ell(s)\},$$

(pues $i < \ell(s)$ es lo mismo que $i \in I_{\ell(s)}$). Más aún, podemos transformar una sucesión en una función del mismo rango mediante el funtor

$$\mathrm{Fn}(s) = \{\langle i, s_i\rangle \mid i < \ell(s)\}.$$

Es fácil ver entonces que $\mathrm{Fn}(s) : I_{\ell(s)} \longrightarrow \mathcal{R}s$ y que $\bigwedge i < \ell(s)\, \mathrm{Fn}(s)(i) = s_i$.

Es fácil transformar de forma análoga toda función $f : I_k \longrightarrow z$ en una sucesión $s(f)$ tal que $\ell(s(f)) = k$ y $\bigwedge i < k\, s(f)_i = f(i)$.

Por otra parte, cada conjunto puede transformarse en una sucesión creciente mediante el funtor dado por $\mathrm{Suc}(x) = F(x, x)$, donde F está definido por las ecuaciones

$$\begin{aligned} F(x, 0) &= \langle 0, x\rangle, \\ F(x, k + 1) &= \chi[F(x, k)_2 = 0] \cdot F(x, k) + \chi[F(x, k)_2 \neq 0] \cdot \\ &\quad \langle F(x, k)_1{}^\frown\langle \mathrm{mín}\, F(x, k)_2\rangle, F(x, k)_2 \setminus \{\mathrm{mín}\, F(x, k)_2\}\rangle. \end{aligned}$$

Notemos que F va construyendo una sucesión de pares (s_k, x_k), que empieza en $(0, x)$ y, en cada paso, añade a la sucesión s_k el mínimo de x_k y le quita dicho mínimo a x_k, hasta el momento en que x_k se vuelve vacío. A partir de ahí, el par $(s_k, \varnothing)$ permanece invariante. El resultado es una enumeración de x. Teniendo esto en cuenta, es una mera rutina demostrar:

$$s = \mathrm{Suc}(x) \to \mathcal{R}s = x \land \bigwedge ij < \ell(s)(i < j \to s_i < s_j).$$

Si definimos el cardinal de un conjunto como

$$|x| = \ell(\mathrm{Suc}(x)),$$

entonces el funtor definido por $e_x = \mathrm{Fn}(\mathrm{Suc}(x))$ cumple que

$$e_x : I_{|x|} \longrightarrow x \text{ biyectiva},$$

y a partir de ahí no hay dificultad alguna en formalizar en ARP todos los teoremas básicos sobre cardinales de conjuntos finitos que se demuestran en cualquier teoría de conjuntos.

Relación con la teoría de conjuntos de Zermelo Terminamos este capítulo observando que los resultados que acabamos de probar sobre la relación de pertenencia muestran que en ARP se pueden demostrar todos los axiomas de la teoría de conjuntos de Zermelo menos el axioma de infinitud (al contrario, se puede demostrar que todo conjunto es finito), incluyendo el axioma de regularidad, si bien no pueden ser enunciados con cuantificadores, sino mediante funtores concretos, así:

Extensionalidad $\bigwedge u \in x\, u \in y \wedge \bigwedge u \in y\, u \in x \rightarrow x = y$

Par $z \in \{x, y\} \leftrightarrow z = x \vee z = y$

Unión $y \in \bigcup x \leftrightarrow \bigvee u \in x\, y \in u$

Especificacion $x \in \{u \in y \mid \alpha(u)\} \leftrightarrow x \in y \wedge \alpha(x)$

Partes $y \in \mathcal{P}x \leftrightarrow y \subset x$

Regularidad $x \neq \varnothing \rightarrow (\text{mín}\, x \in x \wedge x \cap \text{mín}\, x = \varnothing)$

El teorema 4.28 puede verse como una forma débil del axioma de reemplazo. Por otra parte, hemos probado que todo conjunto x es biyectable con $I_{|x|}$, lo cual ya es una forma del axioma de elección, si bien el enunciado que se corresponde literalmente con el enunciado usual de este axioma se obtiene considerando el funtor de elección

$$E_x = \{\langle u, \text{mín}\, u\rangle \mid u \in x\}.$$

Claramente:

$$\bigwedge u \in x\, u \neq \varnothing \rightarrow E_x : x \longrightarrow \bigcup x \wedge \bigwedge u \in x\, E_x(u) \in u.$$

No obstante, conviene tener presente que el axioma de especificación no es exactamente equivalente al axioma correspondiente en la teoría de Zermelo, pues en ella es válido para fórmulas arbitrarias, y en ARP también, pero las fórmulas y los términos $\mathcal{L}_{\text{arp}}$ no tienen la misma capacidad expresiva que las fórmulas del lenguaje $\mathcal{L}_{\text{tc}}$, sino que se corresponden con fórmulas y términos Δ_0 de $\mathcal{L}_{\text{tc}}$

No obstante, debería ser evidente que todo argumento formalizable en la teoría de Zermelo que sólo involucre conjuntos finitos y que sea estrictamente constructivo, es decir, que no pruebe la existencia de algo sin indicar explícitamente cómo puede ser calculado en un número finito de pasos, es formalizable en ARP.

Capítulo V

La aritmética recursiva primitiva II

La aritmética recursiva primitiva que hemos introducido en el capítulo anterior es una teoría formal insólita, en cuanto que "oficialmente" carece de signos lógicos, aunque hemos visto que podemos definir los conectores y hasta cuantificadores acotados, de modo que se comporten del modo usual. En este capítulo vamos a estudiar la relación entre ARP y otras teorías "al uso", como la aritmética de Peano y, más precisamente, con $\mathrm{I}\Sigma_1$.

5.1 ARP como teoría de primer orden

Empezaremos probando que ARP es equivalente a una teoría axiomática de primer orden usual. Empezamos añadiendo los signos lógicos a $\mathcal{L}_{\mathrm{arp}}$.

Definición 5.1 Llamaremos $\mathcal{L}_a^+$ a un lenguaje de primer orden con una constante 0, cuyo único relator sea el igualador y cuyos funtores sean los de $\mathcal{L}_{\mathrm{arp}}$.

En otras palabras, $\mathcal{L}_a^+$ resulta de añadirle a $\mathcal{L}_{\mathrm{arp}}$ los conectores $\neg$, $\vee$, los cuantificadores $\bigvee$, $\bigwedge$ y un conjunto de variables ligadas.

Definimos la teoría axiomática ARP^+ como la teoría determinada por los axiomas asociados a los funtores de $\mathcal{L}_{\mathrm{arp}}$ en ARP más los axiomas siguientes:

1. $Sx \neq 0$
2. $Sx = Sy \to x = y$,
3. $\alpha(0) \wedge \bigwedge u(\alpha(u) \to \alpha(Su)) \to \alpha(x)$, para toda fórmula abierta α de $\mathcal{L}_a^+$ (es decir, toda fórmula sin cuantificadores).

Es claro que una axiomatización equivalente es la determinada por los secuentes siguientes:

1. Los axiomas lógicos $\alpha \Rightarrow \alpha$ y los axiomas del igualador.
2. Los secuentes $\Rightarrow \alpha$, donde α recorre los axiomas asociados a los funtores de $\mathcal{L}_{\mathrm{arp}}$.
3. $St = 0 \Rightarrow$.
4. $Ss = St \Rightarrow s = t$.

y por las reglas de inferencia de LK_i más la regla de inducción para fórmulas abiertas. Exactamente igual que en el caso de la aritmética de Peano, se ve que esta regla equivale a tomar como axiomas los secuentes asociados al principio de inducción (para fórmulas abiertas).

Notemos que todos los axiomas de ARP^+ constan únicamente de fórmulas atómicas.

Vamos a estudiar la relación entre ARP y ARP^+. En primer lugar tenemos lo siguiente:

Teorema 5.2 *Si α es un teorema de* ARP, *entonces $\Rightarrow \alpha$ es un teorema de* ARP^+, *que además admite una demostración formada únicamente por fórmulas atómicas.*

Demostración: El resultado es cierto para los axiomas de ARP, pues en tal caso $\Rightarrow \alpha$ es un axioma de ARP^+. Basta probar que si el enunciado es cierto para las premisas de una regla de inferencia de ARP, entonces también lo es para su conclusión.

Para la regla S_1, si podemos probar $\Rightarrow s_1(x) = s_2(x)$, combinando este secuente con el axioma $\Rightarrow t = t$ y con

$$t = t,\ s_1(x) = s_2(x) \Rightarrow s_1(t) = s_2(t)$$

(dado por 2.14) obtenemos $\Rightarrow s_1(t) = s_2(t)$.

Para S_2, si podemos probar $\Rightarrow t_1 = t_2$, cortando con

$$t_1 = t_2 \Rightarrow s(t_1) = s(t_2)$$

(dado también por 2.14), obtenemos $\Rightarrow s(t_1) = s(t_2)$.

El caso de la regla T es también inmediato, por los teoremas de LK_i sobre simetría y transitividad del igualador.

Consideramos finalmente la regla de inducción. Suponemos demostrados

$$\Rightarrow s_1(0) = s_2(0), \qquad \Rightarrow s_1(Sx) = h(x, s_1(x)), \qquad \Rightarrow s_2(Sx) = h(s, s_2(x)).$$

Cortando con el axioma del igualador

$$s_1(x) = s_2(x),\ s_1(Sx) = h(x, s_1(x)) \Rightarrow s_1(Sx) = h(x, s_2(x)),$$

y con los secuentes que expresan la simetría y la transitividad del igualador, obtenemos el secuente

$$s_1(x) = s_2(x) \Rightarrow s_1(Sx) = s_2(Sx).$$

La regla de inducción nos da $s_1(0) = s_2(0) \Rightarrow s_1(x) = s_2(x)$, de donde a su vez llegamos a $\Rightarrow s_1(x) = s_2(x)$. ■

Nota Un poco más en general, el argumento empleado en la prueba del teorema anterior demuestra que si, suponiendo α, en ARP podemos demostrar β, entonces en ARP^+, suponiendo $\Rightarrow \alpha$, podemos demostrar $\Rightarrow \beta$.

Por ejemplo, sabemos que, suponiendo α, en ARP podemos demostrar $t_\alpha = 0$ y viceversa, luego en ARP^+ podemos demostrar que $\alpha \leftrightarrow t_\alpha = 0$ (donde el coimplicador es el definido a partir de los conectores de $\mathcal{L}_a^+$, no el definido aritméticamente en ARP). ■

La relación entre ARP y ARP^+ es mucho más estrecha que la que muestra el teorema anterior. Para ponerlo de manifiesto necesitamos definir las fórmulas Δ_0 en $\mathcal{L}_a^+$. Para ello observemos que en $\mathcal{L}_a^+$ tenemos definida la fórmula

$$x \leq y \equiv x + (y \dot{-} x) = y.$$

Definición 5.3 Llamaremos semifórmulas Δ_0 de $\mathcal{L}_a^+$ a las semifórmulas determinadas por los criterios siguientes:

1. Toda semifórmula atómica es Δ_0.
2. Si α y β son semifórmulas Δ_0, también lo son $\neg\alpha$ y $\alpha \vee \beta$.
3. Si t es un semitérmino, u es una variable que no esté en t, y $\alpha(u)$ es una semifórmula Δ_0, entonces

   $$\bigvee u \leq t\, \alpha(u) \equiv \bigvee u(u \leq t \wedge \alpha(u)) \quad \text{y} \quad \bigwedge u \leq t\, \alpha(u) \equiv \bigwedge u(u \leq t \rightarrow \alpha(u))$$

   son semifórmulas Δ_0.

De la segunda condición se deduce que $\alpha \wedge \beta$, $\alpha \rightarrow \beta$ y $\alpha \leftrightarrow \beta$ también son semifórmulas Δ_0. Las fórmulas Δ_0 son las semifórmulas Δ_0 que son fórmulas.

A cada fórmula α de $\mathcal{L}_a^+$ de tipo Δ_0 le asociamos una fórmula α_0 de $\mathcal{L}_{\mathrm{arp}}$ con las mismas variables libres mediante el criterio siguiente:

1. Si α es una fórmula atómica, $\alpha^* \equiv \alpha$.
2. $(\neg\alpha)^* \equiv \neg\alpha^*$.
3. $(\alpha \vee \beta)^* \equiv \alpha^* \vee \beta^*$.
4. $(\bigvee u \leq t\, \alpha(u))^* \equiv \bigvee u \leq t\, \alpha^*(u)$.
5. $(\bigwedge u \leq t\, \alpha(u))^* \equiv \bigwedge u \leq t\, \alpha^*(u)$.

En estas condiciones hay que entender que los signos lógicos de los miembros derechos son los definidos aritméticamente en ARP, mientras que los de los miembros izquierdos son los signos lógicos de $\mathcal{L}_a^+$.

En la prueba del teorema siguiente necesitaremos tener en cuenta que todas las fórmulas del teorema 4.10 son demostrables en ARP, pero interpretando los signos lógicos como los de $\mathcal{L}_a^+$ y no como los definidos aritméticamente en ARP.

En efecto, las dos primeras son axiomas, y las restantes se demuestran exactamente con las mismas pruebas. Por ejemplo, la propiedad 3) se prueba por inducción usando que

$$(Sx) \dot{-} 1 = (x+1) \dot{-} 1 = x,$$

lo cual es un teorema de ARP$^+$ porque es un teorema de ARP.

Teorema 5.4 *Si α es una fórmula Δ_0 de $\mathcal{L}_a^+$, entonces en* ARP$^+$ *se demuestra que $\alpha \leftrightarrow \alpha^*$. En particular, si α^* es demostrable en* ARP*, entonces α lo es en* ARP$^+$.

Demostración: Razonamos por inducción sobre la longitud de α. El resultado es trivial si α es una fórmula atómica, pues entonces $\alpha^* \equiv \alpha$.

Si $\alpha \equiv \neg\beta$ y suponemos que $\beta \leftrightarrow \beta^*$ es demostrable en ARP$^+$, entonces

$$(\neg\beta)^* \equiv \neg(\beta^*) \equiv 1 \dot{-} t_{\beta^*} = 0 \leftrightarrow t_{\beta^*} \neq 0 \leftrightarrow \neg(\beta^*) \leftrightarrow \neg\beta.$$

La primera equivalencia se debe a que en ARP podemos probar que[1]

$$1 \dot{-} x = 0 \leftrightarrow x \neq 0,$$

y la segunda por la nota tras el teorema 5.2.

Si $\alpha \equiv \beta \vee \gamma$ y en ARP$^+$ se demuestra que $\beta \leftrightarrow \beta^*$ y $\gamma \leftrightarrow \gamma^*$, entonces

$$(\beta \vee \gamma)^* \equiv \beta^* \vee \gamma^* \equiv t_{\beta^*} \cdot t_{\gamma^*} = 0 \leftrightarrow t_{\beta^*} = 0 \vee t_{\gamma^*} = 0 \leftrightarrow \beta^* \vee \gamma^* \leftrightarrow \beta \vee \gamma.$$

Si $\alpha \equiv \bigvee u \leq t\, \beta(u)$ y el teorema vale para la fórmula $\beta(x)$, entonces

$$(\bigvee u \leq t\, \beta(u))^* \equiv \bigvee u \leq t\, \beta^*(u)$$

y ahora observamos que, por la nota tras el teorema 5.2, dado que en ARP$^+$, suponiendo $y \leq t$ y $\beta^*(y)$ podemos probar $\bigvee u \leq t\, \beta^*(u)$ y, recíprocamente, suponiendo $\bigvee u \leq t\, \beta^*(u)$ podemos probar $\mu u \leq t\, \beta^*(u) \leq t$ y $\beta^*(\mu u \leq t\, \beta^*(u))$, esto es también así en ARP$^+$, lo que se traduce en las implicaciones

$$y \leq t \wedge \beta^*(y) \rightarrow \bigvee u \leq t\, \beta^*(u),$$

$$\bigvee u \leq t\, \beta^*(u) \rightarrow \mu u \leq t\, \beta^*(u) \leq t \wedge \beta^*(\mu u \leq t\, \beta^*(u)),$$

donde las conjunciones y las implicaciones hay que entenderlas ahora como definidas a partir de los conectores de $\mathcal{L}_a^+$ y no aritméticamente. Esto a su vez se traduce en que $\bigvee u \leq t\, \beta^*(u)$ en el sentido aritmético es equivalente en ARP$^+$

[1]Sabemos que si $x \neq 0$, entonces $x = S(x \dot{-} 1)$, luego $1 \dot{-} x = 0 \dot{-} (x \dot{-} 1) = 0$.

a la fórmula que llamamos igual, pero definida a partir del particularizador y los conectores de $\mathcal{L}_a^+$. Por lo tanto,

$$(\bigvee u \leq t\, \beta(u))^* \leftrightarrow \bigvee u \leq t\, \beta^*(u) \leftrightarrow \bigvee u \leq t\, \beta^*(u) \leftrightarrow \bigvee u \leq t\, \beta(u).$$

Si $\alpha \equiv \bigwedge u \leq t\, \beta(u)$, entonces

$$\alpha^* \equiv \bigwedge u \leq t\, \beta(u) \equiv \neg \bigvee u \leq t\, \neg \beta^*(u),$$

donde todos los signos son los definidos aritméticamente, pero usando los casos ya probados del negador y el particularizador acotado, concluimos que

$$\alpha^* \equiv \bigwedge u \leq t\, \beta(u) \equiv \neg \bigvee u \leq t\, \neg \beta^*(u) \leftrightarrow \bigwedge u \leq t\, \beta(u).$$

■

Nota Aunque no ha hecho falta para la prueba del teorema, es fácil ver que

$$(\beta \wedge \gamma)^* \leftrightarrow \beta^* \wedge \gamma^*, \quad (\beta \rightarrow \gamma)^* \leftrightarrow (\beta^* \rightarrow \gamma^*), \quad (\beta \leftrightarrow \gamma)^* \leftrightarrow (\beta^* \leftrightarrow \gamma^*).$$

■

Una consecuencia del teorema anterior es que, puesto que toda fórmula Δ_0 es equivalente en ARP$^+$ a una fórmula atómica, el principio de inducción es válido en ARP$^+$, no sólo para fórmulas abiertas, sino, más en general, para fórmulas Δ_0 cualesquiera.

Pero lo realmente notable es que se cumple el recíproco del teorema anterior:

Teorema 5.5 *Si α es una fórmula Δ_0 de $\mathcal{L}_a^+$, entonces α^* es demostrable en* ARP *si y sólo si α lo es en* ARP$^+$*.*

DEMOSTRACIÓN: Sólo nos falta probar que si α es demostrable en ARP$^+$, entonces α^* lo es en ARP. Como α es equivalente a α^*, basta probar que si α^* es demostrable en ARP$^+$, entonces lo es en ARP. Equivalentemente, podemos supone que α es una fórmula atómica.

En primer lugar observamos que, como toda fórmula α de tipo Δ_0 (en particular, toda fórmula abierta) de $\mathcal{L}_a^+$ es equivalente en ARP$^+$ a una fórmula atómica α^*, toda demostración en ARP$^+$ puede transformarse en otra en la que las inducciones sean a lo sumo sobre fórmulas atómicas.

Así pues, podemos considerar una demostración del secuente $\Rightarrow \alpha$ en la que todas las inducciones sean respecto de fórmulas atómicas. Como además los axiomas de ARP$^+$ constan únicamente de fórmulas atómicas y la clase de las fórmulas atómicas es cerrada para subfórmulas y sustitución, el teorema 3.21 nos da[2] que existe una demostración de α formada únicamente por fórmulas atómicas. Esto supone que en ella no pueden usarse reglas de inferencia lógicas: sólo cortes, debilitaciones e inducción.

[2]Para aplicar el teorema 3.21 necesitamos que los axiomas de ARP$^+$ sean cerrados para sustitución, lo cual exige que consideremos axiomas de APR$^+$ las ecuaciones que definen a los funtores aplicadas a términos cualesquiera, no sólo a variables. Es claro que todas ellas son teoremas de APR, por lo que, con estos axiomas adicionales, los teoremas siguen siendo los mismos.

El teorema quedará probado si demostramos que, para todo secuente

$$S \equiv \gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$$

formado por fórmulas atómicas, si S es un axioma de ARP$^+$, entonces la fórmula

$$\bar{S} \equiv \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n$$

(donde los conectores son los aritméticos) es demostrable en ARP, y que si las fórmulas asociadas a los secuentes superiores de una regla de debilitación, corte o inducción son demostrables en ARP, entonces la fórmula asociada al secuente inferior también lo es.

Para los axiomas lógicos se trata de probar que $\neg\alpha \vee \alpha$ es un teorema de ARP, lo cual es cierto.

Las fórmulas asociadas a los axiomas del igualador son equivalentes (cambiando disyunciones por implicaciones) a

I1. $t = t$.

I2. $t_1 = t_1', \ldots, t_n = t_n' \rightarrow Ft_1 \cdots t_n = Ft_1' \cdots t_n'$.

I3. $t_1 = t_1'$, $t_2 = t_2'$, $t_1 = t_2 \rightarrow t_1' = t_2'$.

Es fácil comprobar que todas ellas son demostrables en APR. Las fórmulas asociadas a los axiomas asociados a los funtores son axiomas de APR, luego obviamente son teoremas. Finalmente, las fórmulas asociadas a los axiomas matemáticos son

$$St \neq 0, \qquad Ss = St \rightarrow s = t,$$

que ya hemos visto que son teoremas de ARP. La validez de las regla de debilitación es trivial, y la de corte se comprueba sin dificultad. La de inducción tampoco ofrece problemas: suponemos que en ARP podemos probar

$$\alpha(x) \wedge \gamma_1 \wedge \cdots \wedge \gamma_m \rightarrow \delta_1 \vee \cdots \vee \delta_n \vee \alpha(Sx),$$

y tenemos que demostrar

$$\alpha(0) \wedge \gamma_1 \wedge \cdots \wedge \gamma_m \rightarrow \delta_1 \vee \cdots \vee \delta_n \vee \alpha(t).$$

Distinguimos dos casos: si se cumple $\neg\gamma_1 \vee \cdots \neg\gamma_m \vee \delta_1 \vee \cdots \delta_n$, entonces la conclusión es inmediata. Si se cumple lo contrario (o no hay fórmulas colaterales), entonces tenemos $\alpha(x) \rightarrow \alpha(Sx)$ y, si suponemos $\alpha(0)$, la regla I nos permite concluir $\alpha(x)$, luego, por S_1, también $\alpha(t)$. El teorema de deducción nos da la implicación $\alpha(0) \rightarrow \alpha(t)$, de la que se sigue trivialmente la fórmula asociada al secuente inferior de la inducción. ■

Así pues, ARP$^+$ es lo que se conoce como una extensión conservativa de ARP: todo teorema de ARP$^+$ expresable en el lenguaje de ARP es, de hecho, un teorema de ARP. En particular, si ARP es consistente, también lo es ARP$^+$.

En la práctica esto significa que la mejor forma de demostrar teoremas de ARP es trabajar en ARP^+, pues cualquier teorema que probemos en ARP^+, si se expresa mediante un fórmula expresable en $\mathcal{L}_{\mathrm{arp}}$ (es decir, mediante una fórmula Δ_0), automáticamente podemos asegurar que es un teorema de ARP (y el argumento es constructivo, es decir, podemos diseñar un algoritmo que traduzca la demostración de una fórmula Δ_0 en ARP^+ a demostraciones en ARP de la fórmula equivalente en $\mathcal{L}_{\mathrm{arp}}$). Por lo tanto, sería tonto trabajar con las limitaciones de ARP cuando podemos hacerlo en ARP^+.

La prueba del teorema 5.4 y la nota posterior se traducen en que todos los resultados que hemos demostrado en ARP pueden reinterpretarse ahora como teoremas de ARP^+ considerando a los signos lógicos como los signos lógicos de $\mathcal{L}_a^+$, y no como los definidos aritméticamente.

Nota En lo sucesivo llamaremos ARP a la teoría que hasta aquí hemos venido llamando ARP^+ y llamaremos $\mathcal{L}_{\mathrm{arp}}$ al lenguaje de primer orden que hasta ahora hemos llamado $\mathcal{L}_a^+$. ■

A la hora de aplicar en la aritmética recursiva primitiva con cuantificadores los resultados que hemos demostrado sin ellos debemos tener la precaución de que los resultados que habíamos demostrado para fórmulas arbitrarias ahora sólo son aplicables en principio a fórmulas Δ_0.

Por ejemplo, si α es una fórmula Δ_0, podemos considerar el funtor $\chi_\alpha \equiv \chi_{\alpha^*}$ que cumple

$$\chi_\alpha(x_1,\ldots,x_n) = 1 \leftrightarrow \alpha(x_1,\ldots,x_n), \quad \chi_\alpha(x_1,\ldots,x_n) = 0 \leftrightarrow \neg\alpha(x_1,\ldots,x_n),$$

pero es necesario que la fórmula sea Δ_0. Similarmente, para que la expresión

$$\mu u \leq x\, \alpha(x_1,\ldots,x_n,u)$$

defina un funtor necesitamos que la fórmula α sea de tipo Δ_0, y lo mismo sucede con el funtor

$$\{u \in y \mid \alpha(u,x_1,\ldots,x_n)\}.$$

De hecho, teniendo en cuenta las últimas observaciones que hemos hecho en el capítulo anterior, ahora es inmediato que en ARP es posible demostrar todos los axiomas de la teoría de conjuntos de Zermelo menos el axioma de infinitud (con sus enunciados usuales, con cuantificadores), si bien con la restricción —que ahora queda explícita— de que el axioma de especificación sólo es demostrable, en principio, para fórmulas de tipo Δ_0.

El modelo natural de ARP A cada funtor F de rango r de $\mathcal{L}_{\mathrm{arp}}$ le podemos asignar una función recursiva primitiva r-ádica $\bar{F}$ de forma obvia:

1. $\bar{S}(n) = n+1$,
2. $\bar{C}(n) = 0$,
3. $\bar{P}_i^r(a_1,\ldots,a_r) = a_i$,

4. Si $F = \kappa G H_1 \cdots H_m$, entonces

$$\bar{F}(a_1, \ldots, a_n) = \bar{G}(\bar{H}_1(a_1, \ldots, a_n), \ldots, \bar{H}_m(a_1, \ldots, a_n)),$$

5. Si $F = \rho G H$, entonces $\bar{F}$ es la función determinada por

$$\begin{aligned} \bar{F}(a_1, \ldots, a_n, 0) &= \bar{G}(a_1, \ldots, a_n), \\ \bar{F}(a_1, \ldots, a_n, a+1) &= \bar{H}(a_1, \ldots, a_n, a, \bar{F}(a_1, \ldots, a_n, a)). \end{aligned}$$

Esto a su vez nos permite definir un modelo $\mathbb{N}$ de $\mathcal{L}_{\mathrm{arp}}$ como el que tiene por universo al conjunto de los números naturales y en el que la constante 0 se interpreta como el número natural 0 y cada funtor F se interpreta como la función recursiva primitiva $\bar{F}$. Es inmediato que todos los axiomas de ARP son verdaderos en $\mathbb{N}$, es decir, que $\mathbb{N}$ es un modelo de ARP, y nos referiremos a él como el *modelo natural de* ARP.

Comparando la demostración del teorema 4.4 con la definición del objeto denotado por un término en un modelo, es inmediato que el número $d(t)$ calculado en dicho teorema no es sino el número natural denotado por el designador t en el modelo natural. Esto nos da el teorema siguiente:

Teorema 5.6 (Σ_1-completitud de ARP) *Si α es una sentencia Σ_1 de $\mathcal{L}_{\mathrm{arp}}$, entonces*

$$\mathbb{N} \vDash \alpha \qquad \textit{syss} \qquad \underset{\mathrm{ARP}}{\vdash} \alpha.$$

Demostración: Que $\underset{\mathrm{ARP}}{\vdash} \alpha$ implica que α es verdadera es un caso particular del teorema de corrección. La implicación relevante es la opuesta. Veámosla primero para sentencias Δ_0. Puesto que toda sentencia Δ_0 es equivalente en ARP a una sentencia atómica, podemos suponer que $\alpha \equiv t_1 = t_2$, para ciertos designadores t_1 y t_2.

Si $\mathbb{N} \vDash \alpha$, esto significa que $d(t_1) = d(t_2)$. Si llamamos n a este número natural, el teorema 4.4 nos da que $\underset{\mathrm{ARP}}{\vdash} t_1 = \bar{n}$ y $\underset{\mathrm{ARP}}{\vdash} t_2 = \bar{n}$, luego $\underset{\mathrm{ARP}}{\vdash} t_1 = t_2$, que es lo mismo que $\underset{\mathrm{ARP}}{\vdash} \alpha$.

Si $\alpha \equiv \bigvee u\, \beta(u)$ es de tipo Σ_1, entonces $\mathbb{N} \vDash \alpha$ significa que existe un número natural n tal que $\mathbb{N} \vDash \beta(\bar{n})$, luego, por el caso ya probado, $\underset{\mathrm{ARP}}{\vdash} \beta(\bar{n})$, de donde a su vez $\underset{\mathrm{ARP}}{\vdash} \alpha$. ■

5.2 Los funtores de ARP en $\mathrm{I}\Sigma_1$

Cada fórmula del lenguaje $\mathcal{L}_a$ de la aritmética elemental puede identificarse de forma natural con una fórmula de $\mathcal{L}_{\mathrm{arp}}$, pues en este lenguaje tenemos, en particular, una constante 0 y funtores S, $+$ y $\cdot$ en correspondencia con los signos eventuales[3] de $\mathcal{L}_a$.

[3] Si consideramos en $\mathcal{L}_a$ el relator diádico $\leq$, las fórmulas atómicas $s \leq t$ de $\mathcal{L}_a$ se identifican de forma natural con la fórmula atómica $s \leq t \equiv s + (t \mathbin{\dot-} s) = t$.

Nota A partir de este momento, para acentuar esta relación, pasaremos a escribir $t' \equiv St$ en $\mathcal{L}_{\mathrm{arp}}$, tal y como hacemos en $\mathcal{L}_a$. ■

Todos los axiomas de AP salvo el principio de inducción se corresponden con axiomas de ARP (dos de ellos se corresponden con los axiomas asociados al funtor $+$ y otros dos con los asociados al funtor $\cdot$). Sin embargo, ARP tiene infinitos funtores y axiomas asociados adicionales. Esto hace que la inducción respecto de fórmulas abiertas (o, equivalentemente, atómicas o Δ_0) de ARP no sea comparable con la inducción en AP, o en fragmentos como $I\Sigma_1$, dado que las fórmulas atómicas o Δ_0 de ARP contienen mucha más información que las fórmulas correspondientes de AP.

Sin embargo, ahora vamos a demostrar que esta diferencia es más aparente que real, pues si añadimos a AP (o incluso a $I\Sigma_1$) los funtores de ARP y sus axiomas asociados, obtenemos una extensión conservativa, en el mismo sentido que ARP es una extensión conservativa de la teoría que habíamos definido inicialmente como ARP.

Para probarlo llamaremos AP^+ (resp. $I\Sigma_n^+$) a la teoría sobre el lenguaje $\mathcal{L}_{\mathrm{arp}}$ cuyos axiomas son los de AP (resp. $I\Sigma_n$) más los de ARP, es decir, que a ARP le añadimos el principio de inducción (para fórmulas de tipo Σ_n) y a AP (resp. $I\Sigma_n$) le añadimos los axiomas asociados a los funtores de $\mathcal{L}_{\mathrm{arp}}$ y extendemos el principio de inducción para admitir dichos funtores en las fórmulas de inducción.

En primer lugar demostraremos que toda fórmula de $\mathcal{L}_{\mathrm{arp}}$ es equivalente en $I\Sigma_1^+$ a una fórmula de $\mathcal{L}_a$. Para ello empezamos asociando a cada término $t(x_1, \ldots, x_k)$ de $\mathcal{L}_{\mathrm{arp}}$ (cuyas variables estén entre las indicadas) una fórmula $\phi_t(x_1, \ldots, x_k, y)$ de $\mathcal{L}_a$ de tipo Σ_1 con una variable adicional de modo que

$$\underset{I\Sigma_1^+}{\vdash} (y = t(x_1, \ldots, x_k) \leftrightarrow \phi_t(x_1, \ldots, x_k, y)), \qquad \underset{I\Sigma_1}{\vdash} \overset{1}{\bigvee} u\, \phi_t(x_1, \ldots, x_k, u).$$

(Por aligerar la notación, en la definición no mencionaremos explícitamente las variables $x_1, \ldots, x_k$.)

1. Si $t \equiv x_i$ es una variable, basta tomar $\phi_t(y) \equiv y = x_i$. La comprobación es trivial.

2. Si $t \equiv 0$, basta tomar $\phi_t(y) \equiv y = 0$.

3. Si $t \equiv F(t_1 \ldots, t_n)$ y algún término t_i no es una variable, entonces

$$\phi_t(y) \equiv \bigvee u_1 \cdots u_n(\phi_{t_1}(u_1) \wedge \cdots \wedge \phi_{t_n}(u_n) \wedge \phi_T(u_1, \ldots, u_n, y)),$$

   donde $T \equiv F(x_1, \ldots, x_n)$.

4. Si $t \equiv x'$, basta tomar

$$\phi_t(y) \equiv y = x'$$

5. Si $t \equiv C(x)$, basta tomar $\phi_t(y) \equiv y = 0$.

6. Si $t \equiv P_i^r(x_1, \ldots x_r)$, basta tomar $\phi_t(y) \equiv y = x_i$.

7. Si $t \equiv (\kappa G H_1 \cdots H_m)(x_1, \ldots, x_n)$, consideramos los términos

$$T_i \equiv H_i(x_1, \ldots, x_n), \quad T^*(y_1, \ldots, y_m) \equiv G(y_1, \ldots, y_m)$$

y definimos

$$\phi_t(y) \equiv \bigvee u_1 \cdots u_m v(\phi_{T_1}(u_1) \land \cdots \land \phi_{T_m}(u_m) \land \phi_{T^*}(u_1, \ldots, u_m, y))$$

8. Si $t \equiv \rho G H(x_1, \ldots, x_{n+1})$, consideramos los términos

$$T \equiv G(x_1, \ldots, x_n), \quad U \equiv H(x_1, \ldots, x_{n+1}, x),$$

y definimos

$$\phi_t(y) \equiv \bigvee s(\mathrm{Suc}(s) \land \ell(s) = x_{n+1} + 1 \land s_{x_{n+1}} = y \land \phi_T(s_0) \land$$
$$\bigwedge i < x_{n+1}\, \phi_U(x_1, \ldots, x_n, i, s_i, s_{i+1})).$$

En el último apartado de la definición usamos el hecho no trivial de que en $\mathrm{I}\Sigma_1$ es posible definir una fórmula[4] $\mathrm{Suc}(s)$ de tipo Δ_1 que expresa que el número natural s codifica una sucesión finita, de longitud $z + 1$ en este caso. (Véase la sección 6.7 de [LM].)

La comprobación de que las fórmulas que acabamos de definir cumplen lo requerido no ofrece ninguna dificultad. Por ejemplo, en el último apartado se trata de probar que la sucesión s cuya existencia se afirma es la sucesión de longitud $z + 1$ que cumple

$$s_0 = G(x_1, \ldots, x_n), \quad s_{i+1} = H(x_1, \ldots, x_n, i, s_i),$$

cuya existencia puede probarse por inducción sobre z, y claramente entonces, teniendo en cuenta los axiomas que definen el funtor $\rho G H$,

$$s_i = \rho G H(x_1, \ldots, x_n, i),$$

luego en particular $y = s_{x_{n+1}} = \rho G H(x_1, \ldots, x_{n+1}) = t$.

Observemos que las fórmulas ϕ_t son de hecho Δ_1, pues

$$\underset{\mathrm{I}\Sigma_1}{\vdash} \neg\phi_t(x_1, \ldots, x_k, y) \leftrightarrow \bigwedge u(\phi_t(x_1, \ldots, x_n, u) \to u = y),$$

y la fórmula de la derecha es de tipo Π_1.

[4]La definición de $\mathrm{Suc}(s)$ es mucho más artificiosa de lo necesario, porque se apoya en el hecho nada trivial de que en $\mathrm{I}\Sigma_1$ se puede definir una relación de pertenencia que cumpla los axiomas básicos de la teoría de conjuntos. Una definición mucho más simple que basta para lo que necesitamos aquí es la definición de Suc(y, z, x) dada en [LM 5.42], teniendo en cuenta el teorema [LM 5.41].

Ahora, para cada fórmula atómica $\alpha \equiv t_1 = t_2$ de $\mathcal{L}_{\mathrm{arp}}$, definimos

$$\alpha^* \equiv \bigvee u(\phi_{t_1}(u) \wedge \phi_{t_2}(u)),$$

que es una fórmula de $\mathcal{L}_a$ de tipo Σ_1 y en $I\Sigma_1^+$ se demuestra que $\alpha \leftrightarrow \alpha^*$. En realidad es Δ_1, pues

$$\underset{I\Sigma_1}{\vdash} (\alpha^* \leftrightarrow \bigwedge u(\phi_{t_1}(u) \wedge \phi_{t_2}(u)).$$

A partir de aquí definimos

$$(\neg\alpha)^* \equiv \neg\alpha^*, \quad (\alpha \vee \beta)^* \equiv \alpha^* \vee \beta^*,$$

$$(\bigvee u\, \alpha(u))^* \equiv \bigvee u\, \alpha^*(u), \qquad (\bigwedge u\, \alpha(u))^* \equiv \bigwedge u\, \alpha^*(u),$$

y se prueba fácilmente que la equivalencia

$$\underset{I\Sigma_1}{\vdash} (\alpha \leftrightarrow \alpha^*)$$

se cumple de hecho para toda fórmula α.

Notemos que si α es una fórmula Δ_0 en $\mathcal{L}_{\mathrm{arp}}$, entonces α^* es Δ_1 en $\mathcal{L}_a$, aunque no es necesariamente Δ_0. No obstante, no deja de ser cierto que si α es de tipo Σ_n o Π_n en $\mathcal{L}_{\mathrm{arp}}$, lo mismo vale para α^* en $\mathcal{L}_a$.

Teorema 5.7 *Una fórmula de $\mathcal{L}_a$ es demostrable en* AP^+ *(resp.* $I\Sigma_n^+$*) si y sólo si es demostrable en* AP *(resp.* $I\Sigma_n$*).*

DEMOSTRACIÓN: Es obvio que todo teorema de AP (resp. $I\Sigma_n$) lo es de AP^+ (resp. $I\Sigma_n^+$). Se trata de probar el recíproco. De hecho, basta probar que si una fórmula α de $\mathcal{L}_{\mathrm{arp}}$ es demostrable en AP (resp. $I\Sigma_n^+$), entonces α^* es demostrable en AP (resp. $I\Sigma_n$).

A su vez, para demostrar esto, basta ver que si un secuente S es un axioma de AP^+ (resp. $I\Sigma_n^+$), entonces el secuente S^* que resulta de sustituir cada una de sus fórmulas α por α^* es demostrable en AP (resp. $I\Sigma_n$), así como que si los secuentes superiores S de una regla de inferencia en AP^+ (resp. $I\Sigma_n^+$) cumplen que los secuentes S^* son demostrables en AP (resp. $I\Sigma_n$), lo mismo vale para el secuente inferior.

De hecho, la parte concerniente a las reglas de inferencia es trivial, pues ninguna se invalida por poner asteriscos a las fórmulas. Sólo tenemos que comprobar la parte relativa a los axiomas. El caso de los axiomas lógicos también es trivial. Tenemos que comprobar los axiomas del igualador, los asociados a funtores y los dos axiomas matemáticos.

Empecemos por los axiomas matemáticos. El primero es $t' = 0 \Rightarrow$. Salvo si t es una variable (en cuyo caso la situación es más simple), la traducción es

$$\bigvee u(\phi_{t'}(u) \wedge \phi_0(u)) \equiv \bigvee u(\bigvee v(\phi_t(v) \wedge u = v') \wedge u = 0)$$

Una demostración es:

$$\begin{array}{c}
x = y',\, x = 0 \Rightarrow y' = 0 \qquad y' = 0 \Rightarrow \\ \hline
x = y',\, x = 0 \Rightarrow \\ \hline
\phi_t(y),\, x = y',\, x = 0 \Rightarrow \\ \hline
\phi_t(y) \land x = y',\, x = 0 \Rightarrow \\ \hline
\bigvee v(\phi_t(v) \land x = v'),\, x = 0 \Rightarrow \\ \hline
\bigvee u(\bigvee v(\phi_t(v) \land u = v'),\, u = 0) \Rightarrow
\end{array}$$

El segundo axioma es $S \equiv t_1' = t_2' \Rightarrow t_1 = t_2$, y su traducción es

$$\bigvee u(\phi_{t_1'}(u) \land \phi_{t_2'}(u)) \Rightarrow \bigvee u(\phi_{t_1}(u) \land \phi_{t_2}(u)).$$

Si t_1 y t_2 no son variables (en caso contrario es más sencillo) esto es:

$$\bigvee u(\bigvee v(\phi_{t_1}(v) \land u = v') \land \bigvee v(\phi_{t_2}(v) \land u = v')) \Rightarrow \bigvee u(\phi_{t_1}(u) \land \phi_{t_2}(u)).$$

Una demostración empieza así:

$$\begin{array}{c}
\begin{array}{cc}
\begin{array}{c} x = y',\, x = z' \Rightarrow y' = z' \qquad y' = z' \Rightarrow y = z \\ \hline x = y',\, x = z' \Rightarrow y = z \end{array} & y = z,\, \phi_{t_1}(y) \Rightarrow \phi_{t_1}(z)
\end{array} \\ \hline
\phi_{t_1}(y),\, x = y',\, x = z' \Rightarrow \phi_{t_1}(z) \\ \hline
\phi_{t_1}(y),\, x = y',\, \phi_{t_2}(z),\, x = z' \Rightarrow \phi_{t_1}(z)
\end{array}$$

Por otro lado, el secuente

$$\phi_{t_1}(y),\, x = y',\, \phi_{t_2}(z),\, x = z' \Rightarrow \phi_{t_2}(z)$$

se deduce por debilitación de $\phi_{t_2}(z) \Rightarrow \phi_{t_2}(z)$, luego la regla derecha del conjuntor nos permite continuar así:

$$\phi_{t_1}(y),\, x = y',\, \phi_{t_2}(z),\, x = z' \Rightarrow \phi_{t_1}(z) \land \phi_{t_2}(z),$$

y ahora basta emplear varias veces la regla izquierda del conjuntor y las reglas del particularizador para llegar a la conclusión deseada.

Nos ocupamos ahora de los axiomas del igualador. El más simple es $\Rightarrow t = t$, cuya traducción es $\Rightarrow \bigvee u(\phi_t(u) \land \phi_t(u))$. Razonamos como sigue:

$$\begin{array}{c}
\phi_t(y) \Rightarrow \phi_t(y) \qquad \phi_t(y) \Rightarrow \phi_t(y) \\ \hline
\phi_t(y) \Rightarrow \phi_t(y) \land \phi_t(y) \\ \hline
\phi_t(y) \Rightarrow \bigvee u(\phi_t(u) \land \phi_t(u)) \\ \hline
\bigvee u\, \phi_t(u) \Rightarrow \bigvee u(\phi_t(u) \land \phi_t(u))
\end{array}$$

y ahora basta cortar con $\Rightarrow \bigvee u\, \phi_t(u)$, que es un teorema de $\mathrm{I}\Sigma_1$.

Como el único relator es el igualador, los axiomas de tipo I3 se reducen a

$$s_1 = t_1,\, s_2 = t_2,\, s_1 = s_2 \Rightarrow t_1 = t_2,$$

y la traducción es

$$\bigvee u(\phi_{s_1}(u) \land \phi_{t_1}(u)),\ \bigvee u(\phi_{s_2}(u) \land \phi_{t_2}(u)),\ \bigvee u(\phi_{s_1}(u) \land \phi_{s_2}(u))$$
$$\Rightarrow \bigvee u(\phi_{t_1}(u) \land \phi_{t_2}(u))$$

Como en $I\Sigma_1$ se puede probar $\overset{1}{\bigvee} u\, \phi_{s_1}(u)$ y $\overset{1}{\bigvee} u\, \phi_{s_2}(u)$, en particular

$$\phi_{s_1}(x),\ \phi_{s_1}(z) \Rightarrow x = z, \qquad \phi_{s_2}(y),\ \phi_{s_2}(z) \Rightarrow y = z,$$

luego también podemos probar

$$\phi_{s_1}(x),\ \phi_{s_2}(y),\ \phi_{s_1}(z),\ \phi_{s_2}(z) \Rightarrow y = x,$$

y cortando con $y = x,\ \phi_{t_2}(y) \Rightarrow \phi_{t_2}(x)$, obtenemos

$$\phi_{s_1}(x),\ \phi_{s_2}(y),\ \phi_{t_2}(y),\ \phi_{s_1}(z),\ \phi_{s_2}(z) \Rightarrow \phi_{t_2}(x).$$

Aplicando la regla derecha del conjuntor con $\phi_{t_1}(x) \Rightarrow \phi_{t_1}(x)$ obtenemos

$$\phi_{s_1}(x),\ \phi_{t_1}(x),\ \phi_{s_2}(y),\ \phi_{t_2}(y),\ \phi_{s_1}(z),\ \phi_{s_2}(z) \Rightarrow \phi_{t_1}(x) \land \phi_{t_2}(x)$$

y ahora basta aplicar varias veces la regla izquierda del conjuntor y las reglas de particularizador para llegar a la conclusión.

El último axioma del igualador es el de la forma

$$s_1 = t_1, \ldots, s_n = t_n \Rightarrow F(s_1, \ldots, s_n) = F(t_1, \ldots, t_n),$$

cuya traducción es

$$\bigvee u_1(\phi_{s_1}(u_1) \land \phi_{t_1}(u_1)), \ldots, \bigvee u_n(\phi_{s_n}(u_n) \land \phi_{t_n}(u_n)) \Rightarrow \bigvee u(\phi_S(u) \land \phi_T(u)),$$

donde $S \equiv F(s_1 \ldots, s_n)$, $T \equiv F(t_1, \ldots, t_n)$.

Si algún s_i no es una variable, entonces

$$\phi_S(u) \equiv \bigvee u_1 \cdots u_n(\phi_{s_1}(u_1) \land \cdots \land \phi_{s_n}(u_n) \land \phi_U(u_1, \ldots, u_n, u)),$$

donde $U \equiv F(x_1, \ldots, x_n)$. Si, por el contrario, todos los s_i son variables, esta expresión sería

$$\phi_S(u) \equiv \bigvee u_1 \cdots u_n(u_1 = s_1 \land \cdots \land u_n = s_n \land \phi_U(u_1, \ldots, u_n, u)),$$

mientras que, según la definición que hemos dado, en este caso tendríamos que en realidad $\phi_S(u) \equiv \phi_U(s_1, \ldots, s_n, u)$, pero es claro que la fórmula precedente es lógicamente equivalente a ésta, luego no perdemos generalidad si trabajamos con aquella. Lo mismo sucede si todos los t_i son variables.

Por abreviar, llamemos Γ al conjunto de fórmulas

$$\phi_{s_1}(x_1),\ \phi_{t_1}(x_1), \ldots, \phi_{s_n}(x_n),\ \phi_{t_n}(x_n),\ \phi_{s_1}(y_1),\ \ldots, \phi_{s_n}(y_n),\ \phi_U(y_1, \ldots, y_n, y).$$

Por la unicidad, $\phi_{s_i}(x_i)$, $\phi_{s_i}(y_i) \Rightarrow x_i = y_i$ luego, cortando con el axioma

$$x_1 = y_1, \ldots, x_n = y_n,\ \phi_U(y_1, \ldots, y_n, y) \Rightarrow \phi_U(x_1, \ldots, x_n, y),$$

llegamos a que

$$\Gamma \Rightarrow \phi_U(x_1, \ldots, x_n, y)$$

Por la regla derecha del conjuntor aplicada con $\phi_{s_i}(x_i) \Rightarrow \phi_{s_i}(x_i)$ llegamos a que

$$\Gamma \Rightarrow \phi_{s_1}(x_1) \wedge \cdots \wedge \phi_{s_n}(x_n) \wedge \phi_U(x_1, \ldots, x_n, y)$$

e igualmente

$$\Gamma \Rightarrow \phi_{t_1}(x_1) \wedge \cdots \wedge \phi_{t_n}(x_n) \wedge \phi_U(x_1, \ldots, x_n, y).$$

Aplicando la regla del particularizador llegamos a

$$\Gamma \Rightarrow \phi_S(y), \qquad \Gamma \Rightarrow \phi_T(y),$$

y por la regla derecha del conjuntor $\Gamma \Rightarrow \bigvee u(\phi_S(u) \wedge \phi_T(u))$. Por otra parte, aplicando la regla izquierda del conjuntor y del particularizador, obtenemos

$$(s_1 = t_1)^*, \ldots, (s_n = t_n)^*,\ \bigvee u\, \phi_S(u) \Rightarrow \bigvee u(\phi_S(u) \wedge \phi_T(u)).$$

Ahora basta cortar con $\Rightarrow \bigvee u\, \phi_S(u)$, que es un teorema de $\mathrm{I}\Sigma_1$.

Finalmente consideramos los axiomas de los funtores. La traducción de $\Rightarrow C(x) = 0$ es $\Rightarrow \bigvee u(u = 0 \wedge u = 0)$, que claramente es un teorema. Lo mismo sucede con la de $\Rightarrow P_i^n(x_1, \ldots, x_n) = x_i$, que es $\Rightarrow \bigvee u(u = x_i \wedge u = x_i)$.

Si $F \equiv \kappa G H_1 \cdots H_m$, su axioma es:

$$\Rightarrow \kappa G H_1 \cdots H_m(x_1, \ldots, x_n) = G(H_1(x_1, \ldots, x_n), \ldots, H_m(x_1, \ldots, x_n)).$$

Su traducción es

$$\Rightarrow \bigvee u(\bigvee u_1 \cdots u_m v(\phi_{T_1}(u_1) \wedge \cdots \wedge \phi_{T_m}(u_m) \wedge \phi_{T^*}(u_1, \ldots, u_m, u)) \wedge$$
$$\bigvee u(\bigvee u_1 \cdots u_m v(\phi_{T_1}(u_1) \wedge \cdots \wedge \phi_{T_m}(u_m) \wedge \phi_{T^*}(u_1, \ldots, u_m, u))),$$

es decir, $\Rightarrow \bigvee u(\phi_F(u) \wedge \phi_F(u))$, y esto es consecuencia de que en $\mathrm{I}\Sigma_1$ se demuestra $\bigvee u\, \phi_F(u)$.

Por último, si $F \equiv \rho G H$, tenemos que considerar sus dos axiomas. El primero es

$$\Rightarrow F(x_1, \ldots, x_n, 0) = G(x_1, \ldots, x_n),$$

cuya traducción es

$$\Rightarrow \bigvee u(\bigvee u_1 \cdots u_{n+1}(u_1 = x_1 \wedge \cdots \wedge u_n = x_n \wedge u_{n+1} = 0 \wedge$$
$$\bigvee s(\mathrm{Suc}(s) \wedge \ell(s) = u_{n+1} + 1 \wedge s_{u_{n+1}} = u \wedge \phi_T(s_0) \wedge$$
$$\bigwedge i < u_{n+1}\, \phi_U(u_1, \ldots, u_n, i, s_i, s_{i+1}))) \wedge \phi_T(u)).$$

Llamamos Γ al conjunto de fórmulas

$$y_1 = x_1, \cdots, y_n = x_n,\ y_{n+1} = 0,\ \mathrm{Suc}(s),\ \ell(s) = x_{n+1} + 1,\ s_{y_{n+1}} = y,\ \phi_T(s_0),$$

$$\bigwedge i < y_{n+1}\, \phi_U(y_1, \ldots, y_n, i, s_i, s_{i+1}).$$

Es fácil ver que $y_{n+1} = 0$, $s_{y_{n+1}} = y$, $\phi_T(s_0) \Rightarrow \phi_T(y)$, luego por debilitación tenemos que $\Gamma \Rightarrow \phi_T(y)$.

Por otro lado, $\Gamma \Rightarrow \gamma$, para cada una de las fórmulas γ de Γ, por lo que aplicando las reglas derechas del conjuntor y del perticularizador, llegamos a que

$$\Gamma \Rightarrow \phi_{Fx_1\cdots x_n 0}(u) \wedge \Phi_T(u),$$

luego, introduciendo un último particularizador,

$$\Gamma \Rightarrow (F(x_1, \ldots, x_n, 0) = G(x_1, \ldots, x_n))^*.$$

Similarmente, introduciendo conjunciones y particularizadores en el antecedente llegamos a que

$$\bigvee u\, \phi_{Fx_1\cdots x_n 0}(u) \Rightarrow (F(x_1, \ldots, x_n, 0) = G(x_1, \ldots, x_n))^*,$$

pero el antecedente es un teorema de $\mathrm{I}\Sigma_1$, luego podemos eliminarlo con un corte.

El segundo axioma es

$$\Rightarrow F(x_1, \ldots, x_n, x'_{n+1}) = H(x_1, \ldots, x_n, x_{n+1}, F(x_1, \ldots, x_n, x_{n+1})).$$

Su traducción es

$$\Rightarrow \bigvee u(\phi_{T_1}(u) \wedge \phi_{T_2}(u)),$$

donde, llamando

$$S \equiv F(x_1, \ldots, x_{n+1}), \quad T \equiv G(x_1, \ldots, x_n), \quad U \equiv H(x_1, \ldots, x_{n+2}),$$

$$\begin{aligned}
\phi_{T_1}(y) \quad &\equiv \quad \bigvee u_1 \cdots u_{n+1}(u_1 = x_1 \wedge \cdots \wedge u_n = x_n \wedge u_{n+1} = x'_{n+1} \wedge \\
&\qquad \bigvee s(\mathrm{Suc}(s) \wedge \ell(s) = u_{n+1} + 1 \wedge s_{u_{n+1}} = y \wedge \phi_T(s_0) \wedge \\
&\qquad \bigwedge i < u_{n+1}\, \phi_U(u_1, \ldots, u_n, i, s_i, s_{i+1}))), \\
\phi_{T_2}(y) \quad &\equiv \quad \bigvee u_1 \cdots u_{n+2}(u_1 = x_1 \wedge \cdots \wedge u_{n+1} = x_{n+1} \wedge \\
&\qquad \phi_S(u_1, \ldots, u_{n+2}) \wedge \phi_U(u_1, \ldots, u_{n+2}, y)).
\end{aligned}$$

Es claro que estas fórmulas son lógicamente equivalentes a

$$\begin{aligned}
\phi^*_{T_1}(y) \quad &\equiv \quad \bigvee s(\mathrm{Suc}(s) \wedge \ell(s) = x'_{n+1} + 1 \wedge s_{x'_{n+1}} = y \wedge \phi_T(s_0) \wedge \\
&\qquad \bigwedge i < x'_{n+1}\, \phi_U(x_1, \ldots, x_n, i, s_i, s_{i+1}))), \\
\phi^*_{T_2}(y) \quad &\equiv \quad \bigvee v(\phi_S(x_1, \ldots, x_{n+1}, v) \wedge \phi_U(x_1, \ldots, x_{n+1}, v, y)).
\end{aligned}$$

Detallar la prueba formalizada de $\Rightarrow \bigvee u(\phi_{T_1}(u) \wedge \phi_{T_2}(u))$ sería muy laborioso, así que nos limitaremos a esbozar la idea:

Partimos de que existe un y tal que $\phi^*_{T_1}(y)$ (esto es demostrable en $\mathrm{I}\Sigma_1$). Así tenemos una sucesión s, y una simple inducción muestra que, para todo $i \leq x'_{n+1}$, la restricción $s|_i$ atestigua que se cumple $\phi_S(x_1, \ldots, x_n, i, s_i)$. En particular tenemos $\phi_S(x_1, \ldots, x_{n+1}, s_{x_{n+1}})$.

Por otra parte, aplicando a $i = x_{n+1}$ la última cláusula de $\phi^*_{T_1}(y)$ obtenemos $\phi_U(x_1, \ldots, x_{n+1}, s_{x_{n+1}}, s_{x'_{n+1}})$, que equivale a $\phi_U(x_1, \ldots, x_{n+1}, s_{x_{n+1}}, y)$. Así pues, $v = s_{x_{n+1}}$ atestigua que se cumple:

$$\phi^*_{T_2}(y) \equiv \bigvee v(\phi_S(x_1, \ldots, x_{n+1}, v) \wedge \phi_U(x_1, \ldots, x_{n+1}, v, y)).$$

En definitiva, el y que cumple $\phi^*_{T_1}(y)$, cumple también $\phi^*_{T_2}(y)$, luego podemos concluir que $\bigvee u(\phi_{T_1}(u) \wedge \phi_{T_2}(u))$. ■

Así pues, AP^+ es una extensión conservativa de AP (y lo mismo sucede con $\mathrm{I}\Sigma_n^+$ e $\mathrm{I}\Sigma_n$). Esto significa que añadir nombres para todas las funciones recursivas primitivas puede simplificar el trabajo en AP, pero no permite demostrar nuevos teoremas sobre números naturales. Se trata de una modificación tan intrascendente a efectos teóricos como lo es incluir un descriptor en una teoría axiomática de primer orden. Es sólo una forma cómoda de disponer de nombres para objetos de los que igualmente podemos hablar en la teoría describiendo el objeto cada vez que querríamos nombrarlo.

Los teoremas de AP^+ que no son teoremas de AP son simplemente aquellos que mencionan los funtores añadidos, y que no pueden probarse en AP porque no son fórmulas de $\mathcal{L}_a$. Sin embargo, todos ellos son equivalentes a fórmulas de $\mathcal{L}_a$ demostrables en AP. En particular AP^+ (resp. $\mathrm{I}\Sigma_n^+$) es consistente si y sólo si lo es AP (resp. $\mathrm{I}\Sigma_n$).

Nota En lo sucesivo no distinguiremos entre AP y AP^+ (ni entre $\mathrm{I}\Sigma_n$ e $\mathrm{I}\Sigma_n^+$). La forma usual de indicar que se quiere trabajar en AP^+ es decir algo como "suponemos que AP incluye nombres para todas las funciones recursivas primitivas junto con axiomas que las definen". ■

Una de las ventajas de incluir en AP nombres para las funciones recursivas primitivas es que ahora podemos considerar a AP (incluso a $\mathrm{I}\Sigma_1$) como una extensión de ARP de forma natural. Al contrario que en AP, en ARP dichos nombres no son redundantes, por lo que necesitamos añadírselos a AP para estar en condiciones de comparar ambas teorías.

En esta situación, la única diferencia entre ARP e $\mathrm{I}\Sigma_1$ es que en ARP el principio de inducción está restringido a fórmulas sin cuantificadores (aunque, según hemos observado, podemos extenderlo a fórmulas Δ_0, pues toda fórmula Δ_0 es equivalente a una fórmula atómica), mientras que en $\mathrm{I}\Sigma_1$ está permitida la inducción respecto de fórmulas Σ_1.

Ahora bien, mientras que la prueba de que $\mathrm{I}\Sigma_1^+$ es una extensión conservativa de $\mathrm{I}\Sigma_1$, por laboriosa que pueda ser, no es más que una comprobación rutinaria, mucho más profundo es el hecho de que $\mathrm{I}\Sigma_1$ también es una extensión conservativa de ARP. Nos ocupamos de ello en la sección siguiente.

5.3 $\mathrm{I}\Sigma_1$ como extensión de ARP

Una aplicación no trivial del cálculo secuencial es la demostración del teorema siguiente, que viene a decir que si, a partir de una fórmula Δ_0, en $\mathrm{I}\Sigma_1$ podemos probar un teorema de existencia, la demostración es necesariamente constructiva:

Teorema 5.8 *Sea $\phi(x_1,\ldots,x_n,x)$ una fórmula Δ_0 de $\mathcal{L}_{\mathrm{arp}}$ tal que*

$$\underset{\mathrm{I}\Sigma_1}{\vdash} \bigvee v\,\phi(x_1,\ldots,x_n,v).$$

Entonces existe un funtor F de rango n de $\mathcal{L}_{\mathrm{arp}}$ tal que

$$\underset{\mathrm{ARP}}{\vdash} \phi(x_1,\ldots,x_n,F(x_1,\ldots,x_n)).$$

Demostración: Tenemos que $\underset{\mathrm{I}\Sigma_1}{\vdash} \Rightarrow \bigvee v\,\phi(x_1,\ldots,x_n,v)$. Por el teorema 3.22 existe una demostración D de este secuente formada únicamente por fórmulas Δ_0 y Σ_1 (en sentido estricto, es decir, con un particularizador no acotado). Sean $y_1,\ldots,y_l$ las variables que aparecen libres en alguna fórmula de D. Vamos a probar que, para cada secuente de D

$$\gamma_1,\ldots,\gamma_r,\bigvee u_1\gamma_1',\ldots,\bigvee u_{r'}\gamma_{r'}' \Rightarrow \delta_1,\ldots,\delta_s,\bigvee v_1\delta_1',\ldots,\bigvee v_{s'}\delta_{s'}',$$

donde[5] todas las fórmulas $\gamma_i,\gamma_i',\delta_i,\delta_i'$ son Δ_0 y $s'>0$, existen funtores

$$F_i(y_1,\ldots,y_l,u_1,\ldots,u_{r'}) \qquad i=1,\ldots,s'$$

tales que

$$\underset{\mathrm{ARP}}{\vdash} \bigwedge u_1\ldots u_{r'}(\gamma_1\land\cdots\land\gamma_r\land\gamma_1'\land\cdots\land\gamma_{r'}'\rightarrow\delta_1\lor\cdots\lor\delta_s\lor\tilde{\delta}_1'\lor\cdots\lor\tilde{\delta}_{s'}'),$$

donde

$$\tilde{\delta}_i(y_1,\ldots,y_l,u_1,\ldots,u_{r'})\equiv\delta_i(y_1,\ldots,y_l,F_i(y_1,\ldots,y_l,u_1,\ldots,u_{r'})).$$

Observemos que lo que estamos afirmando es que, supuesto que se cumplan las fórmulas del antecedente con ciertos valores para las variables y_i y u_i, los funtores F_i determinan valores para las variables v_i que hacen que se cumpla el consecuente.

Vamos a probarlo para los secuentes iniciales de D y, supuesto cierto para los secuentes superiores de una regla de inferencia, lo probamos para el secuente inferior. Esto implica que el resultado es válido para todos los secuentes de D.

Para simplificar la notación, representaremos los secuentes de D en la forma

$$\gamma_i(\bar{y}),\ \bigvee u_j\,\gamma_{i'}'(u_{i'},\bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\,\delta'(v_{j'},\bar{y}),$$

donde i varía de 1 a r, que i' varía de 1 a r', que j varía de 1 a s y que j' varía de 1 a s' (entendiendo que si, por ejemplo $r=0$ hay que eliminar $\gamma_i(\bar{y})$ de la expresión, etc.) y la barra en una variable, como $\bar{y}$, indica que en realidad se trata de un número finito de variables, en este caso $y_1,\ldots,y_l$.

[5]Suponemos tácitamente que en todos los secuentes de D las variables $u_1,\ldots,u_{r'}$ son distintas en cada fórmula del antecedente, pero es claro que, sustituyendo las repetidas por otras nuevas, siempre podemos exigir que sea así.

Similarmente, la conclusión se expresa en la forma

$$\underset{\text{ARP}}{\vdash} \bigwedge \bar{u}(\gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'}, \bar{y}) \to \delta_j(\bar{y}) \lor \delta'_{j'}(F_{j'}(\bar{y}, \bar{u}), \bar{y})).$$

Para los secuentes iniciales es trivial, pues todos ellos (incluyedo los axiomas que definen los funtores de $\mathcal{L}_{\text{arp}}$) son teoremas de ARP y están formados por fórmulas atómicas, luego en ellos $s' = 0$ y no hay que probar la existencia de ningún funtor. Ahora hemos de considerar todas las reglas de inferencia.

Debilitación Partimos del secuente

$$\gamma_i(\bar{y}),\ \bigvee u_j\, \gamma'_{i'}(u_{i'}, \bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\, \delta'(v_{j'}, \bar{y}),$$

y por hipótesis de inducción existen funtores $F_{j'}(\bar{y}, \bar{u})$ tales que en ARP se demuestra

$$\bigwedge \bar{u}(\gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'}, \bar{y}) \to \delta_j(\bar{y}) \lor \delta'_{j'}(F_{j'}(\bar{y}, \bar{u}), \bar{y})).$$

Observemos que si $s' = 0$ esto sigue siendo válido si entendemos que no hay fórmulas $\delta'_{j'}$. En tal caso la fórmula se sigue directamente del hecho de que el secuente es demostrable en ARP.

Si la fórmula principal es Δ_0 el resultado es trivial, pues la fórmula sigue siendo demostrable si añadimos un $\gamma_{r+1}(\bar{y})$ o un $\delta_{s+1}(\bar{y})$.

Si la fórmula principal es Σ_1 y se añade a la izquierda, también es trivial, pues la implicación se conserva si añadimos la fórmula $\gamma'_{r'+1}(u_{r'+1}, \bar{y})$, y cambiamos el funtor $F_{j'}$ por $F^*_{j'}(\bar{y}, \bar{u}, u_{r'+1}) = F_{j'}(\bar{y}, \bar{u})$.

Consideremos finalmente el caso en que la fórmula principal es de la forma $\bigvee v_{s'+1}\, \delta'_{s'+1}(v_{s'+1}, \bar{y})$. Entonces basta tomar $F_{s'+1}(\bar{y}, \bar{u}) = 0$, pues la implicación se conserva si añadimos $\delta'_{s'+1}(F_{s'+1}(\bar{y}, \bar{u}), \bar{y})$.

Corte Supongamos que la fórmula de corte es Σ_1. Partimos de los secuentes

$$\gamma_i(\bar{y}),\ \bigvee u_{i'}\, \gamma'_{i'}(u_j, \bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\, \delta'(v_{j'}, \bar{y}),\ \bigvee w\, \alpha(w, \bar{y}),$$

$$\bigvee w\, \alpha(w, \bar{y}),\ \gamma_i(\bar{y}),\ \bigvee u_{i'}\, \gamma'_{i'}(u_{i'}, \bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee y_{j'}\, \delta'(v_{j'}, \bar{y}),$$

y suponemos que tenemos funtores $F^1_{j'}(\bar{y}, \bar{u})$, $F^2_{j'}(\bar{y}, \bar{u}, w)$ y $F^*(\bar{y}, \bar{u})$ de modo que en ARP se demuestra:

$$\bigwedge \bar{u}(\gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'}, \bar{y}) \to \delta_j(\bar{y}) \lor \delta'_{j'}(F^1_{j'}(\bar{y}, \bar{u}), \bar{y}) \lor \alpha(F^*(\bar{y}, \bar{u}), \bar{y}))$$

$$\bigwedge \bar{u}w(\alpha(w, \bar{y}) \land \gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'}, \bar{y}) \to \delta_j(\bar{y}) \lor \delta'_{j'}(F^2_{j'}(\bar{y}, \bar{u}, w), \bar{y})).$$

Notemos que no hace falta considerar el caso en que no hay fórmulas δ'_l, pues entonces el secuente inferior del corte cumple $s' = 0$ y no hay nada que probar.

Razonando en ARP, suponemos $\gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'}, \bar{y})$ y distingamos dos casos:

Si $\neg\alpha(F^*(\bar{y}, \bar{u}), \bar{y})$, entonces se cumple $\delta_j(\bar{y}) \lor \delta'_{j'}(F^1_{j'}(\bar{y}, \bar{u}), \bar{y})$.

Si $\alpha(F^*(\bar{y}, \bar{u}), \bar{y})$, se cumple $\delta_j(\bar{y}) \lor \delta'_{j'}(F^2_{j'}(\bar{y}, \bar{u}, F^*(\bar{y}, \bar{u})), \bar{y})$.

Esto nos lleva a considerar el funtor

$$F^3_{j'}(\bar{y},\bar{u}) = F^1_{j'}(\bar{y},\bar{u})(1 \dot{-} \chi_\alpha(F^*(\bar{y},\bar{u}),\bar{y})) + F^2_{j'}(\bar{y},\bar{u},F^*(\bar{y},\bar{u}))\chi_\alpha(F^*(\bar{y},\bar{u}),\bar{y}).$$

y así en cualquier caso se cumple $\delta_j(\bar{y}) \vee \delta'_{j'}(F^3_{j'}(\bar{y},\bar{u}),\bar{y})$.

Si la fórmula de corte es Δ_0 es fácil ver que basta tomar

$$F^3_{j'}(\bar{y},\bar{u}) = F^1_{j'}(\bar{y},\bar{u})(1 \dot{-} \chi_\alpha(\bar{y})) + F^2_{j'}(\bar{y},\bar{u})\chi_\alpha(\bar{y}).$$

Negador La fórmula principal de una regla del negador debe ser Δ_0, pues una fórmula Σ_1 en sentido estricto tiene que empezar por un particularizador y no por un negador. Por lo tanto, la fórmula auxiliar $\alpha(\bar{y})$ es también de tipo Δ_0. En el caso de la regla izquierda tenemos

$$\bigwedge \bar{u}(\gamma_i(\bar{y}) \wedge \alpha(\bar{y}) \wedge \gamma'_{i'}(u_{i'},\bar{y}) \rightarrow \delta_j(\bar{y}) \vee \delta'_{j'}(F_{j'}(\bar{y},\bar{u}),\bar{y})),$$

y basta observar que podemos pasar $\alpha(\bar{y})$ al consecuente de la implicación como $\neg\alpha(\bar{y})$, de modo que el secuente inferior cumple lo requerido con los mismos funtores $F_{j'}$ del secuente superior. Lo mismo se aplica a la regla derecha.

Disyuntor Como en el caso anterior, la fórmula principal y las fórmulas auxiliares tienen que ser Δ_0. Para la regla izquierda partimos de dos secuentes

$$\alpha(\bar{y}),\ \gamma_i(\bar{y}),\ \bigvee u_{i'}\,\gamma'_{i'}(u_{i'},\bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\,\delta'_{j'}(v_{j'},\bar{y}),$$

$$\beta(\bar{y}),\ \gamma_i(\bar{y}),\ \bigvee u_{i'}\,\gamma'_{i'}(u_{i'},\bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\,\delta'_{j'}(v_{j'},\bar{y}),$$

y por hipótesis de inducción existen funtores $F^1_{j'}(\bar{y},\bar{u})$, $F^2_{j'}(\bar{y},\bar{u})$ que cumplen lo requerido.

Razonando en ARP, suponemos $(\alpha(\bar{y}) \vee \beta(\bar{y})) \wedge \gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'},\bar{y})$ y distinguimos dos casos:

Si se cumple $\alpha(\bar{y})$, por la hipótesis de inducción $\delta_j(\bar{y}) \vee \delta'_{j'}(F^1_{j'}(\bar{y},\bar{u}),\bar{y})$.

Si no se cumple $\alpha(\bar{y})$, entonces se cumple $\beta(\bar{y})$ y la hipótesis de inducción nos da $\delta_j(\bar{y}) \vee \delta'_{j'}(F^2_{j'}(\bar{y},\bar{u}),\bar{y})$.

Esto nos lleva a definir

$$F^3_{j'}(\bar{y},\bar{u}) = F^1_{j'}(\bar{y},\bar{u})\chi_\alpha(\bar{y}) + F^2_{j'}(\bar{y},\bar{u})(1 \dot{-} \chi_\alpha(\bar{y})).$$

de modo que en ambos casos se cumple $\delta_j(\bar{y}) \vee \delta'_{j'}(F^3_{j'}(\bar{y},\bar{u}),\bar{y})$.

La regla derecha es mucho más simple, pues partimos de un único secuente

$$\gamma_i(\bar{y}),\ \bigvee u_{i'}\,\gamma'_{i'}(u_{i'},\bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\,\delta'_{j'}(v_{j'},\bar{y}),\ \alpha(\bar{y}),\ \beta(\bar{y})$$

y se concluye inmediatamente que el secuente inferior cumple lo requerido con los mismos funtores que el secuente superior.

Particularizador izquierda La fórmula auxiliar debe ser Δ_0, pues al añadir un particularizador a una fórmula Σ_1 en sentido estricto no obtenemos una fórmula Σ_1 en sentido estricto. Ahora bien, la fórmula principal puede ser Σ_1 en sentido estricto o Δ_0. Lo segundo sucederá si la fórmula auxiliar es de la forma $y \leq t(\bar{y}) \wedge \alpha(y, \bar{u})$ y la variable propia es y.

Consideremos primero el caso en que la fórmula principal es Σ_1. Tenemos entonces el secuente

$$\alpha(y', \bar{y}),\ \gamma_i(\bar{y}),\ \bigvee u_{i'}\, \gamma'_{i'}(u_{i'}, \bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\, \delta'_{j'}(v_{j'}, \bar{y}),$$

donde y' es la variable propia y, por consiguiente, no aparece en el grupo de variables $\bar{y}$. Por hipótesis de inducción tenemos funtores $F^1_{j'}(\bar{y}, y', \bar{u})$ que cumplen lo requerido. El secuente inferior es

$$\bigvee u' \alpha(u', \bar{y}),\ \gamma_{i'}(\bar{y}),\ \bigvee u_{i'}\, \gamma'_{i'}(u_{i'}, \bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\, \delta'_{j'}(v_{j'}, \bar{y}),$$

y es inmediato que los funtores $F^1_{j'}(\bar{y}, u', \bar{u})$ cumplen lo requerido.

Supongamos ahora que la fórmula auxiliar es $y \leq t(\bar{y}) \wedge \alpha(y, \bar{y})$, donde y es la variable propia. Consideramos los funtores

$$G_{j'}(\bar{y}) = \mu w \leq t(y)\, \chi_\alpha(w, \bar{y}),$$

$$F^2_{j'}(\bar{y}, \bar{u}) = F^1_{j'}(\bar{y}, G_{j'}(\bar{y}), \bar{u})).$$

Claramente

$$\bigwedge \bar{u}(\bigvee u' \leq t(\bar{y})\, \alpha(u', \bar{y}) \wedge \gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y}) \to \delta_j(\bar{y}) \vee \delta'_{j'}(F^2_{j'}(\bar{y}, \bar{u}), \bar{y})).$$

Particularizador derecha Tenemos que distinguir los mismos dos casos que para la regla izquierda. Partimos de un secuente de la forma

$$\gamma_i(\bar{y}),\ \bigvee u_{i'}\, \gamma'_{i'}(u_{i'}, \bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\, \delta'_{j'}(v_{j'}, \bar{y}),\ \alpha(t(\bar{y}), \bar{y}).$$

Si la fórmula principal es Σ_1, el secuente final es

$$\gamma_i(\bar{y}),\ \bigvee u_{i'}\, \gamma'_{i'}(u_{i'}, \bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\, \delta'_{j'}(v_{j'}, \bar{y}),\ \bigvee v_{s'+1}\, \alpha(v_{s'+1}, \bar{y}).$$

y es fácil ver que basta definir

$$F_{s'+1}(\bar{y}, \bar{u}) = t(\bar{y}).$$

Si la fórmula auxiliar es $t(\bar{y}) \leq t'(\bar{y}) \wedge \alpha(t(\bar{y}), \bar{y})$, de modo que la fórmula principal es $\bigvee w \leq t'(\bar{y})\, \alpha(w, \bar{y})$, es inmediato que el secuente inferior cumple lo requerido con los mismos funtores $F_{j'}$ que el secuente superior.

Generalizador Para las reglas del generalizador podemos dar un argumento análogo al empleado para las del particularizador, aunque más simple, porque la fórmula principal es necesariamente Δ_0, con lo que sólo puede darse uno de los dos casos que hemos distinguido para el caso del particularizador.

Alternativamente, podemos suponer que la demostración D no contiene ninguna regla del generalizador. En efecto, el conjunto Φ de las fórmulas Σ_1 que no tienen generalizadores es cerrado para sustitución y para subfórmulas, y toda semifórmula Σ_1 es lógicamente equivalente a una semifórmula Σ_1 sin generalizadores, ya que en una semifórmula Δ_0 los generalizadores se pueden transformar en particularizadores y negadores. Es claro que si probamos el teorema para una semifórmula equivalente a ϕ, vale también para ϕ, luego podemos suponer que ϕ no tiene generalizadores y, a su vez, que en la demostración D ninguna fórmula tiene generalizadores.

Inducción Supongamos que la fórmula de inducción es Σ_1 en sentido estricto. Entonces el secuente superior es

$$\bigvee u'\alpha(u',y,\bar{y}),\ \gamma_i(\bar{y}),\ \bigvee u_{i'}\,\gamma'_{i'}(u_{i'},\bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\,\delta'_{j'}(v_{j'},\bar{y}),\ \bigvee u'\alpha(u',y{+}1,\bar{y}),$$

donde y es la variable propia. Por hipótesis de inducción tenemos funtores $F^1_{j'}(y,\bar{y},u',\bar{u})$ y $F'(y,\bar{y},u',\bar{u})$ de modo que en ARP se demuestra:

$$\bigwedge u'\bar{u}(\alpha(u',y,\bar{y}) \land \gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'},\bar{y})$$
$$\rightarrow \delta_j(\bar{y}) \lor \delta'_{j'}(F_{j'}(y,\bar{y},u',\bar{u}),\bar{y}) \lor \alpha(F'(y,\bar{y},u',\bar{u}),y+1,\bar{y})).$$

El secuente inferior es

$$\bigvee u'\alpha(u',0,\bar{y}),\ \gamma_i(\bar{y}),\ \bigvee u_{i'}\,\gamma'_{i'}(u_j,\bar{y}) \Rightarrow \delta_j(\bar{y}),\ \bigvee v_{j'}\,\delta'_{j'}(v_{j'},\bar{y}),\ \bigvee u'\alpha(u',t(\bar{y}),\bar{y}).$$

Sea $G(y,\bar{y},u',\bar{u})$ el funtor determinado por

$$G(0,\bar{y},u',\bar{u}) = u', \quad G(y+1,\bar{y},u',\bar{u}) = F'(y,\bar{y},G(y,\bar{y},u',\bar{u}),\bar{u}),$$

a su vez, sean

$$\begin{array}{rcl} G_{j'}(\bar{y},u',\bar{u}) & = & \mu w \leq t(\bar{y})\,\delta'_{j'}(F^1_{j'}(w,\bar{y},G(w,\bar{y},u',\bar{u})),\bar{y}), \\ F^2_{j'}(\bar{y},u',\bar{u}) & = & F^1_{j'}(G_{j'}(\bar{y},u',\bar{u}),\bar{y},G(G_{j'}(\bar{y},u',\bar{u}),\bar{y},u',\bar{u}),\bar{u}). \\ F''(\bar{y},u',\bar{u}) & = & G(t(\bar{y}),\bar{y},u',u). \end{array}$$

Veamos que los funtores $F^2_{j'}$ y F'' cumplen lo requerido. Para ello fijamos $\bar{y}$, u', $\bar{u}$ y suponemos

$$\alpha(u',0,\bar{y}) \land \gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'},\bar{y}).$$

Queremos probar

$$\delta_j(\bar{y}) \lor \delta'_{j'}(F^2_{j'}(\bar{y},u',\bar{u}),\bar{y}) \lor \alpha(F''(\bar{y},u',\bar{u}),t(\bar{y}),\bar{y}).$$

Para ello suponemos que no se cumple ninguna de las fórmulas $\delta_j(\bar{y})$ ni tampoco $\delta'_{j'}(F^2_{j'}(\bar{y},u',\bar{u}),\bar{y})$ y vamos a probar $\alpha(F''(\bar{y},u',\bar{u}),t(\bar{y}),\bar{y})$. Por definición de F'', esto equivale a $\alpha(G(t(\bar{y}),\bar{y},u',\bar{u}),t(\bar{y}),\bar{y})$.

Si existiera un $w \leq t(\bar{y})$ tal que $\delta'_{j'}(F^1_{j'}(w, \bar{y}, G(w, \bar{y}, u', \bar{u})), \bar{y})$, entonces el mínimo sería $w = G_{j'}(\bar{y}, u', \bar{u})$, y a su vez

$$\begin{aligned} F^1_{j'}(w, \bar{y}, G(w, \bar{y}, u', \bar{u})) &= F^1_{j'}(G_{j'}(\bar{y}, u', \bar{u}), \bar{y}, G(G_{j'}(\bar{y}, u', \bar{u}), \bar{y}, u', \bar{u})) \\ &= F^2_{j'}(\bar{y}, u', \bar{u}), \end{aligned}$$

luego se cumpliría $\delta'_{j'}(F^2_{j'}(\bar{y}, u', \bar{u}), \bar{y})$, en contra de lo supuesto.

Así pues, para todo $w \leq t(\bar{y})$, se cumple $\neg\delta'_{j'}(F^1_{j'}(w, \bar{y}, G(w, \bar{y}, u', \bar{u})), \bar{y})$.

Vamos a probar por inducción sobre w que

$$\bigwedge w \leq t(\bar{y})\, \alpha(G(w, \bar{y}, u', \bar{u}), w, \bar{y}).$$

Notemos que la fórmula es Δ_0 en $\mathcal{L}_{\mathrm{arp}}$, por lo que la inducción puede realizarse en ARP. Aplicando esto a $w = t(\bar{y})$ obtenemos la conclusión.

Para $w = 0$ hay que probar $\alpha(u', 0, \bar{y})$, pero ésta es una de nuestras hipótesis. Supuesto cierto para $w < t(\bar{y})$, la hipótesis de inducción sobre el secuente superior de la inducción nos da que

$$\alpha(G(w, \bar{y}, u', \bar{u}), w, \bar{y}) \wedge \gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y}) \rightarrow \delta_j(\bar{y}) \vee$$

$$\delta'_{j'}(F^1_{j'}(w, \bar{y}, G(w, \bar{y}, u', \bar{u}), \bar{u}), \bar{y}) \vee \alpha(F'(w, \bar{y}, G(w, \bar{y}, u', \bar{u}), \bar{u}), w + 1, \bar{y}).$$

Pero estamos suponiendo que no se cumple ninguna de las fórmulas $\delta_j(\bar{y})$ y hemos probado que tampoco se cumple $\delta'_{j'}(F^1_{j'}(w, \bar{y}, G(w, \bar{y}, u', \bar{u}), \bar{u}), \bar{y})$, luego concluimos que se cumple $\alpha(F'(w, \bar{y}, G(w, \bar{y}, u', \bar{u}), \bar{u}), w+1, \bar{y})$, que, por definición de G, es lo mismo que $\alpha(G(w+1, \bar{y}, u', \bar{u}), w+1, \bar{y})$, lo que completa la inducción.

Por último, si la fórmula de inducción es Δ_0, el argumento es una simplificación del que acabamos de dar. Indicamos únicamente la definición de los funtores $F^2_{j'}$:

$$\begin{aligned} G_{j'}(\bar{y}, \bar{u}) &= \mu w \leq t(\bar{y})\, \delta'_{j'}(F^1_{j'}(w, \bar{y}), \bar{y}), \\ F^2_{j'}(\bar{y}, \bar{u}) &= F^1_{j'}(G_{j'}(\bar{y}, \bar{u}), \bar{y}, \bar{u}). \end{aligned}$$

Con esto termina la inducción y tenemos probado que el secuente final de D cumple la propiedad considerada, es decir, existe un funtor $F^*(y_1, \ldots, y_l)$ tal que

$$\underset{\mathrm{ARP}}{\vdash} \phi(x_1, \ldots, x_n, F^*(\bar{y})).$$

En principio, $y_1, \ldots, y_l$ recorre todas las variables libres en algún secuente de D, incluyendo $x_1, \ldots, x_n$, pero podemos particularizar la fórmula anterior sustituyendo por 0 las y_i distintas de las x_i, con lo que F^* da lugar a otro funtor $F(x_1, \ldots, x_n)$ de modo que

$$\underset{\mathrm{ARP}}{\vdash} \phi(x_1, \ldots, x_n, F(x_1, \ldots, x_n)). \qquad \blacksquare$$

Ahora observamos que el teorema anterior se automejora ligeramente:

Teorema 5.9 *Sea $\phi(x_1, \ldots, x_n, c)$ una fórmula Σ_1 de $\mathcal{L}_{\mathrm{arp}}$ tal que*

$$\underset{\mathrm{I}\Sigma_1}{\vdash} \bigvee v\, \phi(x_1, \ldots, x_n, v).$$

Entonces existe un funtor F de $\mathcal{L}_{\mathrm{arp}}$ tal que

$$\underset{\mathrm{ARP}}{\vdash} \phi(x_1, \ldots, x_n, F(x_1, \ldots, x_n)).$$

DEMOSTRACIÓN: Sea $\phi(x_1, \ldots, x_n, v) \equiv \bigvee w\, \chi(w, x_1, \ldots, x_n, v)$, donde la fórmula χ es Δ_0, y sea

$$\phi'(x_1, \ldots, x_n, v) \equiv \bigvee v_0 v_1 \leq v\, (v = (v_0, v_1) \wedge \chi(v_0, x_1, \ldots, x_n, v_1)).$$

Claramente, ϕ' también es Δ_0 y $\underset{\mathrm{I}\Sigma_1}{\vdash} \bigvee v\, \phi'(x_1, \ldots, x_n, v)$. Por el teorema anterior existe un funtor F^* tal que en ARP se demuestra

$$\phi'(x_1, \ldots, x_n, F^*(x_1, \ldots, x_n)).$$

Consideremos el funtor dado por

$$F(x_1, \ldots, x_n) = \mu v_1 \leq F^*(\bar{x}) \bigvee v_0 \leq F^*(\bar{x}) (F^*(\bar{x}) = (v_0, v_1))$$

Así, como se cumple $\phi'(\bar{x}, F^*(\bar{x}))$, tenemos que $F^*(\bar{x}) = (v_0, v_1)$ de modo que $\chi(v_0, \bar{x}, v_1)$, luego $\phi(\bar{x}, v_1)$ y $F(\bar{x}) = v_1$, luego $\phi(\bar{x}, F(\bar{x}))$. ■

De aquí se sigue:

Teorema 5.10 *Si ϕ es una fórmula Π_2 de $\mathcal{L}_{\mathrm{arp}}$, entonces*

$$\underset{\mathrm{ARP}}{\vdash} \phi \quad \textit{si y sólo si} \quad \underset{\mathrm{I}\Sigma_1}{\vdash} \phi.$$

DEMOSTRACIÓN: Sea $\phi \equiv \bigwedge v \bigvee u \phi(x_1, \ldots, x_n, v, u)$ una fórmula de tipo Π_2 en $\mathcal{L}_{\mathrm{arp}}$, y supongamos que es demostrable en IΣ_1. Entonces también lo es la fórmula $\bigvee u\, \phi(\bar{x}, v, u)$ y por el teorema anterior existe un funtor F tal que en ARP se demuestra $\phi(\bar{x}, v, F(\bar{x}, v))$, luego también se demuestra $\bigvee u\, \phi(\bar{x}, v, u)$, luego también ϕ. ■

Este teorema afirma que IΣ_1 es una extensión conservativa de ARP para fórmulas de tipo Π_2. Ahora bien, si recordamos que ARP no es más que un "envoltorio" conveniente de la teoría ARP presentada en el capítulo anterior, de modo que las fórmulas "genuinas" de ARP (las que se corresponden con fórmulas de dicha presentación sin signos lógicos) son las fórmulas Δ_0, entonces podemos afirmar que IΣ_1 es una extensión conservativa de ARP en el sentido de que toda fórmula del lenguaje $\mathcal{L}_{\mathrm{arp}}$ (el original, sin signos lógicos) es demostrable en ARP si y sólo si lo es IΣ_1.

En particular tenemos que ARP es consistente si y sólo si lo es IΣ_1.

El teorema 5.9 tiene otra consecuencia de interés. En [LM 7.13] definimos el concepto de función demostrablemente recursiva en una teoría aritmética dada, y observamos que las funciones recursivas primitivas son demostrablemente recursivas en IΣ_1. Ahora podemos probar el recíproco:

Teorema 5.11 *Las funciones recursivas primitivas son las funciones demostrablemente recursivas en* $\mathrm{I}\Sigma_1$.

DEMOSTRACIÓN: Sólo tenemos que probar una implicación: si una función f es demostrablemente recursiva en $\mathrm{I}\Sigma_1$, esto significa que existe una fórmula[6] $\phi(x_1,\ldots,x_n,y)$ de tipo Σ_1 en $\mathcal{L}_a$ tal que

$$f(a_1,\ldots,a_n)=a \quad \text{syss} \quad \mathbb{N}\underset{\mathrm{I}\Sigma_1}{\vdash}\phi(\bar{a}_1,\ldots,\bar{a}_n,\bar{a})$$

y además $\underset{\mathrm{I}\Sigma_1}{\vdash}\bigwedge x_1\cdots x_n\overset{1}{\bigvee}y\,\phi(x_1,\ldots,x_n,y)$. Por el teorema 5.9 existe un funtor F tal que

$$\underset{\mathrm{I}\Sigma_1}{\vdash}\phi(x_1,\ldots,x_n,F(x_1,\ldots,x_n)).$$

La unicidad de ϕ hace que, de hecho,

$$\underset{\mathrm{I}\Sigma_1}{\vdash}\bigwedge x_1\cdots x_n y(y=F(x_1,\ldots,x_n)\leftrightarrow\phi(x_1,\ldots,x_n,y)).$$

En particular esta equivalencia es verdadera en $\mathbb{N}$, lo que implica que f es la función recursiva primitiva determinada por la definición de F. ■

5.4 La formalización del cálculo secuencial

Los teoremas de incompletitud de Gödel se basan en la posibilidad de formalizar la lógica en cualquier teoría aritmética. Esto se desarrolla con detalle en el capítulo VIII de [LM] para el caso del cálculo deductivo "a la Hilbert" considerado allí, y nada impide hacer lo mismo con el cálculo secuencial. En este capítulo veremos los detalles. Concretamente, veremos que el cálculo secuencial es formalizable en ARP, luego en particular en $\mathrm{I}\Sigma_1$. De aquí extraeremos algunas consecuencias notables, como que en AP puede demostrarse la consistencia de todas las teorías $\mathrm{I}\Sigma_n$, lo que a su vez implica que AP no es finitamente axiomatizable.

Aunque podríamos formalizar el cálculo secuencial sobre un lenguaje formal arbitrario, por simplicidad vamos a considerar únicamente el caso de AP sobre el lenguaje $\mathcal{L}_a$ (sin añadir los funtores que representan a las funciones recursivas primitivas, aunque nada impide incluirlos también).

La formalización de aritmética de Peano en AP o en ARP consiste en identificar los signos de $\mathcal{L}_a$ con números naturales, de modo que los términos y fórmulas de $\mathcal{L}_a$ pueden verse como sucesiones finitas de números naturales, los secuentes pueden verse como pares de conjuntos finitos de números naturales y las demostraciones como árboles finitos de secuentes.

[6]Como en esta demostración no necesitamos el cálculo secuencial, no necesitamos distinguir entre variables libres y ligadas.

Concretamente, podemos suponer que las variables libres de $\mathcal{L}_a$ son las potencias $2, 2^2, 2^3, \ldots$ y las variables ligadas son las potencias $3, 3^2, 3^3, \ldots$, así como que los demás signos de $\mathcal{L}_a$ son los números naturales dados por la tabla siguiente (en la que hemos excluido las potencias de 2 y de 3, reservadas para las variables):

$=$	$\neg$	$\vee$	$\bigwedge$	$\bigvee$	0	S	$+$	$\cdot$	$\leq$
0	1	5	6	7	10	11	12	13	14

Con este convenio, cada cadena de signos de $\mathcal{L}_a$ (en particular, cada término y cada fórmula de $\mathcal{L}_a$) es una sucesión finita de números naturales que, a su vez, a través del convenio establecido en el capítulo anterior, puede identificarse con un número natural.

Cadenas de signos Puesto que en lo sucesivo se van a mezclar signos lógicos, como $\neg$ o $\vee$, con los números naturales que los formalizan en $\mathrm{I}\Sigma_1$, conviene introducir una notación que los distinga. Para ello usaremos ángulos de Quine:

Si ζ es un signo de $\mathcal{L}_a$ (con lo que técnicamente es un número natural), representaremos por $\ulcorner\zeta\urcorner$ el numeral que en la secciones anteriores representábamos por $\bar{\zeta}$. Explícitamente:

$$\ulcorner x_i \urcorner \equiv \overline{2^{i+1}}, \quad \ulcorner u_i \urcorner \equiv \overline{3^{i+1}},$$

$$\ulcorner = \urcorner \equiv \bar{0}, \quad \ulcorner \neg \urcorner \equiv \bar{1}, \quad \ulcorner \vee \urcorner \equiv \bar{5}, \quad \ulcorner \bigwedge \urcorner \equiv \bar{6}, \quad \ulcorner \bigvee \urcorner \equiv \bar{7},$$

$$\ulcorner 0 \urcorner \equiv \overline{10}, \quad \ulcorner S \urcorner \equiv \overline{11}, \quad \ulcorner + \urcorner \equiv \overline{12}, \quad \ulcorner \cdot \urcorner \equiv \overline{13}, \quad \ulcorner \leq \urcorner \equiv \overline{14}.$$

Definición 5.12 Definimos las fórmulas:

$$\begin{aligned}
x \in \mathrm{VarLib}(\ulcorner\mathcal{L}_a\urcorner) &\equiv \textstyle\bigvee i \leq x\, x = \bar{2}^{i+\bar{1}},\\
x \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) &\equiv \textstyle\bigvee i \leq x\, x = \bar{3}^{i+\bar{1}},\\
x \in \mathrm{Var}(\ulcorner\mathcal{L}_a\urcorner) &\equiv x \in \mathrm{VarLib}(\ulcorner\mathcal{L}_a\urcorner) \vee x \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner),\\
x \in \mathrm{Sig}(\ulcorner\mathcal{L}_a\urcorner) &\equiv x = \ulcorner 0 \urcorner \vee x = \ulcorner S \urcorner \vee x = \ulcorner + \urcorner \vee x = \ulcorner \cdot \urcorner \vee x = \ulcorner = \urcorner \vee\\
&\qquad x = \ulcorner \neg \urcorner \vee x = \ulcorner \vee \urcorner \vee x = \ulcorner \textstyle\bigvee \urcorner \vee x \in \mathrm{Var}(\ulcorner\mathcal{L}_a\urcorner),\\
s \in \mathrm{Cad}(\ulcorner\mathcal{L}_a\urcorner) &\equiv \textstyle\bigwedge i < \ell(s)\ s_i \in \mathrm{Sig}(\ulcorner\mathcal{L}_a\urcorner),\\
s \in \mathrm{SucCad}(\ulcorner\mathcal{L}_a\urcorner) &\equiv \textstyle\bigwedge i < \ell(s)\ s_i \in \mathrm{Cad}(\ulcorner\mathcal{L}_a\urcorner).
\end{aligned}$$

En lo sucesivo, cuando no haya posibilidad de confusión, escribiremos simplemente $0, 1, 2, \ldots$ para nombrar los numerales en $\mathcal{L}_a$ en lugar de $\bar{0}, \bar{1}, \bar{2}, \ldots$, como estábamos haciendo. Sin embargo, distinguiremos cuidadosamente, por ejemplo, entre la suma $+$ de números naturales y el número natural $\ulcorner + \urcorner = 12$ que formaliza al funtor suma de $\mathcal{L}_a$.

Semitérminos y semifórmulas Para definir los términos y las fórmulas, primero tenemos que definir los semitérminos y las semifórmulas. Para ello definimos un funtor mediante el teorema de recursión completa 4.19:

$$ST(t) = \chi[\bigvee x \leq t(u \in \mathrm{Var}(\ulcorner\mathcal{L}_a\urcorner) \wedge t = \langle u\rangle) \vee t = \langle\ulcorner 0\urcorner\rangle \vee$$

$$\bigvee uv < t(ST(u) = 1 \wedge ST(v) = 1 \wedge (t = \langle\ulcorner S\urcorner\rangle{}^\frown u \vee$$

$$t = \langle\ulcorner+\urcorner\rangle{}^\frown u^\frown v) \vee t = \langle\ulcorner\cdot\urcorner\rangle{}^\frown u^\frown v))].$$

Definimos la fórmula $t \in \mathrm{STerm}(\ulcorner\mathcal{L}_a\urcorner) \equiv ST(t) = 1$.

Notemos la necesidad de distinguir, al menos teóricamente, entre un número natural n y la sucesión $\langle n\rangle$ de longitud 1 cuyo único término es n. Sin embargo, en la práctica, si $x \in \mathrm{Var}(\ulcorner\mathcal{L}_a\urcorner)$, escribiremos también x para referirnos al semitérmino $\langle x\rangle$. Igualmente escribiremos $\ulcorner 0\urcorner$ en lugar de $\langle\ulcorner 0\urcorner\rangle$.

De la propia definición de ST se sigue que t es un semitérmino si y sólo si se cumple uno de los casos siguientes:

1. Es una variable,
2. Es $\ulcorner 0\urcorner$,
3. Es de la forma $\ulcorner S\urcorner t$ para otro semitérmino t,
4. Es de la forma $t_1\ulcorner+\urcorner t_2$ o $t_1\ulcorner\cdot\urcorner t_2$, para ciertos semitérminos t_1, t_2, donde usamos la notación

$$t_1\ulcorner+\urcorner t_2 \equiv \langle\ulcorner+\urcorner\rangle{}^\frown t_1{}^\frown t_2, \qquad t_1\ulcorner\cdot\urcorner t_2 \equiv \langle\ulcorner\cdot\urcorner\rangle{}^\frown t_1{}^\frown t_2.$$

Similarmente definimos las semifórmulas por recursión completa:

$$SF(\alpha) = \chi[\bigvee t_1 t_2 \leq \alpha(t_1, t_2 \in \mathrm{STerm}(\ulcorner\mathcal{L}_a\urcorner) \wedge$$

$$\alpha = \langle\ulcorner=\urcorner\rangle{}^\frown t_1{}^\frown t_2 \vee \alpha = \langle\ulcorner\leq\urcorner\rangle{}^\frown t_1{}^\frown t_2) \vee$$

$$\bigvee \beta\gamma u < \alpha(SF(\alpha) = 1 \wedge SF(\beta) = 1 \wedge u \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge$$

$$(\alpha = \langle\ulcorner\neg\urcorner\rangle{}^\frown\beta \vee \alpha = \langle\ulcorner\vee\urcorner\rangle{}^\frown\beta^\frown\gamma \vee$$

$$\alpha = \langle\ulcorner\bigwedge\urcorner\rangle{}^\frown\langle u\rangle{}^\frown\beta \vee \alpha = \langle\ulcorner\bigvee\urcorner\rangle{}^\frown\langle u\rangle{}^\frown\beta))]$$

Definimos la fórmula $\alpha \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \equiv SF(\alpha) = 1$.

De la definición se sigue trivialmente que α es una semifórmula si y sólo si se cumple uno de los casos siguientes:

1. Es de la forma $t_1\ulcorner=\urcorner t_2$ o $t_1\ulcorner\leq\urcorner t_2$, para ciertos semitérminos t_1 y t_2,
2. Es de la forma $\ulcorner\neg\urcorner\alpha$, para cierta semifórmula α,
3. Es de la forma $\alpha\ulcorner\vee\urcorner\beta$, para ciertas semifórmulas α y β,

4. Es de la forma $\ulcorner\bigwedge\urcorner u\,\alpha$, para una semifórmula α y una variable ligada u,
5. Es de la forma $\ulcorner\bigvee\urcorner u\,\alpha$, para una semifórmula α y una variable ligada u, donde hemos introducido la notación

$$t_1\ulcorner{=}\urcorner t_2 \equiv \langle\ulcorner{=}\urcorner\rangle^\frown t_1{}^\frown t_2 \quad \text{y} \quad t_1\ulcorner{\leq}\urcorner t_2 \equiv \langle\ulcorner{\leq}\urcorner\rangle^\frown t_1{}^\frown t_2$$

$$\ulcorner\neg\urcorner\alpha \equiv \langle\ulcorner\neg\urcorner\rangle^\frown\alpha, \quad \alpha\ulcorner\vee\urcorner\beta \equiv \big\langle\ulcorner\vee\urcorner\big\rangle^\frown\alpha^\frown\beta,$$

$$\ulcorner\bigwedge\urcorner u\,\alpha \equiv \langle\ \ulcorner\bigwedge\urcorner\ \rangle^\frown\langle u\rangle^\frown\alpha \quad \ulcorner\bigvee\urcorner u\,\alpha \equiv \langle\ \ulcorner\bigvee\urcorner\ \rangle^\frown\langle u\rangle^\frown\alpha.$$

Necesitaremos los funtores que, a partir de un término o una fórmula, nos calculan los elementos a partir de los cuales están compuestos:

$$\begin{aligned}
\mathrm{Pre}_1(z) &= \mu u \leq z(z = \ulcorner S\urcorner u \vee z = \ulcorner\neg\urcorner u \vee \textstyle\bigvee v \leq z(z = \ulcorner\bigwedge\urcorner vu \vee z = \ulcorner\bigvee\urcorner vu \vee \\
&\quad z = u\ulcorner{+}\urcorner v \vee z = u\ulcorner{\cdot}\urcorner v \vee z = u\ulcorner{=}\urcorner v \vee z = u\ulcorner{\leq}\urcorner v \vee z = u\ulcorner\vee\urcorner v)),\\
\mathrm{Pre}_2(z) &= \mu u \leq z(\textstyle\bigvee v \leq z(z = v\ulcorner{+}\urcorner u \vee z = v\ulcorner{\cdot}\urcorner u \vee z = v\ulcorner{=}\urcorner u \vee \\
&\quad z = v\ulcorner{\leq}\urcorner u \vee z = v\ulcorner\vee\urcorner u)),\\
\mathrm{PreV}(z) &= \mu u \leq z(\textstyle\bigvee v \leq z(z = \ulcorner\bigwedge\urcorner uv \vee z = \ulcorner\bigvee\urcorner uv)).
\end{aligned}$$

Variables libres y ligadas Si t es un semitérmino, definimos

$$\mathrm{VLT}(t) = \{u < t \mid u \in \mathrm{Var}(\ulcorner\mathcal{L}_a\urcorner) \wedge u \in \mathcal{R}t\}.$$

El conjunto de las variables libres en una semifórmula α lo definimos por recursión completa:

$$\begin{aligned}
\mathrm{VLF}(\alpha) &= \chi[\textstyle\bigvee t_1t_2 \leq \alpha(t_1, t_2 \in \mathrm{STerm}(\ulcorner\mathcal{L}_a\urcorner)\\
&\quad \wedge (\alpha = t_1\ulcorner{=}\urcorner t_2 \vee \alpha = t_1\ulcorner{\leq}\urcorner t_2))]\\
&\quad \cdot(\mathrm{VLT}(\mathrm{Pre}_1(\alpha)) \cup \mathrm{VLT}(\mathrm{Pre}_2(\alpha)))\\
&+ \chi[\textstyle\bigvee\beta < \alpha(\beta \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \wedge \alpha = \ulcorner\neg\urcorner\beta)]\\
&\quad \cdot\mathrm{VLF}(\mathrm{Pre}_1(\alpha))\\
&+ \chi[\textstyle\bigvee\beta\gamma < \alpha(\beta, \gamma \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \wedge \alpha = \beta\ulcorner\vee\urcorner\gamma)]\\
&\quad \cdot(\mathrm{VLF}(\mathrm{Pre}_1(\alpha)) \cup \mathrm{VLF}(\mathrm{Pre}_2(\alpha)))\\
&+ \chi[\textstyle\bigvee\beta u < \alpha(\beta \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner)\\
&\quad \wedge u \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge (\alpha = \ulcorner\bigwedge\urcorner u\,\beta \vee \alpha = \ulcorner\bigvee\urcorner u\,\beta))]\\
&\quad \cdot(\mathrm{VLF}(\mathrm{Pre}_1(\alpha)) \setminus \{u\}).
\end{aligned}$$

Ahora podemos definir como sigue los términos y las fórmulas de $\ulcorner\mathcal{L}_a\urcorner$:

$$t \in \mathrm{Term}(\ulcorner\mathcal{L}_a\urcorner) \equiv t \in \mathrm{STerm}(\ulcorner\mathcal{L}_a\urcorner) \wedge \textstyle\bigwedge x \leq t(x \in \mathrm{VLT}(t) \rightarrow x \in \mathrm{VLib}(\ulcorner\mathcal{L}_a\urcorner)),$$

$$\alpha \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner) \equiv \alpha \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \wedge \textstyle\bigwedge x \leq \alpha(x \in \mathrm{VLF}(\alpha) \rightarrow x \in \mathrm{VLib}(\ulcorner\mathcal{L}_a\urcorner)).$$

Una ligera variante de la definición de $\alpha \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner)$ permite definir la fórmula $\alpha \in \Delta_0$, que expresa que α es una fórmula de tipo Δ_0. A partir de ahí podemos definir la fórmula con dos variables libres:

$$\alpha \in \Sigma_n^* \equiv n > 0 \land \alpha \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner) \land \ell(\alpha) > 2n \land$$

$$\bigwedge i < n((2 \mid i \to \alpha_{2i} = \ulcorner\bigvee\urcorner) \land (2 \nmid i \to \alpha_{2i} = \ulcorner\bigwedge\urcorner)),$$

(donde $2 \mid i$ expresa simplemente que I es par).

Análogamente se define una fórmula $\alpha \in \Pi_n^*$, también de tipo Δ_1, y a su vez podemos definir

$$\alpha \in \Sigma_n \equiv \bigvee m \leq n(\alpha \in \Sigma_m^* \lor (m < n \land \alpha \in \Pi_m^*)),$$

$$\alpha \in \Pi_n \equiv \bigvee m \leq n(\alpha \in \Pi_m^* \lor (m < n \land \alpha \in \Sigma_m^*)).$$

Sustitución Por último formalizamos la sustitución de una variable por un término en una semiexpresión:

$$\begin{aligned}
\mathtt{S}_x^t Z \;=\;& \chi[Z = \langle x\rangle] \cdot t \\
+\;& \chi[Z = \langle\ulcorner 0\urcorner\rangle \bigvee z \leq Z(z \in \mathrm{Var}(\ulcorner\mathcal{L}_a\urcorner) \land z \neq x \land Z = \langle z\rangle)] \cdot Z \\
+\;& \chi[\bigvee T' < Z(T' \in \mathrm{STerm}(\ulcorner\mathcal{L}_a\urcorner) \land Z = \ulcorner S\urcorner T')] \\
& \cdot(\ulcorner S\urcorner \mathtt{S}_x^t \mathrm{Pre}_1(Z)) \\
+\;& \chi[\bigvee T'T'' < Z(T', T'' \in \mathrm{STerm}(\ulcorner\mathcal{L}_a\urcorner) \land Z = T'\ulcorner+\urcorner T'')] \\
& \cdot(\mathtt{S}_x^t \mathrm{Pre}_1(Z)\ulcorner+\urcorner \mathtt{S}_x^t \mathrm{Pre}_2(Z)) \\
+\;& \chi[\bigvee T'T'' < Z(T', T'' \in \mathrm{STerm}(\ulcorner\mathcal{L}_a\urcorner) \land Z = T'\ulcorner\cdot\urcorner T'')] \\
& \cdot(\mathtt{S}_x^t \mathrm{Pre}_1(Z)\ulcorner\cdot\urcorner \mathtt{S}_x^t \mathrm{Pre}_2(Z)) \\
+\;& \chi[\bigvee t_1 t_2 < Z(Z = t_1\ulcorner=\urcorner t_2)] \cdot (\mathtt{S}_x^t \mathrm{Pre}_1(Z)\ulcorner=\urcorner \mathtt{S}_x^t \mathrm{Pre}_2(Z)) \\
+\;& \chi[\bigvee t_1 t_2 < Z(Z = t_1\ulcorner\leq\urcorner t_2)] \cdot (\mathtt{S}_x^t \mathrm{Pre}_1(Z)\ulcorner\leq\urcorner \mathtt{S}_x^t \mathrm{Pre}_2(Z)) \\
+\;& \chi[\bigvee \beta < Z(\beta \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \land Z = \ulcorner\neg\urcorner\beta)] \\
& \cdot(\ulcorner\neg\urcorner \mathtt{S}_x^t \mathrm{Pre}_1(Z)) \\
+\;& \chi[\bigvee \beta\gamma < Z(\beta, \gamma \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \land Z = \beta\ulcorner\lor\urcorner\gamma)] \\
& \cdot(\mathtt{S}_x^t \mathrm{Pre}_1(Z)\ulcorner\lor\urcorner \mathtt{S}_x^t \mathrm{Pre}_2(Z)) \\
+\;& \bigvee \beta < Z(\beta \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \land Z = \ulcorner\bigwedge\urcorner x\,\beta) \cdot Z \\
+\;& \bigvee \beta u < Z(\beta \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \land u \in \mathrm{VLib}(\ulcorner\mathcal{L}_a\urcorner) \land u \neq x \land Z = \ulcorner\bigwedge\urcorner u\,\beta) \\
& \cdot(\ulcorner\bigwedge\urcorner u\, \mathtt{S}_x^t \mathrm{Pre}_1(Z)) \\
+\;& \bigvee \beta < Z(\beta \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \land Z = \ulcorner\bigvee\urcorner x\,\beta) \cdot Z \\
+\;& \bigvee \beta u < Z(\beta \in \mathrm{SForm}(\ulcorner\mathcal{L}_a\urcorner) \land u \in \mathrm{VLib}(\ulcorner\mathcal{L}_a\urcorner) \land u \neq x \land Z = \ulcorner\bigvee\urcorner u\,\beta) \\
& \cdot(\ulcorner\bigvee\urcorner u\, \mathtt{S}_x^t \mathrm{Pre}_1(Z)).
\end{aligned}$$

Relación entre $\mathcal{L}_a$ y $\ulcorner\mathcal{L}_a\urcorner$ Las definiciones que hemos dado en el apartado precedente pretenden formalizar los conceptos básicos asociados al lenguaje $\mathcal{L}_a$ de la aritmética de Peano, pero necesitamos precisar en qué consiste esta noción de "formalización", es decir, en qué sentido preciso los conceptos formales que hemos definido en ARP se corresponden con los conceptos metamatemáticos que pretenden formalizar.

Si $S = (S_0, \ldots, S_{n-1})$ es una sucesión finita de números naturales, las definiciones de la sección 4.6 nos permiten identificarla con un número natural, y llamaremos $\ulcorner S\urcorner$ al numeral correspondiente en $\mathcal{L}_a$.

Llamando $\mathbb{N}$ al modelo natural de ARP, en el que cada funtor se interpreta como la función recursiva primitiva determinada por sus axiomas asociados, es inmediato a partir de las definiciones dadas que

$$\ell(S) = n \quad \text{syss} \quad \mathbb{N} \vDash \ell(\ulcorner S\urcorner) = \bar{n},$$

donde a la izquierda $\ell(S)$ representa la longitud de la sucesión, mientras que a la derecha $\ell(x) = y$ es la fórmula que tenemos definida en $\mathcal{L}_{\mathrm{arp}}$. Igualmente, si $i < n$, se cumple que

$$S_i = s \quad \text{syss} \quad \mathbb{N} \vDash (\ulcorner S\urcorner)_{\bar{\imath}} = \bar{s}.$$

A su vez, es claro a partir de las definiciones que una sucesión ζ de números naturales es una cadena de signos de $\mathcal{L}_a$ si y sólo si

$$\mathbb{N} \vDash \ulcorner\zeta\urcorner \in \mathrm{Cad}(\ulcorner\mathcal{L}_a\urcorner).$$

Lo mismo se aplica a todas las definiciones que hemos dado. Por ejemplo, es claro que[7] una sucesión α de números naturales es una fórmula de $\mathcal{L}_a$ si y sólo si

$$\mathbb{N} \vDash \ulcorner\alpha\urcorner \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner).$$

Todas las definiciones que hemos dado en el apartado anterior están pensadas para que hechos como éste se cumplan de forma obvia. Es precisamente en este sentido en el que las fórmulas que hemos definido formalizan las nociones metamatemáticas correspondientes que pretenden formalizar.

Esta relación de naturaleza semántica implica otra puramente sintáctica en virtud del teorema 5.6. Por ejemplo, aplicando a la fórmula $x \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner)$, vemos que[8]

$$\text{si } \alpha \text{ es una fórmula de } \mathcal{L}_a \quad \text{entonces} \quad \underset{\mathrm{ARP}}{\vdash} \ulcorner\alpha\urcorner \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner)$$

[7] Cuando decimos que "es claro" nos referimos a que basta interpretar una sentencia como $\ulcorner\alpha\urcorner \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner)$ según la definición de $\mathbb{N} \vDash$ para convencernos de que lo que afirma es precisamente que α es una fórmula de $\mathcal{L}_a$ (apoyándonos, naturalmente, en que esto mismo vale para todos los conceptos previos que aparecen en la definición de $x \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner)$).

[8] El teorema 5.6 nos da equivalencias, pero escribimos aquí únicamente la implicación cuya prueba es, en realidad, puramente sintáctica y finitista.

y, aplicándolo a $x \notin \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner)$, tenemos también que

$$\text{si } \alpha \text{ no es una fórmula de } \mathcal{L}_a \quad \text{entonces} \quad \underset{\mathrm{ARP}}{\vdash} \ulcorner\alpha\urcorner \notin \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner).$$

Esto se aplica a todas las fórmulas que hemos introducido. Por ejemplo, para toda variable x, todo término t y toda semiexpresión θ, en ARP se demuestra que si $\theta^* \equiv \mathtt{S}_x^t\theta$, entonces en ARP se demuestra

$$\ulcorner\theta^*\urcorner = \mathtt{S}_{\ulcorner x\urcorner}^{\ulcorner t\urcorner}\ulcorner\theta\urcorner$$

o, equivalentemente, en ARP se demuestra:

$$\ulcorner\mathtt{S}_x^t\theta\urcorner = \mathtt{S}_{\ulcorner x\urcorner}^{\ulcorner t\urcorner}\ulcorner\theta\urcorner.$$

Árboles finitos Para formalizar el concepto de demostración del cálculo secuencial necesitamos considerar árboles binarios:

Un conjunto A es un *árbol (finito, binario)* si cumple

$$\mathrm{arb}\, A \equiv 0 \in A \land \bigwedge s \in A \bigwedge i < \ell(s)(s|_i \in A \land (s_i = 0 \lor s_i = 1)).$$

Equivalentemente, un árbol (finito, binario) es un conjunto de sucesiones de ceros y unos cerrado para restricciones.

Si h es un número natural, podemos definir $2^{<h}$ como el conjunto de todas las sucesiones de ceros y unos de longitud menor que h. Explícitamente:

$$2^{<h} = \{s < (1)_h \mid \ell(s) < h \land \bigwedge i < \ell(s)(s_i = 0 \lor s_i = 1)\},$$

donde $(1)_h$ es la sucesión que consta de h unos, que se define inmediatamente por recursión. Claramente $2^{<h}$ es un árbol.

En todo árbol consideraremos la relación de orden

$$s \sqsubseteq t \equiv \ell(s) \leq \ell(t) \land t|_{\ell(s)} = s.$$

La sucesión vacía 0 es el mínimo elemento de cualquier árbol y nos referiremos a él como su *raíz.* Los elementos de un árbol se llaman *nodos*, La longitud de un nodo (considerado como sucesión) se llama también su *altura.* Así, la raíz es el único nodo de altura cero. La *altura* de un árbol A se define como[9]

$$\mathrm{alt}\, A = \mathrm{máx}\{\ell(s) \mid s \in A\} + 1.$$

Equivalentemente, la altura de A es el mínimo h tal que $A \subset 2^{<h}$.

Diremos que un nodo de un árbol A es *terminal* si no está estrictamente contenido en ningún otro nodo. Un nodo es *ramificado* si está contenido en dos nodos distintos de altura una unidad mayor. Si no se da ninguno de estos dos casos diremos que es *no ramificado.*

[9]Técnicamente, podemos considerar la enumeración $\mathrm{Suc}(A)$, a partir de ella definir por recurrencia $F(0) = 0$, $F(n+1) = F(n) \cup \{\ell(\mathrm{Suc}(A)_n)\}$ y $\mathrm{alt}\, A = \mathrm{máx}\, F(|A|)$.

Si A es un árbol de altura h y $s \in A$, podemos definir el árbol

$$A_s = \{t \in 2^{<h} \mid s^\frown t \in A\}.$$

Si A es un árbol de altura h, podemos definir la aplicación $\operatorname{rang}_A : A \longrightarrow I_h$ mediante $\operatorname{rang}_A(s) = \operatorname{alt} A_s - 1$.

Así, $s \in A$ es un nodo terminal si y sólo si $A_s = \{0\}$, si y sólo si $\operatorname{rang}_A(s) = 0$ y, en general,

$$\operatorname{rang}_A(s) = \sup\{\operatorname{rang}_A(t) + 1 \mid s \sqsubset t\},$$

entendiendo que el supremo del conjunto vacío es 0.

Secuentes Un número natural S es un *secuente* si cumple

$$\sec S \equiv \bigvee S_0 S_1 \leq S(S = \langle S_0, S_1\rangle \land S_0 \subset \operatorname{Form}(\ulcorner\mathcal{L}_a\urcorner) \land S_1 \subset \operatorname{Form}(\ulcorner\mathcal{L}_a\urcorner)).$$

Si Γ y Δ son números naturales tales que $\Gamma \subset \operatorname{Form}(\ulcorner\mathcal{L}_a\urcorner) \land \Delta \subset \operatorname{Form}(\ulcorner\mathcal{L}_a\urcorner)$, escribiremos

$$\Gamma \Rightarrow \Delta \equiv \langle \Gamma, \Delta\rangle\,,$$

de modo que todo secuente S cumple $S = (S_0 \Rightarrow S_1)$.

Un *árbol de secuentes* es un número natural D que cumple[10]

$$\operatorname{arbsec} D \equiv \bigvee A \leq D \operatorname{arb} A \land D : A \longrightarrow \mathbb{N} \land \bigwedge s \in A \sec D_s.$$

Llamaremos $F(D)$ al conjunto de todas las fórmulas que aparecen en los secuentes de D (cuya existencia se prueba en ARP por Δ_0-especificación a partir de I_D).

Axiomas Definimos la fórmula "ser un axioma lógico" como

$$\operatorname{Axl} S \equiv \bigvee \alpha \leq S(\alpha \in \operatorname{Form}(\ulcorner\mathcal{L}_a\urcorner) \land S = (\{\alpha\} \Rightarrow \{\alpha\})).$$

Similarmente podemos definir los axiomas del igualador. La fórmula $\operatorname{Axi} S$ es la disyunción de las fórmulas siguientes:

1. $\bigvee t \leq S(t \in \operatorname{Term}(\ulcorner\mathcal{L}_a\urcorner) \land S = (\varnothing \Rightarrow \{t \ulcorner{=}\urcorner t\}))$,
2. $\bigvee s_1 t_1 \leq S(t_1, t_2 \in \operatorname{Term}(\ulcorner\mathcal{L}_a\urcorner) \land S = (\{s_1 \ulcorner{=}\urcorner t_1\} \Rightarrow \{\ulcorner S\urcorner s_1 \ulcorner{=}\urcorner \ulcorner S\urcorner t_1\}))$,
3. $\bigvee s_1 s_2 t_1 t_2 \leq S(s_1, s_2, t_1, t_2 \in \operatorname{Term}(\ulcorner\mathcal{L}_a\urcorner) \land$
   $S = (\{s_1 \ulcorner{=}\urcorner t_1, s_2 \ulcorner{=}\urcorner t_2\} \Rightarrow \{s_1 \ulcorner{+}\urcorner s_2 \ulcorner{=}\urcorner t_1 \ulcorner{+}\urcorner t_2\}))$,

[10] La fórmula $D : A \longrightarrow \mathbb{N}$ debe entenderse como que D es un conjunto de pares ordenados cuyo dominio es A y de modo que no contenga dos pares ordenados distintos con la misma primera componente. La $\mathbb{N}$ como conjunto imagen sólo indica que no especificamos ningún conjunto imagen.

4. $\bigvee s_1 s_2 t_1 t_2 \leq S(s_1, s_2, t_1, t_2 \in \mathrm{Term}(\ulcorner\mathcal{L}_a\urcorner) \wedge$
$S = (\{s_1 \ulcorner=\urcorner t_1, s_2 \ulcorner=\urcorner t_2\} \Rightarrow \{s_1 \ulcorner\cdot\urcorner s_2 \ulcorner=\urcorner t_1 \ulcorner\cdot\urcorner t_2\})),$

5. $\bigvee s_1 s_2 t_1 t_2 \leq S(s_1, s_2, t_1, t_2 \in \mathrm{Term}(\ulcorner\mathcal{L}_a\urcorner) \wedge$
$S = (\{s_1 \ulcorner=\urcorner t_1, s_2 \ulcorner=\urcorner t_2, s_1 \ulcorner=\urcorner s_2\} \Rightarrow \{t_1 \ulcorner=\urcorner t_2\})),$

6. $\bigvee s_1 s_2 t_1 t_2 \leq S(s_1, s_2, t_1, t_2 \in \mathrm{Term}(\ulcorner\mathcal{L}_a\urcorner) \wedge$
$S = (\{s_1 \ulcorner=\urcorner t_1, s_2 \ulcorner=\urcorner t_2, s_1 \ulcorner\leq\urcorner s_2\} \Rightarrow \{t_1 \ulcorner\leq\urcorner t_2\})),$

Similarmente se define la fórmula $\mathrm{Axp}\, S$ que determina los axiomas propios de AP, que incluyen los seis esquemas considerados en el teorema 3.3 más los siete añadidos en la definición 3.4. Así, $\mathrm{Axp}\, S$ es la disyunción de 13 fórmulas, la última de las cuales es:

$$\bigvee st \leq S(s, t \in \mathrm{Term}(\ulcorner\mathcal{L}_a\urcorner) \wedge S = \{s \ulcorner\leq\urcorner \ulcorner S\urcorner t\} \Rightarrow \{s \ulcorner\leq\urcorner t, s \ulcorner=\urcorner \ulcorner S\urcorner t\}).$$

Definimos $\mathrm{Ax}\, S \equiv \mathrm{Axl}\, S \vee \mathrm{Axi}\, S \vee \mathrm{Axp}\, S$.

Reglas de inferencia Ahora podemos definir las diez reglas de inferencia. Explicitamos sólo cuatro de ellas como ejemplo:

$$\mathrm{DebI}(S, T, \alpha) \equiv \sec S \wedge \sec T \wedge \bigvee \Gamma\Delta \leq T(S = (\Gamma \Rightarrow \Delta) \wedge T = (\Gamma \cup \{\alpha\} \Rightarrow \Delta)),$$

$$\mathrm{Corte}(S, S', T, \alpha) \equiv \sec S \wedge \sec S' \wedge \sec T \wedge \bigvee \Gamma\Delta \leq T(S = (\Gamma \Rightarrow \Delta \cup \{\alpha\}) \wedge$$
$$S' = (\Gamma \cup \{\alpha\} \Rightarrow \Delta) \wedge T = (\Gamma \Rightarrow \Delta)),$$

$$\mathrm{PartiI}(S, T, u, y, \alpha) \equiv \sec S \wedge \sec T \wedge u \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge y \in \mathrm{VarLib}(\ulcorner\mathcal{L}_a\urcorner) \wedge$$
$$\ulcorner\bigvee\urcorner u\alpha \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner) \wedge \bigvee \Gamma\Delta \leq T(S = (\{\mathsf{S}_u^y \alpha\} \cup \Gamma \Rightarrow \Delta) \wedge$$
$$T = (\{\ulcorner\bigvee\urcorner u\, \alpha\} \cup \Gamma \Rightarrow \Delta) \wedge \bigwedge \beta \in \Gamma \cup \Delta \cup \{\alpha\}\ y \notin \mathrm{VLF}(\beta)).$$

$$\mathrm{Ind}(S, T, \alpha, t, y) \equiv \sec S \wedge \sec T \wedge \alpha \in \mathrm{Form}(\ulcorner\mathcal{L}_a\urcorner) \wedge t \in \mathrm{Term}(\ulcorner\mathcal{L}_a\urcorner) \wedge$$
$$y \in \mathrm{Var}(\ulcorner\mathcal{L}_a\urcorner) \wedge \bigvee \Gamma\Delta \leq T(S = (\{\alpha\} \cup \Gamma \Rightarrow \Delta \cup \{\mathsf{S}_y^{\ulcorner S\urcorner y} \alpha\})$$
$$\wedge\, T = (\{\mathsf{S}_y^0 \alpha\} \cup \Gamma \Rightarrow \Delta \cup \{\mathsf{S}_y^t \alpha\}) \wedge \bigwedge \beta \in \Gamma \cup \Delta\ y \notin \mathrm{VLF}(\beta)).$$

Demostraciones A partir de aquí podemos definir el concepto de demostración:

$$\mathrm{Dm}_{\mathrm{AP}}\, D \equiv \mathrm{arbsec}\, D \wedge \bigwedge s \in \mathcal{D}D((\mathrm{Nt}\, s \wedge \mathrm{Ax}\, D_s)$$
$$\vee\, (\mathrm{Nnr}\, s \wedge (\cdots)) \vee (\mathrm{Nr}\, s \wedge (\cdots))),$$

donde $\mathrm{Nt}\, s$, $\mathrm{Nnr}\, s$ y $\mathrm{Nr}\, s$ son las fórmulas que formalizan los conceptos de "nodo terminal", "nodo no ramificado" y "nodo ramificado", respectivamente, y los puntos suspensivos representan disyunciones que recorren todas las reglas de inferencia con un secuente superior en el primer caso y con dos secuentes superiores en el segundo. Por ejemplo, los segundos puntos suspensivos son la disyunción:

$$\bigvee \alpha \leq D_s \ \mathrm{Corte}(D_{s^\frown\langle 0\rangle}, D_{s^\frown\langle 1\rangle}, D_s, \alpha) \lor$$

$$\bigvee \alpha\beta \leq D_s \ \mathrm{DisI}(D_{s^\frown\langle 0\rangle}, D_{s^\frown\langle 1\rangle}, D_s, \alpha, \beta),$$

donde DisI es la regla izquierda del disyuntor, definida de forma obvia.

Definimos $\mathrm{Dm}_{\mathrm{I}\Sigma_\mathrm{n}} D$ modificando la definición de $\mathrm{Dm}_{\mathrm{AP}}$ en el punto en que aparece la regla de inducción, añadiendo la exigencia de que la fórmula de inducción sea Σ_n.

Si en la definición de $\mathrm{Dm}_{\mathrm{AP}} D$ o $\mathrm{Dm}_{\mathrm{I}\Sigma_\mathrm{n}} D$ añadimos $\mathrm{Sec}(S)$ y $A_\varnothing = S$ obtenemos las fórmulas

$$\overset{D}{\underset{\mathrm{AP}}{\vdash}} S, \qquad \overset{D}{\underset{\mathrm{I}\Sigma_\mathrm{n}}{\vdash}} S,$$

que expresan que D es una demostración del secuente S en AP o $\mathrm{I}\Sigma_n$, respectivamente.

Si D es una demostración en AP (o en $\mathrm{I}\Sigma_n$) de un secuente S, podemos codificarla como una asignación de secuentes a los nodos de un árbol binario finito.[11] Los convenios que estamos utilizando nos permiten codificar dicha asignación como un número natural, cuyo numeral $\ulcorner D \urcorner$ cumple

$$\mathbb{N} \vDash \overset{\ulcorner D\urcorner}{\underset{\mathrm{AP}}{\vdash}} \ulcorner S \urcorner, \qquad \text{o} \qquad \mathbb{N} \vDash \overset{\ulcorner D\urcorner}{\underset{\mathrm{I}\Sigma_\mathrm{n}}{\vdash}} \ulcorner S \urcorner,$$

respectivamente, con lo que dicha sentencia es demostrable en ARP. Finalmente, podemos definir

$$\underset{\mathrm{AP}}{\vdash} S \equiv \bigvee D \overset{D}{\underset{\mathrm{AP}}{\vdash}} S, \qquad \underset{\mathrm{I}\Sigma_\mathrm{n}}{\vdash} S \equiv \bigvee D \overset{D}{\underset{\mathrm{I}\Sigma_\mathrm{n}}{\vdash}} S,$$

que son claramente fórmulas de tipo Σ_1, pero, así como todas las fórmulas que hemos definido hasta aquí eran trivialmente Δ_0, no sucede así en este caso.

Para cada $\alpha \in \mathrm{Form}(\ulcorner \mathcal{L}_a \urcorner)$, podemos definir

$$\underset{\mathrm{AP}}{\vdash} \alpha \equiv \underset{\mathrm{AP}}{\vdash} (\varnothing \Rightarrow \{\alpha\}), \qquad \underset{\mathrm{I}\Sigma_\mathrm{n}}{\vdash} \alpha \equiv \underset{\mathrm{I}\Sigma_\mathrm{n}}{\vdash} (\varnothing \Rightarrow \{\alpha\}),$$

y podemos probar (en ARP) que estas fórmulas son equivalentes a las fórmulas análogas definidas en términos de cualquier cálculo deductivo "a la Hilbert", formalizando para ello un procedimiento explícito para obtener una demostración secuencial de α a partir de una no secuencial y viceversa.[12]

[11] Dicho árbol será único si adoptamos, por ejemplo, el convenio, irrelevante en la práctica, de que los nodos no ramificados se prolongan siempre con un 0 y no con un 1.

[12] Si consideramos dos conceptos distintos de lenguaje formal, por ejemplo, uno en el que los signos primitivos sean $\neg$, $\rightarrow$ y $\bigwedge$ y otro en el que sean $\neg$, $\lor$ y $\bigvee$, además hay que formalizar un criterio para transformar una fórmula de un lenguaje formal en otra semánticamente equivalente del otro.

La formalización del teorema de eliminación de cortes libres En los apartados anteriores hemos visto cómo es posible ir formalizando paulatinamente en ARP todos los conceptos del cálculo secuencial. Sólo hemos considerado los más básicos, pero el lector debería convencerse de que no hay ningún impedimento teórico para formalizar en ARP toda la parte sintáctica del cálculo secuencial (es decir, excluyendo los resultados que involucran modelos, como el teorema de completitud semántica). En particular, podemos formalizar la demostración del teorema de eliminación de cortes libres y su consecuencia, el teorema 3.21.

Por ejemplo, la demostración del teorema de eliminación de cortes libres no es más que la descripción de un proceso del que no hemos dado todos los detalles por no perdernos en precisiones farragosas, pero que, debidamente detallado, podría expresarse como un programa de ordenador que, dándole como entrada cualquier demostración en las condiciones del teorema, nos calcularía una demostración del mismo secuente final sin cortes libres. Formalizar en ARP la demostración del teorema de eliminación de cortes libres no es ni más ni menos complicado que escribir detalladamente un algoritmo que pueda entender un ordenador para eliminar cortes libres (y justificar que el algoritmo realmente cumple su objetivo para cualquier demostración dada).

El hecho de que todo el proceso sea calculable en la práctica se traduce en que todos los objetos involucrados pueden formalizarse mediante funtores adecuados que los calculan, y en que todas las fórmulas consideradas sean de tipo Δ_0. Esto a su vez nos asegura que podemos probar la existencia de todos los objetos que necesitamos considerar (pues el axioma de especificación está restringido en ARP a fórmulas Δ_0) y que podemos llevar a cabo todo argumento inductivo necesario (pues la inducción también está restringida a fórmulas Δ_0).

En suma, lo que sucede es que las limitaciones lógicas que impone ARP (como la restricción de la inducción a fórmulas Δ_0, etc.) están pensadas para excluir toda forma de razonamiento no constructivo, pero no oponen resistencia alguna a los razonamientos finitistas constructivos.[13]

Más precisamente, una vez constatamos que sólo necesitamos trabajar con términos definibles en ARP y con fórmulas Δ_0, nos encontramos con que ARP pone a nuestra disposición toda la potencia de la teoría de conjuntos de Zermelo sin el axioma de infinitud (incluso con el axioma de elección, si queremos, aunque éste es trivial en nuestro contexto, ya que sólo estamos tratando con números naturales), y esto es garantía suficiente de que cualquier argumento finitista que maneje tales conceptos es formalizable.[14]

[13]Se puede objetar que el cálculo secuencial maneja conjuntos infinitos, como el conjunto de todas las variables, o el de todas las fórmulas, etc., pero estos “conjuntos” pueden tratarse en todo momento como propiedades posibles de objetos finitos determinadas por fórmulas, de modo que nunca necesitamos operar con el conjunto de todas las fórmulas, sino únicamente distinguir los números naturales que son fórmulas de los que no lo son, y esto se consigue con la fórmula $x \in \mathrm{Form}(\ulcorner \mathcal{L}_a \urcorner)$.

[14]El axioma de reemplazo de ZFC sólo se necesita para definir ordinales y justificar la recursión transfinita, nada de lo cual es relevante en nuestro contexto. De todos modos, recordemos que en ARP se cumple el teorema 4.28, que es una versión “efectiva” del axioma de reemplazo, en la que se garantiza que podemos reemplazar cada $u \in y$ por otro número $t(u)$ dado por un término, y esta forma de determinarlo (en lugar de mediante una fórmula

Por ello, lo único relevante de toda la formalización del cálculo secuencial que hemos venido exponiendo es el hecho de que hemos podido definir todos los conceptos mediante funtores y fórmulas Δ_0. Que esto basta para formalizar todos los resultados relacionados con tales conceptos es poco menos que inmediato.

Vamos a dedicar el resto de esta sección a mostrar que los conceptos más relevantes que hacen falta para demostrar el teorema de eliminación de cortes libres (como el concepto de corte libre, sin ir más lejos) también se pueden formalizar mediante funtores y fórmulas Δ_0, con lo cual el lector debería convencerse de que, como estamos indicando, este teorema es formalizable en ARP.

Aquí nos encontramos con una pequeña dificultad, consistente en que en la exposición informal del argumento hemos omitido muchos detalles técnicos irrelevantes a la hora de convencernos de que, en efecto, los cortes libres son eliminables, pero que hay que tener en cuenta a la hora de justificar que la prueba es formalizable respetando las restricciones que impone ARP.

Por ejemplo, a menudo hemos asociado conceptos a fórmulas o secuentes que, en sentido estricto, no dependen únicamente de la fórmula o de secuente considerado, sino de su posición en una demostración prefijada. Para precisar este hecho introducimos el concepto de fórmula situada en una demostración:

$$\mathrm{fs}_D\,\sigma \equiv \bigvee si\alpha < \sigma(\sigma = \langle s, i, \alpha\rangle \land s \in \mathcal{D}D \land i \in \{0,1\} \land \alpha \in (D_s)_i)$$

En otras palabras, una *fórmula situada* en una demostración D es una terna formada por un nodo del dominio de D, un índice $i \in \{0,1\}$ que hace referencia al antecedente o al consecuente del secuente D_s y una fórmula α perteneciente a dicho antecedente o consecuente. El conjunto $\mathrm{FS}(D)$ de todas las fórmulas situadas de D puede especificarse como subconjunto de $A \times \{0,1\} \times F(D)$.

La *relación de posición* en $\mathrm{FS}(D)$ es la relación de orden parcial dada por

$$\sigma < \sigma' \equiv \sigma, \sigma' \in \mathrm{FS}(D) \land \bigvee si\alpha < \sigma \bigvee s'\alpha' < \sigma'(\sigma = \langle s, i, \alpha\rangle \land$$

$$\sigma' = \langle s', i, \alpha'\rangle \land s \sqsubseteq s' \land s \neq s'),$$

que significa que σ' está situada sobre σ en el árbol de secuentes.

Ahora podemos definir la función $\mathrm{fp} : \mathcal{D}D \longrightarrow \mathcal{P}\mathrm{FS}(D)$ que a cada nodo s le asigna el conjunto $\mathrm{fp}(s)$ de fórmulas principales del secuente D_s. Convenimos en que se trata del conjunto vacío si D_s es un secuente inicial de la demostración y si es el secuente inferior de una regla de corte. En los demás casos, $\mathrm{fp}(s)$ consta de una única fórmula salvo si D_s es el secuente inferior de una regla de inducción, en cuyo caso hay dos fórmulas principales.

Similarmente podemos definir $\mathrm{fa} : \mathcal{D}D \longrightarrow \mathcal{P}\mathrm{FS}(D)$ que a cada nodo s le asigna el conjunto de fórmulas auxiliares de la regla cuyo secuente inferior es D_s, entendiendo que dicho conjunto es vacío en el caso en que D_s es un secuente inicial o el secuente inferior de una regla de debilitación.

$\phi(u, v))$, garantiza que sabemos cómo construir $t(u)$ a partir de u.

Definimos también la relación "ser un descendiente directo inmediato"

$$\sigma <_{\mathrm{ddi}} \sigma' \equiv \sigma, \sigma' \in \mathrm{FS}(D) \land \bigvee si\alpha < \sigma \bigvee s'i'\alpha' < \sigma'(\sigma = \langle s, i, \alpha\rangle \land$$
$$\sigma' = \langle s', i', \alpha'\rangle \land s \sqsubseteq s' \land \ell(s') = \ell(s) + 1 \land i = i' \land \alpha = \alpha').$$

a partir de la cual podemos definir la relación "ser un descendiente directo"

$$\sigma <_{\mathrm{dd}} \sigma' \equiv \bigvee n < D \bigvee f \in \mathrm{FS}(D)^n (n > 0 \land f(0) = \sigma \land f(n-1) = \sigma' \land$$
$$\bigwedge i < n \; f(i) <_{\mathrm{ddi}} f(i+1)).$$

Con estos ingredientes ya es pura rutina formalizar la definición de *profundidad* mediante una aplicación $p : \mathrm{FS}(D) \longrightarrow \mathbb{N}$. Para tener en cuenta la posibilidad de que la profundidad tome el valor $-\infty$ podemos convenir en que $p(\sigma) = 0$ significa que la profundidad es $-\infty$, mientras que $p(\sigma) = 1$ significa que la profundidad es 0, etc. Así, al formalizar, por ejemplo, el apartado 4) de la definición, es decir, que la profundidad de la fórmula principal de una regla de inferencia lógica es una unidad mayor que el máximo de las profundidades de las fórmulas auxiliares de la regla, hay que modificar esto estableciendo que es una unidad mayor si dicho máximo es distinto de 0 y es 0 en caso contrario.

Si D es una demostración y $A = \mathcal{D}$, podemos partir A en trece subconjuntos disjuntos,

$$\mathrm{Axl}(D), \quad \mathrm{Axi}(D), \quad \mathrm{Axp}(D), \quad \mathrm{Debi}(D), \quad \mathrm{Debd}(D), \quad \mathrm{Cor}(D), \quad \mathrm{Ni}(D),$$
$$\mathrm{Nd}(D), \quad \mathrm{Disi}(D), \quad \mathrm{Disd}(D), \quad \mathrm{Pi}(D), \quad \mathrm{Pd}(D), \quad \mathrm{Ind}(D),$$

cada uno de los cuales contiene a un nodo s según si el secuente D_s es un axioma lógico, un axioma del igualador, un axioma propio, el secuente inferior de una regla de debilitación izquierda, etc.

Si $s \in \mathrm{Cor}(D)$, el conjunto $\mathrm{fa}(s)$ de sus fórmulas auxiliares tiene exactamente dos elementos (las dos fórmulas de corte), en términos de los cuales podemos definir la función $p : \mathrm{Cor}(D) \longrightarrow \mathbb{N}$ que asigna a cada corte su profundidad, lo que a su vez permite definir los cortes libres, etc.

Similarmente podemos formalizar todos los conceptos sintácticos necesarios para describir las demostraciones. Por ejemplo, podemos definir la función

$$\mathrm{vp} : \mathrm{Pi}(D) \cup \mathrm{Ind}(D) \longrightarrow \mathrm{Var}(\ulcorner \mathcal{L}_a \urcorner)$$

que a cada regla del particularizador izquierda o de inducción le asigna su variable propia, etc.

Aunque seguir la prueba del teorema de eliminación de cortes libres paso por paso justificando que todos los conceptos involucrados se pueden formalizar en ARP sería laboriosísimo, los ejemplos que hemos dado sobre la forma en que podemos proceder en la práctica, junto con los argumentos generales que muestran que no cabe esperar ningún inconveniente teórico a que el proceso de formalización pueda completarse sin dificultad, deberían bastar para que el lector se convenciera de que es pura rutina obtener una demostración en ARP de dicho teorema, así como del teorema 3.21, cuya versión formalizada es la siguiente:

Teorema 5.13 *La sentencia siguiente es un teorema de* ARP:

$$\bigwedge n \bigwedge \alpha \in \Sigma_n (\underset{\mathrm{I\Sigma_n}}{\vdash} \alpha \rightarrow \bigvee D(\underset{\mathrm{I\Sigma_n}}{\overset{D}{\vdash}} (\varnothing \Rightarrow \{\alpha\}) \wedge F(D) \subset \Sigma_n)).$$

Observemos que en el enunciado de este teorema aparece la fórmula $\underset{\mathrm{I\Sigma_n}}{\vdash} \alpha$, que es Σ_1, pero no Δ_0. No obstante, de esta hipótesis se deduce inmediatamente que existe una demostración D^* tal que

$$\underset{\mathrm{I\Sigma_n}}{\overset{D^*}{\vdash}} (\varnothing \Rightarrow \{\alpha\})$$

y el resto de la prueba consiste en obtener a partir de D^* otra demostración D que cumpla además la condición $F(D) \subset \Sigma_n$. Una vez fijada D^*, todos los conceptos involucrados en la prueba se formalizan mediante funtores y fórmulas Δ_0, y por ello la prueba es ciertamente formalizable en ARP. En la sección siguiente extraeremos una consecuencia notable de este resultado.

5.5 La reflexividad de AP

Ahora estamos en condiciones de probar un resultado que podría parecer elemental, pero que no lo es:

Teorema 5.14 *Si n es un número natural y α es una sentencia de clase Σ_n en $\mathcal{L}_a$, entonces*

$$\underset{\mathrm{I\Sigma_{n+1}}}{\vdash} (\underset{\ulcorner \mathrm{I\Sigma_n} \urcorner}{\vdash} \ulcorner \alpha \urcorner \rightarrow \alpha).$$

Demostración: Podemos entender la hipótesis del teorema en el sentido débil de que α es una sentencia equivalente en $\mathrm{I}\Sigma_n$ a una sentencia α_0 de clase Σ_n en sentido estricto. En efecto, tenemos que $\underset{\mathrm{I\Sigma_n}}{\vdash} (\alpha \leftrightarrow \alpha_0)$, luego

$$\mathbb{N} \vDash \underset{\ulcorner \mathrm{I\Sigma_n} \urcorner}{\vdash} (\ulcorner \alpha \urcorner \leftrightarrow \ulcorner \alpha_0 \urcorner),$$

pero la fórmula a la derecha de $\vDash$ es una sentencia Δ_0 de $\mathcal{L}_{\mathrm{arp}}$, luego el teorema 5.6 nos da que $\underset{\mathrm{ARP}}{\vdash} \underset{\ulcorner \mathrm{I\Sigma_n} \urcorner}{\vdash} (\ulcorner \alpha \urcorner \leftrightarrow \ulcorner \alpha_0 \urcorner)$.

Por lo tanto, si en $\mathrm{I}\Sigma_{n+1}$ suponemos $\underset{\ulcorner \mathrm{I\Sigma_n} \urcorner}{\vdash} \ulcorner \alpha \urcorner$, de ahí deducimos $\underset{\ulcorner \mathrm{I\Sigma_n} \urcorner}{\vdash} \ulcorner \alpha_0 \urcorner$ y si a partir de aquí (supuesto que el teorema sea cierto para sentencias Σ_n en sentido estricto) podemos demostrar α_0, a su vez de α_0 concluimos α, y el teorema queda probado bajo la forma débil de la hipótesis.

Equivalentemente, no perdemos generalidad si suponemos que α es Σ_n en sentido estricto (no meramente equivalente a una fórmula Σ_n).

Según el teorema 5.13, a partir de $\underset{\mathrm{I\Sigma_n}}{\vdash} \ulcorner \alpha \urcorner$, en ARP, luego en particular en $\mathrm{I}\Sigma_{n+1}$, puede probarse que $\underset{\mathrm{I\Sigma_n}}{\vdash} (\varnothing \Rightarrow \{\ulcorner \alpha \urcorner\})$ mediante una demostración D cuyos secuentes contienen únicamente fórmulas de $\mathcal{L}_a$ de tipo Σ_n (en sentido estricto).

En [LM 8.32] definimos las fórmulas $\mathbb{N} \vDash_{\Sigma_n} \delta[v]$ y $\mathbb{N} \vDash_{\Pi_n} \delta[v]$ de tipos Σ_n y Π_n respectivamente, que tienen sentido cuando δ es una fórmula de tipo[15] exactamente Σ_n o Π_n y que satisfacen el teorema [LM 8.33]. Un poco más en general, podemos considerar la fórmula[16] Σ_n:

$$\mathbb{N} \vDash^*_{\Sigma_n} \delta[v] \equiv (\delta \in \Sigma_0 \wedge \mathbb{N} \vDash_{\Sigma_0} \delta[v]) \vee (\delta \in \Sigma_1 \wedge \mathbb{N} \vDash_{\Sigma_1} \delta[v]) \vee$$

$$(\delta \in \Pi_1 \wedge \mathbb{N} \vDash_{\Pi_1} \delta[v]) \vee \cdots \vee (\delta \in \Sigma_{n-1} \wedge \mathbb{N} \vDash_{\Sigma_{n-1}} \delta[v]) \vee$$

$$(\delta \in \Pi_{n-1} \wedge \mathbb{N} \vDash_{\Pi_{n-1}} \delta[v]) \vee (\delta \in \Sigma_n \wedge \mathbb{N} \vDash_{\Sigma_n} \delta[v]).$$

Sea X el conjunto (finito) de las variables que aparecen en las fórmulas de la demostración D. Definimos

$$\phi(s) \equiv \bigwedge v(v : X \longrightarrow \mathrm{Var}(\ulcorner \mathcal{L}_a \urcorner) \rightarrow$$

$$\bigvee \gamma \in (D_s)_0 \ \neg \mathbb{N} \vDash^*_{\Sigma_n} \gamma[v] \vee \bigvee \delta \in (D_s)_1 \mathbb{N} \vDash^*_{\Sigma_n} \delta[v]),$$

que es una fórmula Σ_{n+1}. Sea $A = \mathcal{D}D$. Finalmente consideramos la fórmula

$$\bigwedge m \bigwedge s \in A\,(\mathrm{rang}(s) = m \rightarrow \phi(s)).$$

La parte tras $\bigwedge m$ es claramente de tipo Σ_{n+1}, luego podemos probar la fórmula por inducción en $\mathrm{I}\Sigma_{n+1}$. Esto significa demostrar que el secuente D_s es verdadero supuesto que lo sean todos los secuentes situados por encima en la demostración. A su vez, esto se reduce a comprobar que todos los axiomas son verdaderos y que todas las reglas de inferencia transforman secuentes verdaderos en secuentes verdaderos. En suma, se trata de formalizar en $\mathrm{I}\Sigma_n$ la corrección del cálculo secuencial.

Mostraremos únicamente algunos casos representativos de todos los casos que habría que considerar. Por ejemplo, consideremos un axioma de la forma

$$S = (\{s = t\} \Rightarrow \{Ss = St\}).$$

Se trata de comprobar que, fijada una valoración v, se cumple

$$\neg \vDash_0 (s = t)[v] \vee \ \vDash_0 (Ss = St)[v],$$

que a su vez, aplicando las definiciones correspondientes (véase [LM 8.28]), se reduce a

$$\mathrm{Dn}(s, v) = \mathrm{Dn}(t, v) \rightarrow \mathrm{Dn}(s, v) + 1 = \mathrm{Dn}(t, v) + 1,$$

lo cual se cumple trivialmente. La comprobación de los demás axiomas es similar.

[15] Una ligera modificación del enunciado y la prueba del teorema [LM 8.30] hace que estas fórmulas tengan sentido considerando la definición de fórmula Δ_0 que hemos adoptado en el capítulo anterior.

[16] Notemos que aquí n no es una variable de $\mathcal{L}_a$, sino un número natural metamatemático.

Veamos ahora la validez de la regla izquierda del disyuntor, es decir, partimos de dos secuentes de la forma

$$S_1 = (\{\alpha\} \cup \Gamma \Rightarrow \Delta) \qquad \text{y} \qquad S_2 = (\{\beta\} \cup \Gamma \Rightarrow \Delta)$$

y, suponiéndolos verdaderos, hay que probar que lo es $S = (\{\alpha \vee \beta\} \cup \Gamma \Rightarrow \Delta)$.

Notemos que, como la demostración D consta exclusivamente de fórmulas Σ_n en sentido estricto, podemos suponer que α, β y $\alpha \vee \beta$ son Σ_n en sentido estricto, lo cual sólo es posible si de hecho son de tipo Δ_0. Así pues, la hipótesis es que, para toda valoración v,

$$\neg\mathbb{N} \vDash_0 \alpha[v] \vee \bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash^*_{\Sigma_n} \gamma[v] \vee \bigvee\delta \in \Delta\, \mathbb{N} \vDash^*_{\Sigma_n} \delta[v]$$

y

$$\neg\mathbb{N} \vDash_0 \beta[v] \vee \bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash^*_{\Sigma_n} \gamma[v] \vee \bigvee\delta \in \Delta\, \mathbb{N} \vDash^*_{\Sigma_n} \delta[v]$$

y queremos probar que, para toda valoración v,

$$\neg\mathbb{N} \vDash_0 (\alpha \vee \beta)[v] \vee \bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash^*_{\Sigma_n} \gamma[v] \vee \bigvee\delta \in \Delta\, \mathbb{N} \vDash^*_{\Sigma_n} \delta[v].$$

Fijada una valoración v, suponemos que no se cumplen los dos últimos casos de la conclusión, con lo que las hipótesis nos dan que $\neg\mathbb{N} \vDash_0 \alpha[v] \wedge \neg\mathbb{N} \vDash_0 \neg\beta[v]$, pero esto equivale a $\neg\mathbb{N} \vDash_0 (\alpha \vee \beta)[v]$, con lo que se da el primer caso.

Las demás reglas de inferencia se comprueban de modo similar. Mostraremos, de todos modos, la validez de la regla de inducción. Tenemos como hipótesis la validez de un secuente

$$S_0 = (\{\alpha\} \cup \Gamma \Rightarrow \Delta \cup \{\mathtt{S}_y^{Sy}\alpha\}),$$

donde la variable y no aparece libre en ninguna fórmula de Γ o Δ, y tenemos que probar la validez de

$$S = (\{\mathtt{S}_y^0\alpha\} \cup \Gamma \Rightarrow \Delta \cup \{\mathtt{S}_y^t\alpha\}).$$

La hipótesis es que, para toda valoración v,

$$\bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash^*_{\Sigma_n} \gamma[v] \vee \bigvee\delta \in \Delta\ \mathbb{N} \vDash^*_{\Sigma_n} \delta[v] \vee \neg\mathbb{N} \vDash^*_{\Sigma_n} \alpha[v] \vee \mathbb{N} \vDash^*_{\Sigma_n} \mathtt{S}_y^{Sy}\alpha[v]$$

y tenemos que probar, para toda valoración v, que

$$\bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash^*_{\Sigma_n} \gamma[v] \vee \bigvee\delta \in \Delta\ \mathbb{N} \vDash^*_{\Sigma_n} \delta[v] \vee \neg\mathbb{N} \vDash^*_{\Sigma_n} \mathtt{S}_y^0\alpha[v] \vee \mathbb{N} \vDash^*_{\Sigma_n} \mathtt{S}_y^t\alpha[v].$$

Para ello fijamos una valoración v y suponemos que no se dan los tres primeros casos de la conclusión. En particular suponemos $\mathbb{N} \vDash^*_{\Sigma_n} \mathtt{S}_y^0\alpha[v]$. Para cada natural a, consideramos la valoración v_y^a que difiere de v a lo sumo en que asigna a la variable y el valor a. Como y no está libre en las fórmulas de Γ y Δ, tenemos que tampoco se cumple

$$\neg\mathbb{N} \vDash^*_{\Sigma_n} \gamma[v_y^a] \vee \bigvee\delta \in \Delta\ \mathbb{N} \vDash^*_{\Sigma_n} \delta[v_y^a],$$

luego tiene que cumplirse

$$\neg \mathbb{N} \vDash^*_{\Sigma_n} \alpha[v_y^a] \vee \mathbb{N} \vDash^*_{\Sigma_n} \mathtt{S}_y^{Sy}\alpha[v_y^a]$$

o, lo que es lo mismo,

$$\mathbb{N} \vDash^*_{\Sigma_n} \alpha[v_y^a] \to \mathbb{N} \vDash^*_{\Sigma_n} \mathtt{S}_y^{Sy}\alpha[v_y^a].$$

Pero una comprobación rutinaria[17] muestra que esto equivale a

$$\mathbb{N} \vDash^*_{\Sigma_n} \alpha[v_y^a] \to \mathbb{N} \vDash^*_{\Sigma_n} \alpha[v_y^{a+1}],$$

y por el mismo argumento tenemos también $\mathbb{N} \vDash^*_{\Sigma_n} \alpha[v_y^0]$. Ahora, por Σ_n-inducción podemos concluir que

$$\bigwedge a\ \mathbb{N} \vDash^*_{\Sigma_n} \alpha[v_y^a],$$

y si aplicamos esto tomando $a = \mathrm{Dn}(t, v)$, obtenemos $\mathbb{N} \vDash^*_{\Pi_n} \mathtt{S}_y^t\alpha[v]$, como había que probar.

Así, una vez comprobados todos los axiomas y todas las reglas de inferencia, podemos concluir que $\bigwedge s \in A\,\phi(s)$. En particular, lo aplicamos a $s = \varnothing$ y concluimos $\mathbb{N} \vDash_{\Sigma_n} \ulcorner\alpha\urcorner$ (y no hace falta especificar ninguna valoración porque $\ulcorner\alpha\urcorner$ es una sentencia), y por último el teorema [LM 8.33] nos permite concluir α. ■

Si aplicamos el teorema precedente a la sentencia $0 \neq 0$ obtenemos que

$$\underset{\mathrm{I\Sigma_{n+1}}}{\vdash} (\underset{\ulcorner\mathrm{I\Sigma_n}\urcorner}{\vdash} \ulcorner 0 \neq 0\urcorner \to 0 \neq 0),$$

pero la hipótesis de la implicación es $\neg\,\mathrm{Consis}\ulcorner\mathrm{I\Sigma_n}\urcorner$, es decir, la fórmula que se interpreta como que $\mathrm{I}\Sigma_n$ es contradictorio, luego:

Teorema 5.15 *Para cada número natural n se cumple*

$$\underset{\mathrm{I\Sigma_{n+1}}}{\vdash} \mathrm{Consis}\ulcorner\mathrm{I\Sigma_n}\urcorner.$$

En particular, en AP se demuestra la consistencia de todas las teorías $\mathrm{I}\Sigma_n$. Más en general:

Teorema 5.16 (Teorema de reflexión) *Si Γ es cualquier conjunto finito consistente de sentencias demostrables en* AP, *entonces* $\underset{\mathrm{AP}}{\vdash} \mathrm{Consis}\ulcorner\Gamma\urcorner$.

Demostración: Como cada sentencia de Γ es demostrable en $\mathrm{I}\Sigma_n$, para un n suficientemente grande, podemos tomar un mismo n que valga para todas las sentencias de Γ. Es claro entonces que

$$\underset{\mathrm{AP}}{\vdash} \mathrm{Consis}\ulcorner\mathrm{I\Sigma_n}\urcorner \to \mathrm{Consis}\ulcorner\Gamma\urcorner.$$

y basta aplicar el teorema anterior. ■

[17] Se trata de formalizar para $\mathbb{N} \vDash^*$ el teorema 2.7. Ello supone demostrarlo primero para $\mathbb{N} \vDash_0$, de ahí generalizarlo a $\mathbb{N} \vDash_{\Sigma_n}$ y $\mathbb{N} \vDash_{\Pi_n}$ y de ahí a $\mathbb{N} \vDash^*_{\Sigma_n}$. Los argumentos son todos elementales.

Ahora podemos dar una prueba alternativa, puramente sintáctica, del teorema [LM 9.26]:

Teorema 5.17 *Ninguna extensión consistente de* AP *es finitamente axiomatizable.*

DEMOSTRACIÓN: Observemos que un conjunto finito de axiomas puede reducirse a un único axioma formando su conjunción. Se trata de probar que si una sentencia γ de $\mathcal{L}_a$ implica todos los axiomas de AP entonces es contradictoria. Pongamos que la sentencia es Σ_n. Vamos a probar que $\gamma \vdash \operatorname{Consis}\ulcorner\gamma\urcorner$, lo cual, por el segundo teorema de incompletitud, implica que γ es contradictoria.

Suponemos, pues γ y, por reducción al absurdo, suponemos $\neg \operatorname{Consis}\ulcorner\gamma\urcorner$, es decir, suponemos que $\ulcorner\gamma\urcorner \vdash \ulcorner 0 \neq 0\urcorner$. Esto implica $\vdash \ulcorner\gamma \rightarrow 0 \neq 0\urcorner$ y, en particular, $\underset{\ulcorner \mathrm{I}\Sigma_\mathrm{n}\urcorner}{\vdash} \ulcorner\gamma \rightarrow 0 \neq 0\urcorner$. Por el teorema 5.14, en $\mathrm{I}\Sigma_{n+1}$, luego en particular a partir de γ, podemos concluir $\gamma \rightarrow 0 \neq 0$ y, de nuevo porque estamos suponiendo γ, obtenemos que $0 \neq 0$. Esta contradicción prueba $\operatorname{Consis}\ulcorner\gamma\urcorner$. ∎

Nota Hay un argumento más directo para probar que AP no es finitamente axiomatizable: si lo fuera, todos sus axiomas (luego todos sus teoremas) serían teoremas de $\mathrm{I}\Sigma_n$, para un n suficientemente grande, pero entonces tendríamos que

$$\underset{\mathrm{I}\Sigma_\mathrm{n}}{\vdash} \operatorname{Consis}\ulcorner \mathrm{I}\Sigma_\mathrm{n}\urcorner,$$

y el teorema de incompletitud nos daría que $\mathrm{I}\Sigma_n$ es contradictorio. ∎

Capítulo VI

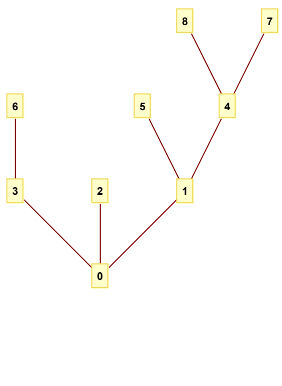
Ordinales

La teoría de conjuntos permite definir los ordinales, que son una generalización de los números naturales capaces de "contar" cualquier conjunto, aunque sea infinito, cualquiera que sea su cardinal. Los primeros ordinales son los números naturales, $0, 1, 2, 3, \ldots$, tras los cuales viene el menor ordinal infinito, ω, seguido de $\omega + 1, \omega + 2, \cdots, \omega + \omega = \omega \cdot 2, \ldots$ Se define una suma, un producto y una exponenciación de ordinales, de modo que en particular están definidos los ordinales

$$\omega < \omega^{\omega} < \omega^{\omega^{\omega}} < \omega^{\omega^{\omega^{\omega}}} < \quad \cdots$$

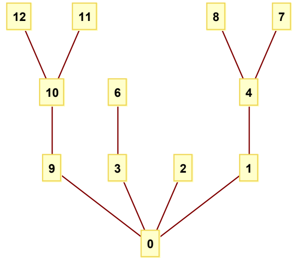
el supremo de todos estos ordinales se llama ϵ_0, y es el menor ordinal que no puede expresarse en términos de números naturales y ω mediante sumas, productos o potencias. En este capítulo veremos que los ordinales menores que ϵ_0 pueden definirse en la aritmética de Peano, de modo que es posible razonar con ellos en términos finitistas independientes de los axiomas (o de cualquier posible modelo) de la teoría de conjuntos. Previamente, en la primera sección plantearemos un problema que resolveremos posteriormente empleando ordinales.

6.1 Hércules y la Hidra I

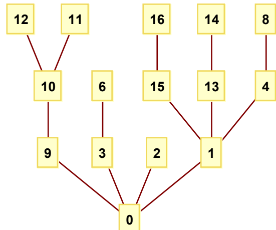


La figura muestra una *hidra*. Es simplemente un árbol con una raíz (en la figura marcada con un 0), de la que sale un número finito de ramas, de cada una de las cuales sale a su vez un número finito de ramas, y así sucesivamente, hasta alcanzar una cierta altura finita. Los nodos terminales de los que no salen más ramas son las *cabezas* de la hidra. La de la figura tiene cinco cabezas, con los números 2, 5, 6, 7, 8. Las aristas que terminan en cabezas son los *cuellos* de la hidra.

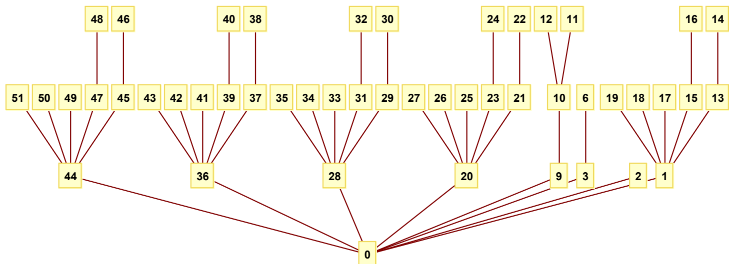
Hay que entender que hemos numerado los nodos simplemente para facilitar las referencias, pero la numeración no forma parte de la hidra. Si renumeramos los nodos seguiremos teniendo la misma hidra.



A Hércules le han encargado que mate a la Hidra, para lo cual tiene que cortarle todas sus cabezas. Pongamos que en un primer asalto decide cortar la cabeza número 5 (con su cuello correspondiente). Nos fijamos entonces en la rama de la que salía el cuello amputado, que es la que une los nodos 0 y 1. La Hidra es capaz de generar una copia de dicha rama con todo lo que tiene por encima de ella, y el resultado es el que muestra la segunda figura. La copia de la arista $0-1$ es la arista $0-9$. Ahora la Hidra tiene 6 cabezas.



Pongamos que, en el segundo asalto, Hércules decide cortar la cabeza número 7. Entonces, la Hidra produce, no una copia, sino dos copias de la arista $1-4$, que son las nuevas aristas $1-13$ y $1-15$. Ahora la Hidra tiene 7 cabezas. Si en el tercer asalto Hércules corta la cabeza número 8, la Hidra genera tres copias de la arists $1-4$ y si, en el cuarto asalto corta la cabeza número 4, la Hidra genera cuatro copias de la arista $0-1$. El resultado tras este cuarto asalto es el que vemos en la figura siguiente:



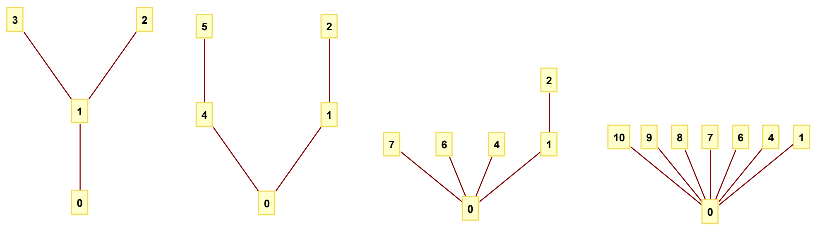
En el tercer asalto, la arista $1-4$ generó los cuellos de las cabezas 17, 18 y 19, mientras que en el cuarto asalto la arista $0-1$ ha generado las cuatro aristas $0-20$, $0-28$, $0-36$ y $0-44$. Ahora la Hidra tiene 29 cabezas.

Es importante señalar que si Hércules corta una cabeza que sale directamente de la raíz de la Hidra, entonces no se produce regeneración alguna. Por ejemplo, si en el quinto asalto Hércules corta la cabeza número 2, la Hidra no sufrirá más cambio que la amputación de dicha cabeza.

En este punto surge la pregunta de si Hércules logrará matar a la Hidra (es decir, dejarla reducida a su raíz) tras un número finito de pasos. Naturalmente, esto puede depender de la Hidra concreta contra la que se enfrente.

Por ejemplo, si consideramos una “Hidra-bebé” cuyas cabezas salgan todas de su raíz, como éstas no tienen capacidad de regeneración, Hércules puede cortarlas todas una a una y la Hidra acaba muerta al cabo de tantos pasos como cabezas tenga.

Un caso menos trivial, pero sencillo, es la hidra que muestra la figura siguiente a la izquierda, con dos cabezas de altura 2.



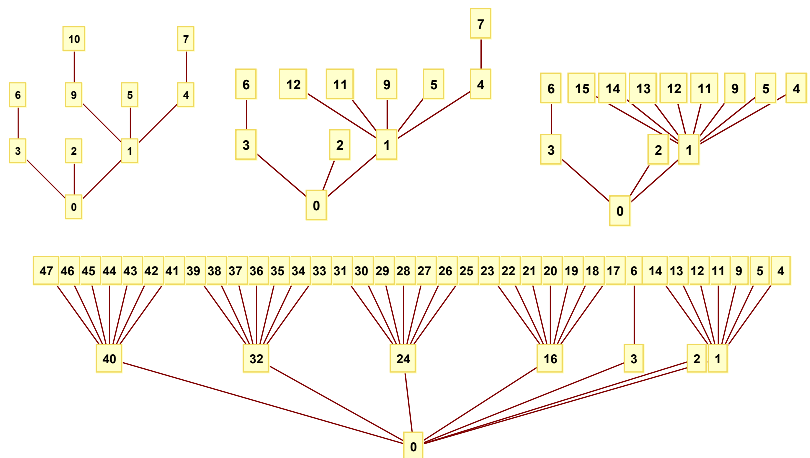
Vemos que al tercer asalto ha quedado reducida a una hidra-bebé, que tras el décimo asalto estará muerta.

La cuestión es si Hércules tiene opciones de matar en un número finito de pasos a cualquier hidra contra la que se enfrente, o si, por el contrario, existe alguna hidra capaz de mantenerse viva indefinidamente a lo largo de cualquier combate.

En principio, esto puede depender de la estrategia que siga Hércules en la elección de la cabeza que corta en cada asalto. Por ejemplo, vamos a considerar la estrategia siguiente:

En cada asalto, se corta una cabeza de altura máxima.

Si aplicamos esta estrategia a la Hidra que hemos mostrado al principio de esta sección, los primeros combates producen el efecto siguiente:



La Hidra inicial tenía 5 cabezas. En el primer asalto Hércules corta la cabeza número 8, y la Hidra se mantiene en 5 cabezas. En el segundo asalto le corta la cabeza número 10, y la Hidra pasa a tener 7 cabezas. En el tercer asalto le corta la cabeza número 7 y la Hidra pasa a tener 10 cabezas. La siguiente es la cabeza número 15, y la Hidra pasa a tener 37 cabezas. La tabla siguiente muestra el número de cabezas de la Hidra tras los 10 primeros asaltos:

Asalto	0	1	2	3	4	5	6	7	8	9	10
Cabezas	5	5	7	10	37	66	101	142	189	242	291

Tras el milésimo asalto, el número de cabezas es de 2 002 251. No parece razonable apostar por Hércules y, sin embargo, con una pequeña precisión que hemos estado teniendo en cuenta tácitamente, podemos probar fácilmente que la estrategia es ganadora: si Hércules la sigue, matará en un número finito de pasos a cualquier hidra a la que se enfrente.

Para introducir la precisión a la que acabamos de hacer referencia, diremos que dos cabezas de la Hidra son *hermanas* si sus cuellos nacen del mismo nodo. Por ejemplo, la Hidra inicial tiene dos cabezas hermanas de altura máxima 3, mientras que, tras el tercer asalto, tiene 8 cabezas hermanas de altura máxima 2 y otra más sin hermanas. La estrategia precisada es:

> *En cada asalto se corta una cabeza de altura máxima que tenga el mayor número posible de hermanas.*

Vamos a demostrar que, si Hércules sigue esta estrategia, tiene la victoria asegurada ante cualquier hidra.

Para ello asociemos tres números (h, m, s) a la Hidra en un instante dado, donde h es su altura, m es el máximo número de cabezas hermanas de altura h y s es el número de estos grupos. Por ejemplo, nuestra hidra inicial tiene $(h, m, s) = (3, 2, 1)$.

Si en el asalto n-simo cortamos cualquier cabeza de un grupo con el mayor número posible de cabezas hermanas, éste deja de tener m cabezas y pasa a tener $m-1$. Por otra parte, la Hidra genera n nuevos grupos de $m-1$ cabezas hermanas, por lo que el número de grupos de m cabezas hermanas ha pasado de s a $s-1$. Así pues, la nueva terna es $(h, m, s-1)$.

Tras s asaltos ya no quedarán grupos de m cabezas hermanas, luego este máximo pasara a ser $m-1$, es decir, la terna ha pasado a ser $(h, m-1, s)$, donde ahora s es el número de grupos de $m-1$ cabezas hermanas.

En nuestro ejemplo vemos que el primer asalto se traduce en el cambio $(3, 2, 1) \mapsto (3, 1, 2)$, pues la hidra pasa a tener dos grupos de cabezas de altura 3 sin hermanas. Al continuar el combate obtenemos:

$$(3,2,1) \mapsto (3,1,2) \mapsto (3,1,1) \mapsto (2,8,1) \mapsto (2,7,5) \mapsto (2,7,4)$$

$$\mapsto (2,7,3) \mapsto (2,7,2) \mapsto (2,7,1) \mapsto (2,6,40) \mapsto \cdots$$

En general, en cada asalto s se reduce una unidad y, cuando llega a 0, es m el que se reduce una unidad y s asciende a un valor arbitrario, desde el que empieza a descender.

Tras un número finito de pasos, m llegará a 1, lo que significa que ninguna cabeza de altura máxima tendrá hermanas. Cuando se corta una cabeza de altura h sin hermanas, la Hidra genera muchas cabezas de altura $h-1$, luego cuando Hércules corta todas estas cabezas de altura h, la Hidra pasa a tener altura $h-1$. En otras palabras: después de una terna $(h,1,1)$ se pasa a otra de la forma $(h-1,m,s)$, donde m es ahora el número máximo de cabezas hermanas de altura $h-1$ y s el número de estos grupos.

Tras un número finito de asaltos llegaremos a una terna $(1,m,1)$, lo que significa que la Hidra tendrá altura $h=1$ y constará de un único grupo de m cabezas hermanas, es decir, se habrá convertido en una hidra-bebé, que morirá tras m asaltos adicionales.

En resumen, la terna (h,m,s) se comporta como un cronómetro en cuenta atrás: cuando los segundos llegan a 0, se reduce un minuto y s sube (no hasta 60, como en un reloj auténtico, sino hasta un número determinado por la Hidra), y cuando los minutos llegan a 0 las horas se reducen en una unidad. Así pues, este "reloj" mide el tiempo de vida —necesariamente finito— que le queda a la Hidra.

No es difícil calcular cuántos asaltos resistirá la Hidra que hemos tomado como ejemplo ante una batalla en la que Hércules siga la estrategia que estamos considerando, pero más adelante estaremos en mejores condiciones de hacer las cuentas. Anticipamos el resultado: la Hidra morirá tras

$$\begin{gathered}989\,053\,388\,168\,938\,379\,565\,429\,552\,367\,644\,648\,402\,300\,582\\ 379\,429\,351\,736\,318\,357\,588\,790\,729\,278\,822\,309\,452\,445\,327\end{gathered}$$

asaltos. Si Hércules pudiera cortar 100 cabezas por segundo, tardaría aproximadamente $3.13\cdot 10^{80}$ años en matar a la Hidra.

Otra cuestión que nos podemos plantear es qué sucede si Hércules no sigue una estrategia adecuada. ¿Puede ocurrir entonces que el número de cabezas de la Hidra tienda a infinito o, al menos, que no descienda nunca hasta cero?

Un caso particular de esta pregunta consiste en plantearse qué sucede si Hércules sigue la estrategia diametralmente opuesta a la que hemos considerado:

> *En cada asalto se corta una cabeza de altura mínima que tenga el menor número posible de hermanas.*

Veremos que, aunque parezca que no hay nada más fácil que el que un combate contra la Hidra quede fuera de control y el número de cabezas tienda irremisiblemente a infinito, lo cierto es que no es así: la Hidra muere tras un número finito de pasos en cualquier combate, sin que importe el orden en que se van cortando sus cabezas (a lo sumo, el orden hará que el combate conste de más o menos asaltos, pero siempre terminará con la Hidra completamente decapitada).

Para probar que esto es así utilizaremos ordinales. En principio nos servirían los ordinales tal cual se definen en teoría de conjuntos, pero aprovechamos este punto para mostrar cómo (los ordinales menores que ϵ_0) pueden introducirse aritméticamente.

6.2 Ordinales en la aritmética

Trabajamos en la aritmética recursiva primitiva ARP, donde consideramos el funtor definido como sigue:

$$\begin{aligned} F_{\preceq}(0) &= 0, \\ F_{\preceq}(n+1) &= \{x \leq \langle n, n\rangle \mid \bigvee \alpha\beta \leq n(x = \langle \alpha, \beta\rangle \land \cdots)\}, \end{aligned}$$

donde los puntos suspensivos son la conjunción de las fórmulas siguientes:

1. $\bigwedge ij < \ell(\alpha)(i \leq j \to \langle \alpha_j, \alpha_i\rangle \in F_{\preceq}(n))$,
2. $\bigwedge ij < \ell(\beta)(i \leq j \to \langle \beta_j, \beta_i\rangle \in F_{\preceq}(n))$,
3. $\alpha \sqsubseteq \beta \lor \bigvee i < \ell(\alpha)(i < \ell(\beta) \land \alpha|_i = \beta|_i \land \alpha_i \neq \beta_i \land \langle \alpha_i, \beta_i\rangle \in F_{\preceq}(n))$.

Definimos

$$\alpha \preceq \beta \equiv \langle \alpha, \beta\rangle \in F_{\preceq}(\alpha + \beta + 1).$$

Vamos a analizar esta definición. En primer lugar observamos que

$$\alpha < n \land \beta < n \to (\langle \alpha, \beta\rangle \in F_{\preceq}(n) \leftrightarrow \langle \alpha, \beta\rangle \in F_{\preceq}(n+1)).$$

En efecto, razonamos por inducción sobre n. Para $n = 0$ es trivial, y si vale para n y α, $\beta < n+1$, entonces, para cada $i < \ell(\alpha)$, se cumple que $\alpha_i < \alpha < n+1$, luego $\alpha_i < n$, e igualmente $\beta_i < n$, luego, por hipótesis de inducción,

$$\langle \alpha_j, \alpha_i\rangle \in F_{\preceq}(n) \leftrightarrow \langle \alpha_j, \alpha_i\rangle \in F_{\preceq}(n+1),$$

$$\langle \beta_j, \beta_i\rangle \in F_{\preceq}(n) \leftrightarrow \langle \beta_j, \beta_i\rangle \in F_{\preceq}(n+1),$$

$$\langle \alpha_i, \beta_i\rangle \in F_{\preceq}(n) \leftrightarrow \langle \alpha_i, \beta_i\rangle \in F_{\preceq}(n+1),$$

de donde, sin más que comparar las definiciones, vemos que

$$\langle \alpha, \beta\rangle \in F_{\preceq}(n+1) \leftrightarrow \langle \alpha, \beta\rangle \in F_{\preceq}(n+2).$$

A su vez, una inducción trivial nos da ahora que

$$\alpha < n \land \beta < n \land n \leq m \to (\langle \alpha, \beta\rangle \in F_{\preceq}(n) \leftrightarrow \langle \alpha, \beta\rangle \in F_{\preceq}(m)).$$

Así pues, teniendo en cuenta que en $\langle \alpha, \beta\rangle \in F_{\preceq}(n)$ el valor de n es irrelevante con tal de que $\alpha < n$ y $\beta < n$, obtenemos la caracterización recurrente siguiente de la relación $\preceq$:

$$\alpha \preceq \beta \leftrightarrow \bigwedge ij < \ell(\alpha)(i \leq j \to \alpha_j \preceq \alpha_i) \land \bigwedge ij < \ell(\beta)(i \leq j \to \beta_j \preceq \beta_i) \land$$
$$\alpha \sqsubseteq \beta \lor \bigvee i < \ell(\alpha)(i < \ell(\beta) \land \alpha|_i = \beta|_i \land \alpha_i \prec \beta_i),$$

donde hemos usado la notación $x \prec y \equiv (x \preceq y \land x \neq y)$.

Equivalentemente, $\alpha \preceq \beta$ significa que α y β son sucesiones finitas decrecientes respecto de $\preceq$ y, o bien β extiende a α, o bien el primer índice i en el cual difieren cumple que $\alpha_i \prec \beta_i$.

Llamaremos *ordinales* (menores que ϵ_0) a los números naturales que cumplen

$$\alpha \in E \equiv \alpha \preceq \alpha.$$

Explícitamente, teniendo en cuenta que siempre se cumple $\alpha \sqsubseteq \alpha$, tenemos

$$\alpha \in E \leftrightarrow \bigwedge ij < \ell(\alpha)(i \leq j \to \alpha_j \preceq \alpha_i).$$

En particular, ahora es inmediato que

$$\alpha \preceq \beta \to \alpha \in E \wedge \beta \in E,$$

de modo que la relación $\preceq$ sólo está definida sobre ordinales. Más aún,

$$\alpha \in E \to \bigwedge i < \ell(\alpha)\, \alpha_i \in E,$$

pues ciertamente se cumple $\alpha_i \preceq \alpha_i$. En definitiva, concluimos que los ordinales satisfacen la siguiente definición recurrente:

> *Un ordinal es una sucesión finita de ordinales decreciente respecto de la relación* $\preceq$.

En realidad, para que podamos hablar de sucesiones decrecientes tenemos que comprobar que $\preceq$ es una relación de orden. Nos ocupamos de ello inmediatamente:

Teorema 6.1 (ARP) *La relación $\preceq$ es una relación de orden total en E, es decir:*

1. $\bigwedge \alpha \in E\, \alpha \preceq \alpha$,
2. $\bigwedge \alpha\beta \in E(\alpha \preceq \beta \wedge \beta \preceq \alpha \to \alpha = \beta)$,
3. $\bigwedge \alpha\beta\gamma \in E(\alpha \preceq \beta \wedge \beta \preceq \gamma \to \alpha \preceq \gamma)$,
4. $\bigwedge \alpha\beta \in E(\alpha \preceq \beta \vee \beta \preceq \alpha)$.

Demostración: 1) La reflexividad es inmediata.

2) Supongamos que existe un par (α, β) que incumple la propiedad 2, de modo que $\alpha \preceq \beta \wedge \beta \preceq \alpha$, pero $\alpha \neq \beta$. En tal caso podemos tomar un par tal que $\max\{\alpha, \beta\}$ tome el menor valor posible.

Si existe un $i < \ell(\alpha)$, $i < \ell(\beta)$ de modo que $\alpha|_i = \beta|_i$ y $\alpha_i \neq \beta_i$, entonces de $\alpha \preceq \beta$ deducimos que $\alpha_i \prec \beta_i$ y de $\beta \preceq \alpha$ deducimos que $\beta_i \prec \alpha_i$, pero como $\max\{\alpha_i, \beta_i\} < \max\{\alpha, \beta\}$, la minimalidad de este máximo implica $\alpha_i = \beta_i$, con lo que tenemos una contradicción.

Por consiguiente, de $\alpha \preceq \beta$ se deduce $\alpha \sqsubseteq \beta$ y de $\beta \preceq \alpha$ se deduce $\beta \sqsubseteq \alpha$, de donde $\alpha = \beta$ y tenemos igualmente una contradicción.

4) Como en el caso anterior, si existe un par (α, β) que no cumpla la propiedad 4, podemos tomar uno tal que $\max\{\alpha, \beta\}$ tome el menor valor posible.

Estamos suponiendo $\alpha \preceq \alpha \wedge \beta \preceq \beta$. Si se cumple $\alpha \sqsubseteq \beta$ o $\beta \sqsubseteq \alpha$ es inmediato que se cumple $\alpha \preceq \beta \vee \beta \preceq \alpha$. En caso contrario existe un $i < \ell(\alpha)$, $i < \ell(\beta)$ tal que $\alpha|_i = \beta|_i$, pero $\alpha_i \neq \beta_i$. Como $\max\{\alpha_i, \beta_i\} < \max\{\alpha, \beta\}$, la minimalidad de este máximo implica que $\alpha_i \preceq \beta_i \vee \beta_i \preceq \alpha_i$, luego de hecho $\alpha_i \prec \beta_i \vee \beta_i \prec \alpha_i$, y esto implica $\alpha \preceq \beta \vee \beta \preceq \alpha$, con lo que tenemos una contradicción.

3) La transitividad es la propiedad más laboriosa de justificar, porque hay que distinguir muchos casos, pero el razonamiento no ofrece ninguna dificultad. Partimos de un posible contraejemplo con el menor valor posible para $\max\{\alpha, \beta, \gamma\}$ y se llega a una contradicción como en los apartados precedentes. ■

Ahora es fácil poner ejemplos de ordinales. En general, si

$$\alpha = \langle \eta_0, \ldots, \eta_{n-1} \rangle \in E,$$

definimos α' como la sucesión que resulta de prolongar α con un 0, es decir:

$$\alpha' = \langle \eta_0, \ldots, \eta_{n-1}, 0 \rangle .$$

El teorema siguiente afirma que 0 es el mínimo ordinal y que, para todo ordinal α, se cumple que α' es el menor ordinal mayor que α:

Teorema 6.2 (ARP) *Se cumple:*

1. $0 \in E \wedge \bigwedge \alpha \in E\, 0 \preceq \alpha$.
2. $\bigwedge \alpha \in E(\alpha' \in E \wedge \alpha \prec \alpha')$.
3. $\bigwedge \alpha\beta \in E(\alpha \prec \beta \rightarrow \alpha' \preceq \beta)$.

Demostración: 1) El número natural 0 se corresponde con la sucesión vacía, que obviamente es una sucesión decreciente de ordinales (o, alternativamente, es fácil ver que cumple trivialmente la definición de $0 \preceq 0$). Por lo tanto $0 \in E$ y, como toda sucesión extiende a la sucesión vacía, también es obvio que $\bigwedge \alpha \in E\, 0 \preceq \alpha$.

2) Si $\alpha = \langle \eta_0, \ldots, \eta_{n-1} \rangle$, tenemos que

$$\eta_0 \succeq \eta_1 \succeq \cdots \succeq \eta_{n-1}$$

y, como 0 es el mínimo ordinal, también se cumple

$$\eta_0 \succeq \eta_1 \succeq \cdots \succeq \eta_{n-1} \succeq 0,$$

por lo que $\alpha' \in E$. Como α' extiende (estrictamente) a α, se cumple que $\alpha \prec \alpha'$.

3) Sea $n = \ell(\alpha)$. Si $\alpha \prec \beta$, supongamos en primer lugar que β extiende estrictamente a α, en cuyo caso, o bien también extiende a α' (y así $\alpha' \preceq \beta$), o bien tenemos que $(\alpha')_n = 0 \prec \beta_n$, por lo que $\alpha' \prec \beta$.

Si, por el contrario β no extiende a α, el mínimo índice i en el que difieren cumple que $\alpha_i \prec \beta_i$, pero claramente i es también el mínimo índice en el que α' difiere de β, luego también $\alpha' \prec \beta$. ■

Vemos así que los primeros ordinales son

$$\hat{0} \prec \hat{1} \prec \hat{2} \prec \hat{3} \prec \cdots$$

donde $\hat{0} = 0$ y, en general, $\widehat{n+1} = \hat{n}'$. Equivalentemente, $\hat{n} = \langle 0, \ldots, 0 \rangle$ es la sucesión formada por n ceros, que es obviamente una sucesión decreciente de ordinales. A los ordinales de la forma $\hat{n}$ los llamaremos *ordinales finitos.*

Aunque es totalmente irrelevante, no es difícil comprobar que los primeros ordinales finitos son los números naturales dados por la tabla siguiente (compárese con la tabla de la página 135):

n	0	1	2	3	4	5	6	7	8	9	10	$\cdots$
$\hat{n}$	0	1	3	6	10	15	21	28	36	45	55	$\cdots$

Definición 6.3 Los ordinales de la forma α', para $\alpha \in E$, se llaman *ordinales sucesores.* Equivalentemente, los ordinales sucesores son los ordinales no nulos cuya última componente es nula. Los ordinales no nulos que no son ordinales sucesores, es decir, cuya última componente no es nula, se llaman *ordinales límite.*

Así, todo ordinal está en uno (solo) de los tres casos siguientes:

1. Es 0 (con lo que no tiene ordinales anteriores),

2. Es un ordinal sucesor (con lo que tiene un ordinal inmediatamente anterior),

3. Es un ordinal límite (con lo que tiene ordinales anteriores, pero no uno inmediatamente anterior).

Definimos[1] $\omega = \langle \hat{1} \rangle$, de modo que el teorema siguiente prueba que es el supremo del conjunto de los ordinales finitos. En particular es el menor ordinal infinito, y también el menor ordinal límite.

Teorema 6.4 (ARP) *Se cumple:*

1. $\omega \in E$,

2. $\bigwedge n\, \hat{n} \prec \omega$,

3. $\bigwedge \alpha \in E(\bigvee n\, \alpha = \hat{n} \vee \omega \preceq \alpha)$.

[1] Incidentalmente, es $\omega = \langle \hat{1} \rangle = \langle 1 \rangle = 2$.

DEMOSTRACIÓN: 1) Obviamente ω es una sucesión decreciente de ordinales, luego $\omega \in E$.

2) Obviamente $0 \prec \omega$ y, si n no es nulo, entonces $\hat{n}$ es una sucesión de n ceros, por lo que $\hat{n}_0 = \hat{0} \prec \hat{1} = \omega_0$, luego $\hat{n} \prec \omega$.

3) Si α no es nulo, o bien $\alpha_0 = 0$, en cuyo caso, al ser una sucesión decreciente, resulta que α es una sucesión de ceros, luego $\alpha = \hat{n}$, donde $n = \ell(\alpha)$, o bien $0 \prec \alpha_0$, en cuyo caso $\omega_0 = \hat{1} = \hat{0}' \preceq \alpha_0$, luego $\omega \preceq \alpha$. ■

Vamos a introducir una notación conveniente para representar los ordinales. En primer lugar, en lo sucesivo escribiremos n en lugar de $\hat{n}$, dejando que el contexto determine si estamos considerando a n como número natural o como ordinal finito. Por ejemplo, el ordinal 5 no es el número natural 5, sino de la sucesión de 5 ceros (que, según la codificación de sucesiones que estamos considerando, es el número natural 15, pero esto es irrelevante).

En segundo lugar, si $\alpha = \langle \eta_0, \ldots, \eta_n \rangle$ es un ordinal no nulo, donde

$$\eta_0 \succeq \eta_1 \succeq \cdots \succeq \eta_n,$$

usaremos la notación alternativa:

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n}.$$

Con esta notación tenemos que $1 = \langle 0 \rangle = \omega^0$, mientras que $\omega = \langle 1 \rangle = \omega^1$.

En tercer lugar, si hay varios sumandos consecutivos iguales, los agruparemos expresando la repetición multiplicativamente. Por ejemplo, el ordinal

$$\omega^\omega + \omega^\omega + \omega^\omega + \omega^\omega + \omega^\omega + \omega^3 + \omega^3 + \omega^3 + \omega^0 + \omega^0 + \omega^0 + \omega^0$$

lo representaremos más abreviadamente como

$$\omega^\omega \cdot 5 + \omega^3 \cdot 3 + 4.$$

Con esta notación, la relación de orden se puede comprobar a simple vista. Por ejemplo, es inmediato que

$$\omega^{\omega^5+\omega} + \omega^{\omega^3+\omega\cdot 2+4} + \omega^\omega \cdot 10 + \omega^5 + 7 \prec \omega^{\omega^5+\omega} + \omega^{\omega^3+\omega\cdot 3+1} + \omega^{\omega^2} + 100.$$

Para comprobarlo, comparamos el primer término de cada ordinal y vemos que es el mismo, luego pasamos a comparar el segundo, para lo cual comparamos los exponentes y vemos que

$$\omega^3 + \omega \cdot 2 + 4 = \omega^3 + \omega^1 + \omega^1 + \omega^0 + \omega^0 + \omega^0 + \omega^0 \prec$$
$$\omega^3 + \omega^1 + \omega^1 + \omega^1 + \omega^0 = \omega^3 + \omega \cdot 3 + 1.$$

Esto a su vez se obtiene viendo en primer lugar que ambos exponentes coinciden hasta su tercer término, mientras que el cuarto es $\omega^0 \prec \omega^1$, porque $0 \prec 1$. En la práctica no es necesario desarrollar la notación multiplicativa, y podemos concluir directamente que el primer exponente es menor porque $\omega \cdot 2 \prec \omega \cdot 3$.

Ahora ya podemos formarnos una imagen clara de los primeros ordinales. La sucesión de los ordinales empieza con los ordinales finitos, seguidos de ω y sus sucesores:

$$0 \prec 1 \prec 2 \prec 3 \prec \cdots \prec \omega \prec \omega + 1 \prec \omega + 2 \prec \omega + 3 \prec \cdots$$

La primera serie está formada por las sucesiones de ceros, mientras que la segunda está formada por los ordinales de la forma $\langle 1, 0, \ldots, 0\rangle$. Es fácil ver que el menor ordinal mayor que todos ellos es $\langle 1, 1\rangle = \omega + \omega = \omega \cdot 2$, por lo que la sucesión de los ordinales continúa así:

$$\cdots \prec \omega \cdot 2 \prec \omega \cdot 2 + 1 \prec \omega \cdot 2 + 2 \prec \cdots \prec \omega \cdot 3 \prec \omega \cdot 3 + 1 \prec \cdots$$

donde $\omega \cdot 3 = \langle 1, 1, 1\rangle$, y así, tenemos la sucesión de los primeros ordinales límite:

$$\omega \prec \cdots \prec \omega \cdot 2 \prec \cdots \prec \omega \cdot 3 \prec \cdots$$

Entre los cuales se encuentran únicamente los sucesores del precedente. Pero es fácil ver que la sucesión de los ordinales $\langle 1\rangle$, $\langle 1, 1\rangle$, $\langle 1, 1, 1\rangle$, ... tiene por supremo al ordinal $\omega^2 = \langle 2\rangle$, que es el primer ordinal límite supremo de ordinales límite.

Entre $\omega^2 = \langle 2\rangle$ y $\omega^3 = \langle 3\rangle$ se encuentran todos los ordinales de la forma

$$\omega^2 \cdot k_2 + \omega \cdot k_1 + k_0,$$

y por encima de la sucesión $\omega \prec \omega^2 \prec \omega^3 \prec \cdots$ figura como supremo el ordinal $\omega^\omega = \langle \omega\rangle = \langle\langle 1\rangle\rangle$ (que incidentalmente es el número natural 4). Los ordinales menores que ω^ω son exactamente los de la forma

$$\omega^n \cdot k_n + \omega^{n-1} \cdot k_{n-1} + \cdots + \omega \cdot k_1 + k_0.$$

Definición 6.5 Consideramos el funtor dado por las ecuaciones

$$\omega^{(0)} = 1, \qquad \omega^{(n+1)} = \omega^{\omega(n)}.$$

Así

$$\omega^{(0)} = 1, \quad \omega^{(1)} = \omega, \quad \omega^{(2)} = \omega^\omega, \quad \omega^{(3)} = \omega^{\omega^\omega}, \quad \omega^{(4)} = \omega^{\omega^{\omega^\omega}}, \quad \ldots$$

El teorema siguiente prueba que esta sucesión de ordinales no tiene supremo:

Teorema 6.6 (ARP) *Se cumple:*

1. $\bigwedge mn(m < n \rightarrow \omega^{(m)} \prec \omega^{(n)})$,
2. $\bigwedge \alpha \in E \bigvee n\ \alpha \prec \omega^{(n)}$.

DEMOSTRACIÓN: Es claro que $\omega^{(0)} \prec \omega^{(1)}$ y, a partir de aquí, una simple inducción prueba que $\bigwedge n\, \omega^{(n)} \prec \omega^{(n+1)}$, de donde a su vez otra inducción prueba 1).

Para probar 2) basta razonar por inducción sobre α. Trivialmente es cierto para $\alpha = 0$ y, si vale para ordinales menores que α (respecto al orden usual de los números naturales, no respecto de $\preceq$), como $\alpha_0 < \alpha$, existe un n tal que $\alpha_0 \prec \omega^{(n)}$, y de aquí se sigue que $\alpha \prec \omega^{(n+1)}$. ■

Observemos finalmente que en la práctica es muy fácil reconocer qué números naturales son ordinales. Sin más que ver la tabla de la página 135 es fácil completar la tabla siguiente

0		0	10	$0,0,0,0$	4	20	$0,0,0,0,1$	–
1	0	1	11	4	$\omega^{(3)}$	21	$0,0,0,0,0,0$	6
2	1	ω	12	$0,2$	–	22	6	ω^3
3	$0,0$	2	13	$0,1,0$	–	23	$2,0$	–
4	2	$\omega^{(2)}$	14	$0,0,0,1$	–	24	$0,1,1$	–
5	$0,1$	–	15	$0,0,0,0,0$	5	25	$0,0,0,2$	–
6	$0,0,0$	3	16	5	–	26	$0,0,0,1,0$	–
7	3	ω^2	17	$1,1$	$\omega\cdot 2$	27	$0,0,0,0,0,1$	–
8	$1,0$	–	18	$0,0,2$	–	28	$0,0,0,0,0,0,0$	7
9	$0,0,1$	–	19	$0,0,1,0$	–	29	7	ω^{ω^2}

En general, para determinar si un número es un ordinal, sólo tenemos que calcular la sucesión que representa y ver si sus términos son todos ordinales y forman una sucesión decreciente, para lo cual sólo tenemos que examinar los números naturales precedentes. Así, por ejemplo, 5 no es un ordinal porque codifica una sucesión de ordinales que no es decreciente, mientras que 16 no es un ordinal porque codifica la sucesión $\langle 5\rangle$, y 5 no es un ordinal. ■

Ordinales en AP Hemos definido los ordinales en ARP usando la posibilidad que esta teoría ofrece de definir funtores por recursión. Vamos a dar aquí una definición alternativa que permite introducir los ordinales en AP (incluso en $\mathrm{I}\Sigma_1$) sin necesidad de considerar los funtores de $\mathcal{L}_{\mathrm{arp}}$. Recordemos que en $\mathrm{I}\Sigma_1$ podemos definir una relación de pertenencia que satisface los axiomas de la teoría de conjuntos de Zermelo sin el axioma de infinitud.

Definición 6.7

$$\alpha \preceq \beta \equiv \bigvee fn(\mathrm{Suc}(\alpha) \land \mathrm{Suc}(\beta) \land \alpha < n \land \beta < n \land f : I_n \times I_n \longrightarrow \{0,1\} \land$$

$$f(\alpha,\beta) = 1 \land \bigwedge \gamma\delta < n(f(\gamma,\delta) = 1 \leftrightarrow o(\gamma,f) \land o(\delta,f) \land r(\gamma,\delta,f))),$$

donde a su vez:

$$o(\gamma,f) \equiv \bigwedge ij < \ell(\gamma)(i \leq j \rightarrow f(\gamma_j,\gamma_i) = 1),$$

$$r(\gamma,\delta,f) \equiv \gamma \subset \delta \lor \bigvee i < \ell(\gamma)(i < \ell(\delta) \land \gamma|_i = \delta|_i \land \gamma_i \neq \delta_i \land f(\gamma_i,\delta_i) = 1).$$

Aquí $\mathrm{Suc}(\alpha)$ indica que α es una sucesión finita, respecto de cualquier codificación de las sucesiones finitas como números naturales que queramos considerar. Si usamos la que estamos considerando en este libro, todos los números naturales codifican sucesiones finitas, luego podemos eliminar las condiciones $\mathrm{Suc}(\alpha) \wedge \mathrm{Suc}(\beta)$ de la definición. No obstante, en [LM] usamos otra codificación alternativa, de modo que $\mathrm{Suc}(\alpha)$ significa que α es una aplicación (en el sentido conjuntista) de dominio el conjunto I_k de los números naturales menores que k, para cierto k.

Notemos que $\alpha \preceq \beta$, así definida, es una fórmula de tipo Σ_1, pero es equivalente a

$$\bigwedge Xn(\alpha < n \wedge \beta < n \wedge X = \{0,1\}^{I_n \times I_n} \to \bigvee f \in X(\cdots))$$

donde los puntos suspensivos son la misma fórmula que sigue a $\bigvee f$ en la definición de $\alpha \preceq \beta$, y así tenemos una definición equivalente de tipo Π_1. Por consiguiente, la fórmula $\alpha \preceq \beta$ es de tipo Δ_1, al igual que

$$\alpha \in E \equiv \alpha \preceq \alpha.$$

A partir de esta definición podemos probar que si $f : I_n \times I_n \longrightarrow \{0,1\}$ y $g : I_m \times I_m \longrightarrow \{0,1\}$ cumplen la definición de $\alpha \preceq \beta$ con $n \leq m$, entonces $g|_{I_n \times I_n} = f$.

En efecto, si existe un par $(\gamma, \delta) \in I_n \times I_n$ tal que $f(\gamma, \delta) \neq g(\gamma, \delta)$, podemos tomar uno en el que el máximo de γ y δ sea el menor posible. Supongamos que $f(\gamma, \delta) = 1$ y $g(\gamma, \delta) = 0$ (el caso contrario es análogo).

Entonces, si $i, j < \ell(\gamma)$ con $i \leq j$, tenemos que $\max\{\gamma_j, \gamma_i\} < \gamma \leq \max\{\gamma, \delta\}$, luego $o(\gamma, f)$ y la minimalidad de (γ, δ) nos dan que $g(\gamma_j, \gamma_i) = f(\gamma_j, \gamma_i) = 1$, es decir, que $o(\gamma, g)$, e igualmente concluimos que $o(\delta, g)$.

Finalmente, si $\gamma \subset \delta$, entonces se cumple $r(\gamma, \delta, g)$, luego $g(\gamma, \delta) = 1$ y tenemos una contradicción. En caso contrario, como se cumple $r(\gamma, \delta, f)$, tiene que existir un $i < \ell(\gamma)$, $i < \ell(\delta)$ tal que $\gamma|_{I_i} = \delta|_{I_i} \wedge \gamma_i \neq \delta_i \wedge f(\gamma_i, \delta_i) = 1$, pero $\gamma_i < \gamma$ y $\delta_i < \delta$ implican que $\max\{\gamma_i, \delta_i\} < \max\{\gamma, \delta\}$, luego por la minimalidad de (γ, δ) tenemos que $g(\gamma_i, \delta_i) = 1$, luego se cumple $r(\gamma, \delta, g)$, y también $g(\gamma, \delta) = 1$ y de nuevo tenemos una contradicción. ■

De la unicidad que acabamos de probar se sigue que si $f : I_n \times I_n \longrightarrow \{0,1\}$ cumple la definición de $\alpha \preceq \beta$, necesariamente

$$\bigwedge \gamma\delta < n(f(\gamma, \delta) = 1 \leftrightarrow \gamma \preceq \delta),$$

lo que nos da la caracterización recurrente de la relación $\preceq$:

$$\alpha \preceq \beta \leftrightarrow \bigwedge ij < \ell(\alpha)(i \leq j \to \alpha_j \preceq \alpha_i) \wedge \bigwedge ij < \ell(\beta)(i \leq j \to \beta_j \preceq \beta_i) \wedge$$
$$(\alpha \subset \beta \vee \bigvee i < \ell(\alpha)(i < \ell(\beta) \wedge \alpha|_i = \beta|_i \wedge \alpha_i \prec \beta_i)).$$

A partir de aquí, todos los resultados que hemos demostrado en ARP se demuestran en $\mathrm{I}\Sigma_1$ con literalmente las mismas demostraciones. Sólo hemos usado otra definición de un funtor por recursión al definir $\omega^{(n)}$, pero una definición alternativa es

$$\alpha = \omega^{(n)} \equiv \bigvee s(\ell(s) = n+1 \land \alpha = s(n) \land s(0) = 1 \land \bigwedge i < n\ s(i+1) = \omega^{s(i)}).$$

Es claro que en $\mathrm{I}\Sigma_1$ se prueba que para cada n existe un único α que cumple $\alpha = \omega^{(n)}$, por lo que $\omega^{(n)}$ está bien definido. La fórmula es claramente Σ_1, luego de hecho es Δ_1. ■

Ordinales metamatemáticos Aunque estamos trabajando en ARP (o, equivalentemente, en $\mathrm{I}\Sigma_1$), la definición de ordinal tiene sentido al margen de cualquier axiomática. Concretamente, podemos definir la relación

$$m \preceq n \quad \text{syss} \quad \mathbb{N} \vDash \bar{m} \preceq \bar{n},$$

y el hecho de que la fórmula $\alpha \preceq \beta$ sea Δ_0 en ARP se traduce en que la relación es recursiva primitiva, al igual que lo es el conjunto E formado por los números naturales que cumplen $n \preceq n$.

Los razonamientos que hemos presentado en $\mathrm{I}\Sigma_1$ se traducen en razonamientos metamatemáticos que justifican que $\preceq$ es una relación de orden total en el conjunto E, de modo que expresiones como

$$\omega^{\omega^2+\omega\cdot 5+8}\cdot 3 + \omega^{\omega\cdot 3+5}\cdot 9 + \omega^7\cdot 6 + \omega^4 + \omega^2 + 12$$

son meras formas de nombrar a ciertos números naturales y, en la medida en que, metamatemáticamente, podemos afirmar que todo número natural es 0 o 1 o 2, etc., también podemos afirmar que todo ordinal está determinado por una única expresión de esta forma. ■

Ordinales en la teoría de conjuntos El lector familiarizado con la teoría de conjuntos sabrá que en cualquier teoría de conjuntos "fuerte" como ZF es posible definir un concepto general de "ordinal", de modo que los ordinales representan todas las formas posibles de ordenar bien un conjunto, salvo semejanza. Así, todos los conjuntos con 7 elementos admiten un único tipo de orden, que es el asociado al ordinal 7, mientras que ω es el ordinal correspondiente al buen orden usual de los números naturales, etc.

Los ordinales que hemos definido aritméticamente se corresponden con los primeros ordinales definibles en la teoría de conjuntos, concretamente con los menores que el ordinal conocido como ϵ_0, que se define como el supremo de la sucesión $\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots$

La relación entre la definición general de ordinal y la definición aritmética que hemos dado aquí se establece a través de la llamada *forma normal de Cantor*. Según [TC 3.51], todo ordinal $\alpha > 0$, (en el sentido conjuntista usual) admite una única expresión en la forma

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n},$$

para ciertos ordinales $\eta_0 \geq \eta_1 \geq \cdots \geq \eta_n$. Si además α es menor que ϵ_0, entonces $\eta_0 < \alpha$. Esto permite definir por recurrencia una aplicación $\phi : \epsilon_0 \longrightarrow E$ dada por $\phi(0) = 0$ y

$$\phi(\omega^{\eta_0} + \cdots + \omega^{\eta_n}) = (\phi(\eta_0), \ldots, \phi(\eta_n)).$$

La discusión de la forma normal de Cantor al final de la sección 3.6 de [TC] justifica inmediatamente que ϕ es una semejanza.

Así pues, los ordinales que hemos definido aquí como números naturales son esencialmente "los mismos" que los ordinales $< \epsilon_0$ que se definen de forma usual en la teoría de conjuntos, sólo que la definición que hemos dado aquí es válida en cualquier sistema aritmético, como la teoría de conjuntos ZF menos el axioma de infinitud, o la aritmética de Peano, o incluso en teorías más débiles como es el caso de $\mathrm{I}\Sigma_1$.

En la teoría de conjuntos se define una suma, un producto y una exponenciación de ordinales de forma natural. Por ejemplo, si α y β son dos ordinales, el ordinal $\alpha+\beta$ es el ordinal correspondiente al tipo de orden que resulta de unir dos conjuntos disjuntos, uno bien ordenado con tipo de orden α y otro con tipo de orden β, y de forma que todos los elementos del primero se consideran menores que cualquiera de los elementos del segundo. Al final de la sección 3.6 de [TC] mostramos también cómo calcular la forma normal de la suma y el producto de dos ordinales en forma normal, y aquí vamos a convertir en las definiciones de la suma y el producto de orinales lo que allí son teoremas deducidos de la definición general de suma y producto de ordinales. Las definiciones aritméticas que vamos a dar parecerán arbitrarias y caprichosas al lector no familiarizado con la teoría de conjuntos, igual que parecería arbitrario y caprichoso definir la derivada de $\operatorname{sen} x$ como $\cos x$ y la derivada de $\cos x$ como $-\operatorname{sen} x$ en lugar de demostrar estos hechos a partir de la definición general de derivada. El caso es que, con las definiciones que vamos a dar, la función $\phi : \epsilon_0 \longrightarrow E$, no sólo conserva el orden, sino también la suma y el producto de ordinales. ■

Suma de ordinales En principio, la suma que aparece en $\omega^3+\omega^2$ es una mera notación, que no justifica que "sumemos" ordinales cualesquiera. Por ejemplo, $\omega^2 + \omega^3$ no está definido, ya que la sucesión de exponentes no es decreciente. Sin embargo, podemos definir la suma de dos ordinales cualesquiera conviniendo que $\alpha + 0 = 0 + \alpha = \alpha$ y, para ordinales no nulos

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n} \qquad \text{y} \qquad \beta = \omega^{\zeta_0} + \cdots + \omega^{\zeta_m},$$

la suma es $\alpha + \beta = \beta$ si $\eta_0 < \zeta_0$ o bien

$$\alpha + \beta = \omega^{\eta_0} + \cdots + \omega^{\eta_k} + \omega^{\zeta_0} + \cdots + \omega^{\zeta_m}$$

si $\eta_{k+1} < \zeta_0 \leq \eta_k$.

En particular, si $\eta < \eta'$ se cumple que $\omega^\eta + \omega^{\eta'} = \omega^{\eta'}$, y esta identidad basta para sumar fácilmente dos ordinales cualesquiera. Basta escribir la suma completa

$$\omega^{\eta_0} + \cdots + \omega^{\eta_n} + \omega^{\zeta_0} + \cdots + \omega^{\zeta_m}$$

y aplicar tantas veces como se pueda la relación precedente para cancelar sumandos intermedios. Es pura rutina comprobar que la suma de ordinales así definida es asociativa (pero no conmutativa),[2] así como que lo que habíamos definido en principio como una mera notación al expresar un ordinal en la forma $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n}$, ahora puede verse como la suma de los ordinales ω^{η_i} en el sentido que acabamos de definir.

En particular, la suma de los ordinales finitos se corresponde con la suma usual de números naturales, pues, por ejemplo,

$$2 + 3 = (\omega^0 + \omega^0) + (\omega^0 + \omega^0 + \omega^0) = 5.$$

Por otra parte, es inmediato que $\alpha' = \alpha + 1$, por lo que, una vez introducida la suma de ordinales, ya no necesitamos emplear una notación específica para el siguiente de un ordinal dado. ■

Producto de ordinales Similarmente podemos definir un producto de ordinales estableciendo que en primer lugar que $\alpha \cdot 0 = 0 \cdot \alpha = 0$, $\alpha \cdot 1 = \alpha$. En segundo lugar, para

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n}, \qquad \zeta > 0,$$

definimos $\alpha \cdot \omega^{\zeta} = \omega^{\eta_0 + \zeta}$, y, en general, si además $\beta = \omega^{\zeta_0} + \cdots + \omega^{\zeta_m}$, definimos

$$\alpha\beta = \alpha\omega^{\zeta_0} + \cdots + \alpha\omega^{\zeta_m},$$

donde cada término se calcula con los criterios precedentes.

Por ejemplo:

$$\begin{gathered}
(\omega^{\omega^{\omega^3+\omega}} + \omega^7 + 8)(\omega^5 + \omega + 3) = \omega^{\omega^{\omega^3+\omega}+5} + \omega^{\omega^{\omega^3+\omega}+1} + \\
\omega^{\omega^{\omega^3+\omega}} + \omega^7 + 8 + \omega^{\omega^{\omega^3+\omega}} + \omega^7 + 8 + \omega^{\omega^{\omega^3+\omega}} + \omega^7 + 8 \\
= \omega^{\omega^{\omega^3+\omega}+5} + \omega^{\omega^{\omega^3+\omega}+1} + \omega^{\omega^{\omega^3+\omega}} + \omega^{\omega^{\omega^3+\omega}} + \omega^{\omega^{\omega^3+\omega}} + \omega^7 + 8 \\
= \omega^{\omega^{\omega^3+\omega}+5} + \omega^{\omega^{\omega^3+\omega}+1} + \omega^{\omega^{\omega^3+\omega}} \cdot 3 + \omega^7 + 8.
\end{gathered}$$

Notemos que los dos primeros sumandos corresponden a $\alpha\omega^5$ y $\alpha\omega^1$, mientras que, para calcular la multiplicación por $3 = 1 + 1 + 1$, hemos copiado tres veces el primer factor, para luego reducir la suma.

El producto de ordinales finitos se corresponde con el producto usual de números naturales, pues, por ejemplo,

$$2 \cdot 3 = 2 \cdot (1 + 1 + 1) = 2 + 2 + 2 = 6.$$

[2] El hecho de que podamos definirla en ARP prueba que es recursiva primitiva o, más precisamente, que podemos definir una función recursiva primitiva $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ que se restringe a la suma en $E \times E$.

Más en general, si k es un ordinal finito, se cumple que $\alpha \cdot k = \alpha + \cdots + \alpha$ con k sumandos.

Una comprobación rutinaria muestra[3] que el producto de ordinales es asociativo y cumple la propiedad distributiva $\alpha(\beta+\gamma) = \alpha\beta+\alpha\gamma$, pero no es cierto en general que $(\alpha+\beta)\gamma = \alpha\gamma+\beta\gamma$. ■

Exponenciación de ordinales Es posible definir una exponenciación de ordinales, pero no vamos a hacerlo. No obstante, usaremos la notación α^k con el sentido usual para exponentes finitos, y también tenemos definida la exponenciación ω^α, que claramente cumple la relación

$$\omega^\alpha\omega^\beta = \omega^{\alpha+\beta},$$

de donde en particular $(\omega^\alpha)^k = \omega^{\alpha k}$.

Hemos definido también la exponenciación iterada $\omega^{(n)}$. Un poco más en general, conviene definir

$$\omega_0(\alpha) = \alpha, \qquad \omega_{n+1}(\alpha) = \omega^{\omega_n(\alpha)}.$$

Así $\omega^{(n)} = \omega_n(1)$.

Suma formal de ordinales Hay una operación entre ordinales que vamos a necesitar y que no se considera habitualmente en teoría de conjuntos. Definimos $\alpha\#0 = 0\#\alpha = \alpha$ y, si

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n} \qquad \text{y} \qquad \beta = \omega^{\zeta_0} + \cdots + \omega^{\zeta_m},$$

entonces

$$\alpha\#\beta = \omega^{\theta_0} + \cdots + \omega^{\theta_{n+m+1}},$$

donde la sucesión $\theta_0 \succeq \cdots \succeq \theta_{n+m+1}$ es la que resulta de intercalar las dos sucesiones $\eta_0 \succeq \cdots \succeq \eta_n$ y $\zeta_0 \succeq \cdots \succeq \zeta_n$ en una misma sucesión decreciente.

Es claro que, al contrario que la suma ordinaria, la suma formal de ordinales es conmutativa. Usaremos también que si $\alpha \prec \beta$, entonces $\alpha\#\gamma \prec \beta\#\gamma$. ■

Necesitaremos un par de resultados elementales sobre las operaciones con ordinales:

Teorema 6.8 *Si $\alpha \preceq \beta$ son ordinales, existe un único δ tal que $\alpha + \delta = \beta$.*

Demostración: No sólo vamos a probar que existe dicho δ, sino que podemos obtenerlo explícitamente[4] si conocemos α y β. Si

$$\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_n} \qquad \text{y} \qquad \beta = \omega^{\zeta_0} + \cdots + \omega^{\zeta_m},$$

o bien β extiende a α, en cuyo caso δ es necesariamente la suma de los términos que faltan para completar β, o bien existe un $i < n$ tal que $\eta_j = \zeta_j$ para $j < i$ y $\eta_i < \zeta_i$, en cuyo caso necesariamente $\delta = \omega^{\zeta_i} + \cdots + \omega^{\zeta_m}$. ■

[3]También es claro que el producto de ordinales se extiende a una aplicación recursiva primitiva $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.

[4]Por ello la prueba es formalizable en APR y la aplicación $(\alpha, \beta) \mapsto \delta$ es recursiva primitiva.

Teorema 6.9 *Si α y β son dos ordinales no nulos, entonces*

$$\omega_k(\alpha\#\beta) \geq \omega_k(\alpha)\#\omega_k(\beta).$$

DEMOSTRACIÓN: Para $k = 0$ es inmediato. Para $k = 1$ basta tener en cuenta que $\alpha\#\beta > \text{máx}\{\alpha, \beta\}$ y el caso general se prueba fácilmente por inducción:

$$\omega_{k+1}(\alpha\#\beta) = \omega^{\omega_k(\alpha\#\beta)} \geq \omega^{\omega_k(\alpha)\#\omega_k(\beta)} \geq \omega^{\omega_k(\alpha)}\#\omega^{\omega_k(\beta)} = \omega_{k+1}(\alpha)\#\omega_{k+1}(\beta).$$

■

6.3 Sucesiones fundamentales

Una característica importante de la representación aritmética que hemos dado de los ordinales menores que ϵ_0 es que, podemos asociar explícitamente a cada ordinal límite λ una sucesión estrictamente creciente de ordinales cuyo supremo sea λ. Por conveniencia la definimos también de forma trivial para ordinales que no sean límite:

Definición 6.10 *Para cada ordinal α y cada número natural n definimos:*

$$\alpha[n] = \begin{cases} 0 & si\ \alpha = 0, \\ \beta & si\ \alpha = \beta + 1, \\ \beta + \omega^\eta \cdot n & si\ \alpha = \beta + \omega^{\eta+1}, \\ \beta + \omega^{\eta[n]} & si\ \alpha = \beta + \omega^\eta,\ con\ \eta\ límite. \end{cases}$$

La sucesión $\{\alpha[n]\}_{n=0}^\infty$ se llama sucesión fundamental de α.

Aquí hay que entender que cuando planteamos $\alpha = \beta + \omega^{\eta+1}$ o $\alpha = \beta + \omega^\eta$ no estamos considerando sumas arbitrarias, sino que nos referimos a que $\omega^{\eta+1}$ (resp. ω^η) es el último término de la expresión de α como suma de potencias de ω con exponentes decrecientes, y que β es la suma de los términos anteriores.

Notemos que se trata de una definición por recursión completa sobre la relación de orden usual en $\mathbb{N}$, ya que para definir $\alpha[n]$ sólo necesitamos suponer que $\eta[n]$ está definido sobre un exponente η de α, que, como número natural, será menor que α. Por lo tanto, podemos ver a $\alpha[n]$ como un funtor de rango 2 de ARP.

Vemos que la sucesión fundamental de 0 está definida como la sucesión constante 0, mientras que la sucesión fundamental de un ordinal sucesor $\beta + 1$ está definida como la sucesión constante β.

He aquí algunos ejemplos de sucesiones fundamentales de ordinales límite:

ω	$\{n\}_{n=0}^\infty$
$\omega \cdot 5$	$\{\omega^4 + n\}_{n=0}^\infty$
ω^5	$\{\omega^4 \cdot n\}_{n=0}^\infty$
ω^ω	$\{\omega^n\}_{n=0}^\infty$

Teorema 6.11 *Si λ es un ordinal límite, entonces $\lambda[n] \prec \lambda[n+1] \prec \lambda$.*

DEMOSTRACIÓN: Razonamos por inducción sobre λ, es decir, suponemos que el resultado es cierto para todo ordinal que, como número natural, sea menor que λ.

Si $\lambda = \beta + \omega^{\eta+1}$, entonces

$$\beta = \langle \zeta_0, \ldots, \zeta_{m-1} \rangle, \quad \text{y} \quad \lambda = \langle \zeta_0, \ldots, \zeta_{m-1}, \eta + 1 \rangle,$$

mientras que

$$\lambda[n] = \langle \zeta_0, \ldots, \zeta_{m-1}, \overbrace{\eta, \ldots, \eta}^{n} \rangle.$$

Es claro entonces que la sucesión fundamental es estrictamente creciente y que sus términos son todos anteriores a λ.

Supongamos ahora que $\lambda = \beta + \omega^\eta$, donde η es un ordinal límite. Como como $\eta < \lambda$ (en el orden usual de los números naturales), por hipótesis de inducción tenemos que

$$\eta[n] \prec \eta[n+1] \prec \eta.$$

Ahora

$$\lambda = \langle \zeta_0, \ldots, \zeta_{m-1}, \eta \rangle, \quad \lambda[n] = \langle \zeta_0, \ldots, \zeta_{m-1}, \eta[n] \rangle,$$

luego claramente $\lambda[n] \prec \lambda[n+1] \prec \lambda$. ■

En otras palabras, tenemos que la sucesión fundamental de un ordinal límite λ es estrictamente creciente y está siempre por debajo de λ. Nos falta probar que tiene a λ por supremo. En principio, esto significa que

$$\alpha \prec \lambda \rightarrow \bigvee n (\alpha \prec \lambda[n]).$$

No es difícil probar esto por inducción sobre λ, pero esta fórmula no es Δ_0, por lo que, en principio, la inducción no puede llevarse a cabo en ARP. Esto se debe a que ARP nos obliga a especificar cuál es el n que cumple lo requerido, y sucede que podemos especificarlo si nos preocupamos de hacerlo. Para ello tenemos que introducir la definición siguiente:

Definición 6.12 La *complejidad* de un ordinal α se define como

$$c(\alpha) = \sum_{i < \ell(\alpha)} (c(\alpha_i) + 1).$$

Se trata de una definición por recursión completa. Claramente:

1. $c(0) = 0$.
2. Si n es un ordinal finito, entonces $c(n) = n$ (más precisamente, $c(\hat{n}) = n$).
3. $c(\omega^\eta) = c(\eta) + 1$.
4. Si $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_{n-1}}$, con $\eta_0 \succ \cdots \succ \eta_{n-1}$, entonces

$$c(\alpha) = c(\omega^{\eta_0}) + \cdots + c(\omega^{\eta_{n-1}}).$$

Es fácil ver que (si α y β son no nulos, para la segunda desigualdad)

$$c(\alpha+\beta) \leq c(\alpha) + c(\beta), \qquad c(\alpha\beta) \leq c(\alpha)c(\beta),$$

Ahora podemos probar:[5]

Teorema 6.13 *Si λ es un ordinal límite, $\alpha \prec \lambda$ y $c(\alpha) \leq n$, entonces $\alpha \prec \lambda[n]$.*

Demostración: Razonamos por inducción sobre λ (notemos que el enunciado es una fórmula Δ_0 en ARP), es decir, suponemos que el teorema es cierto para todo ordinal menor que λ (como número natural). Pongamos que

$$\alpha = \alpha_0 + \omega^{\eta_1} \cdot m_1 + \cdots + \omega^{\eta_k} \cdot m_k, \quad \lambda = \alpha_0 + \omega^{\delta_1} \cdot n_1 + \cdots + \omega^{\delta_l} \cdot n_l,$$

de modo que $\eta_1 \succ \cdots \succ \eta_k$, $\delta_1 \succ \cdots \succ \delta_l$, $m_i \neq 0 \neq n_j$ y, o bien $k = 0$, o bien $\omega^{\eta_1} \cdot m_1 \prec \omega^{\delta_1} \cdot n_1$. Entonces

$$\lambda[n] \succeq \alpha_0 + \omega^{\delta_1}(n_1 - 1) + \omega^{\delta_1}[n],$$

pues si $l = 1$ se da la igualdad y, en caso contrario,

$$\lambda[n] \succ \alpha_0 + \omega^{\delta_1}(n_1 - 1) + \omega^{\delta_1} \succ \alpha_0 + \omega^{\delta_1}(n_1 - 1) + \omega^{\delta_1}[n].$$

Notemos que si $k = 0$, es decir, si $\alpha = \alpha_0$, se cumple trivialmente que $\alpha \prec \lambda[n]$, así que podemos suponer que $k \geq 1$.

La desigualdad $\omega^{\eta_1} \cdot m_1 \prec \omega^{\delta_1} \cdot n_1$ puede darse en dos casos:

1) Si $\eta_1 \prec \delta_1$, entonces, si $\delta_1 = \epsilon + 1$, entonces $\omega^{\delta_1}[n] = \omega^{\epsilon_1} \cdot n \succeq \omega^{\eta_1} \cdot n$ y, como $n \geq c(\alpha) \geq m_1$, tenemos que $\omega^{\delta_1}[n] \succeq \omega^{\eta_1}(m_1 + 1)$, luego

$$\lambda[n] \succeq \alpha_0 + \omega^{\eta_1}(m_1 + 1) \succ \alpha.$$

Si δ_1 es un ordinal límite, entonces $\omega^{\delta_1}[n] = \omega^{\delta_1[n]} \succ \omega^{\eta_1}$ por la hipótesis de inducción aplicada a $\delta_1 < \lambda$, ya que $c(\eta_1) \leq n$. Por lo tanto, $\lambda[n] \succ \alpha$.

2) Si $\eta_1 = \delta_1$ y $m_1 < n_1$, entonces, si $\delta_1 = \epsilon + 1$, es $\omega^{\delta_1}(n_1 - 1) \succeq \omega^{\eta_1} \cdot m_1$ y

$$\omega^{\delta_1}[n] \succ \omega^{\eta_2} \cdot m_2 + \cdots + \omega^{\eta_k} \cdot m_k$$

por la hipótesis de inducción aplicada a $\omega^{\delta_1} < \lambda$, pues

$$n \geq c(\alpha) \geq c(\omega^{\eta_2} \cdot m_2 + \cdots + \omega^{\eta_k} \cdot m_k).$$

[5] En realidad el teorema 6.13 vale, con la misma prueba, usando la siguiente definición alternativa de la complejidad de un ordinal: Si

$$\alpha = \omega^{\eta_0} \cdot k_0 + \cdots + \omega^{\eta_{n-1}} \cdot k_{n-1} \quad \text{con} \quad \eta_0 \succ \cdots \succ \eta_{n-1},$$

entonces $c(\alpha) = \max\{k_0, \ldots, k_{n-1}, c(\eta_0), \ldots, c(\eta_{n-1})\}$, entendiendo que $c(0) = 0$. Por ejemplo, con esta definición, $c(\omega^5 \cdot 3) = 5$, mientras que con la anterior $c(\omega^5 \cdot 3) = 9$. Esta definición es un poco más compleja, pero el número asignado a cada ordinal es menor o igual (y a menudo mucho menor) que el asignado con la otra definición.

Si δ_1 es un ordinal límite y $k = 1$, entonces

$$\lambda[n] \succeq \alpha_0 + \omega^{\eta_1} \cdot m_1 + \omega^{\eta_1}[n] \succ \alpha_0 + \omega^{\eta_1} \cdot m_1 = \alpha.$$

Si $k \geq 2$, entonces

$$\lambda[n] \succeq \alpha_0 + \omega^{\eta_1} \cdot m_1 + \omega^{\eta_1[n]} \succ \alpha,$$

pues por hipótesis de inducción $\eta_1[n] \succ \eta_2$, ya que $n \geq c(\alpha) \geq c(\eta_2)$. ■

Expresado con cuantificadores, el teorema anterior afirma que si λ es un ordinal límite, entonces

$$\bigwedge \alpha \prec \lambda \bigvee n\, \alpha \prec \lambda[n],$$

y esto expresa que λ es el supremo de la sucesión fundamental $\{\lambda[n]\}_{n=0}^{\infty}$.

6.4 La buena ordenación

La teoría que hemos expuesto en las sección 6.2 nos permite considerar a los ordinales —entenderemos siempre que nos referimos a los ordinales menores que ϵ_0— como objetos puramente finitistas en lugar de como objetos abstractos de los que no tiene sentido hablar si no es en el contexto de una teoría axiomática de conjuntos.

Así, mientras es más que cuestionable que tenga sentido plantearse si una afirmación conjuntista abstracta como la hipótesis del continuo es "en realidad" (?) verdadera o falsa, ahora podemos plantearnos si determinadas propiedades sobre los ordinales son realmente verdaderas o falsas independientemente de lo que digan los axiomas de la teoría de conjuntos.

A priori, no está claro que esto se aplique a una propiedad que, en el contexto de la teoría de conjuntos, se prueba trivialmente para todos los ordinales, y es que están bien ordenados: todo conjunto de ordinales no vacío tiene un mínimo elemento.

Decimos que no está claro *a priori* que tenga sentido plantearse si los ordinales están "de verdad" bien ordenados porque esto no es, en principio, una afirmación sobre todos los ordinales, sino sobre la totalidad de los conjuntos de ordinales, y no tenemos forma alguna de representarnos la totalidad de los conjuntos de ordinales como para asegurar que cada uno de ellos (salvo el vacío) tiene un mínimo elemento. Esta propiedad ni siquiera puede formalizarse en AP, donde podemos hablar de conjuntos finitos de ordinales, incluso de conjuntos infinitos definidos aritméticamente a través de fórmulas, pero no de conjuntos arbitrarios como para afirmar algo sobre la totalidad de los conjuntos de ordinales.

Una formulación "más tangible" del principio de buena ordenación es la siguiente:

> *No existen sucesiones infinitas de ordinales que sean estrictamente decrecientes.*

Se podría objetar que "la totalidad de las sucesiones (infinitas) de ordinales" es un concepto igual de escurridizo que el de "la totalidad de los conjuntos de ordinales". Enseguida discutiremos este punto, pero antes conviene entender por qué es relevante esta cuestión.

En el capítulo siguiente demostraremos este famoso resultado de Gentzen:

> *Si la aritmética de Peano es contradictoria, entonces existe una sucesión infinita de ordinales estrictamente decreciente.*

La prueba es estrictamente finitista, en el sentido de que el argumento prueba realmente que es posible programar un ordenador de modo que si le proporcionamos la demostración de una contradicción en la aritmética de Peano, a partir de ella generará una sucesión estrictamente decreciente de ordinales. Más precisamente, en tal supuesto podremos escribir en un papel un ordinal "de verdad" y dispondremos de un criterio que nos permitirá calcular explicitamente otro ordinal "de verdad" menor , y a su vez otro menor, etc., con la garantía de que el proceso no terminará nunca.

Si de algún modo podemos convencernos de que es del todo imposible generar una sucesión estrictamente decreciente de ordinales "de verdad", de ordinales que podamos escribir en un papel (sin entrar en consideraciones sobre si el papel necesario cabría o no en nuestro Universo), entonces tendremos una prueba de la consistencia de la aritmética de Peano que será tan finitista como lo sea el argumento que nos ha convencido de tal hecho (porque el resto del argumento, es decir, la prueba del resultado de Gentzen que hemos citado, es incuestionablemente finitista en el sentido más estricto del término).

Respecto a la cuestión de si realmente tiene sentido objetivo plantearse si existen o no sucesiones infinitas de ordinales estrictamente decrecientes, observemos en primer lugar que el concepto de "la totalidad de las sucesiones de ordinales" no es ni más ni menos inabarcable que "la totalidad de las sucesiones de números naturales" y, pese a ello, sí que podemos afirmar con convicción que no existen sucesiones infinitas decrecientes de números naturales. Podemos afirmarlo porque podemos razonar que es así: si uno intenta construir una sucesión infinita de números naturales estrictamente decreciente, tendrá que empezar especificando su primer término y, en cuanto lo haga, habrá fijado la máxima longitud que puede tener la sucesión: si empieza por 7, como máximo podrá tener 8 términos, y si empieza por 1 000, como máximo tendrá 1 001 términos, pero será finita en cualquier caso. No hemos necesitado considerar "la totalidad de las sucesiones de números naturales" para razonar que, si nos dan una cualquiera, no puede ser estrictamente decreciente.[6]

[6]No es algo nuevo que, ante una afirmación que —en principio— es dudoso que tenga un significado objetivo preciso, podamos convencernos de que lo tiene precisamente razonando que es cierta. Por ejemplo, es el caso de la afirmación *"los teoremas lógicos son verdaderos en cualquier modelo"*. No tenemos forma de representarnos "la totalidad de los modelos de un lenguaje formal", pero desde el momento en que disponemos de un argumento que justifica que, dado cualquier modelo concreto bien definido, cualquier teorema lógico va a ser necesariamente verdadero en él, esto da pleno sentido a la afirmación, pues podemos justificar que es inconcebible tener un modelo bien definido de un lenguaje formal en el que cualquier teorema lógico pueda no ser verdadero.

Así, podemos plantearnos si sucede algo parecido con la buena ordenación de los ordinales, expresada en términos de sucesiones decrecientes: ¿existe un argumento que nos convenza de que es imposible que una sucesión infinita de ordinales sea estrictamente decreciente sin necesidad de apelar a "la totalidad de las sucesiones de ordinales"?

Aquí vamos a dar un argumento debido a Takeuti (el lector deberá juzgar por sí mismo si lo considera "convincente" y, más en particular, hasta qué punto lo considera finitista). Para formularlo introducimos el concepto siguiente:

Definición 6.14 Diremos que un ordinal α es *accesible* si podemos razonar que no existen sucesiones infinitas estrictamente decrecientes de ordinales menores que α.

Nota Debemos resaltar que no estamos diciendo que α es accesible si no existen sucesiones infinitas estrictamente decrecientes de ordinales menores que α, sino que sólo afirmaremos que α es accesible cuando tengamos un argumento que nos convenza sin margen de dudas de que así es. Si el lector considera que el concepto de "sucesión infinita de ordinales" es demasiado "nebuloso" fuera del marco de una teoría axiomática que nos permita hablar con rigor de sucesiones arbitrarias, para nuestros fines no hay inconveniente en considerar únicamente sucesiones de ordinales generadas mediante un criterio explícito, es decir, mediante una función recursiva que vaya calculando sus términos o, dicho de otro modo, sucesiones que pueda ir generando un programa de ordenador. ■

Observemos que para demostrar el principio de buena ordenación (en su versión en términos de sucesiones decrecientes) basta demostrar que los ordinales

$$\omega \prec \omega^{(2)} \prec \omega^{(3)} \prec \omega^{(4)} \prec \cdots$$

son todos accesibles. En efecto, si podemos estar seguros de que no existen sucesiones infinitas estrictamente decrecientes de ordinales menores que ningún $\omega^{(n)}$, podemos asegurar que no hay ninguna en absoluto, ya que si hubiera una, digamos, $\xi_0 \succ \xi_1 \succ \xi_1 \succ \cdots$ tendría que existir un número natural n tal que $\xi_0 \prec \omega^{(n)}$ (que podríamos calcular explícitamente a la vista de ξ_0), y así tendríamos una sucesión decreciente por debajo de un $\omega^{(n)}$.

Una ligera variante del argumento que acabamos de dar prueba también el teorema siguiente:

Teorema 6.15 *Si $\alpha_0 \prec \alpha_1 \prec \alpha_2 \prec \cdots$ es una sucesión infinita estrictamente creciente de ordinales que tiene a α por supremo y cada α_i es accesible, entonces α también lo es.*

Otro hecho fundamental es el siguiente:

Teorema 6.16 *Si α y β son accesibles, entonces $\alpha + \beta$ también lo es.*

DEMOSTRACIÓN: Supongamos que tenemos una sucesión infinita

$$\alpha + \beta \succ \xi_0 \succ \xi_1 \succ \xi_2 \succ \cdots$$

¿Puede ocurrir que todos los términos de la sucesión cumplan $\xi_i \succeq \alpha$? En tal caso, el teorema 6.8 nos da que $\xi_i = \alpha + \mu_i$, para ciertos ordinales μ_i (que podemos calcular explícitamente a partir de ξ_i y de α), y además las desigualdades $\alpha + \mu_i \prec \alpha + \beta$ y $\alpha + \mu_i \succ \alpha + \mu_{i+1}$ implican que

$$\beta \succ \mu_0 \succ \mu_1 \succ \mu_2 \succ \cdots$$

Estamos suponiendo que tenemos justificado que no puede haber sucesiones infinitas estrictamente decrecientes de ordinales menores que β, luego podemos asegurar que esto no va a suceder,[7] es decir, que tiene que haber un índice i tal que $\xi_i \prec \alpha$, pero entonces, la sucesión a partir de este ξ_i sería una sucesión infinita estrictamente decreciente de ordinales menores que α, cosa que sabemos que tampoco puede darse. Concluimos así que es imposible que exista la sucesión de partida. ■

Combinando los dos resultados anteriores obtenemos:

Teorema 6.17 *Si α es un ordinal accesible, también lo es $\alpha \cdot \omega$.*

DEMOSTRACIÓN: Es fácil ver que $\alpha \cdot \omega$ es el supremo de la sucesión

$$\alpha \prec \alpha \cdot 2 \prec \alpha \cdot 3 \prec \cdots$$

o, lo que es lo mismo,

$$\alpha \prec \alpha + \alpha \prec \alpha + \alpha + \alpha \prec \cdots$$

Si sabemos justificar que no hay sucesiones decrecientes por debajo de α, el argumento de la prueba del teorema 6.16 nos convence de que no puede haber sucesiones decrecientes por debajo de $\alpha \cdot 2$, luego tampoco por debajo de $\alpha \cdot 3$, ni por debajo de $\alpha \cdot 4$, etc. y una vez estamos convencidos de que esto es así para todo $\alpha \cdot n$, el argumento del teorema 6.15 nos convence de que lo mismo vale para $\alpha \cdot \omega$, que es, pues, accesible. ■

Este teorema y 6.15 contienen el germen de toda la demostración. Vamos a hacernos una idea de hasta dónde podemos llegar únicamente a partir de ellos:

1. Es inmediato que ω es accesible, pues si $\omega \succ n_0 \succ n_1 \succ n_2 \succ \cdots$ es una sucesión decreciente de ordinales finitos, es claro que no puede tener más de $n_0 + 1$ términos.

2. Aplicando reiteradamente 6.17 nos convencemos de que todos los ordinales

$$\omega \prec \omega^2 \prec \omega^3 \prec \cdots$$

son accesibles, luego el supremo ω^ω también es accesible.[8]

[7] En particular, si un ordenador estuviera generando la sucesión ξ_i, tenemos la garantía de que, esperando lo suficiente, acabaría apareciendo un término $\xi_i \prec \alpha$.

[8] Esto es interesante porque en el capítulo siguiente veremos que implica la consistencia de $\mathrm{I}\Sigma_1$.

3. Volviendo a aplicar 6.17 nos convencemos de la accesibilidad de
$$\omega^{\omega+1} \prec \omega^{\omega+2} \prec \omega^{\omega+3} \prec \cdots,$$
luego también de la de $\omega^{\omega\cdot 2}$.

4. Una nueva oleada de aplicaciones de 6.17 nos convence de la accesibilidad de
$$\omega^{\omega\cdot 2+1} \prec \omega^{\omega\cdot 2+2} \prec \omega^{\omega\cdot 2+3} \prec \cdots,$$
y por consiguiente de la de $\omega^{\omega\cdot 3}$.

5. Como este argumento se puede repetir indefinidamente, no podemos sino convencernos de la accesibilidad de
$$\omega^{\omega} \prec \omega^{\omega\cdot 2} \prec \omega^{\omega\cdot 3} \prec \omega^{\omega\cdot 4} \prec \cdots,$$
luego también de la de ω^{ω^2}.

6. La oleada siguiente de aplicaciones de 6.17 nos da la accesibilidad de
$$\omega^{\omega^2+1} \prec \omega^{\omega^2+2} \prec \omega^{\omega^2+3} \prec \cdots,$$
luego también de la de $\omega^{\omega^2+\omega}$.

7. En este punto podemos vislumbrar una idea general: igual que hemos ascendido desde ω^ω hasta ω^{ω^2} mediante diversos pasos consistentes en ir sumando 1 al exponente (multiplicando por ω) y tomando supremos, podemos reproducir los mismos pasos partiendo de ω^{ω^2} y, sin necesidad de repasarlos todos uno a uno, nos convencemos de que esos mismos pasos nos permiten llegar hasta $\omega^{\omega^2+\omega^2} = \omega^{\omega^2\cdot 2}$, pero repitiendo de nuevo el mismo bloque de pasos llegamos hasta $\omega^{\omega^2\cdot 3}$ y, como queda claro que podemos repetir indefinidamente este bloque de pasos, acabamos convencidos de la accesibilidad de
$$\omega^{\omega^2} \prec \omega^{\omega^2\cdot 2} \prec \omega^{\omega^2\cdot 3} \prec \cdots$$
y, por consiguiente, de la de ω^{ω^3}.

8. Pero el mismo bloque de pasos (mayor que el considerado antes) que nos permite pasar de ω a ω^{ω^3}, aplicado ahora a ω^{ω^3}, nos permite pasar a $\omega^{\omega^3\cdot 2}$, y aplicando sistemáticamente dicho bloque de pasos, nos convencemos de la accesibilidad de
$$\omega^{\omega^3} \prec \omega^{\omega^3\cdot 2} \prec \omega^{\omega^3\cdot 3} \prec \omega^{\omega^3\cdot 4} \prec \cdots,$$
luego también de la de ω^{ω^4}.

9. Y una vez que nos convencemos de que este proceso puede seguirse para justificar la accesibilidad de
$$\omega^{\omega} \prec \omega^{\omega^2} \prec \omega^{\omega^3} \prec \omega^{\omega^4} \prec \cdots,$$
concluimos que ω^{ω^ω} es accesible.

Y en este punto uno se plantea si sería legítimo concluir con un “y así sucesivamente”. El propio Gentzen consideraba que sí:

> *Podemos, por ejemplo, visualizar los casos iniciales con características* 1, 2, 3 *con detalle. A medida que la característica crece, no se añade nada básicamente nuevo, el método de progresión es siempre el mismo. Desde luego, hay que admitir que la complejidad de los infinitos múltiplemente anidados que hay que recorrer crece considerablemente; este recorrido debe considerarse siempre como potencial* [...] *La dificultad reside en que, aunque el sentido finitista preciso de “recorrer” los ordinales es razonablemente claro en los casos iniciales, se vuelve de tal complejidad en el caso general que apenas es remotamente visualizable.*

Pero Gödel no estuvo de acuerdo:

> *La situación, a grandes rasgos, puede ser descrita como sigue: La inducción transfinita hasta ϵ_0 podría probarse finitistamente si y sólo si la consistencia de la teoría de números pudiera probarse finitistamente. Por otra parte, la validez de esta inducción no puede hacerse inmediatamente evidente, como sucede, por ejemplo, en el caso de ω^2. Es decir, uno no puede captar de un vistazo las diversas posibilidades estructurales que existen para las sucesiones decrecientes y no existe, por lo tanto, un conocimiento concreto inmediato de la terminación de cada una de dichas sucesiones. Pero, más aún, tal conocimiento concreto (en el sentido de Hilbert) no puede alcanzarse a través de una transición gradual de ordinales menores a otros mayores, porque los pasos concretamente evidentes, como $\alpha \mapsto \alpha^2$ son tan pequeños que tendrían que repetirse ϵ_0 veces para llegar hasta ϵ_0.*

Takeuti fue alumno de Gödel y uno de los principales continuadores del trabajo de Gentzen. Vamos a ver cómo resolvió la cuestión del sospechoso “y así sucesivamente”, mostrando con precisión cómo es posible usar bloques de razonamientos para aumentar exponentes situados cada vez más arriba en una torre de potencias de ω. Para ello introdujo la definición siguiente:

Definición 6.18 Diremos que un ordinal α es 1-*accesible* si es accesible y, supuesto definido el concepto de ordinal n-accesible, diremos que α es $n+1$-*accesible* si podemos asegurar que cuando β es n-accesible, entonces $\beta \cdot \omega^\alpha$ es n-accesible.

Ahora podemos probar los análogos de los teoremas 6.15 y 6.17:

Teorema 6.19 *Si $\alpha_0 \prec \alpha_1 \prec \alpha_2 \prec \cdots$ es una sucesión infinita estrictamente creciente de ordinales que tiene a α por supremo y cada α_i es n-accesible, entonces α también lo es.*

Demostración: Para $n = 1$ es el teorema 6.15. Supongamos que es cierto para n y vamos a ver que si cada α_i es $n+1$-accesible, lo mismo le sucede a α. Para ello tomamos un ordinal β del que sabemos que es n-accesible β, y entonces, por hipótesis, podemos asegurar que cada $\beta \cdot \omega^{\alpha_i}$ es n-accesible, luego por el caso n-simo sabemos que el supremo $\beta \cdot \omega^{\alpha}$ es n-accesible, y esto prueba que α es $n+1$-accesible. ■

Teorema 6.20 *Si α es un ordinal n-accesible, también lo es $\alpha \cdot \omega$.*

Demostración: Para $n = 1$ es el teorema 6.17. Si el resultado es cierto para n y α es $n+1$-accesible, tomamos un ordinal β de que sabemos que es n-accesible, y tenemos que probar que $\beta \cdot \omega^{\alpha\cdot\omega}$ también lo es. Pero éste es el supremo de la sucesión

$$\beta \cdot \omega^{\alpha} \prec \beta \cdot \omega^{\alpha\cdot 2} \prec \beta \cdot \omega^{\alpha\cdot 3} \prec \beta \cdot \omega^{\alpha\cdot 4} \prec \cdots,$$

luego, por el teorema anterior, basta probar que cada $\beta \cdot \omega^{\alpha\cdot k}$ es n-accesible. Ahora bien, $\beta \cdot \omega^{\alpha\cdot k} = \beta \cdot \omega^{\alpha} \cdots \omega^{\alpha}$ y basta usar k veces que α es $n+1$-accesible. ■

Como consecuencia inmediata:

Teorema 6.21 *El ordinal 1 es n-accesible, para todo número natural $n \geq 1$.*

Demostración: Es trivial que 1 es accesible. Si β es un ordinal n-accesible, entonces $\beta \cdot \omega^1$ es n-accesible por el teorema anterior, luego 1 es $n+1$-accesible. ■

Ahora ya es fácil probar:

Teorema 6.22 *Los ordinales $\omega \prec \omega^{(2)} \prec \omega^{(3)} \prec \cdots$ son accesibles.*

Demostración: Vamos a demostrar, por ejemplo, que $\omega^{(5)}$ es accesible, pero el argumento vale claramente para cualquier otro caso.

1. Por el teorema anterior, 1 es 6-accesible.
2. Como 1 también es 5-accesible, la definición de 6-accesible nos da que $\omega = 1 \cdot \omega^1$ es 5-accesible.
3. Como 1 es 4 accesible, la definición de 5-accesible nos da que $\omega^{(2)} = 1 \cdot \omega^{\omega}$ es 4-accesible.
4. Como 1 es 3-accesible, la definición de 4-accesible nos da que $\omega^{(3)} = 1 \cdot \omega^{\omega^{(2)}}$ es 3-accesible.
5. Como 1 es 2-accesible, la definición de 3-accesible nos da que $\omega^{(4)} = 1 \cdot \omega^{\omega^{(3)}}$ es 2-accesible.
6. Como 1 es accesible, la definición de 2-accesible nos da que $\omega^{(5)} = 1 \cdot \omega^{\omega^{(4)}}$ es accesible. ■

Según hemos observado tras la definición 6.14, esto prueba el principio de buena ordenación. El lector debería meditar sobre si está dispuesto a considerar finitista la prueba que acabamos de dar.

6.5 Inducción transfinita

Hay un hecho que podría hacernos desconfiar de que el principio de buena ordenación pueda tener una prueba que merezca el calificativo de "finitista", y es que, dado que implica la consistencia de AP, en virtud del segundo teorema de incompletitud de Gödel no puede ser formalizable en AP. ¿Podemos admitir como puramente finitista un argumento no formalizable en AP (o, equivalentemente, en ZFC sin el axioma de infinitud más el axioma "todo conjunto es finito")? Vamos a ver que no es descabellado responder que sí.

En primer lugar nos encontramos con el obstáculo obvio, y es que en AP no es posible hablar de sucesiones infinitas arbitrarias. No obstante, la consistencia de AP no requiere que no existan sucesiones infinitas arbitrarias de ordinales estrictamente decrecientes, sino que basta con que no exista ninguna definida aritméticamente (mediante una función recursiva primitiva, de hecho), y esto sí que es expresable en el lenguaje $\mathcal{L}_a$. Podríamos introducir fácilmente un concepto de "sucesión infinita de ordinales definida por una fórmula", pero en realidad es más práctico trabajar con una formulación equivalente del principio de buena ordenación.

Inducción transfinita hasta $\boldsymbol{\epsilon_0}$ *Si, para un ordinal arbitrario α, bajo la hipótesis de inducción de que todos los ordinales $\beta \prec \alpha$ cumplen una propiedad $P(\beta)$, podemos demostrar $P(\alpha)$, entonces podemos asegurar que todos los ordinales (de E) cumplen $P(\alpha)$.*

Si el lector considera que el concepto de "propiedad arbitraria" es nebuloso fuera del marco de una teoría axiomática formal, señalamos que, en lo tocante a la consistencia de AP, sólo necesitaremos considerar una en concreto, que podemos definir explícitamente.

La demostración de Takeuti del principio de buena ordenación dada en la sección anterior implica que la inducción transfinita hasta ϵ_0 es válida, pues si $P(\alpha)$ cumple la hipótesis del principio de inducción, pero existe un ordinal α_0 que no cumple $P(\alpha_0)$, tiene que existir $\alpha_1 \prec \alpha_0$ que tampoco cumpla $P(\alpha_1)$, luego a su vez tiene que existir un $\alpha_2 \prec \alpha_1$ que tampoco cumpla $P(\alpha_2)$, y de este modo construimos una sucesión infinita estrictamente decreciente de ordinales.

Recíprocamente, el principio de inducción transfinita implica que no existen sucesiones decrecientes de ordinales, pues si hubiera una, basta tomar como $P(\alpha)$ la propiedad "α no aparece en la sucesión" para concluir que ningún ordinal aparece en la sucesión.

Por descontado, en una teoría de conjuntos como ZF, la inducción transfinita hasta ϵ_0 puede probarse trivialmente a partir de la buena ordenación del ordinal ϵ_0 tal y como se define usualmente, pero, dado que implica la consistencia de AP, es interesante saber que es posible demostrarla "de verdad", en lugar de demostrar una mera formalización del principio en una teoría de conjuntos, pues el hecho de que la teoría de conjuntos permite probar la consistencia de AP es poco menos que trivial.

Ahora es fácil formalizar el principio de inducción transfinita en $\mathcal{L}_a$, al menos si consideramos únicamente propiedades definibles mediante fórmulas. Para cada fórmula $\phi(\alpha, x_1, \ldots, x_n)$ de $\mathcal{L}_a$, podemos considerar la fórmula

$$\phi - \mathrm{IND}(\epsilon_0) \equiv \bigwedge \alpha \in E(\bigwedge \delta \prec \alpha\, \phi(\delta) \to \phi(\alpha)) \to \bigwedge \alpha \in E\, \phi(\alpha).$$

El resultado de Gentzen que ya hemos citado y que demostraremos en el capítulo siguiente admite una prueba completamente finitista, por lo que es formalizable en ARP, concretamente mediante la fórmula

$$\phi - \mathrm{IND}(\epsilon_0) \to \mathrm{Consis}\ulcorner \mathrm{AP} \urcorner,$$

para una cierta fórmula[9] ϕ.

El segundo teorema de incompletitud de Gödel implica entonces que la sentencia $\phi - \mathrm{IND}(\epsilon_0)$ no es demostrable en AP. Sin embargo, el argumento puramente aritmético que hemos dado en la sección anterior prueba que es verdadera en su interpretación natural, así que es natural preguntarse qué hay en dicho argumento que no "quepa" en AP.

Sucede que "casi todo" el argumento de Takeuti es formalizable en AP. Para explicar esto consideramos las versiones parciales siguientes del principio de inducción transfinita:

$$\phi - \mathrm{IND}(\theta) \equiv \bigwedge \alpha \in E\, (\bigwedge \delta \prec \alpha\, \phi(\delta) \to \phi(\alpha)) \to \bigwedge \beta \preceq \theta\, \phi(\alpha).$$

La hipótesis de $\phi - \mathrm{IND}(\theta)$ es la misma que la de $\phi - \mathrm{IND}(\epsilon_0)$, pero en lugar de concluir que todos los ordinales cumplen $\phi(\alpha)$, limita la conclusión a los ordinales menores o iguales que θ.

Si definimos formalmente los ordinales ϕ-accesibles como los que cumplen $\phi-$ $\mathrm{IND}(\theta)$, sucede que el argumento que prueba teorema el 6.22 puede formalizarse en AP. No obstante, vamos a dar otro argumento más simple debido a Gentzen:

Teorema 6.23 (Gentzen) *Para toda fórmula $\phi(\alpha, x_1, \ldots, x_m)$ de $\mathcal{L}_a$, se cumple:*

$$\underset{\mathrm{AP}}{\vdash} \phi - \mathrm{IND}(\omega^{(1)}), \quad \underset{\mathrm{AP}}{\vdash} \phi - \mathrm{IND}(\omega^{(2)}), \quad \underset{\mathrm{AP}}{\vdash} \phi - \mathrm{IND}(\omega^{(3)}), \quad \ldots$$

Esto significa que en AP, bajo la hipótesis

$$\bigwedge \alpha \in E\, (\bigwedge \delta \prec \alpha\, \phi(\delta) \to \phi(\alpha)),$$

podemos demostrar que todos los ordinales menores que ω cumplen $\phi(\alpha)$, y que todos los ordinales menores que $\omega^{(2)}$ cumplen $\phi(\alpha)$, y que todos los ordinales menores que $\omega^{(3)}$ cumplen $\phi(\alpha)$, etc. En particular, podemos probar que cualquier ordinal α en concreto (representado por un designador, como $\alpha \equiv \omega^{\omega^5} + \omega^{\omega+7} + 9$), cumple $\phi(\alpha)$, pero —al menos para algunas fórmulas ϕ— no es posible demostrar $\bigwedge \alpha \in E\, \phi(\alpha)$.

[9] Concretamente

$$\phi(\alpha) \equiv \neg \bigvee D (\overset{D}{\underset{\mathrm{AP}}{\vdash}} (\varnothing \Rightarrow \varnothing) \land o(D) = \alpha),$$

donde $o(D) = \alpha$ es una fórmula Δ_1 en AP (o Δ_0 en ARP) que formaliza el concepto de ordinal de una demostración. Vemos que $\phi(\alpha)$ es una fórmula de tipo Π_1.

Demostración: Definimos $\phi^*(\alpha) \equiv \bigwedge \beta \preceq \alpha\, \phi(\beta)$ y

$$\phi'(\eta) \equiv \bigwedge \alpha(\phi^*(\alpha) \to \phi^*(\alpha + \omega^\eta)).$$

En primer lugar vamos a demostrar en AP la implicación:

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi(\beta) \to \phi(\alpha)) \to \bigwedge \eta \in E(\bigwedge \delta \prec \eta\, \phi'(\delta) \to \phi'(\eta)). \tag{6.1}$$

Suponemos, pues,

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi(\beta) \to \phi(\alpha)) \tag{6.2}$$

y observamos que esto implica

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi^*(\beta) \to \phi^*(\alpha)). \tag{6.3}$$

En efecto, fijamos $\alpha \in E$ y suponemos $\bigwedge \beta \prec \alpha\, \phi^*(\beta)$. Como $\phi^*(\beta) \to \phi(\beta)$, tenemos $\bigwedge \beta \prec \alpha\, \phi(\beta)$, luego por (6.2), podemos concluir $\phi(\alpha)$, luego concluimos $\bigwedge \beta \preceq \alpha\, \phi(\beta)$, que es $\phi^*(\alpha)$.

Fijamos ahora $\eta \in E$ y suponemos

$$\bigwedge \delta \prec \eta\, \phi'(\delta). \tag{6.4}$$

Tenemos que probar $\phi'(\eta)$. Para ello fijamos un ordinal α, suponemos $\phi^*(\alpha)$ y tenemos que probar $\phi^*(\alpha + \omega^\eta)$.

Distinguimos tres casos, según que si $\eta = 0$, o bien η es un ordinal sucesor $\eta = \delta + 1$, o bien η es un ordinal límite.

Si $\eta = 0$ tenemos que probar $\phi^*(\alpha + 1)$, pero la hipótesis $\phi^*(\alpha)$ equivale a $\bigwedge \beta \prec \alpha + 1\, \phi(\beta)$ y por (6.2) concluimos $\phi(\alpha + 1)$, lo que nos da $\phi^*(\alpha + 1)$.

Si $\eta = \delta + 1$ tenemos que demostrar $\phi^*(\alpha + \omega^{\delta+1})$. Para ello demostramos por inducción sobre k, que se cumple

$$\bigwedge k\, \phi^*(\alpha + \omega^\delta \cdot k). \tag{6.5}$$

Para $k = 0$ esto se reduce a $\phi^*(\alpha)$, y estamos suponiendo que se cumple. Ahora suponemos $\phi^*(\alpha + \omega^\delta \cdot k)$. Por (6.4) tenemos $\phi'(\delta)$, que, por definición, implica

$$\phi^*(\alpha + \omega^\delta \cdot k) \to \phi^*(\alpha + \omega^\delta \cdot k + \omega^\delta),$$

luego concluimos $\phi^*(\alpha + \omega^\delta(k + 1))$.

Esto termina la prueba de (6.5), y de aquí se sigue $\bigwedge \beta \prec \alpha + \omega^\delta \cdot \omega\, \phi^*(\beta)$, pues es fácil ver que, si $\beta \prec \alpha + \omega^\delta \cdot \omega$, existe un k tal que $\beta \prec \alpha + \omega^\delta \cdot k$, y por (6.5) se cumple $\phi^*(\alpha + \omega^\delta \cdot k)$, luego también $\phi^*(\beta)$. Por (6.3) concluimos $\phi^*(\alpha + \omega^\delta \cdot \omega)$, que es lo mismo que $\phi^*(\alpha + \omega^{\delta+1})$.

Por último, si η es un ordinal límite, para cada $\beta \prec \alpha + \omega^\eta$ existe un $\delta \prec \eta$ tal que $\beta \prec \alpha+\omega^\delta$. Por (6.4) tenemos $\phi'(\delta)$, lo cual nos da $\phi^*(\alpha) \to \phi^*(\alpha+\omega^\delta)$, luego de hecho tenemos $\phi^*(\alpha+\omega^\delta)$ y también $\phi^*(\beta)$. Esto prueba que

$$\bigwedge\beta \prec \alpha + \omega^\eta\, \phi^*(\beta),$$

luego por (6.3) tenemos $\phi^*(\alpha + \omega^\eta)$.

En segundo lugar vamos a probar la implicación

$$\bigwedge\alpha \preceq \omega^{(n)}\, \phi'(\alpha) \to \bigwedge\alpha \preceq \omega^{(n+1)}\, \phi(\alpha). \tag{6.6}$$

En efecto, si se cumple $\bigwedge\alpha \preceq \omega^{(n)}\, \phi'(\alpha)$, en particular tenemos $\phi'(\omega^{(n)})$, es decir,

$$\bigwedge\alpha(\phi^*(\alpha) \to \phi^*(\alpha + \omega^{(n+1)})),$$

luego haciendo $\alpha = 0$ obtenemos $\phi^*(\omega^{(n+1)})$, que es $\bigwedge\alpha \preceq \omega^{(n+1)}\, \phi(\alpha)$.

Con esto ya podemos concluir. Por ejemplo, para demostrar $\phi - \mathrm{IND}(\omega^{(4)})$, suponemos

$$\bigwedge\alpha \in E(\bigwedge\beta \prec \alpha\, \phi(\beta) \to \phi(\alpha)),$$

de donde, aplicando repetidamente (6.1),

$$\bigwedge\alpha \in E(\bigwedge\beta \prec \alpha\, \phi'(\beta) \to \phi'(\alpha)),$$

$$\bigwedge\alpha \in E(\bigwedge\beta \prec \alpha\, \phi''(\beta) \to \phi''(\alpha)),$$

$$\bigwedge\alpha \in E(\bigwedge\beta \prec \alpha\, \phi'''(\beta) \to \phi'''(\alpha)). \tag{6.7}$$

En particular (6.7) vale para todo ordinal finito α, luego por inducción concluimos que $\bigwedge\alpha \prec \omega^{(1)}\, \phi'''(\alpha)$, y aplicando (6.7) a $\alpha = \omega$ tenemos $\bigwedge\alpha \preceq \omega^{(1)}\, \phi'''(\alpha)$. Ahora aplicamos repetidamente (6.6) y obtenemos

$$\bigwedge\alpha \preceq \omega^{(2)}\, \phi''(\alpha), \quad \bigwedge\alpha \preceq \omega^{(3)}\, \phi'(\alpha), \quad \bigwedge\alpha \preceq \omega^{(4)}\, \phi(\alpha),$$

lo que concluye la prueba de $\phi - \mathrm{IND}(\omega^{(4)})$.

Es obvio que el mismo procedimiento permite demostrar $\phi - \mathrm{IND}(\omega^{(n)})$ para todo numeral $n \equiv 0, 1, 2, 3, 4\ldots$ ■

Nota Observemos que el argumento de la demostración anterior no permite demostrar

$$\bigwedge n\, \phi - \mathrm{IND}(\omega^{(n)}),$$

lo cual permitiría a su vez demostrar $\phi - \mathrm{IND}(\epsilon_0)$, porque necesitamos que n sea un número natural concreto, por ejemplo, 4, para aplicar tres veces (6.1) (pasando de la hipótesis sobre ϕ a la hipótesis análoga sobre ϕ''') y luego aplicar tres veces (6.6) para llegar a la conclusión. Con una variable n en lugar de un numeral no podríamos pasar a ϕ seguida de n "comitas". El razonamiento vale para $n = 4$ o $n = 2\,000$ o el n que sea, pero sólo tiene sentido si se trata de un n en particular, y la demostración será más larga cuanto mayor sea n. ■

Así pues, el único paso del argumento que demuestra el principio de inducción transfinita que no es formalizable en AP es el paso que nos lleva de la accesibilidad de cada ordinal $\omega^{(n)}$ a la accesibilidad de todos los ordinales. Esto se debe a que, aunque en AP podemos demostrar, ciertamente, que

$$\bigwedge \alpha \in E \bigvee n\, \alpha \preceq \omega^{(n)},$$

no podemos demostrar que todo ordinal α sea anterior a ω, o bien a $\omega^{(2)}$, o bien a $\omega^{(3)}$, etc., sino que AP admitirá modelos no estándar en los que haya ordinales $\omega^{(n)}$ con n mayor que cualquier número natural "de verdad".

Ahora bien, si estamos dispuestos a admitir, no sólo que AP es consistente, sino que tiene un modelo natural de modo que todos los teoremas de AP son verdaderos en su interpretación natural, entonces podemos concluir que el principio de inducción transfinita es válido sin más base que el teorema 6.23. En efecto, si para un ordinal arbitrario α, bajo la hipótesis de inducción de que todos los ordinales $\beta \prec \alpha$ cumplen una propiedad $P(\beta)$, podemos demostrar $P(\alpha)$, entonces:

1. Todos los ordinales $\alpha \preceq \omega$ cumplen $P(\alpha)$ (porque[10] $\phi - \mathrm{IND}(\omega)$ es demostrable en AP),

2. Todos los ordinales $\alpha \preceq \omega^{(2)}$ cumplen $P(\alpha)$ (porque $\phi - \mathrm{IND}(\omega^{(2)})$ es demostrable en AP),

3. Todos los ordinales $\alpha \preceq \omega^{(3)}$ cumplen $P(\alpha)$ (porque $\phi - \mathrm{IND}(\omega^{(3)})$ es demostrable en AP), ...

Y la conclusión de estos hechos es que todos los ordinales cumplen $P(\alpha)$, porque todo ordinal α cumple $\alpha \preceq \omega$, o bien $\alpha \preceq \omega^{(2)}$, o bien $\alpha \preceq \omega^{(3)}$, etc.

Así pues, podemos afirmar —sin contradecir al segundo teorema de incompletitud de Gödel— que la aritmética de Peano es capaz de demostrar la validez de la inducción transfinita hasta ϵ_0, no en el sentido —obviamente falso— de que en AP se pueda demostrar $\phi - \mathrm{IND}(\epsilon_0)$, sino en el sentido de que alguien convencido de que los teoremas de AP son verdaderos debe admitir que $\phi - \mathrm{IND}(\epsilon_0)$ también lo es, a pesar de que no sea demostrable (y de que, por consiguiente, no será verdadero en todos los modelos de AP, pero sí en el natural).

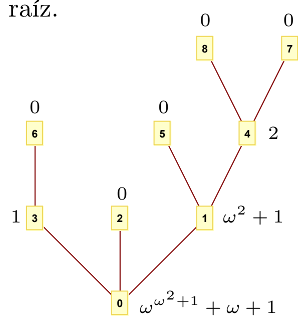
[10]En principio, el argumento que estamos dando requiere que la propiedad $P(\alpha)$ sea formalizable en términos de una fórmula $\phi(\alpha)$ de $\mathcal{L}_a$, pero en realidad esto no es necesario, pues la prueba del teorema anterior no ha usado en ningún momento que ϕ sea precisamente una fórmula de $\mathcal{L}_a$. Nada impide considerar un lenguaje $\mathcal{L}_a^*$ que resulte de añadir a $\mathcal{L}_a$ un relator monádico $R\alpha$ y considerar la teoría AP* que consta de los axiomas de AP con el esquema de inducción extendido a fórmulas de $\mathcal{L}_a^*$. Entonces cualquier propiedad $P(\alpha)$ objetivamente definida puede usarse para extender el modelo natural de $\mathcal{L}_a$ a un modelo de $\mathcal{L}_a^*$ en el que el relator R se interprete como la propiedad P, y la prueba del teorema anterior vale igualmente para la fórmula $\phi(\alpha) \equiv R\alpha$, lo cual prueba la validez de la inducción transfinita respecto de la propiedad P hasta cualquier ordinal $\omega^{(n)}$. Esto permite aplicar la inducción transfinita hasta ϵ_0 a los combates entre Hércules y la Hidra sin presuponer que Hércules sigue una estrategia "aritmética" a la hora de decidir qué cabeza corta en cada asalto.

6.6 Hércules y la Hidra II

Veamos ahora conexión entre los ordinales y el problema de Hércules y la Hidra. La clave está en que a cada hidra le podemos asociar un ordinal. Para ello vamos asignando un ordinal a cada uno de sus nodos según el criterio siguiente:

1. El ordinal asociado a una cabeza es 0.
2. Si de un nodo salen n ramas que llegan a nodos cuyos ordinales asociados son $\eta_0 \succeq \eta_1 \succeq \cdots \succeq \eta_n$, el ordinal de dicho nodo es $\omega^{\eta_0} + \cdots + \omega^{\eta_n}$.

El ordinal asociado a la Hidra es el asociado a su raíz.



Por ejemplo, el ordinal asociado a hidra que hemos considerado al principio de la sección 6.1 es

$$\alpha = \omega^{\omega^2+1} + \omega + 1.$$

Notemos que a partir de α podemos reconstruir el árbol. El hecho de que α conste de tres sumandos nos indica que de la raíz de la Hidra salen tres ramas, de las cuales, la correspondiente a $1 = \omega^0$ termina en una cabeza, la correspondiente a ω^1 termina en un nodo de ordinal $1 = \omega^0$, lo que indica que de él sale una única rama que termina en una cabeza y, por último, la tercera rama tiene ordinal $\omega^2 + \omega^0$, lo cual indica que de ella salen otras dos ramas, una que termina en una cabeza y otra de ordinal $2 = \omega^0 + \omega^0$, de la cual salen dos ramas que terminan en otras tantas cabezas.

Así pues, cada ordinal $\alpha \in E$ se corresponde biunívocamente con una hidra. La hidra muerta (a la que sólo le queda la raíz) es la de ordinal 0. Los números naturales corresponden a las "hidras bebés", cuyas cabezas salen todas de la raíz.

La tabla siguiente muestra el ordinal de la Hidra después de cada asalto en el que empleamos la estrategia de cortar la cabeza más alta con el mayor número de hermanas. Es fácil calcular el número de cabezas. Por ejemplo, tras el quinto asalto, de la raíz salen 12 ramas, de las cuales 4 conducen a grupos de 7 cabezas hermanas, otras 6 conducen a grupos de 6 cabezas hermanas y luego hay otras dos cabezas sin hermanas, en total $7 \cdot 4 + 6 \cdot 6 + 1 + 1 = 66$ cabezas.

Asalto	Ordinal	Asalto	Ordinal
0	$\omega^{\omega^2+1} + \omega + 1$	6	$\omega^7 \cdot 3 + \omega^6 \cdot 13 + \omega + 1$
1	$\omega^{\omega\cdot 2+1} + \omega + 1$	7	$\omega^7 \cdot 2 + \omega^6 \cdot 21 + \omega + 1$
2	$\omega^{\omega+4} + \omega + 1$	8	$\omega^7 + \omega^6 \cdot 30 + \omega + 1$
3	$\omega^8 + \omega + 1$	9	$\omega^6 \cdot 40 + \omega + 1$
4	$\omega^7 \cdot 5 + \omega + 1$	10	$\omega^6 \cdot 39 + \omega^5 \cdot 11 + \omega + 1$
5	$\omega^7 \cdot 4 + \omega^6 \cdot 6 + \omega + 1$	11	$\omega^6 \cdot 38 + \omega^5 \cdot 23 + \omega + 1$

La clave de la victoria de Hércules está en que, aunque el número de cabezas va aumentando, el ordinal de la Hidra disminuye en cada asalto, y eso no es casual, sino que es cierto sea cual sea la cabeza que Hércules le corte a la Hidra.

En efecto, supongamos que le cortamos a la Hidra una cabeza que no sale de la raíz, sino de un nodo que tiene por debajo otro nodo de ordinal α. Este α será de la forma

$$\alpha = \omega^{\eta_0} \cdot k_0 + \cdots + \omega^{\eta_n} \cdot k_n,$$

con $\eta_0 \succ \eta_1 \succ \cdots \succ \eta_n$. Pongamos que la cabeza cortada está en una de las ramas de ordinal η_i. Entonces $\eta_i = \eta' + 1$, donde el 1 corresponde a la cabeza cortada. Por lo tanto, tras la decapitación, tenemos que cambiar uno de los sumandos ω^{η_i}, con lo que nos queda $\omega^{\eta_i}(k_i - 1)$, y por otra parte tenemos que añadir $m+1$ sumandos $\omega^{\eta'}$, donde m es el número de asalto en curso. En total, hemos de cambiar:

$$\omega^{\eta_i} \cdot k_i \mapsto \omega^{\eta_i}(k_i - 1) + \omega^{\eta'} \cdot (m+1).$$

En suma, quitamos un término ω^{η_i} y añadimos $m+1$ términos $\omega^{\eta'} \prec \omega^{\eta_i}$. Claramente, esto hace que α cambie a un ordinal $\alpha' \prec \alpha$, y es claro que entonces el ordinal de la raíz también pasa de un ordinal β a otro $\beta' \prec \beta$, pues para compararlos nos encontraremos todos los términos iguales hasta llegar al correspondiente a la rama donde estaba la cabeza, para comparar estos términos comparamos los exponentes, y serán todos iguales excepto los correspondientes a la rama donde estaba la cabeza, y así vamos subiendo hasta llegar a los exponentes $\alpha' \prec \alpha$. Si la cabeza cortada sale de la raíz, el ordinal de la Hidra pasa de un cierto $\alpha + 1$ hasta α, luego también disminuye estrictamente.

Así pues, dado que el ordinal de la Hidra disminuye estrictamente en cada asalto, el hecho de que la Hidra muere necesariamente tras un número finito de asaltos (sea cual sea el criterio que siga Hércules para elegir la cabeza que corta en cada uno de ellos) es consecuencia inmediata del principio de buena ordenación: Una batalla en la que Hércules no venciera se correspondería con una sucesión infinita estrictamente decreciente de ordinales.

La estrategia "izquierda" Ahora podemos analizar más cómodamente la estrategia que hemos discutido anteriormente, es decir, la consistente en cortar una cabeza de altura máxima y con el mayor número de hermanas. En términos de ordinales es fácil ver que consiste en cortar la cabeza situada "más a la izquierda", en el sentido siguiente: partimos de la raíz subimos hasta cualquiera de los nodos de ordinal mayor, y desde éste a cualquiera tenga a su vez ordinal mayor, y así hasta llegar a una cabeza, y ésa es la que cortamos.

En nuestro ejemplo, para el primer asalto, partimos de la raíz 0, que tiene ordinal $\omega^{\omega^2+1} + \omega + 1$, subimos al nodo 1, que tiene ordinal $\omega^2 + 1$, desde ahí al nodo 2, que tiene ordinal 2 y luego a cualquiera de los nodos 7 u 8, que tienen ordinal 0 (son cabezas), así que cortamos cualquiera de ellas.

Analizar en general la evolución de la Hidra bajo esta estrategia puede ser complicado, pero la situación se simplifica cuando llegamos a un ordinal $\prec \omega^\omega$, cosa que en nuestro ejemplo sucede en el tercer asalto.

En general, si tras el asalto n la Hidra tiene ordinal

$$\omega^a \cdot b + \omega^{a-1} \cdot c + \cdots,$$

(compárese con $n = 4$, $a = 7$, $b = 5$, $c = 0$ en nuestro ejemplo), tras el asalto $n+1$, tenemos que b se reduce a $b-1$ (hay un grupo menos de cabezas hermanas de tamaño máximo a) y c aumenta hasta $c+n+2$ (un grupo de a cabezas hermanas ha pasado a tener $a-1$ y se han generado otros $n+1$ grupos iguales). Por consiguiente, tras el asalto $n+b$ el ordinal será

$$\omega^{a-1}(c + (n+2) + (n+3) + \cdots + (n+b+1))) + \cdots$$
$$= \omega^{a-1}\Big(c + \frac{(2n+b+3)b}{2}\Big) + \cdots$$

de modo que a se ha convertido en $a-1$ y b se ha convertido en $c+(2n+b+3)b/2$.

El lector puede comprobar que esta fórmula predice el ordinal que muestra la tabla siguiente para el asalto $n+b=9$. Si la vamos aplicando sucesivamente, obtenemos los resultados de la tabla. Así, tras el número de asaltos n que se indica en la última fila de la tabla, la Hidra llega a tener altura 1 con tantas cabezas como se indica en la columna b.

n	a	b	c
3	8	1	0
4	7	5	0
9	6	40	0
49	5	1 220	0
1 269	4	805 810	0
807 079	3	325 688 659 655	0
325 689 466 734	2	53 036 814 370 901 491 046 740	1
53 036 814 371 227 180 513 474	1	1 406 451 839 324 004 993 542 381 326 234 890 768 738 031 071	1
1 406 451 839 324 004 993 542 434 363 049 261 995 918 544 545	0	989 053 388 168 938 379 565 429 552 367 644 648 402 300 580 972 977 512 412 313 364 046 356 366 229 560 313 533 900 782	

Por lo tanto, la Hidra muere al cabo de $n+b$ asaltos, que es el valor

989 053 388 168 938 379 565 429 552 367 644 648 402 300 582
379 429 351 736 318 357 588 790 729 278 822 309 452 445 327

que ya habíamos adelantado.

En general, es inmediato que la función $N_i(\alpha)$ que a cada ordinal α le asigna el número de asaltos necesarios para matar la Hidra de ordinal α siguiendo la estrategia "izquierda" es recursiva (para calcularla, basta programar un ordenador para que vaya calculando el combate y cuente los asaltos que transcurren hasta que la Hidra muere). No es inmediato que sea recursiva primitiva, pues *a priori* no sabemos cuánto tendremos que esperar hasta que el cálculo termine (eso es justo lo que queremos calcular). Sin embargo, la prueba que hemos dado en la sección 6.1 de que la estrategia "izquierda" siempre acaba matando a la Hidra prueba que lo es, es decir, que podemos llegar al final del combate sin tener que esperar a ver cuándo sucede.

En efecto, es pura rutina comprobar que la función $H_i(\alpha, n)$ que proporciona el ordinal de la hidra que resulta de cortar la cabeza "izquierda" de la hidra de ordinal α en el n-simo asalto es recursiva primitiva, así como las funciones $h(\alpha)$, $m(\alpha)$ y $s(\alpha)$ que proporcionan la altura, el máximo número de cabezas hermanas de altura máxima y el número de grupos de tales cabezas, respectivamente, de la hidra de ordinal α (todas ellas se pueden calcular sin considerar en ningún momento números naturales mayores que α). Definimos entonces

$$H_i(\alpha, n, 0) = H_i(\alpha, n), \qquad H_i(\alpha, n, j+1) = H_i(H_i(\alpha, n, j), n+j),$$

que nos da el ordinal de la Hidra tras j asaltos. A su vez, definimos

$$B_0(n, k) = \left\langle H_i(n_1^2, n_2^2, k), n_2^2 + k \right\rangle_2,$$

que cumple $B_0(\langle \alpha, n \rangle_2, k) = \langle H_i(\alpha, n, k), n+k \rangle_2$, que a cada par $\langle \alpha, n \rangle$ correspondiente a un ordinal y un número de asalto, le asigna el par correspondiente tras k nuevos asaltos.

Seguidamente definimos $B_1(\langle \alpha, n \rangle_2) = B_0(\langle \alpha, n \rangle_2, s(\alpha))$, que proporciona el estado de la Hidra (y el número de asalto siguiente) tras los asaltos necesarios para reducir $m(\alpha)$ en una unidad. A su vez definimos

$$B_2(\langle \alpha, n \rangle_2, 0) = \langle \alpha, n \rangle_2, \qquad B_2(\langle \alpha, n \rangle_2, j+1) = B_1(B_2(\langle \alpha, n \rangle_2, j)),$$

que aplica repetidamente la función B_1, y $B_3(\langle \alpha, n \rangle_2) = B_2(\langle \alpha, n \rangle, m(\alpha))$, que proporciona el estado de la Hidra (y el número de asaltos siguiente) tras los asaltos necesarios para reducir $h(\alpha)$ en una unidad.

Finalmente definimos $B_5(\alpha) = B_4(\langle \alpha, 1 \rangle_2, h(\alpha))$, que nos da el estado de la Hidra (y el número de asalto siguiente) tras los asaltos necesarios para reducir su altura a 0. Así, la Hidra muere tras el asalto

$$N_i(\alpha) = B_4(\alpha)_2^2 + m(B_4(\alpha)_2^2) - 1.$$

La estrategia "derecha" Hemos mencionado también la estrategia opuesta a la "estrategia izquierda", es decir, la consistente en cortar en cada asalto la cabeza de la Hidra de menor altura y con un menor número de hermanas. Es fácil convencerse de que se trata de la cabeza situada "más a la derecha", en el sentido de que es la cabeza a la que llegamos ascendiendo por la Hidra desde su raíz pasando en cada paso al nodo de menor ordinal, es decir, el correspondiente al exponente de la derecha del ordinal del nodo de partida.

Es fácil describir el ordinal $H_d(\alpha, n)$ de la hidra que resulta de cortar una cabeza en el asalto $n-1$-simo a la hidra de ordinal α:

$$H_d(\alpha, n) = \begin{cases} 0 & \text{si } \alpha = 0, \\ \beta & \text{si } \alpha = \beta + 1, \\ \beta + \omega^\eta \cdot n & \text{si } \alpha = \beta + \omega^{\eta+1}, \\ \beta + \omega^{H_d(\eta, n)} & \text{si } \alpha = \beta + \omega^\eta, \text{ con } \eta \text{ límite.} \end{cases}$$

Vemos que se trata simplemente del término n-simo $\alpha[n]$ de la sucesión fundamental de α.

En otras palabras, si Hércules emplea la estrategia derecha y la Hidra tiene ordinal α, entonces el combate es

$$\alpha \mapsto \alpha[2] \mapsto \alpha[2][3] \mapsto \alpha[2][3][4] \mapsto \cdots$$

Por ejemplo, la tabla siguiente muestra los ordinales correspondientes a los primeros asaltos del combate contra la hidra que estamos tomando de ejemplo si Hércules aplica la estrategia derecha:

n	$\alpha[n]$	n	$\alpha[n]$	n	$\alpha[n]$
	$\omega^{\omega^2+1}+\omega+1$	7	$\omega^{\omega^2}\cdot 7$	19	$\omega^{\omega^2}\cdot 6+\omega^{\omega\cdot 6+19}$
2	$\omega^{\omega^2+1}+\omega$	8	$\omega^{\omega^2}\cdot 6+\omega^{\omega\cdot 8}$	$\vdots$	
3	$\omega^{\omega^2+1}+3$	9	$\omega^{\omega^2}\cdot 6+\omega^{\omega\cdot 7+9}$	38	$\omega^{\omega^2}\cdot 6+\omega^{\omega\cdot 6}$
$\vdots$		$\vdots$		39	$\omega^{\omega^2}\cdot 6+\omega^{\omega\cdot 5+39}$
6	ω^{ω^2+1}	18	$\omega^{\omega^2}\cdot 6+\omega^{\omega\cdot 7}$	$\vdots$	

Si llamamos $L_\alpha(n)$ a la función que da el número de asaltos para derrotar a una hidra que antes del asalto $n-1$-simo tiene ordinal α, claramente se cumple que

$$L_0(n)=0, \qquad L_\alpha(n)=L_{\alpha[n]}(n+1)+1.$$

La segunda ecuación afirma que para derrotar a una hidra que antes del asalto $n-1$-simo tiene ordinal α es necesario un asalto más que para derrotar a una hidra que antes del asalto n-ésimo tiene ordinal $\alpha[n]$.

El número de asaltos necesarios para derrotar a una Hidra de ordinal α con esta estrategia es

$$N_d(\alpha)=L_\alpha(2).$$

Como el en caso de $N_i(\alpha)$, es claro que esta función es recursiva, pero veremos que no es recursiva primitiva. ■

6.7 Inducción transfinita aritmética

Ya hemos señalado que la demostración del teorema 6.23 no se apoya en ningún momento en que la fórmula $\phi(\alpha)$ sea aritmética, por lo que vale sin cambio alguno si sustituimos AP por cualquier teoría aritmética sin exigir que la fórmula ϕ sea aritmética (en AP no hay nada que exigir porque todas las fórmulas son aritméticas).

Terminamos este capítulo con un ejemplo de que puede ocurrir que una relación de orden definida sobre un conjunto de números naturales puede admitir sucesiones infinitas estrictamente decrecientes y, al mismo tiempo, satisfacer el principio de inducción transfinita para fórmulas aritméticas (lo que se traduce en que tales sucesiones infinitas no pueden ser definidas mediante fórmulas aritméticas). Más precisamente, vamos a demostrar lo siguiente:

Teorema 6.24 *Existen fórmulas $x \in A$ y $x \trianglelefteq y$ de tipo Δ_1 en $\mathcal{L}_a$ tales que en* AP *se demuestra:*

1. $\bigwedge s \in A\, s \trianglelefteq s$,
2. $\bigwedge st \in A(s \trianglelefteq t \wedge t \trianglelefteq s \rightarrow s = t)$,
3. $\bigwedge stu \in A(s \trianglelefteq t \wedge t \trianglelefteq u \rightarrow s \trianglelefteq u)$,
4. $\bigwedge st \in A(s \trianglelefteq t \vee t \trianglelefteq s)$.

así como el principio de inducción transfinita

$$\bigwedge t(\bigwedge s \lhd t\, \alpha(s) \rightarrow \alpha(t)) \rightarrow \bigwedge s \in A\, \alpha(s)$$

para toda fórmula $\alpha(s; x_1, \ldots, x_n)$ de $\mathcal{L}_a$, pero a la vez existe una sucesión de numerales $\{\sigma_n\}_{n=0}^{\infty}$ tales que en AP *se demuestra, para cada número natural n, que*

$$\sigma_n \in A \wedge \sigma_{n+1} \lhd \sigma_n.$$

Demostración: Por comodidad trabajaremos en $\mathcal{L}_{\mathrm{arp}}$. Consideramos los funtores dados por

$$N(0) = \ulcorner 0 \urcorner, \qquad N(n+1) = \ulcorner S \urcorner \frown N(n).$$

$$\begin{aligned} D(t) &= \chi[\bigvee t_1 < t\, t = \ulcorner S \urcorner t_1](D(\mathrm{Pre}_1(t)) + 1) \\ &+ \chi[\bigvee t_1 t_2 < t\, t = t_1 \ulcorner + \urcorner t_2](D(\mathrm{Pre}_1(t)) + D(\mathrm{Pre}_2(t))) \\ &+ \chi[\bigvee t_1 t_2 < t\, t = t_1 \ulcorner \cdot \urcorner t_2] D(\mathrm{Pre}_1(t)) D(\mathrm{Pre}_2(t)), \end{aligned}$$

donde Pre_1 y Pre_2 son los funtores definidos en la página 175.

Así, $N(n)$ es el numeral de $\ulcorner \mathcal{L}_a \urcorner$ que denota a n. En particular, si n es un número natural metamatemático, en ARP se demuestra que $N(\ulcorner n \urcorner) = \ulcorner \ulcorner n \urcorner \urcorner$.

Por otra parte, si t es un designador de $\ulcorner \mathcal{L}_a \urcorner$, entonces $D(t)$ es el número natural denotado por t en el modelo natural. En particular, si t es un designador metamatemático, en ARP se demuestra que $D(\ulcorner t \urcorner) = \mathbb{N}(t)$.

Consideremos ahora la función

$$\mathcal{F}(\alpha) = \begin{cases} 1 & \text{si } \alpha \text{ es una sentencia de } \mathcal{L}_a \text{ y } \mathbb{N} \vDash \alpha, \\ 0 & \text{en otro caso.} \end{cases}$$

El teorema de Tarski [LM 9.7] afirma que $\mathcal{F}$ no puede definirse en AP. Vamos a explotar este hecho para construir la relación de orden requerida.

Aunque no podamos definir $\mathcal{F}$ en AP, podemos añadir un funtor F a $\mathcal{L}_{\mathrm{arp}}$ y considerar el modelo $\mathbb{N}_{\mathcal{F}}$ de $\mathcal{L}_{\mathrm{arp}}$ más el nuevo funtor que extiende al modelo natural de $\mathcal{L}_{\mathrm{arp}}$ interpretando F como la función $\mathcal{F}$. Es claro que $N_{\mathcal{F}} \vDash \Phi$, donde

$$\Phi \equiv \bigwedge u((F(u) = 0 \vee F(u) = 1) \wedge$$

$$(F(u) = 1 \rightarrow (u \in \mathrm{Form}(\ulcorner \mathcal{L}_a \urcorner) \wedge \mathrm{VLF}(u) = 0 \wedge \cdots)) \wedge$$

$$(F(u) = 0 \wedge u \in \mathrm{Form}(\ulcorner \mathcal{L}_a \urcorner) \wedge \mathrm{VLF}(u) = 0 \rightarrow \cdots))$$

donde los primeros puntos suspensivos son la conjunción de las fórmulas siguientes:

1. $\bigvee t_1 t_2 < u(u = t_1 \ulcorner = \urcorner t_2 \rightarrow D(t_1) = D(t_2))$,
2. $\bigwedge \alpha(u = \ulcorner \neg \urcorner \alpha \rightarrow F(\alpha) = 0)$,
3. $\bigwedge \alpha\beta(u = \alpha \ulcorner \vee \urcorner \beta \rightarrow F(\alpha) = 1 \vee F(\beta) = 1)$,
4. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner \mathcal{L}_a \urcorner) \wedge u = \ulcorner \bigwedge \urcorner v\alpha \rightarrow \bigwedge m\, F(\mathtt{S}_v^{N(m)} \alpha) = 1)$,
5. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner \mathcal{L}_a \urcorner) \wedge u = \ulcorner \bigvee \urcorner v\alpha \rightarrow \bigvee n\, F(\mathtt{S}_v^{N(n)} \alpha) = 1)$.

y los segundos puntos suspensivos son la conjunción de:

1. $\bigvee t_1 t_2 < u(u = t_1 \ulcorner = \urcorner t_2 \rightarrow D(t_1) \neq D(t_2))$,
2. $\bigwedge \alpha(u = \ulcorner \neg \urcorner \alpha \rightarrow F(\alpha) = 1)$,
3. $\bigwedge \alpha\beta(u = \alpha \ulcorner \vee \urcorner \beta \rightarrow F(\alpha) = 0 \wedge F(\beta) = 0)$,
4. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner \mathcal{L}_a \urcorner) \wedge u = \ulcorner \bigwedge \urcorner v\alpha \rightarrow \bigvee n\, F(\mathtt{S}_v^{N(n)} \alpha) = 0)$,
5. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner \mathcal{L}_a \urcorner) \wedge u = \ulcorner \bigvee \urcorner v\alpha \rightarrow \bigwedge m\, F(\mathtt{S}_v^{N(m)} \alpha) = 0)$.

Más aún, la sentencia Φ determina completamente a F, en el sentido de que si M es un modelo que extiende al modelo natural de $\mathcal{L}_{\mathrm{arp}}$ y $M \vDash \Phi$, entonces $M(F)$ es necesariamente la función $\mathcal{F}$.

Observemos también que si α es cualquier sentencia de $\mathcal{L}_a$, una simple inducción sobre la longitud de α prueba que

$$\underset{\mathrm{ARP}}{\vdash} (\Phi \rightarrow (F(\ulcorner \alpha \urcorner) \leftrightarrow \alpha)).$$

El teorema de Tarski implica que la presencia del funtor F en este resultado es esencial. No obstante, vamos a ver que "casi" podemos eliminar F de Φ. Para ello empezamos reescribiéndola de modo que F intervenga de la forma más simple posible. La sentencia siguiente es claramente equivalente a Φ:

$$\begin{gathered}\Phi' \equiv \bigwedge u_0 u_1 u_2 u_3 v_0 v_1 v_2 v_3 v m \bigvee u_4 v_4 n(u_0 = F(v_0) \wedge \cdots \wedge u_4 = F(v_4) \wedge \\ v_3 = \mathtt{S}_v^{N(m)} u_1 \wedge v_4 = \mathtt{S}_v^{N(n)} u_1 \rightarrow ((u_0 = 0 \vee u_0 = 1) \wedge \\ (u_0 = 1 \rightarrow v_0 \in \mathrm{Form}(\ulcorner \mathcal{L}_a \urcorner) \wedge \mathrm{VLF}(v_0) = 0 \wedge \cdots) \wedge \\ (u_0 = 0 \wedge v_0 \in \mathrm{Form}(\ulcorner \mathcal{L}_a \urcorner) \wedge \mathrm{VLF}(v_0) = 0 \rightarrow \cdots)))\end{gathered}$$

donde los primeros puntos suspensivos son la conjunción de las fórmulas siguientes:

1. $\bigvee t_1 t_2 < v_0(u = t_1 \ulcorner = \urcorner t_2 \rightarrow V(t_1) = V(t_2))$,
2. $v_0 = \ulcorner \neg \urcorner v_1 \rightarrow u_1 = 0$,

3. $v_0 = v_1 \ulcorner\vee\urcorner v_2 \rightarrow u_1 = 1 \vee u_2 = 1)$,
4. $v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge v_0 = \ulcorner\bigwedge\urcorner vv_1 \rightarrow u_3 = 1$,
5. $v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge v_0 = \ulcorner\bigvee\urcorner vv_1 \rightarrow u_4 = 1$.

y los segundos son la conjunción de las fórmulas siguientes:

1. $\bigvee t_1 t_2 < v_0 (u = t_1 \ulcorner=\urcorner t_2 \rightarrow V(t_1) \neq V(t_2))$,
2. $v_0 = \ulcorner\neg\urcorner v_1 \rightarrow u_1 = 1$,
3. $v_0 = v_1 \ulcorner\vee\urcorner v_2 \rightarrow u_1 = 0 \wedge u_2 = 0)$,
4. $v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge v_0 = \ulcorner\bigwedge\urcorner vv_1 \rightarrow u_4 = 0$,
5. $v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge v_0 = \ulcorner\bigvee\urcorner vv_1 \rightarrow u_3 = 0$.

A su vez, podemos contraer los cuantificadores, de modo que Φ' es equivalente a $\bigwedge u \bigvee v\, \Psi(u,v)$, donde

$$\Psi(u,v) \equiv \ell(u) = 10 \wedge \ell(v) = 3 \wedge u_0 = F(u_4) \wedge u_1 = F(u_5) \wedge u_2 = F(u_6) \wedge$$

$$u_3 = F(u_7) \wedge v_0 = F(v_1) \rightarrow \phi(u,v),$$

donde ϕ es una fórmula Δ_0 de $\mathcal{L}_{\mathrm{arp}}$. Tenemos que $\mathbb{N}_{\mathcal{F}} \vDash \bigwedge u \bigvee v\, \Psi(u,v)$, luego podemos definir la función

$$\mathcal{G}(n) = \mu m\, \mathbb{N}_{\mathcal{F}} \vDash \Psi(n,m).$$

Si añadimos otro funtor G a $\mathcal{L}_{\mathrm{arp}}$ y consideramos el modelo $\mathbb{N}_{\mathcal{F},\mathcal{G}}$ en el que F y G se interpretan respectivamente como $\mathcal{F}$ y $\mathcal{G}$, tenemos que

$$\mathbb{N}_{\mathcal{F},\mathcal{G}} \vDash \bigwedge uv\, \Psi'(u,v),$$

donde

$$\Psi'(u,v) \equiv \ell(u) = 10 \wedge \ell(v) = 3 \wedge v = G(u) \wedge$$

$$u_0 = F(u_4) \wedge u_1 = F(u_5) \wedge u_2 = F(u_6) \wedge u_3 = F(u_7) \wedge v_0 = F(v_1) \rightarrow \phi(u,v)$$

y, más aún, si un modelo M extiende al modelo natural de $\mathcal{L}_{\mathrm{arp}}$ y cumple

$$M \vDash \bigwedge uv\, \Psi'(u,v),$$

necesariamente $M(F)$ es $\mathcal{F}$. Igualmente, para toda sentencia α de $\mathcal{L}_a$,

$$\underset{\mathrm{ARP}}{\vdash} (\bigwedge uv\, \Psi'(u,v) \rightarrow (F(\ulcorner\alpha\urcorner) \leftrightarrow \alpha)).$$

Ahora consideramos la función

$$\mathcal{H}(n) = \begin{cases} \mathcal{F}(k) & \text{si } n = 2k, \\ \mathcal{G}(k) & \text{si } n = 2k+1, \end{cases}$$

así como el lenguaje que resulta de añadir a $\mathcal{L}_{\mathrm{arp}}$ un funtor H y el modelo $\mathbb{N}_{\mathcal{H}}$ en el que H se interpreta como $\mathcal{H}$. Entonces $\mathbb{N}_{\mathcal{H}} \vDash \bigwedge uv\, \Psi''(u,v)$, donde

$$\Psi''(u,v) \equiv \ell(u) = 10 \land \ell(v) = 3 \land v = H(2u+1) \land u_0 = H(2u_4) \land$$

$$u_1 = H(2u_5) \land u_2 = H(2u_6) \land u_3 = H(2u_7) \land v_0 = H(2v_1) \to \phi(u,v),$$

y si un modelo M que extiende al modelo natural de $\mathcal{L}_{\mathrm{arp}}$ cumple

$$M \vDash \bigwedge uv\, \Psi''(u,v),$$

entonces la función $M(H)(2k)$ es $\mathcal{F}$. Además, para toda sentencia α de $\mathcal{L}_a$, se cumple que

$$\underset{\mathrm{ARP}}{\vdash} (\bigwedge uv\, \Psi''(u,v) \to (H(2\ulcorner\alpha\urcorner) \leftrightarrow \alpha)).$$

Nuevamente podemos contraer los cuantificadores definiendo

$$\Psi'''(u) \equiv \ell(u) = 16 \land \ell(u_{10}) = 3 \land u_{10} = 2u|_{10} + 1 \land u_{11} = 2u_4 \land$$

$$u_{12} = 2u_5 \land u_{13} = 2u_6 \land u_{14} = 2u_7 \land u_{15} = 2(u_{10})_1 \land u_0 = H(u_{11}) \land$$

$$u_1 = H(u_{12}) \land u_2 = H(u_{13}) \land u_3 = H(u_{14}) \land (u_{10})_0 = H(u_{15}) \to \phi'(u),$$

donde $\phi'(u) \equiv \phi(u|_{10}, u_{10})$ es una fórmula Δ_0 de $\mathcal{L}_{\mathrm{arp}}$. Claramente, la sentencia $\bigwedge uv\, \Psi''(u,v)$ es equivalente a $\bigwedge u\, \Psi'''(u)$.

Ahora observamos que en $\Psi'''(u)$ el funtor H actúa únicamente sobre términos $u_i < u$, luego $\Psi'''(u)$ depende únicamente de la restricción de H a u. Esto nos lleva a definir

$$s \in A \equiv \bigwedge u \leq \ell(s)(\ell(u) = 16 \land \ell(u_{10}) = 3 \land u_{10} = 2u|_{10} + 1 \land$$

$$u_{11} = 2u_4 \land u_{12} = 2u_5 \land u_{13} = 2u_6 \land u_{14} = 2u_7 \land u_{15} = 2(u_{10})_1 \land$$

$$u_0 = s(u_{11}) \land u_1 = s(u_{12}) \land u_2 = s(u_{13}) \land u_3 = s(u_{14}) \land$$

$$(u_{10})_0 = s(u_{15}) \to \phi'(u)),$$

de modo que $s \in A$ es una fórmula Δ_0 de $\mathcal{L}_{\mathrm{arp}}$ (sin funtores añadidos) que obviamente cumple

$$\bigwedge st(s \sqsubseteq t \land t \in A \to s \in A).$$

Ahora $\bigwedge u\, \Psi'''(u)$ es equivalente a

$$\bigwedge s(\bigwedge i < \ell(s)\, s_i = H(i) \to s \in A).$$

En particular, si llamamos σ_n al numeral correspondiente a la sucesión

$$\langle \mathcal{H}(0), \ldots, \mathcal{H}(n-1) \rangle,$$

tenemos que[11]

$$\underset{\mathrm{ARP}}{\vdash} (\sigma_n \in A \land \sigma_n \sqsubset \sigma_{n+1}).$$

[11]En principio tenemos que $\sigma_n \in A \land \sigma_n \sqsubset \sigma_{n+1}$ es una sentencia verdadera en el modelo natural de $\mathcal{L}_{\mathrm{arp}}$, pero es una sentencia Δ_0, luego es demostrable por el teorema 5.6.

Definimos[12]

$$s \trianglelefteq t \equiv s \in A \land t \in A \land (t \sqsubseteq s \lor \bigvee i < \ell(s)(i < \ell(t) \land s|_i = t_i \land s(i) < t(i))).$$

Notemos que tanto $s \in A$ como $s \trianglelefteq t$ son fórmulas Δ_0 en $\mathcal{L}_{\mathrm{arp}}$, luego son equivalentes en $\mathrm{I}\Sigma_1$ a fórmulas Δ_1 en $\mathcal{L}_a$.

Es fácil probar en ARP que $\trianglelefteq$ es una relación de orden total, es decir, las cuatro sentencias enumeradas en el enunciado de 6.24. Esto no depende de la definición de A. Como obviamente $t \sqsubset s \to s \triangleleft t$, los numerales σ_n que tenemos definidos cumplen

$$\underset{\mathrm{ARP}}{\vdash}(\sigma_n \in A \land \sigma_{n+1} \triangleleft \sigma_n).$$

Finalmente vamos a probar en AP el principio de inducción transfinita.

Para ello suponemos que $\bigwedge t \in A(\bigwedge s \triangleleft t\, \alpha(s) \to \alpha(t))$, pero que existe un $s \in A$ tal que $\neg\alpha(s)$. Notemos que entonces,

$$\bigwedge t \in A(\neg\alpha(t) \to \bigvee s \in A(s \triangleleft t \land \neg\alpha(s))).$$

Recordemos que en AP podemos demostrar que si $\bigvee u, \phi(u)$ existe un (único) mínimo número natural que cumple $\phi(u)$ (teorema [LM 5.26]), y lo podemos representar por $\mu u\, \phi(u)$. En particular podemos definir

$$s_0 \equiv \mu s\, (s \in A \land \neg\alpha(s)), \quad s_{n+1} \equiv \mu s(s \in A \land \neg\alpha(s) \land s \triangleleft s_n),$$

y una simple inducción prueba que

$$\bigwedge n(s_n \in A \land \neg\alpha(s_n) \land s_{n+1} \triangleleft s_n).$$

Ahora distinguimos dos casos:

1) $\bigwedge m \bigvee n \geq m\, s_n \not\sqsubseteq s_{n+1}$. Entonces llamamos

$$n_0 = \mu n\, s_n \not\sqsubseteq s_{n+1}, \qquad n_{k+1} = \mu n(n \geq n_k + 1 \land s_n \not\sqsubseteq s_{n+1}).$$

Así $s_{n_k} \not\sqsubseteq s_{n_k+1} \sqsubseteq s_{n_{k+1}}$, luego $s_{n_k} \not\sqsubseteq s_{n_{k+1}}$ y llamando $s'_k \equiv s_{n_k}$ tenemos que

$$\bigwedge n(s'_n \in A \land s'_{n+1} \triangleleft s'_n \land s'_n \not\sqsubseteq s'_{n+1}).$$

Por lo tanto, para cada n existe un único i_n tal que

$$i_n < \ell(s'_n) \land i_n < \ell(s'_{n+1}) \land s'_n|_{i_n} = s'_{n+1}|_{i_n} \land s'_{n+1}(i_n) < s'_n(i_n).$$

Veamos que no puede existir un k tal que $\bigwedge m \bigvee n \geq m\, i_n \leq k$. En tal caso tomamos el mínimo posible, con lo que existe un r tal que $\bigwedge m \geq r\, i_m \geq k$, luego, más concretamente, $\bigwedge m \geq r \bigvee n \geq m\, i_n = k$. Podemos definir

$$n_0 = \mu n(n \geq r \land i_n = k), \quad n_{j+1} = \mu n(n \geq n_j + 1 \land i_n = k),$$

con lo que $s'_{n_{j+1}}(k) = s'_{n_j+1}(k) < s'_{n_j}(k)$, con lo que tendríamos definida una sucesión decreciente de números naturales, lo cual es imposible.

[12] La situación de fondo es que la fórmula $s \in A$ define un subárbol de $2^{<\omega}$ y la relación $s \trianglelefteq t$ que estamos definiendo no es sino el orden de Brower-Kleene asociado [TD 4.20].

Así pues, $\bigwedge k\bigvee m\bigwedge n\geq m\, i_n>k$, lo que nos permite definir

$$n_0=\mu m\bigwedge n\geq m\ i_n>i_0,\qquad n_{j+1}=\mu m\bigwedge n\geq m\ i_n>i_{n_j}.$$

Entonces, si llamamos $t_j\equiv s'_{n_j}|_{i_{n_j}}$, tenemos que $t_j\in A$ y

$$t_j=s'_{n_j}|_{i_{n_j}}=s'_{n_{j+1}}|_{i_{n_j}}\sqsubset s'_{n_{j+1}}|_{i_{n_{j+1}}}=t_{j+1}.$$

2) $\bigvee m\bigwedge n\geq m\, s_n\sqsubset s_{n+1}$. En tal caso definimos $t_n\equiv s_{m+n}$, y asi se cumple igualmente que

$$\bigwedge n(t_n\in A\wedge t_n\sqsubset t_{n+1}).$$

En ambos casos tenemos que

$$\bigwedge n\overset{1}{\bigvee} k\bigvee m(n<\ell(t_m)\wedge t_m(n)=k),$$

por lo que podemos definir

$$H(n)=k\equiv\bigvee m(n<\ell(t_m)\wedge t_m(n)=k),$$

Así, trivialmente se cumple

$$\bigwedge s(\bigwedge i<\ell(s)\, s_i=H(i)\rightarrow s\in A),$$

Es claro entonces que se cumple $\bigwedge u\,\Psi'''(u)$, pero interpretando ahora $\Psi'''(u)$ como una fórmula de $\mathcal{L}_{\mathrm{arp}}$, donde H ya no es un funtor añadido, sino el término que acabamos de definir. A su vez, esto implica que si definimos $F(n)=H(2n)$ y $V(n)\equiv F(2n)=1$, en AP podemos demostrar:

1. Si t_1 y t_2 son designadores de $\ulcorner\mathcal{L}_a\urcorner$, entonces
$$V(t_1\ulcorner=\urcorner t_2)\leftrightarrow V(t_1)=V(t_2).$$

2. Si α es una sentencia de $\ulcorner\mathcal{L}_a\urcorner$, entonces
$$V(\ulcorner\neg\urcorner\alpha)\leftrightarrow\neg V(\alpha).$$

3. Si α y β son sentencias de $\ulcorner\mathcal{L}_a\urcorner$, entonces
$$V(\alpha\ulcorner\vee\urcorner\beta)\leftrightarrow V(\alpha)\vee V(\beta).$$

4. Si $\ulcorner\bigwedge\urcorner v\,\alpha$ es una sentencia de $\ulcorner\mathcal{L}_a\urcorner$, entonces
$$V(\ulcorner\bigwedge\urcorner v\,\alpha)\leftrightarrow\bigwedge n\,V(\mathsf{S}_v^{N(n)}\alpha)).$$

5. Si $\ulcorner\bigvee\urcorner v\,\alpha$ es una sentencia de $\ulcorner\mathcal{L}_a\urcorner$, entonces
$$V(\ulcorner\bigvee\urcorner v\,\alpha)\leftrightarrow\bigvee m\,V(\mathsf{S}_v^{N(m)}\alpha)).$$

De aquí se sigue que si α es una sentencia de $\mathcal{L}_a$, entonces en AP podemos demostrar

$$V(\ulcorner\alpha\urcorner) \leftrightarrow \alpha.$$

Basta razonar por inducción sobre la longitud de α. Pero el teorema de Tarski [LM 9.7 d] afirma que esto es imposible. Más concretamente, en su demostración se ve que de aquí se deduce una contradicción, que en este caso no nos permite concluir que AP sea contradictorio, sino que meramente termina la demostración por reducción al absurdo que habíamos planteado. ■

Observemos que en ARP se prueba que A tiene que tener un mínimo elemento respecto de la relación $\trianglelefteq$, pues en caso contrario podríamos definir

$$s_0 \equiv \sigma_0, \quad s_{n+1} \equiv \mu s(s \in A \land s \lhd s_n),$$

y el mismo razonamiento empleado en la prueba del principio de inducción transfinita para $\trianglelefteq$ nos llevaría a una contradicción.

Similarmente, todo $s \in A$ tiene un siguiente, pues si s_0 no lo tuviera podríamos definir

$$s_{n+1} \equiv \mu s(s \in A \land s_0 \lhd s \lhd s_n),$$

y nuevamente llegaríamos a una contradicción. Si llamamos $s' \in A$ al siguiente de $s \in A$ y llamamos $\hat{0} \in A$ al mínimo de A, podemos definir

$$\widehat{n+1} = \hat{n}',$$

y de este modo podemos identificar los números naturales con los primeros elementos de A:

$$\hat{0} \lhd \hat{1} \lhd \hat{2} \lhd \hat{3} \lhd \cdots$$

Así, A con el orden $\trianglelefteq$ podría parecer una formalización aritmética de un cierto segmento de los ordinales conjuntistas análoga a la que hemos presentado para los ordinales menores que ϵ_0, pero en realidad no es así, ya que $\trianglelefteq$ no se interpreta como un buen orden en el modelo natural.

Capítulo VII

La consistencia de la aritmética

En este capítulo expondremos la demostración de Gentzen de la consistencia de la aritmética de Peano. En los términos introducidos en el capítulo anterior, lo que vamos a probar es que si la inducción transfinita es válida hasta ϵ_0, entonces AP es consistente. Nos ocuparemos de ello en la primera sección, mientras que en la segunda veremos que el argumento puede simplificarse bastante para probar la consistencia de $\mathrm{I}\Sigma_1$ a partir de la validez de la inducción transfinita hasta ω^ω. En la tercera sección combinaremos las ideas de ambas pruebas para obtener otros resultados relacionados.

7.1 La consistencia de AP

Tal y como hemos explicado en el capítulo anterior, la prueba de Gentzen consiste esencialmente en asignar un ordinal a cada demostración en AP y probar que si existe una demostración del secuente vacío, es posible transformarla en otra de ordinal estrictamente menor.

El ordinal de una demostración Para definir el ordinal de una demostración necesitamos introducir algunos conceptos previos:

Definición 7.1 Definimos el *grado* de una fórmula como el número de signos lógicos que contiene (entre conectores y cuantificadores). El *grado* de un corte es el grado de la fórmula de corte. El *grado* de una inducción es el grado de la fórmula de inducción. La *altura* $h(S; D)$ de un secuente S en una demostración D es el máximo de los grados de los cortes e inducciones que hay bajo[1] S. Si no hay ninguno, la altura es 0. En particular, el secuente final de una demostración siempre tiene altura 0.

[1]Aquí hay que entender que una regla de inferencia se considera que está por debajo de su secuente superior y por encima de su secuente inferior.

Notemos que si una regla de inferencia tiene dos secuentes superiores, ambos tienen necesariamente la misma altura, pues ambos tienen exactamente las mismas reglas de inferencia por debajo. Además, la altura de un secuente es obviamente mayor o igual que la de todos los secuentes situados bajo él.

A cada secuente S en una demostración D en AP le asociamos un ordinal $o(S; D)$ según el criterio siguiente:

1. Si S es un secuente inicial de D, entonces $o(S; D) = 1$.

2. Si S es el secuente inferior de una regla de debilitación con secuente superior S_1, entonces $o(S; D) = o(S_1; D)$.

3. Si S es el secuente inferior de una regla izquierda del disyuntor con secuentes superiores S_1 y S_2, entonces $o(S; D) = o(S_1; D)\#o(S_2; D)$.

4. Si S es el secuente inferior de una regla de inferencia lógica con secuente superior S_1, entonces $o(S; D) = o(S_1; D) + 1$.

5. Si S es el secuente inferior de una regla de corte con secuentes superiores S_1 y S_2, entonces $o(S; D) = \omega_{h_1 - h_0}(\mu_1\#\mu_2)$, donde
$$h_1 = h(S_1; D) = h(S_2; D), \quad h_0 = h(S; D), \quad \mu_i = o(S_i; D).$$

6. Si S es el secuente inferior de una inducción con secuente superior S', entonces $o(S; D) = \omega_{h_1 - h_0 + 1}(\eta + 1)$, donde
$$h_1 = h(S'; D), \quad h_0 = h(S; D), \quad o(S'; D) = \omega^\eta + \cdots$$

El ordinal $o(D)$ de una demostración D es el ordinal de su secuente final.

Ejemplo La demostración del ejemplo de la página 68 tiene ordinal $\omega^{\omega^{\omega^2+5}}$. La figura muestra los ordinales de los últimos secuentes:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{1 \qquad 2}{3}}{3}}{4}}{5} \qquad \dfrac{\dfrac{\dfrac{\dfrac{6}{7} \quad \dfrac{10}{11}}{17}}{18}}{\omega^2}}{\omega^{\omega^{\omega^2+5}}}$$

■

El teorema siguiente lo usaremos a menudo:

Teorema 7.2 *Sea D una demostración que contenga un secuente S_1 de modo que no haya ninguna inducción bajo S_1. Sea D_1 la subdemostración de D formada por los secuentes situados por encima de S_1 y sea D_1' otra demostración de S_1 tal que $o(S_1; D_1') < o(S_1; D)$. Sea D' la demostración que resulta de reemplazar D_1 por D_1' en D. Entonces $o(D') < o(D)$.*

Demostración: Consideremos un hilo de D que pase por S_1 y vamos a probar que cada secuente S de dicho hilo situado por debajo de S_1 cumple $o(S;D') < o(S;D)$. Luego, basta aplicar esto al secuente final de ambas pruebas.

Por hipótesis se cumple cuando $S = S_1$, y basta probar que si un secuente S' cumple la desigualdad, lo mismo sucede con el secuente S que está inmediatamente por debajo en el hilo. Esto se comprueba regla a regla.

Si la regla que pasa de S' a S es de debilitación, tenemos que

$$o(S;D') = o(S';D') < o(S';D) = o(S;D).$$

Si se trata de la regla izquierda del disyuntor y sus secuentes superiores son S' y S'', entonces $o(S'';D') = o(S'';D)$ y

$$o(S;D') = o(S';D')\#o(S'';D') < o(S';D)\#o(S'';D) = o(S;D).$$

Si se trata de una regla de inferencia lógica con un único secuente superior, entonces

$$o(S;D') = o(S';D') + 1 < o(S';D) + 1 = o(S;D).$$

Si la inferencia es un corte, entonces las alturas h_0 y h_1 son las mismas en D y en D', luego, llamando S'' al segundo secuente superior, tenemos que $o(S'';D') = o(S'';D)$ y

$$\begin{aligned} o(S;D') &= \omega_{h_1-h_0}(o(S';D')\#o(S'';D')) \\ &< \omega_{h_1-h_0}(o(S';D)\#o(S'';D)) = o(S;D). \end{aligned}$$

Si la inferencia fuera una inducción la conclusión ya no sería cierta, pero por hipótesis estamos excluyendo este caso. ■

La parte final de una demostración Nuestro objetivo es demostrar que si existe una demostración D del secuente vacío en AP, a partir de ella podemos construir otra de ordinal menor. Las manipulaciones que le haremos a D para obtener esta nueva demostración afectarán únicamente a lo que llamaremos su parte final, que definimos a continuación.

Recordemos que una *fibra* en una demostración es una sucesión de fórmulas que empieza en una *fórmula inicial,* es decir, en una fórmula que forma parte de un secuente inicial (un axioma) o bien es la fórmula principal de una regla de debilitación, y termina en una *fórmula final,* es decir, en una fórmula del secuente final de la demostración o bien en una fórmula de corte. En el primer caso diremos que la fibra es *explícita,* mientras que en el segundo caso es *implícita.* Notemos que en una demostración del secuente vacío todas las fibras son implícitas.

Una fórmula de una demostración es *explícita* o *implícita* según lo sean las fibras que la contienen.

Una aplicación de una regla de inferencia lógica es *explícita* o *implícita* según lo sea su fórmula principal.

Definición 7.3 La *parte final* de una demostración está formada por los secuentes que no tienen por debajo ninguna regla de inferencia lógica implícita.

Recordemos que toda regla de inferencia está por debajo de sus secuentes superiores y por encima de su secuente inferior. Por consiguiente, si una regla de inferencia lógica es implícita, pero no hay ninguna otra regla lógica implícita bajo ella, entonces su secuente inferior está en la parte final de la demostración, pero su secuente o sus secuentes superiores no lo están. Diremos entonces que la regla es *fronteriza.* Cuando hablemos de las reglas de inferencia de la parte final de una demostración, no incluiremos entre ellas a las reglas fronterizas.

Un corte en la parte final de una demostración en AP es *adecuado* si las dos fórmulas de corte tienen un ascendiente directo que es la fórmula principal de una regla fronteriza.

Ejemplo En la demostración del ejemplo de la página 68 las dos últimas aplicaciones de la regla izquierda del particularizador son implícitas, pues los hilos de sus fórmulas principales terminan en el último corte. Por lo tanto, la parte final de la demostración está formada por los cuatro secuentes situados bajo ellas.

$$\dfrac{\dfrac{\Rightarrow 0 = 2\cdot 0 \vee 0 = 2\cdot 0+1}{\Rightarrow \bigvee u(0 = 2u \vee 0 = 2u+1)} \qquad \dfrac{\dfrac{x = 2y \vee x = 2y+1 \Rightarrow \phi(x')}{\bigvee u(x = 2u \vee x = 2u+1) \Rightarrow \phi(x')}}{\bigvee u(0 = 2u \vee 0 = 2u+1) \Rightarrow \phi(x)}}{\Rightarrow \bigvee u(x = 2u \vee x = 2u+1)}$$

■

Vamos a necesitar el teorema siguiente que garantiza la existencia de cortes adecuados en determinadas circunstancias:

Teorema 7.4 *Supongamos que una demostración en* AP *no coincide con su parte final, que los secuentes iniciales de dicha parte final no contienen signos lógicos y que en ella no hay más reglas de inferencia que cortes. Entonces la parte final contiene un corte adecuado.*

Demostración: Como la demostración no coincide con su parte final, tiene alguna regla de inferencia lógica (implícita) fronteriza, lo que significa que su fórmula principal, que tiene signos lógicos, tiene que eliminarse con un corte situado bajo ella, luego en la parte final de la demostración, y dicho corte será un corte esencial. Vamos a probar el teorema por inducción sobre el número de cortes esenciales que contiene la parte final de la demostración.

Consideremos un corte esencial que no tenga ninguno más por debajo. Si es adecuado, ya tenemos la conclusión. En caso contrario será de la forma

$$\dfrac{\begin{matrix} D_1 \\ \vdots \\ \Gamma \Rightarrow \Delta,\, \alpha \end{matrix} \qquad \begin{matrix} D_2 \\ \vdots \\ \alpha,\, \Gamma' \Rightarrow \Delta' \end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

donde una de las dos fórmulas de corte (pongamos que la de la izquierda) no desciende de la fórmula principal de una regla fronteriza.

Entonces D_1 contiene una regla fronteriza, pues, en caso contrario, como en la parte final de D no hay debilitaciones, α tendría que descender de un secuente inicial de la parte final de D y, como ella no hay más que cortes, dicho ascendente sería idéntico a α y por hipótesis no tendría signos lógicos, lo que contradice que el corte sea esencial.

Ahora observamos que una regla de inferencia lógica fronteriza contenida en D_1 es implícita en D_1 si y sólo si lo es en D.

Obviamente, si es implícita en D_1 es que su fórmula principal se elimina en un corte en D_1, luego se elimina en un corte en D, luego la regla es implícita para D. Recíprocamente, si la regla es implícita en D, su fórmula principal (que tiene signos lógicos y no es α) se elimina en un corte de D, pero el corte tiene que estar en D_1, porque el corte que elimina a α no tiene por debajo otros cortes esenciales. Por lo tanto, la regla es implícita en D_1.

Veamos ahora que una regla lógica contenida en D_1 es fronteriza para D_1 si y sólo si lo es para D.

En efecto, si es fronteriza para D, entonces es implícita para D, y también, según acabamos de ver, para D_1, y de hecho es fronteriza para D_1, pues cualquier regla de inferencia lógica contenida en D_1 por debajo de ella que sea implícita para D_1 es también implícita para D, lo que contradice que la regla inicial sea fronteriza para D.

Recíprocamente, si la regla es fronteriza para D_1, es implícita para D_1, luego para D, y tiene que ser fronteriza para D, pues si tuviera por debajo otra regla lógica implícita para D, no puede estar en D_1, ya que entonces sería implícita para D_1 y contradiría que la regla dada es fronteriza para D_1, luego tiene que estar por debajo del secuente $\Gamma \Rightarrow \Delta, \alpha$, y esto contradiría que el corte esté en la parte final de D.

Así pues, como D_1 tiene reglas fronterizas, no coincide con su parte final. De hecho, la parte final de D_1 está formada por los secuentes de la parte final de D contenidos en D_1. Esto nos permite aplicar la hipótesis de inducción a D_1, que tiene al menos un corte sustancial menos que D. Por lo tanto, D_1 contiene un corte adecuado. Esto significa que las fórmulas de corte descienden de fórmulas principales de reglas fronterizas de D_1, que también son fronterizas en D, luego el corte es adecuado para D. ■

Demostraciones con sentencias $\boldsymbol{\Delta_0}$ Necesitamos descartar que una hipotética demostración del secuente vacío sea excesivamente simple:

Teorema 7.5 *No existen demostraciones del secuente vacío en* AP *formadas únicamente por sentencias* Δ_0.

Demostración: Observemos que una demostración formada únicamente por sentencias Δ_0 no puede tener aplicaciones de la regla de inducción, pues las fórmulas auxiliares no pueden ser sentencias, ya que tienen libre la variable propia.

En 3.8 hemos visto que la verdad o falsedad de una sentencia Δ_0 en el modelo natural de AP se puede definir en términos puramente finitistas, de modo que existe un algoritmo para determinar si una sentencia Δ_0 es verdadera o falsa en un número finito de pasos.

Todos los axiomas de AP son fórmulas Δ_0, y es fácil comprobar que todos los formados únicamente por sentencias son verdaderos, así como que el secuente inferior de cualquier regla de inferencia en la que sólo intervengan sentencias Δ_0 (lo cual descarta la inducción) es verdadero si lo son sus secuentes superiores.

Esto implica que, en una demostración formada únicamente por sentencias Δ_0 todos los secuentes tienen que ser verdaderos, por lo que el secuente final no puede ser vacío. ■

Observaciones En realidad, para la prueba que vamos a ver en esta sección es suficiente un resultado mucho más débil. Nos bastará saber que no puede haber demostraciones del secuente vacío formadas únicamente por sentencias atómicas. La prueba se simplifica sustancialmente, pues en una demostración formada por sentencias atómicas no puede haber reglas lógicas ni de inducción, sólo secuentes iniciales y reglas de debilitación y de corte.

El argumento del teorema anterior es esencialmente el argumento típico por el que una teoría que tiene un modelo es consistente, el mismo por el que podríamos decir que AP es consistente porque admite el modelo natural formado por los números naturales con las operaciones aritméticas usuales, pero la diferencia es que al restringirnos a secuentes formados por sentencias Δ_0 el concepto de "secuente verdadero" se vuelve estrictamente finitista, al igual que el argumento que hemos empleado. ■

Ahora ya podemos probar el resultado principal:

Teorema 7.6 *Si D es una demostración del secuente vacío en* AP, *existe otra D' tal que $o(D') < o(D)$.*

Demostración: Observemos que en una demostración del secuente vacío todas las reglas de inferencia son implícitas, por lo que la parte final de D está formada simplemente por los secuentes que no tienen por debajo ninguna regla de inferencia lógica. En particular, la parte final no contiene reglas de inferencia lógicas.

El teorema 3.13 nos permite transformar D en una demostración regular sin alterar su ordinal. Alternativamente, podemos suponer que D es regular.

• Si en la parte final de D aparece una variable libre que no es la variable propia de ninguna regla de inferencia, por el teorema 3.11 podemos sustituirla por la constante 0, y obtenemos así una demostración (también del secuente vacío) con el mismo ordinal.

Repitiendo este proceso un número finito de veces podemos suponer que en la parte final de D no hay ninguna variable libre que no esté usada como variable propia de una (única) regla de inferencia.

• Supongamos que la parte final de D contiene una regla de inducción y consideremos una que no tenga ninguna otra por debajo. Pongamos que es

$$\frac{\alpha(y),\,\Gamma \overset{\mu}{\Rightarrow} \Delta,\,\alpha(y') \quad (h_1)}{\alpha(0),\,\Gamma \Rightarrow \Delta,\,\alpha(t) \quad (h_0)}.$$

En lo sucesivo, una letra sobre la flecha de un secuente denotará su ordinal en la demostración en la que aparece. En este caso, estamos diciendo que el secuente superior S tiene ordinal $o(S;D) = \mu = \omega^\eta + \cdots$ y el secuente inferior S_0 tiene ordinal $o(S_0) = \omega_{h_1-h_0+1}(\eta+1)$ y h_1, h_0 son las alturas de S y S_0, respectivamente.

Puesto que debajo de esta regla no hay más inducciones ni tampoco reglas de inferencia lógicas, no puede haber variables libres (ya que toda variable libre es la variable propia de una inducción o de una regla de un cuantificador), luego en particular el término t no tiene variables libres.

Sea $m = d(t)$, de modo que el teorema 3.7 nos da una demostración de $\Rightarrow \bar{m} = t$ y a su vez de otra demostración E del secuente $\alpha(\bar{m}) \overset{q}{\Rightarrow} \alpha(t)$ en la que no se usan inducciones ni cortes esenciales. Como en un corte inesencial la altura de los secuentes superiores coincide con la del secuente inferior, se comprueba inmediatamente que $q = o(E)$ es un número natural.

Si llamamos D_0 a la subdemostración de D formada por los secuentes situados sobre el secuente superior S, sucede que la variable y no se usa como variable propia en D_0 (pues por la regularidad de D sólo se usa como variable propia una vez, y es en la inferencia S/S_0), luego el teorema 3.11 nos da que, para todo número natural n, al sustituir y por $\bar{n}$ en D_0 obtenemos una demostración $D_0(\bar{n})$ del secuente

$$\alpha(\bar{n}), \Gamma \Rightarrow \Delta,\, \alpha(\overline{n+1})$$

(notemos que y no puede aparecer en Γ o en Δ). Ahora encadenamos así las demostraciones $D_0(\bar{n})$:

$$\dfrac{\dfrac{\begin{array}{c}D_0(\bar{0})\\ \vdots\\ \alpha(\bar{0}),\,\Gamma \overset{\mu}{\Rightarrow} \Delta,\,\alpha(\bar{1})\end{array} \quad \begin{array}{c}D_0(\bar{1})\\ \vdots\\ \alpha(\bar{1}),\,\Gamma \overset{\mu}{\Rightarrow} \Delta,\,\alpha(\bar{2})\end{array}}{\alpha(\bar{0}),\,\Gamma \Rightarrow \Delta,\,\alpha(\bar{2})} \quad \begin{array}{c}D_0(\bar{2})\\ \vdots\\ \alpha(\bar{2}),\,\Gamma \overset{\mu}{\Rightarrow} \Delta,\,\alpha(\bar{3})\end{array}}{\alpha(\bar{0}),\,\Gamma \Rightarrow \Delta,\,\alpha(\bar{3})}$$

hasta llegar a una demostración del secuente

$$\alpha(\bar{0}), \Gamma \Rightarrow \Delta,\, \alpha(\bar{m})$$

y, a su vez, combinando la prueba con E, obtenemos:

$$\dfrac{\begin{array}{c}\vdots\\ \alpha(\bar{0}),\,\Gamma \Rightarrow \Delta,\,\alpha(\bar{m})\end{array} \qquad \begin{array}{c}E\\ \vdots\\ \alpha(\bar{m}) \Rightarrow \alpha(t)\end{array}}{\alpha(0),\,\Gamma \Rightarrow \Delta,\,\alpha(t)}$$

En suma, obtenemos una demostración alternativa D_0' del secuente S_0. Al sustituir D_0 por D_0' obtenemos una demostración D' alternativa a D en la que hemos eliminado la inducción que estamos considerando. Vamos a calcular su ordinal.

En primer lugar observamos que S tiene altura h_1 en D, lo que significa que h_1 es el máximo de los grados de los cortes situados bajo S y del grado de la fórmula de inducción $\alpha(y)$. Pero todas las fórmulas $\alpha(\bar{n})$ tienen el mismo grado que $\alpha(y)$, luego todos los cortes situados en D' entre un secuente

$$\alpha(\bar{n}), \Gamma \Rightarrow \Delta,\, \alpha(\overline{n+1})$$

y el secuente $\alpha(0)$, $\Gamma \Rightarrow \Delta$, $\alpha(t)$ tienen el grado de $\alpha(y)$, lo que se traduce en que las alturas de los cortes e inducciones contenidos en $D_0(\bar{n})$ como parte de D' son las mismas que las que tienen en D_0 como parte de D, luego el ordinal en D' de los secuentes

$$\alpha(\bar{n}), \Gamma \Rightarrow \Delta,\, \alpha(\overline{n+1})$$

sigue siendo μ. Además, todos los cortes que combinan estos secuentes en D_0' están formados por secuentes de altura h_1, por lo que el ordinal del secuente inferior cada corte es la suma formal de los de los secuentes superiores. Concretamente:

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{2}); D') = \mu\#\mu,$$

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{3}); D') = \mu\#\mu\#\mu$$

y así:

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{m}); D') = \mu * m,$$

donde $\mu * m = \mu\# \cdots \#\mu$ (m veces).

Por último, en el último corte de D_0', los secuentes superiores tienen altura h_1 en D' y el secuente inferior tiene la misma altura h_0 que en D, luego

$$o(S_0; D') = \omega_{h_1-h_0}(\mu * m + q)$$

y

$$\mu * m + q = \omega^\eta + \cdots < \omega^{\eta+1},$$

luego

$$o(S_0; D') = \omega_{h_1-h_0}(\mu * m + q) < \omega_{h_1-h_0}(\omega^{\eta+1}) = \omega_{h_1-h_0+1}(\eta + 1) = o(S_0; D).$$

El teorema 7.2 nos da entonces que $o(D') < o(D)$.

A partir de aquí podemos suponer que la parte final de D no contiene inducciones.

• Supongamos ahora que la parte final de D contiene un axioma lógico, es decir, un secuente de la forma $\alpha \Rightarrow \alpha$.

Como en la parte final no hay reglas lógicas ni inducciones y el secuente final es vacío, los descendientes de las dos fórmulas α son idénticos a α y tienen que acabar desapareciendo en un corte. Supongamos que en primer lugar desaparece un descendiente del antecedente, así:

$$
\begin{array}{c}
\begin{array}{cc}
D_0 & \alpha \Rightarrow \alpha \\
\vdots & \vdots \\
\Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha & \alpha,\, \Gamma' \stackrel{\nu}{\Rightarrow} \Delta'
\end{array} \\
\hline
\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\
\vdots \\
\Rightarrow
\end{array}
$$

donde Δ' contiene todavía un descendiente directo del α situado en el consecuente del axioma. Entonces podemos simplificar D hasta una demostración D' de la forma

$$
\begin{array}{c}
D_0 \\
\vdots \\
\Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha \\
\hline
\Gamma,\, \Gamma' \stackrel{\mu}{\Rightarrow} \Delta,\, \Delta' \\
\vdots \\
\Rightarrow
\end{array}
$$

Llamemos S al secuente $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'$. Notemos que en los últimos puntos suspensivos tiene que haber otro corte que elimine la fórmula α contenida en Δ'. Por lo tanto, al pasar a D' hemos eliminado un corte del grado de α, pero más abajo hay otro del mismo grado, luego las alturas en D de todos los secuentes de la subdemostración D_0 que acaba en $\Gamma \Rightarrow \Delta,\, \alpha$ son las mismas que sus alturas en D', luego

$$\mu = o(\Gamma \Rightarrow \Delta, \alpha; D) = o(\Gamma \Rightarrow \Delta, \alpha; D') = o(S; D').$$

Más aún, como la altura de los dos secuentes superiores del corte de D es la misma que la del secuente inferior, si los secuentes superiores tienen ordinales μ y ν en D, entonces

$$o(S; D) = \mu \# \nu > \mu = o(S; D').$$

El teorema 7.2 nos da entonces que $o(D') < o(D)$. Si en D se corta antes la fórmula α del consecuente del axioma, un razonamiento totalmente análogo nos lleva a la misma conclusión.

Así pues, a partir de aquí podemos suponer que la parte final de la demostración D no contiene ningún axioma lógico.

• Supongamos ahora que la parte final de D contiene una regla de debilitación y tomemos una que no tenga otra por debajo. Supongamos que es una regla izquierda, pero el caso de la regla derecha se trata análogamente. Como el secuente final es vacío, la fórmula introducida, digamos α, tiene que eliminarse posteriormente con un corte, por lo que D tiene que tener esta estructura:

$$\begin{array}{c}\dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\mu}{\Rightarrow} \Delta, \alpha\end{array} \qquad \begin{array}{c}\vdots\\ \dfrac{\Gamma''\Rightarrow\Delta''}{\alpha,\,\Gamma''\Rightarrow\Delta''}\\ \vdots\\ \alpha,\,\Gamma'\overset{\nu}{\Rightarrow}\Delta'\end{array}}{\Gamma,\,\Gamma'\Rightarrow\Delta,\,\Delta'}\\ \vdots\\ \Rightarrow\end{array}$$

Distinguimos dos posibilidades:

A) Si α figura en el antecedente de algún secuente que se corta con otro situado bajo $\alpha, \Gamma'' \Rightarrow \Delta''$, entonces α "aparece" aunque no usemos la regla de debilitación que la introduce en D, con lo que podemos considerar demostración alternativa D':

$$\begin{array}{c}\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta, \alpha\end{array} \qquad \begin{array}{c}\vdots\\ \Gamma''\Rightarrow\Delta''\\ \vdots\\ \alpha,\,\Gamma'\Rightarrow\Delta'\end{array}}{\Gamma,\,\Gamma'\Rightarrow\Delta,\,\Delta'}\\ \vdots\\ \Rightarrow\end{array}$$

que tiene el mismo ordinal, pero una debilitación menos en su parte final.

B) Si α no figura el en antecedente de ningún secuente que se corta con alguno de los secuentes situados bajo $\alpha, \Gamma'' \Rightarrow \Delta''$, entonces todas las reglas intermedias siguen siendo válidas si eliminamos α de los secuentes situados bajo $\alpha, \Gamma'' \Rightarrow \Delta''$ (pues α es siempre una fórmula colateral y no hay debilitaciones que puedan volverla a introducir), con lo que obtenemos la demostración alternativa:

$$\begin{array}{c}\vdots\\ \Gamma''\Rightarrow\Delta''\\ \vdots\\ \dfrac{\Gamma'\overset{\nu'}{\Rightarrow}\Delta'}{\Gamma,\,\Gamma'\overset{\nu'}{\Rightarrow}\Delta,\,\Delta'}\\ \vdots\\ \Rightarrow\end{array}$$

La altura h_0 del secuente $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ es la misma en D y en D', pero al haber eliminado un corte, la altura de los secuentes situados sobre él puede cambiar. Sea S un secuente en D situado sobre α, $\Gamma' \Rightarrow \Delta'$ y sea S' el secuente correspondiente en D'. Sea $h = h(S, D)$ y $h' = h(S', D')$. Claramente $h' \leq h$ y, más precisamente, vamos a ver que

$$\omega_{h-h'}(o(S; D)) \geq o(S'; D'). \tag{7.1}$$

Admitiendo esto, tenemos en particular que $\omega_{h_1-h_0}(\nu) \geq \nu'$ y

$$\xi = \omega_{h_1-h_0}(\mu \# \nu) > \omega_{h_1-h_0}(\nu) \geq \nu',$$

luego el teorema 7.2 nos da que $o(D') < o(D)$.

Como en cada paso de tipo A) eliminamos una debilitación implícita de la parte final, al cabo de un número finito de pasos, o bien se da en algún momento el caso B) y hemos reducido el ordinal, o bien llegamos a una demostración en cuya parte final todas las fórmulas principales de las reglas de debilitación implícitas son de tipo Δ_0.

La prueba de (7.1) es laboriosa. Obviamente la relación es cierta cuando S es un secuente inicial, pues los dos ordinales valen 1, luego basta probar que si la cumplen los secuentes superiores de una regla de inferencia, también la cumple el secuente inferior. Distinguimos todos los casos posibles:

1. En el caso de una regla de debilitación S/S_0, se cumple que ambos secuentes tienen la misma altura h y los correspondientes S'/S'_0 en D' también tienen la misma altura h', por lo que
$$\omega_{h-h'}(o(S_0; D)) = \omega_{h-h'}(o(S; D)) \geq o(S'; D') = o(S'_0; D').$$

2. En el caso de una regla izquierda del disyuntor, los secuentes superiores S y $\bar{S}$ tienen la misma altura h que el secuente inferior S_0, y lo mismo sucede con la regla correspondiente en D'. Por lo tanto, teniendo en cuenta el teorema 6.9,
$$\omega_{h-h'}(o(S_0; D) = \omega_{h-h'}(o(S; D) \# o(\bar{S}; D)) \geq$$
$$\omega_{h-h'}(o(S; D)) \# \omega_{h-h'}(o(\bar{S}; D)) \geq o(S'; D') \# o(\bar{S}'; D') = o(S'_0; D').$$

3. En el caso de una regla lógica S/S_0, ambos secuentes tienen la misma altura h, e igualmente, en la regla S'/S'_0 ambos secuentes tienen altura h'. Entonces
$$\omega_{h-h'}(o(S; D) + 1) \geq \omega_{h-h'}(o(S; D)) \# \omega_{h-h'}(1) \geq o(S'; D') + 1.$$

4. Consideremos ahora un corte en D y el correspondiente en D':
$$\frac{S_1 \qquad S_2}{S_0} \qquad \frac{S'_1 \qquad \bar{S}'_2}{S'_0}$$
Llamemos h_1 y h_0 a las alturas de los secuentes superiores y del secuente inferior en D, respectivamente, y h'_1 y h'_0 a las alturas de los secuentes correspondientes en D'. Sean $\mu_i = o(S_i; D)$ y $\mu'_i = o(S'_i; D)$. Llamemos g al grado del corte y distinguimos tres casos:

(a) Si $h_0' \leq h_0 \leq g$, entonces $h_1 = g = h_1'$, luego la hipótesis de inducción es que $\mu_i \geq \mu_i'$. A su vez,

$$\omega_{h_0-h_0'}(\omega_{h_1-h_0}(\mu_1 \# \mu_2)) = \omega_{h_1-h_0'}(\mu_1 \# \mu_2) \geq \omega_{h_1'-h_0'}(\mu_1' \# \mu_2').$$

(b) Si $g \leq h_0' \leq h_0$, entonces $h_1 = h_0$ y $h_1' = h_0'$ y de nuevo la hipótesis de inducción es $\mu_i \geq \mu_i'$. Tenemos entonces que

$$\omega_{h_0-h_0'}(\mu_1 \# \mu_2) \geq \mu_1 \# \mu_2 \geq \mu_1' \# \mu_2'.$$

(c) Si $h_0' \leq g \leq h_0$, entonces $h_1 = h_0$, $h_1' = g$ y la hipótesis de inducción es $\omega_{h_0-g}(\mu_i) \geq \mu_i'$. Entonces

$$\omega_{h_0-h_0'}(\mu_1 \# \mu_2) = \omega_{g-h_0'}(\omega_{h_0-g}(\mu_1 \# \mu_2)) \geq$$

$$\omega_{h_1'-h_0'}(\omega_{h_0-g}(\mu_1) \# \omega_{h_0-g}(\mu_2)) \geq \omega_{h_1'-h_0'}(\mu_1' \# \mu_2').$$

5. Finalmente consideramos una regla de inducción S/S_0. Como en el caso anterior, llamamos h_1 y h_0 a las alturas del secuente superior y del secuente inferior en D, respectivamente, y h_1' y $h' : 0$ a las alturas de los secuentes correspondientes en D'. Sean

$$\mu = o(S; D) = \omega^\eta + \cdots, \qquad \mu' = o(S'; D') = \omega^{\eta'} + \cdots$$

Llamamos g al grado de la fórmula de inducción y distinguimos los mismos tres casos que antes:

(a) Si $h_0' \leq h_0 \leq g$, entonces $h_1 = g = h_1'$, luego la hipótesis de inducción es que $\mu \geq \mu'$, lo que implica que $\eta \geq \eta'$. A su vez,

$$\omega_{h_0-h_0'}(\omega_{h_1-h_0+1}(\eta+1)) = \omega_{h_1-h_0'+1}(\eta+1) \geq \omega_{h_1'-h_0'+1}(\eta'+1).$$

(b) Si $g \leq h_0' \leq h_0$, entonces $h_1 = h_0$ y $h_1' = h_0'$ y de nuevo la hipótesis de inducción es $\mu \geq \mu'$. Tenemos entonces que

$$\omega_{h_0-h_0'}(\omega^{\eta+1}) \geq \omega^{\eta+1} \geq \omega^{\eta'+1}.$$

(c) Si $h_0' < g \leq h_0$, entonces $h_1 = h_0$, $h_1' = g$ y la hipótesis de inducción es $\omega_{h_0-g}(\mu) \geq \mu'$. Esto significa que

$$\omega_{h_0-g}(\omega^\eta + \cdots) = \omega^{\omega_{h_0-g-1}(\omega^\eta+\cdots)} \geq \omega^{\eta'} + \cdots,$$

luego $\omega_{h_0-g-1}(\omega^{\eta+1}) > \omega_{h_0-g-1}(\omega^\eta + \cdots) \geq \eta'$, luego

$$\omega_{h_0-g-1}(\omega^{\eta+1}) \geq \eta' + 1,$$

luego $\omega_{h_0-g}(\omega^{\eta+1}) \geq \omega^{\eta'+1}$, luego

$$\omega_{h_0-h_0'}(o(S; D) = \omega_{h_0-h_0'}(\omega^{\eta+1}) = \omega_{g-h_0'}(\omega_{h_0-g}(\omega^{\eta+1})) \geq$$

$$\omega_{g-h_0'}(\omega^{\eta'+1}) = \omega_{h_1'-h_0'+1}(\eta'+1) = o(S'; D').$$

En suma, podemos restringirnos al caso en que la parte final de D sólo contiene axiomas del igualador o axiomas matemáticos y cortes. Más aún, por el primer paso de la prueba, en ella no hay variables libres. Observemos que todas las fórmulas que aparecen en los axiomas del igualador y en los axiomas matemáticos son atómicas.

Ahora vemos que D no puede coincidir con su parte final, pues si se diera el caso tendríamos que D sería una demostración del secuente vacío formada por sentencias atómicas, en contra del teorema 7.5.

• Por el teorema 7.4 tenemos que la parte final de D contiene un corte adecuado. Tomemos uno que no tenga ningún otro por debajo. La fórmula de corte tiene que tener signos lógicos. Hay cuatro casos posibles.

A) Si la fórmula de corte es $\neg\alpha$, la demostración es de la forma

$$\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \dfrac{\alpha,\,\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1}{\Gamma_1 \Rightarrow \Delta_1,\,\neg\alpha}\\ \vdots\\ \Gamma \overset{\mu_1}{\Rightarrow} \Delta,\,\neg\alpha\end{array} \quad (h_1) \quad \begin{array}{c}\vdots\\ \dfrac{\Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1',\,\alpha}{\neg\alpha,\,\Gamma_1' \Rightarrow \Delta_1'}\\ \vdots\\ \neg\alpha,\,\Gamma' \overset{\mu_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}\\
\vdots\\
\Gamma'' \overset{\nu}{\Rightarrow} \Delta'' \quad (h_0)\\
\vdots\\
\Rightarrow
\end{array}$$

Hemos destacado el secuente más alto $\Gamma'' \Rightarrow \Delta''$ situado bajo $\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'$ (podría ser éste mismo) cuya altura h_0 es estrictamente menor que la altura h_1 de los dos secuentes superiores del corte. Notemos que tiene que existir, pues la altura del secuente final de una demostración siempre es 0 y $h_1 > 0$, pues el grado de $\neg\alpha$ no es nulo. Consideramos esta demostración alternativa:

$$\begin{array}{c}
\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\xi_1}{\Rightarrow} \Delta,\,\neg\alpha\end{array} \quad (h_1) \quad \begin{array}{c}\vdots\\ \dfrac{\Gamma_1' \overset{\nu_1}{\Rightarrow} \Delta_1',\,\alpha}{\neg\alpha,\,\Gamma_1' \Rightarrow \Delta_1',\,\alpha}\\ \vdots\\ \neg\alpha,\,\Gamma' \overset{\xi_2}{\Rightarrow} \Delta',\,\alpha\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta',\,\alpha}\\ \vdots\\ \Gamma'' \Rightarrow \Delta'',\,\alpha \quad (h)\end{array} \qquad \begin{array}{c}\dfrac{\begin{array}{c}\vdots\\ \dfrac{\alpha,\,\Gamma_1 \overset{\nu_2}{\Rightarrow} \Delta_1}{\alpha,\,\Gamma_1 \Rightarrow \Delta_1,\,\neg\alpha}\\ \vdots\\ \alpha,\,\Gamma \overset{\xi_3}{\Rightarrow} \Delta,\,\neg\alpha\end{array} \quad (h_1) \quad \begin{array}{c}\vdots\\ \neg\alpha,\,\Gamma' \overset{\xi_4}{\Rightarrow} \Delta'\end{array}}{\alpha,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}\\ \vdots\\ (h) \quad \alpha,\,\Gamma'' \Rightarrow \Delta''\end{array}}{\Gamma'' \overset{\nu'}{\Rightarrow} \Delta'' \quad (h_0)}\\
\vdots\\
\Rightarrow
\end{array}$$

Observemos que, al dejar α, hemos sustituido las reglas del negador por reglas de debilitación. Como todas las inferencias por debajo de las reglas fronterizas son cortes, éstos siguen siendo válidos aunque hayamos añadido α en el antecedente o en el consecuente, por lo que podemos llegar a los secuentes superiores del corte original con la adición de α. Cortando dos veces $\neg\alpha$ podemos continuar la deducción con el α adicional hasta eliminarlo justo antes del secuente $\Gamma'' \Rightarrow \Delta''$, y a partir de ahí continuamos la deducción original hasta el secuente vacío.

Vamos a probar que la nueva demostración D' tiene ordinal menor que la original D. En primer lugar observamos que los secuentes superiores de los cortes de $\neg\alpha$ en D' siguen teniendo altura h_1, pues por debajo no tienen ninguna inducción y tienen los mismos cortes, salvo un corte añadido con fórmula de corte α, pero ésta no aumenta la altura, ya que h_1 es mayor o igual que el grado de $\neg\alpha$, que es mayor que el de α. Obviamente la altura de $\Gamma'' \Rightarrow \Delta''$ en D' es la misma que en D.

Si llamamos m a la altura de los secuentes superiores del corte de α en D', tenemos que $h = h_0$ si h_0 es mayor que el grado de α y h es el grado de α en caso contrario. En cualquier caso $h_0 \leq h < h_1$.

Claramente, $\xi_1 = \mu_1$, $\xi_2 < \mu_2$, $\xi_3 < \mu_1$, $\xi_4 = \mu_2$, donde las desigualdades estrictas se deben a que al pasar de D a D' hemos eliminado una regla del negador.

Todos los secuentes entre $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ y $\Gamma'' \Rightarrow \Delta''$ tienen altura h_1 en D menos el último, y lo mismo vale en las dos ramas de D'. Como uno de los secuentes anteriores a $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ tiene ordinal estrictamente menor en D que en las ramas de D', una inducción trivial nos permite concluir que el ordinal de cada secuente bajo $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ en D es mayor estrictamente que el ordinal del secuente correspondiente en cada una de las dos ramas correspondientes en D', salvo quizá en el caso del secuente $\Gamma'' \Rightarrow \Delta''$, cuya altura pasa de ser h_0 en D a ser h en cada rama de D'. Si la inferencia que lleva a $\Gamma'' \Rightarrow \Delta''$ en D es un corte

$$\frac{S_1 \qquad S_2}{\Gamma'' \Rightarrow \Delta''}$$

cuyos secuentes superiores tienen ordinales ϵ_1 y ϵ_2, en D' tenemos

$$\frac{\dfrac{S_1' \qquad S_2'}{\Gamma'' \Rightarrow \Delta'', \alpha} \qquad \dfrac{S_1'' \qquad S_2''}{\alpha, \Gamma'' \Rightarrow \Delta''}}{\Gamma'' \Rightarrow \Delta''}$$

y los ordinales son:

$$\frac{\dfrac{\epsilon_1' \qquad \epsilon_2'}{\omega_{h_1-h}(\epsilon_1' \# \epsilon_2')} \qquad \dfrac{\epsilon_1'' \qquad \epsilon_2''}{\omega_{h_1-h}(\epsilon_1'' \# \epsilon_2'')}}{\omega_{h_1-h_0}\big(\omega_{h_1-h}(\epsilon_1' \# \epsilon_2') \# \omega_{h_1-h}(\epsilon_1'' \# \epsilon_2'')\big)}$$

De los ordinales ϵ_1' y ϵ_2', uno de ellos es igual al correspondiente ϵ_1 o ϵ_2 y el otro es estrictamente menor, luego $\epsilon_1' \# \epsilon_2' < \epsilon_1 \# \epsilon_2$, e igualmente $\epsilon_1'' \# \epsilon_2'' < \epsilon_1 \# \epsilon_2$, luego[2]

$$\omega_{m-k}(\omega_{l-m}(\epsilon_1'\#\epsilon_2')\#\omega_{l-m}(\epsilon_1''\#\epsilon_2'')) < \omega_{m-k}(\omega_{l-m}(\epsilon_1\#\epsilon_2)) = \omega_{l-m}(\epsilon_1\#\epsilon_2),$$

o, lo que es lo mismo,

$$\nu = o(\Gamma'' \Rightarrow \Delta'', D') < o(\Gamma'' \Rightarrow \Delta'', D) = \nu'.$$

El teorema 7.2 nos da entonces que $o(D') < o(D)$.

B) A) Si la fórmula de corte es $\alpha \vee \beta$, la demostración es de la forma

$$\begin{array}{c}
\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\vdots\\ \Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\,\alpha\end{array}}{\Gamma_1 \Rightarrow \Delta_1,\,\alpha\vee\beta}\\ \vdots\\ \Gamma \overset{\mu_1}{\Rightarrow} \Delta,\,\alpha\vee\beta \quad (h_1)\end{array} \qquad \begin{array}{c}\dfrac{\begin{array}{cc}\vdots & \vdots\\ \alpha,\,\Gamma_1' \Rightarrow \Delta_1' & \beta,\,\Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'\end{array}}{\alpha\vee\beta,\,\Gamma_1' \Rightarrow \Delta_1'}\\ \vdots\\ \alpha\vee\beta,\,\Gamma' \overset{\mu_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}\\
\vdots\\
\Gamma'' \overset{\nu}{\Rightarrow} \Delta'' \quad (h_0)\\
\vdots\\
\Rightarrow
\end{array}$$

donde nuevamente $\Gamma'' \Rightarrow \Delta''$ es el secuente más alto cuya altura h_0 es menor que la altura h_1 de los secuentes superiores del corte que elimina $\alpha \vee \beta$. Ahora consideramos la demostración D' siguiente:

$$\begin{array}{c}
\dfrac{\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\vdots\\ \Gamma_1 \Rightarrow \Delta_1,\,\alpha\end{array}}{\Gamma_1 \Rightarrow \Delta_1,\,\alpha,\,\alpha\vee\beta}\\ \vdots\\ \Gamma \overset{\xi_1}{\Rightarrow} \Delta,\alpha,\alpha\vee\beta \quad (h_1)\end{array} \quad \begin{array}{c}\vdots\\ \alpha\vee\beta,\,\Gamma' \overset{\xi_2}{\Rightarrow} \Delta'\end{array}}{\begin{array}{c}\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta',\,\alpha\\ \vdots\\ \Gamma'' \overset{\nu_1}{\Rightarrow} \Delta'',\,\alpha \quad (h)\end{array}} \qquad \dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\xi_3}{\Rightarrow} \Delta,\,\alpha\vee\beta \quad (h_1)\end{array} \quad \begin{array}{c}\dfrac{\begin{array}{c}\vdots\\ \alpha,\,\Gamma_1' \Rightarrow \Delta_1'\end{array}}{\alpha\vee\beta,\,\alpha,\,\Gamma_1' \Rightarrow \Delta_1'}\\ \vdots\\ \alpha\vee\beta,\,\alpha,\,\Gamma' \overset{\xi_4}{\Rightarrow} \Delta'\end{array}}{\begin{array}{c}\alpha,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'\\ \vdots\\ (h)\ \ \alpha,\,\Gamma'' \overset{\nu_2}{\Rightarrow} \Delta''\end{array}}}{\Gamma'' \overset{\nu'}{\Rightarrow} \Delta'' \quad (h_0)}\\
\vdots\\
\Rightarrow
\end{array}$$

Los secuentes superiores de los cortes de $\alpha \vee \beta$ en D' siguen teniendo altura h_1, pues por debajo no tienen ninguna inducción y tienen los mismos cortes, salvo un corte añadido con fórmula de corte α, pero ésta no aumenta la altura, ya que h_1 es mayor o igual que el grado de $\alpha \vee \beta$, que es mayor que el de α. Por otra parte, la altura de $\Gamma'' \Rightarrow \Delta''$ en D' es la misma que en D.

Si llamamos h a la altura de los secuentes superiores del corte de α en D', tenemos que $h = h_0$ si h_0 es mayor que el grado de α y h es el grado de α en caso contrario. En cualquier caso $h_0 \leq h < h_1$.

[2] Aquí usamos que si $\eta' \leq \eta'' < \eta$, entonces $\omega^{\eta'}\#\omega^{\eta''} = \omega^{\eta''} + \omega^{\eta'} < \omega^{\eta}$.

Por otro lado, $\xi_1 < \mu_1$, $\xi_2 = \mu_2$, $\xi_3 = \mu_1$, $\xi_4 < \mu_2$, donde las desigualdades estrictas se deben a que al pasar de D a D' hemos eliminado una regla del disyuntor.

Todos los secuentes entre $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ y $\Gamma'' \Rightarrow \Delta''$ tienen altura h_1 menos el último. Como todas las inferencias son cortes, el ordinal de cada nuevo secuente es la suma formal de los dos secuentes superiores del corte que lo genera, salvo quizá en el caso de los secuentes del corte que elimina α en D'. Por consiguiente, salvo en este caso, el ordinal de cada secuente bajo $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ en D es mayor que el ordinal del secuente correspondiente en cada una de las dos ramas correspondientes en D'.

Para los secuentes del corte que elimina a α en D', el cálculo es exactamente el mismo que el del caso anterior. Si la inferencia que lleva a $\Gamma'' \Rightarrow \Delta''$ en D es un corte

$$\frac{S_1 \qquad S_2}{\Gamma'' \Rightarrow \Delta''}$$

cuyos secuentes superiores tienen ordinales ϵ_1 y ϵ_2, exactamente las mismas cuentas que en el caso anterior nos permiten concluir que $o(D') < o(D)$.

C) Si la fórmula de corte es $\bigvee u\, \alpha(u)$, la demostración es de la forma

$$\begin{array}{c}
\begin{array}{ccc}
\vdots & & \vdots \\
\dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \Rightarrow \Delta_1,\, \bigvee u\, \alpha(u)} & & \dfrac{\alpha(y),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}{\bigvee u\, \alpha(u),\, \Gamma_1' \Rightarrow \Delta_1'} \\
\vdots & & \vdots
\end{array} \\
\dfrac{\Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\, \alpha(u) \qquad (h_1) \qquad \bigvee u\, \alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'} \\
\vdots \\
\Gamma'' \overset{\nu}{\Rightarrow} \Delta'' \quad (h_0) \\
\vdots \\
\Rightarrow
\end{array}$$

donde nuevamente $\Gamma'' \Rightarrow \Delta''$ es el secuente más alto cuya altura h_0 es menor que la altura h_1 de los secuentes superiores del corte que elimina $\bigvee u\, \alpha(u)$. Ahora consideramos la demostración alternativa D' siguiente, que por razones tipográficas descomponemos en dos bloques:

$$\begin{array}{c}
\begin{array}{ccc}
\vdots & & \\
\dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \Rightarrow \Delta_1,\, \alpha(t),\, \bigvee u\, \alpha(u)} & & \\
\vdots & & \vdots
\end{array} \\
\dfrac{\Gamma \overset{\xi_1}{\Rightarrow} \Delta,\, \alpha(t), \bigvee u\, \alpha(u) \qquad (h_1) \qquad \bigvee u\, \alpha(u),\, \Gamma' \overset{\xi_2}{\Rightarrow} \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha(t)} \\
\vdots \\
\Gamma'' \Rightarrow \Delta'',\, \alpha(t) \quad (h)
\end{array}$$

$$\cfrac{\cfrac{\vdots}{\Gamma \overset{\xi_3}{\Rightarrow} \Delta, \bigvee u\, \alpha(u)} \quad (h_1) \quad \cfrac{\vdots}{\cfrac{\cfrac{\vdots}{\alpha(t), \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\, \alpha(u), \alpha(t), \Gamma_1' \Rightarrow \Delta_1'}} \;\; \vdots \;\; \bigvee u\, \alpha(u), \alpha(t), \Gamma' \overset{\xi_4}{\Rightarrow} \Delta'}{\alpha(t), \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}$$

$$\vdots$$

$$(h) \quad \alpha(t), \Gamma'' \Rightarrow \Delta''$$

Estos dos bloques se combinan mediante un corte:

$$\cfrac{\cfrac{\vdots}{\Gamma'' \Rightarrow \Delta'', \alpha(t)} \quad (h) \quad \cfrac{\vdots}{\alpha(t), \Gamma'' \Rightarrow \Delta''}}{\Gamma'' \overset{\nu'}{\Rightarrow} \Delta'' \quad (h_0)}$$

$$\vdots$$

$$\Rightarrow$$

Empezamos ambos bloques sustituyendo las reglas del particularizador por reglas de debilitación sin más que conservar $\alpha(t)$ en el secuente final. Todas las reglas de inferencia siguen siendo válidas sin más que añadir por debilitación $\alpha(t)$ en el segundo secuente superior de las posibles reglas izquierdas del disyuntor, con lo que podemos llegar a los secuentes superiores del corte original con la adición de $\alpha(t)$. Cortando dos veces $\bigvee u\, \alpha(u)$ podemos continuar la deducción manteniendo el $\alpha(t)$ adicional hasta eliminarlo justo antes de $\Gamma'' \Rightarrow \Delta''$, y a partir de ahí continuamos la deducción original hasta el secuente vacío.

Tenemos que

$$o(\alpha(t), \Gamma_1' \Rightarrow \Delta_1'; D') = o(\alpha(y), \Gamma_1' \Rightarrow \Delta_1'; D) = \nu_2,$$

pues por debajo de estos secuentes hemos añadido el corte de $\alpha(t)$, pero su grado es menor que el del corte de $\bigvee u\, \alpha(u)$, luego las alturas de los secuentes correspondientes en ambas subdemostraciones son las mismas.

Ahora observamos que los secuentes superiores de los cortes de $\bigvee u\, \alpha(u)$ en D' siguen teniendo altura h_1, pues por debajo no tienen ninguna inducción y tienen los mismos cortes, salvo un corte añadido con fórmula de corte $\alpha(t)$, pero ésta no aumenta la altura, ya que h_1 es mayor o igual que el grado de $\bigvee u\, \alpha(u)$, que es mayor que el de $\alpha(t)$. Obviamente la altura de $\Gamma'' \Rightarrow \Delta''$ en D' es la misma que en D.

Si llamamos h a la altura de los secuentes superiores del corte de $\alpha(t)$ en D', tenemos que $h = h_0$ si h_0 es mayor que el grado de $\alpha(t)$ y h es el grado de $\alpha(t)$ en caso contrario. En cualquier caso $h_0 \leq h < h_1$.

Claramente, $\xi_1 = \mu_1$, $\xi_2 < \mu_2$, $\xi_3 < \mu_1$, $\xi_4 = \mu_2$, donde las desigualdades estrictas se deben a que al pasar de D a D' hemos eliminado una regla del particularizador.

Como en los casos anteriores, vemos que todos los secuentes situados entre $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ y $\Gamma'' \Rightarrow \Delta''$ tienen altura h_1 menos el último. Como todas las inferencias son cortes, el ordinal de cada nuevo secuente es la suma formal de los dos secuentes superiores del corte que lo genera, salvo quizá en el caso de los secuentes del corte que elimina α en D'. Por consiguiente, salvo en este caso, el ordinal de cada secuente bajo $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ en D es mayor que el ordinal del secuente correspondiente en cada una de las dos ramas correspondientes en D'.

Para los secuentes del corte que elimina a α en D', el cálculo es nuevamente el mismo que el de los casos precedentes. Si la inferencia que lleva a $\Gamma'' \Rightarrow \Delta''$ en D es un corte cuyos secuentes superiores tienen ordinales ϵ_1 y ϵ_2, exactamente las mismas cuentas nos permiten concluir que $o(D') < o(D)$.

D) El caso en que la fórmula de corte es $\bigwedge u\, \alpha(u)$ se trata de forma totalmente análoga. ■

Por consiguiente:

Teorema 7.7 (Gentzen) *Si la aritmética de Peano es contradictoria, existe una sucesión infinita estrictamente decreciente de ordinales.*

Naturalmente, por ordinales entendemos ordinales menores que ϵ_0, tal y como los hemos definido en el capítulo precedente. La prueba es estrictamente constructiva y finitista. Podemos programar un ordenador para que, si le damos una demostración del secuente vacío en AP, nos genere una sucesión infinita estrictamente decreciente de ordinales.

¿Probó Gentzen la consistencia de la aritmética? Nadie cuestiona la corrección formal de la demostración del teorema anterior, pero éste sí que ha generado controversias sobre su auténtico valor epistemológico, es decir, sobre si realmente sirve para convencer a alguien de que la aritmética de Peano es consistente.

Por ejemplo, se dice que Alfred Tarski dijo en cierta ocasión que la prueba de Gentzen mediante inducción hasta ϵ_0 había aumentado su confianza en la consistencia de la aritmética "en un ϵ" (es decir, que el incremento fue insignificante), pero esto refleja únicamente el hecho de que para alguien que no dude de la consistencia de la aritmética ninguna prueba podrá hacer que aumente su confianza en ella.

Más mordaz fue Hermann Weyl cuando afirmó que Gentzen había demostrado la consistencia de la aritmética, es decir, de la inducción hasta el ordinal ω, mediante la inducción hasta ϵ_0 (un ordinal mucho mayor).

La crítica que encierra la frase de Tarski supone una acusación de circularidad trivial: "no tengo objeción alguna a tus argumentos porque acepto de salida la conclusión a la que quieres llegar, y ella los justifica todos", mientras que la de Weyl sugiere una circularidad destructiva: "pretendes convencerme de algo pidiéndome que acepte de entrada algo mucho más fuerte que tu conclusión".

En palabras de Kleene:

> *Hasta qué punto puede aceptarse que la prueba de Gentzen sirve de fundamento a la teoría de números clásica en el sentido en que este problema ha sido planteado es, en la situación actual, una cuestión que queda al juicio de cada cual, dependiendo de en qué medida está uno dispuesto a aceptar la inducción hasta ϵ_0 como método finitista.*

Ya hemos comentado en el capítulo anterior cómo Gentzen consideraba incuestionable la inducción hasta ϵ_0 y Gödel mostró su escepticismo al respecto (no a que fuera correcta, por descontado, sino a que fuera un principio más evidente que la propia consistencia de la aritmética). Takeuti, por su parte, cuando presenta la prueba de Gentzen dice:

> *Por supuesto, la importancia de este teorema reside en su demostración* [...] *¡Nadie duda de la consistencia de la aritmética de Peano!*

Además, contesta a Weyl observando que su afirmación es equívoca, pues Gentzen prueba la consistencia de la aritmética a partir de la accesibilidad de ϵ_0, que es un hecho que a su vez puede ser justificado satisfactoriamente. El lector tendrá que juzgar por sí mismo si le parece convincente la demostración de Takeuti que hemos presentado en la sección 6.4, aunque es difícil juzgar si un argumento es convincente cuando uno ya está convencido *a priori* de su conclusión. ■

Tanto si la prueba de Gentzen nos convence de algo como si no, lo cierto es que de ella se deduce un hecho no trivial. Puesto que la prueba del teorema 7.6 es completamente finitista, es formalizable en APR, lo que significa que podemos definir un funtor $F(D)$ de modo que

$$\underset{\mathrm{APR}}{\vdash}(\overset{D}{\underset{\ulcorner\mathrm{AP}\urcorner}{\vdash}}(\varnothing \Rightarrow \varnothing) \rightarrow \overset{F(D)}{\underset{\ulcorner\mathrm{AP}\urcorner}{\vdash}}(\varnothing \Rightarrow \varnothing) \land o(F(D)) < o(D)).$$

Llamando

$$\phi(\alpha) \equiv \neg\bigvee D(\overset{D}{\underset{\mathrm{AP}}{\vdash}}(\varnothing \Rightarrow \varnothing) \land o(D) = \alpha),$$

obtenemos que

$$\underset{\mathrm{APR}}{\vdash}\bigwedge\alpha \in E(\neg\phi(\alpha) \rightarrow \bigvee\beta \prec \alpha\, \neg\phi(\beta))),$$

y esto equivale a

$$\underset{\mathrm{APR}}{\vdash}(\bigwedge\alpha \in E(\bigwedge\beta \prec \alpha\, \phi(\beta)) \rightarrow \phi(\alpha)),$$

Por consiguiente,

$$\underset{\mathrm{APR}}{\vdash}(\phi - \mathrm{IND}(\epsilon_0) \rightarrow \bigwedge\alpha \in E\, \phi(\alpha)\,),$$

pero $\bigwedge\alpha \in E\,\phi(\alpha)$ afirma que hay una fórmula que no puede ser demostrada en AP, luego implica Consis$\ulcorner\mathrm{AP}\urcorner$ y así concluimos que

$$\underset{\mathrm{APR}}{\vdash}(\phi - \mathrm{IND}(\epsilon_0) \rightarrow \mathrm{Consis}\ulcorner\mathrm{AP}\urcorner),$$

tal y como ya avanzábamos en el capítulo anterior. Así tenemos la prueba de que la inducción transfinita hasta ϵ_0 (al menos para una fórmula ϕ de tipo Π_1) no es demostrable en AP.

7.2 La consistencia de $\mathrm{I}\Sigma_1$

Veamos ahora una variante del argumento que hemos empleado en la sección anterior que nos permitirá demostrar la consistencia de $\mathrm{I}\Sigma_1$ a partir de la validez de la inducción transfinita hasta ω^ω.

Si existiera una demostración del secuente vacío en $\mathrm{I}\Sigma_1$, el teorema 3.22 nos permitiría construir otra a partir de ella formada exclusivamente por fórmulas de tipo Σ_1. A partir de este momento, cuando hablemos de demostraciones en $\mathrm{I}\Sigma_1$, entenderemos que nos referimos a demostraciones formadas por fórmulas de tipo Σ_1.

Llamaremos reglas de inferencia *relevantes* en una demostración D a las reglas de los cuantificadores cuya fórmula principal no sea Δ_0 o, lo que es lo mismo, las reglas que introducen cuantificadores no acotados.

Ahora definimos una nueva asignación de ordinales a las demostraciones:

A cada secuente S en una demostración D en $\mathrm{I}\Sigma_1$ (formada por fórmulas de tipo Σ_1) le asociamos un ordinal $o(S;D)$ según el criterio siguiente:

1. Si S es un secuente inicial de D, entonces $o(S;D)=0$.
2. Si S es el secuente inferior de una regla de debilitación o de una regla lógica irrelevante con un único secuente superior S_1, entonces $o(S;D)=o(S_1;D)$.
3. Si S es el secuente inferior de una regla izquierda del disyuntor o de corte con secuentes superiores S_1 y S_2, entonces $o(S;D)=o(S_1;D)\#o(S_2;D)$.
4. Si S es el secuente inferior de una regla de inferencia relevante con secuente superior S_1, entonces $o(S;D)=o(S_1;D)+1$.
5. Si S es el secuente inferior de una inducción con secuente superior S_1, entonces
$$o(S;D)=\begin{cases}\omega & \text{si } o(S_1;D)<\omega,\\ \omega^{n+1} & \text{si } o(S_1;D)=\omega^n+\cdots\end{cases}$$

El ordinal $o(D)$ de una demostración D es el ordinal de su secuente final. Es inmediato que, con esta definición, se cumple que $o(D)<\omega^\omega$.

Ejemplo En la demostración del ejemplo de la página 68 todas las fórmulas son Σ_1 y, según la definición precedente, todos los secuentes tienen ordinal 0 hasta que se aplican las reglas del particularizador, al final:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{0}}{0}}{1}\qquad \dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\\ 0\end{matrix}}{1}\quad \dfrac{\begin{matrix}\vdots\\ 0\end{matrix}}{1}}{2}}{3}}{\omega}}{\omega+1}$$

■

Ahora podemos afinar un poco más el enunciado del teorema 3.9:

Teorema 7.8 *Si α es una sentencia de tipo Δ_0, entonces en* AP($\varnothing$) *puede probarse el secuente $\Rightarrow \alpha$ o bien $\alpha \Rightarrow$ según si α es verdadera o falsa, y la demostración puede tomarse formada sólo por sentencias Δ_0 y con ordinal* 0.

DEMOSTRACIÓN: La prueba del teorema 3.9 muestra explícitamente como construir una demostración D de $\Rightarrow \alpha$ o de $\alpha \Rightarrow$ sin inducciones, y en ella se ve que D consta únicamente de sentencias Δ_0, por lo que no se usan reglas lógicas relevantes. Es claro entonces que todos los secuentes tienen ordinal 0. ■

Al haber cambiado la definición de ordinal, tenemos que demostrar de nuevo el teorema análogo a 7.2. De hecho necesitamos una versión ligeramente más general:

Teorema 7.9 *Sea D una demostración que contenga un secuente S_1 de modo que no haya ninguna inducción bajo S_1. Sea D_1 la subdemostración de D formada por los secuentes situados por encima de S_1 y sea D_1' otra demostración de S_1 tal que $o(S_1; D_1') < o(S_1; D)$ (resp. $o(S_1; D_1') \leq o(S_1; D)$). Sea D' la demostración que resulta de reemplazar D_1 por D_1' en D. Entonces $o(D') < o(D)$ (resp. $o(D') \leq o(D)$).*

La prueba es una simplificación de la de 7.2, en la que las reglas lógicas irrelevantes con un único secuente superior se tratan como la regla de debilitación y la de corte se trata como la regla izquierda del disyuntor. El argumento para la desigualdad no estricta es exactamente el mismo.

Aunque de momento nos interesará únicamente el caso de demostraciones en $I\Sigma_1$, vamos a dar aquí unas definiciones más generales:

Definición 7.10 La *parte final* de una demostración en AP está formada por los secuentes que no tienen por debajo ninguna regla de inferencia relevante implícita. Las reglas fronterizas se definen igual que en la sección anterior.

Un corte en una demostración en AP es *sustancial* si la fórmula de corte no es Δ_0. El corte es *adecuado* si además las dos fórmulas de corte tienen un ascendiente directo que es la fórmula principal de una regla fronteriza.

Probamos ahora una variante del teorema 7.4:

Teorema 7.11 *Supongamos que una demostración en* AP *contiene únicamente fórmulas de tipo Σ_n o Π_n, que no coincide con su parte final y que dicha parte final cumple las condiciones siguientes:*

1. *Sus secuentes iniciales están formados por fórmulas Δ_0,*
2. *Las fórmulas principales de las reglas de debilitación implícitas son Δ_0,*
3. *No contiene reglas relevantes o de inducción.*

Entonces la parte final contiene un corte adecuado.

Demostración: Como la demostración no coincide con su parte final, tiene alguna regla relevante implícita fronteriza. Su fórmula principal α no es Δ_0, y no puede ser la fórmula auxiliar de ninguna regla lógica posterior, ya que su fórmula principal no sería Σ_n o Π_n a menos que la regla introdujera un cuantificador que alternara con el primer cuantificador de α, pero entonces sería una regla relevante en la parte final de la demostración, en contra de lo supuesto. Como la regla fronteriza es implícita, α tiene que eliminarse con un corte situado bajo ella, luego en la parte final de la demostración, y dicho corte será un corte sustancial.

Vamos a probar el teorema por inducción sobre el número de cortes sustanciales contenidos en la parte final de la demostración. Consideremos un corte sustancial que no tenga ninguno más por debajo. Si es adecuado, ya tenemos la conclusión. En caso contrario será de la forma

$$\frac{\begin{array}{c} D_1 \\ \vdots \\ \Gamma \Rightarrow \Delta,\, \alpha \end{array} \qquad \begin{array}{c} D_2 \\ \vdots \\ \alpha,\, \Gamma' \Rightarrow \Delta' \end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

donde una de las dos fórmulas de corte (pongamos que la de la izquierda) no desciende directamente de la fórmula principal de una regla fronteriza.

Entonces D_1 contiene una regla fronteriza, pues, como α no es Δ_0, no puede descender directamente ni de un secuente inicial de la parte final de D ni de la fórmula principal de una regla de debilitación (implícita) de dicha parte final, ni de una inducción de la parte final (porque no hay), luego todos los hilos que pasan por α contenidos en D_1 tienen que pasar por una regla fronteriza contenida en D_1 (y, más concretamente, por una de sus fórmulas colaterales, ya que estamos suponiendo que α no desciende de la fórmula principal de ninguna regla fronteriza).

Observemos ahora que toda regla relevante contenida en D_1 es implícita para D_1 si y sólo si lo es para D.

Una implicación es obvia, pues si la fórmula principal tiene un descendiente se elimina con un corte de D_1, éste también es un corte de D, luego la regla es implícita para D. Y, recíprocamente, si la regla es implícita para D, como su fórmula principal no es Δ_0 y no puede tener a α como descendiente (pues en tal caso α descendería de la fórmula principal de una regla fronteriza), tiene que eliminarse en D_1, ya que el corte que elimina a α no tiene por debajo otros cortes sustanciales que puedan eliminarla.

Veamos ahora que una regla relevante contenida en D_1 es fronteriza para D_1 si y sólo si lo es para D.

En efecto, si es fronteriza para D, entonces es implícita para D, y también, según acabamos de ver, para D_1, y de hecho es fronteriza para D_1, pues cualquier regla de inferencia relevante contenida en D_1 por debajo de ella que sea implícita para D_1 es también implícita para D, lo que contradice que la regla inicial sea fronteriza para D.

Recíprocamente, si la regla es fronteriza para D_1, es implícita para D_1, luego para D, y tiene que ser fronteriza para D, pues si tuviera por debajo otra regla relevante implícita para D, no puede estar en D_1, ya que entonces sería implícita para D_1 y contradiría que la regla dada es fronteriza para D_1, luego tiene que estar por debajo del secuente $\Gamma \Rightarrow \Delta, \alpha$, y esto contradiría que el corte esté en la parte final de D.

Así pues, como D_1 tiene reglas fronterizas, no coincide con su parte final. De hecho, la parte final de D_1 está formada por los secuentes de la parte final de D contenidos en D_1. Esto nos permite aplicar la hipótesis de inducción a D_1, que tiene al menos un corte sustancial menos que D. Por lo tanto, D_1 contiene un corte adecuado. Esto significa que las fórmulas de corte descienden directamente de fórmulas principales de reglas fronterizas de D_1, que también son fronterizas en D, luego el corte es adecuado para D. ■

Con esto ya podemos demostrar:

Teorema 7.12 *Si D es una demostración del secuente vacío en $\mathrm{I}\Sigma_1$ existe otra D' tal que $o(D') < o(D)$.*

Demostración: Estamos suponiendo tácitamente que D consta únicamente de fórmulas de tipo Σ_1. El teorema 3.13 nos permite transformar D en una demostración regular sin alterar su ordinal. Alternativamente, podemos suponer que la demostración D es regular.

• Si en la parte final de D aparece una variable libre que no es la variable propia de ninguna regla de inferencia, por el teorema 3.11 podemos sustituirla por la constante 0, y obtenemos así una demostración del secuente vacío con el mismo ordinal.

Repitiendo este proceso un número finito de veces podemos suponer que en la parte final de D no hay ninguna variable libre que no esté usada como variable propia de una (única) regla de inferencia.

Llamamos *reglas de inferencia propias* a las reglas de inferencia que tienen variables propias, es decir, la regla derecha de generalizador, la regla izquierda del particularizador y la de inducción.

• Supongamos que la parte final de D contiene una regla propia y consideremos una que no tenga ninguna otra por debajo. Esto implica que todos los secuentes situados bajo ella constan únicamente de sentencias, pues, como la demostración es regular, cada variable libre es la variable propia de una regla de inferencia y sólo aparece por encima de ella. Distinguimos tres casos según el tipo de regla:

A) Generalizador derecha La fórmula principal tiene que ser una sentencia Δ_0 (o se trataría de una regla relevante), luego será de la forma:

$$\cfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\ y \leq t \to \alpha(y)\end{array}}{\begin{array}{c}\Gamma \overset{\mu}{\Rightarrow} \Delta,\ \bigwedge u \leq t\, \alpha(u)\\ \vdots\\ \Rightarrow\end{array}}$$

(Recordemos que las letras sobre las flechas de los secuentes denotarán siempre el ordinal del secuente.) Si la fórmula principal es falsa, existe un $k \leq d(t)$ tal que $\alpha(\bar{k})$ es falsa, pero entonces $\bar{k} \leq t \to \alpha(\bar{k})$ es falsa, y por 7.8 podemos demostrar el secuente $\bar{k} \leq t \to \alpha(\bar{k}) \overset{0}{\Rightarrow}$ de modo que la prueba contiene únicamente sentencias Δ_0. Por otra parte, como y no se usa como variable propia en la demostración del secuente superior, el teorema 3.11 nos da una demostración del secuente

$$\Gamma \overset{\mu}{\Rightarrow} \Delta,\ \bar{k} \leq t \to \alpha(\bar{k}).$$

Consideramos la demostración alternativa:

$$\cfrac{\cfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\ \bar{k} \leq t \to \alpha(\bar{k})\end{array} \qquad \begin{array}{c}\vdots\\ \bar{k} \leq t \to \alpha(\bar{k}) \overset{0}{\Rightarrow}\end{array}}{\Gamma \overset{\mu}{\Rightarrow} \Delta}}{\begin{array}{c}\Gamma \overset{\mu}{\Rightarrow} \Delta,\ \bigwedge u \leq t\, \alpha(u)\\ \vdots\\ \Rightarrow\end{array}}$$

Si la fórmula principal en verdadera, entonces por 7.8 podemos demostrar $\overset{0}{\Rightarrow} \bigwedge u \leq t\, \alpha(u)$ con una demostración formada únicamente por sentencias Δ_0, y tenemos la prueba alternativa

$$\cfrac{\begin{array}{c}\vdots\\ \overset{0}{\Rightarrow} \bigwedge u \leq t\, \alpha(u)\end{array}}{\begin{array}{c}\Gamma \overset{0}{\Rightarrow} \Delta,\ \bigwedge u \leq t\, \alpha(u)\\ \vdots\\ \Rightarrow\end{array}}$$

Como por debajo del secuente $\Gamma \overset{\mu}{\Rightarrow} \Delta,\ \bigwedge u \leq t\, \alpha(u)$ no hay inducciones (porque no hay reglas propias), podemos aplicar el teorema 7.16 para sustituir la subdemostración de este secuente por la alternativa que acabamos de construir (en cualquiera de los dos casos) y así obtenemos una demostración D' del secuente vacío con $o(D') \leq o(D)$, pero con una variable libre menos en su parte final.

B) Particularizador izquierda Este caso es completamente análogo al anterior. La fórmula principal tiene que ser una sentencia Δ_0, de modo que tenemos

$$\cfrac{\begin{array}{c}\vdots\\ y \leq t \wedge \alpha(y),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\end{array}}{\begin{array}{c}\bigvee u \leq t\, \alpha(u),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\\ \vdots\\ \Rightarrow\end{array}}$$

Si la fórmula principal es verdadera, entonces existe un $k \leq d(t)$ tal que $\alpha(\bar{k})$ es verdadera, luego podemos construir la demostración alternativa:

$$\cfrac{\cfrac{\begin{array}{cc}\vdots & \vdots\\ \overset{0}{\Rightarrow} \bar{k} \leq t \wedge \alpha(\bar{k}) & \bar{k} \leq t \wedge \alpha(\bar{k}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\end{array}}{\Gamma \overset{\mu}{\Rightarrow} \Delta}}{\begin{array}{c}\bigvee u \leq t\, \alpha(u),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\\ \vdots\\ \Rightarrow\end{array}}$$

mientras que si la fórmula principal es falsa, tenemos simplemente

$$\cfrac{\begin{array}{c}\vdots\\ \bigvee u \leq t\, \alpha(u) \overset{0}{\Rightarrow}\end{array}}{\begin{array}{c}\bigvee u \leq t\, \alpha(u),\, \Gamma \overset{0}{\Rightarrow} \Delta\\ \vdots\\ \Rightarrow\end{array}}$$

y llegamos igualmente a una demostración alternativa D' del secuente vacío con $o(D') \leq o(D)$ y con una variable libre menos en su parte final.

C) Inducción La regla será de la forma

$$\frac{\alpha(y),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(y')}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t)},$$

donde las fórmulas principales son sentencias.

Sea $m = d(t)$, de modo que el teorema 3.7 nos da una demostración de $\overset{0}{\Rightarrow} \bar{m} = t$ y a su vez de otra demostración E del secuente $\alpha(\bar{m}) \overset{q}{\Rightarrow} \alpha(t)$ en la que no se usan inducciones ni cortes esenciales, lo que implica obviamente que $q = o(E)$ es un número natural.

Observemos también que una demostración sin cortes esenciales de un secuente formado por fórmulas Σ_1 tiene que constar únicamente de fórmulas Σ_1, pues, tal y como razonábamos en la prueba del teorema 3.21, si una fórmula no es de tipo Σ_1, sus descendientes tampoco pueden serlo y, como ninguno puede eliminarse en un corte inesencial, si en E apareciera una fórmula no Σ_n, tendría que haber también una en el secuente final, y no es el caso.

Llamemos S al secuente superior de la regla de inducción y S_0 al inferior. Si llamamos D_0 a la subdemostración de D formada por los secuentes situados sobre S, sucede que la variable y no se usa como variable propia en D_0 (pues por la regularidad de D sólo se usa como variable propia una vez, y es en la inferencia S/S_0), luego el teorema 3.11 nos da que, para todo número natural n, al sustituir y por $\bar{n}$ en D_0 obtenemos una demostración $D_0(\bar{n})$ del secuente

$$\alpha(\bar{n}), \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\overline{n+1})$$

(notemos que y no puede aparecer en Γ o en Δ). Ahora encadenamos así las demostraciones $D_0(\bar{n})$:

$$\dfrac{\dfrac{\begin{matrix} D_0(\bar{0}) \\ \vdots \\ \alpha(\bar{0}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\bar{1}) \end{matrix} \qquad \begin{matrix} D_0(\bar{1}) \\ \vdots \\ \alpha(\bar{1}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\bar{2}) \end{matrix}}{\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{2})} \qquad \begin{matrix} D_0(\bar{2}) \\ \vdots \\ \alpha(\bar{2}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\bar{3}) \end{matrix}}{\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{3})}$$

hasta llegar a una demostración del secuente

$$\alpha(\bar{0}), \Gamma \Rightarrow \Delta,\, \alpha(\bar{m})$$

y, a su vez, combinando la prueba con E obtenemos:

$$\dfrac{\begin{matrix} \vdots \\ \alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{m}) \end{matrix} \qquad \begin{matrix} E \\ \vdots \\ \alpha(\bar{m}) \Rightarrow \alpha(t) \end{matrix}}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t)}$$

En suma, obtenemos una demostración alternativa D_0' del secuente S_0. Al sustituir D_0 por D_0' obtenemos una demostración D' alternativa a D en la que hemos eliminado la inducción que estamos considerando. Vamos a calcular su ordinal.

En primer lugar observamos que el ordinal en D' de los secuentes

$$\alpha(\bar{n}), \Gamma \Rightarrow \Delta,\, \alpha(\overline{n+1})$$

sigue siendo μ (pues ahora el ordinal de un secuente sólo depende de los secuentes que tiene por encima). A su vez:

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{2}); D') = \mu\#\mu,$$

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{3}); D') = \mu\#\mu\#\mu$$

y así:

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{m}); D') = \mu * m,$$

donde $\mu * m = \mu\# \cdots \#\mu$ (m veces), de donde, a su vez,

$$o(S_0; D') = \mu * m + q.$$

Ahora distinguimos dos casos: si $\mu < \omega$, entonces

$$o(S_0; D') = \mu * m + q < \omega = o(S_0; D).$$

Por otra parte, si $\mu = \omega^n + \cdots$, entonces

$$o(S_0; D') = \mu * m + q = \omega^n + \cdots < \omega^{n+1} = o(S_0; D).$$

El teorema 7.16 nos da entonces que $o(D') < o(D)$.

Ahora podemos razonar así:

Si la parte final de D contiene una regla de inducción, aplicando repetidamente los casos anteriores a una regla propia que no tenga otra por debajo, o bien tras un número finito de aplicaciones de los casos A) y B) llegamos a una demostración D' con $o(D') \leq o(D)$ y sin variables libres en su parte final (pues en cada paso eliminamos una), o bien se da el caso C), en cuyo caso obtenemos una demostración con $o(D') < o(D)$.

Por lo tanto, a partir de aquí podemos suponer que la parte final de D está formada exclusivamente por sentencias, lo que en particular implica que en ella no hay reglas propias (y en particular no hay inducciones).

Observemos ahora que si una sentencia α no es Δ_0 y aparece en la parte final de D, no puede ser la fórmula auxiliar de ninguna regla de inferencia salvo la de corte, pues las reglas de inferencia lógicas darían lugar a una fórmula principal que no sería de tipo Σ_1. En principio, α podría ser una fórmula auxiliar de una regla de inducción, pero estamos suponiendo que no hay inducciones en la parte final. Por lo tanto, los descendientes de α tienen que ser idénticos a α.

• Supongamos ahora que la parte final de D contiene un axioma lógico $\alpha \Rightarrow \alpha$ cuya fórmula α no es Δ_0.

Según acabamos de razonar, los descendientes de α tienen que ser idénticos a α y, como el secuente final es vacío, cada una de las dos fórmulas α tiene un descendiente que se elimina en un corte. Supongamos que en primer lugar desaparece un descendiente del antecedente, así:

$$\begin{array}{c}
\begin{array}{cc} D_0 & \alpha \Rightarrow \alpha \\ \vdots & \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta, \alpha & \alpha, \Gamma' \overset{\nu}{\Rightarrow} \Delta' \end{array} \\ \hline
\Gamma, \Gamma' \Rightarrow \Delta, \Delta' \\
\vdots \\
\Rightarrow
\end{array}$$

donde Δ' contiene un descendiente del α situado en el consecuente del axioma.

Entonces podemos simplificar D hasta una demostración D' de la forma

$$\begin{array}{c} D_0 \\ \vdots \\ \dfrac{\Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha}{\Gamma,\, \Gamma' \stackrel{\mu}{\Rightarrow} \Delta,\, \Delta'} \\ \vdots \\ \Rightarrow \end{array}$$

Llamemos S al secuente $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'$. Como el ordinal de un secuente depende únicamente de los que tiene por encima:

$$\mu = o(\Gamma \Rightarrow \Delta, \alpha; D) = o(\Gamma \Rightarrow \Delta, \alpha; D') = o(S; D').$$

A su vez, si los secuentes superiores del corte de D tienen ordinales μ y ν en D, entonces

$$o(S; D) = \mu \# \nu \geq \mu = o(S; D').$$

El teorema 7.16 nos da entonces que $o(D') \leq o(D)$. Si en D se corta antes la fórmula α del consecuente del axioma, un razonamiento totalmente análogo nos lleva a la misma conclusión.

Como en cada paso se elimina un axioma, aplicando este proceso un número finito de veces, tenemos que llegar finalmente a otra demostración con ordinal menor o igual en cuya parte final todos los secuentes iniciales constan únicamente de fórmulas Δ_0 (ya que los axiomas del igualador y los axiomas propios constan únicamente de fórmulas Δ_0 en cualquier caso).

En resumen, en este punto podemos suponer que los secuentes iniciales de la parte final de D constan únicamente de fórmulas Δ_0.

• Supongamos ahora que la parte final de D contiene una regla de debilitación que introduce una fórmula α que no es Δ_0 y tomemos una que no tenga otra por debajo. Supongamos que es una regla izquierda, pero el caso de la regla derecha se trata análogamente. Como ya hemos explicado, los descendientes de α tienen que ser idénticos a α y, como el secuente final es vacío, uno de ellos tiene que eliminarse posteriormente con un corte, por lo que D tiene que tener esta estructura:

$$\begin{array}{c} \begin{array}{cc} & \vdots \\ & \dfrac{\Gamma'' \Rightarrow \Delta''}{\alpha,\, \Gamma'' \Rightarrow \Delta''} \\ \vdots & \vdots \\ \Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha & \alpha,\, \Gamma' \stackrel{\nu}{\Rightarrow} \Delta' \end{array} \\ \hline \Gamma,\, \Gamma' \stackrel{\xi}{\Rightarrow} \Delta,\, \Delta' \\ \vdots \\ \Rightarrow \end{array}$$

Distinguimos dos posibilidades:

A) Si α figura en el antecedente de algún secuente que se combina mediante un corte o una regla izquierda del disyuntor con otro situado bajo $\alpha,\, \Gamma'' \Rightarrow \Delta''$, entonces α "aparece" aunque no usemos la regla de debilitación que la introduce en D, con lo que podemos considerar demostración alternativa D':

$$\dfrac{\begin{array}{cc} & \vdots \\ & \Gamma'' \Rightarrow \Delta'' \\ \vdots & \vdots \\ \Gamma \Rightarrow \Delta,\, \alpha & \alpha,\, \Gamma' \Rightarrow \Delta' \end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$
$$\begin{array}{c} \vdots \\ \Rightarrow \end{array}$$

que tiene el mismo ordinal, pero una debilitación menos en su parte final.

B) Si α no figura el en antecedente de ningún secuente que se combina con alguno de los secuentes situados bajo $\alpha,\, \Gamma'' \Rightarrow \Delta''$, entonces todas las reglas intermedias siguen siendo válidas si eliminamos α de los secuentes situados bajo $\alpha,\, \Gamma'' \Rightarrow \Delta''$ (pues α es siempre una fórmula colateral y no hay debilitaciones que puedan volverla a introducir), con lo que ahora obtenemos la demostración alternativa D':

$$\dfrac{\begin{array}{c} \vdots \\ \Gamma'' \Rightarrow \Delta'' \\ \vdots \\ \Gamma' \overset{\nu}{\Rightarrow} \Delta' \end{array}}{\Gamma,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta,\, \Delta'}$$
$$\begin{array}{c} \vdots \\ \Rightarrow \end{array}$$

Es claro que $\nu = o(\alpha,\, \Gamma' \Rightarrow \Delta'; D) = o(\Gamma' \Rightarrow \Delta'; D')$, luego $\xi = \mu \# \nu \geq \nu$ y el teorema 7.16 nos da que $o(D') \leq o(D)$.

En cada paso del caso B) eliminamos una regla de debilitación de la parte final de las que introducen fórmulas no Δ_0, pero podemos introducir muchas otras al llegar a $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'$. No obstante el número total de secuentes iniciales de la demostración disminuye (y en el caso A no aumenta), por lo que tras un número finito de pasos llegaremos a una demostración en cuya parte final todas las fórmulas principales de las reglas de debilitación son de tipo Δ_0.

Así pues, podemos suponer que en la parte final de D los secuentes iniciales están formados por sentencias Δ_0, que las fórmulas principales de las reglas de debilitación implícitas son Δ_0 y que no hay reglas relevantes ni reglas propias. Si D coincidiera con su parte final, al no contener reglas relevantes, se trataría de una demostración del secuente vacío formada únicamente por sentencias Δ_0, lo cual contradice al teorema 7.5.

Por consiguiente, podemos aplicar el teorema 7.11, según el cual en la parte final de D hay un corte adecuado.

• Consideremos un corte adecuado en la parte final de D que no tenga ningún otro por debajo. La fórmula de corte tiene que ser de la forma $\bigvee u\, \alpha(u)$ o bien de la forma $\bigwedge u\, \alpha(u)$. Podemos suponer que se da el primer caso, pues el segundo se trata de forma totalmente análoga. Tenemos la estructura siguiente:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}}{\Gamma_1 \overset{\nu_1+1}{\Rightarrow} \Delta_1,\, \bigvee u\, \alpha(u)}}{\vdots}\!\!\!\!\!\!\!\!\;\;\Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\, \alpha(u) \qquad \dfrac{\dfrac{\vdots}{\alpha(y),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\, \alpha(u),\, \Gamma_1' \overset{\nu_2+1}{\Rightarrow} \Delta_1'} \;\vdots\; \bigvee u\, \alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'}{\begin{array}{c}\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\ \vdots \\ \Rightarrow\end{array}}$$

Como la demostración D es regular, el término t no puede contener ninguna variable propia usada en la subdemostración del secuente $\alpha(y),\, \Gamma_1' \Rightarrow \Delta_1'$, y la variable y no se usa como variable propia en dicha subdemostración, ni aparece en Γ_1' o Δ_1', luego podemos aplicar el teorema 3.11, según el cual, al sustituir y por t en toda la subdemostración obtenemos una demostración del secuente $\alpha(t),\, \Gamma_1' \Rightarrow \Delta_1'$.

Como $\alpha(t)$ es una sentencia Δ_0, el teorema 7.8 nos da que uno de los secuentes $\Rightarrow \alpha(t)$ o $\alpha(t) \Rightarrow$ es demostrable (mediante sentencias Δ_0) con una demostración de ordinal 0. Pongamos que el secuente en cuestión es, concretamente, $\Rightarrow \alpha(t)$. Consideramos la demostración alternativa:

$$\dfrac{\begin{array}{c}\vdots \\ \dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \overset{\nu_1+1}{\Rightarrow} \Delta_1,\, \bigvee u\, \alpha(u)} \\ \vdots \\ \Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\, \alpha(u)\end{array} \quad (h_1) \quad \begin{array}{c}\dfrac{\dfrac{\begin{array}{cc}\vdots & \vdots \\ \overset{0}{\Rightarrow} \alpha(t) & \alpha(t),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'\end{array}}{\Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\, \alpha(u),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'} \\ \vdots \\ \bigvee u\, \alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'\end{array}}{\begin{array}{c}\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\ \vdots \\ \Rightarrow\end{array}}$$

Puesto que

$$o(\bigvee u\, \alpha(u),\, \Gamma_1' \Rightarrow \Delta_1'; D') = \nu_2 < \nu_2 + 1 = o(\bigvee u\, \alpha(u),\, \Gamma_1' \Rightarrow \Delta_1'; D),$$

el teorema 7.16 nos da que $o(D') < o(D)$. ■

Por consiguiente:

Teorema 7.13 *Si* $\mathrm{I}\Sigma_1$ *es contradictoria, existe una sucesión infinita estrictamente decreciente de ordinales menores que* ω^ω.

Por lo tanto, si la inducción transfinita vale hasta ω^ω, podemos asegurar que $\mathrm{I}\Sigma_1$ es consistente.

7.3 La consistencia de $\mathrm{I}\Sigma_n$

En esta sección vamos a combinar las ideas de las dos secciones precedentes para probar que la inducción transfinita hasta $\omega^{(n+1)}$ implica la consistencia de $\mathrm{I}\Sigma_n$. Más aún, vamos a obtener un resultado que no se aplicará únicamente a hipotéticas demostraciones del secuente vacío, sino a demostraciones "reales", del que podremos extraer otras consecuencias de interés.

Vamos a tratar con demostraciones en $\mathrm{I}\Sigma_n$ de las que supondremos tácitamente que constan únicamente de fórmulas de tipo Σ_n o Π_n.

Empezamos por redefinir los conceptos de grado y altura:

Definición 7.14 Definimos el *grado* de una fórmula Σ_n o Π_n como una unidad menos que el número de cuantificadores no acotados que contiene, si es que contiene al menos uno, y como 0 si la fórmula es de tipo Δ_0.

De este modo, las fórmulas de grado 0 son ahora las de tipo Σ_1 o Π_1.

El *grado* de un corte es el grado de la fórmula de corte. El *grado* de una inducción es el grado de la fórmula de inducción.

La *altura* $h(S; D)$ de un secuente S en una demostración D es el máximo de los grados de los cortes e inducciones que hay bajo S. Si no hay ninguno, la altura es 0. En particular, el secuente final de una demostración siempre tiene altura 0.

Como en la sección anterior, llamaremos reglas de inferencia *relevantes* en una demostración D a las reglas de los cuantificadores cuya fórmula principal no sea Δ_0 o, lo que es lo mismo, las reglas que introducen cuantificadores no acotados.

Y a continuación introducimos una tercera forma de asociar ordinales a demostraciones, que combina las dos definiciones anteriores:

A cada secuente S en una demostración D en $\mathrm{I}\Sigma_n$ le asociamos un ordinal $o(S; D)$ según el criterio siguiente:

1. Si S es un secuente inicial de D, entonces
$$o(S; D) = \begin{cases} 0 & \text{si } S \text{ todas sus fórmulas tienen grado nulo,} \\ 1 & \text{en caso contrario.} \end{cases}$$

2. Si S es el secuente inferior de una regla de debilitación cuyo secuente superior es S_1 y cuya fórmula principal es α, entonces
$$o(S; D) = \begin{cases} o(S_1; D) & \text{si } \alpha \text{ tiene grado } 0, \\ o(S_1; D) + 1 & \text{si } \alpha \text{ tiene grado } > 0. \end{cases}$$

3. Si S es el secuente inferior de una regla lógica irrelevante con un único secuente superior S_1, entonces $o(S; D) = o(S_1; D)$.

4. Si S es el secuente inferior de una regla izquierda del disyuntor con secuentes superiores S_1 y S_2, entonces $o(S;D) = o(S_1;D)\#o(S_2;D)$.

5. Si S es el secuente inferior de una regla de inferencia relevante con secuente superior S_1, entonces $o(S;D) = o(S_1;D) + 2$.

6. Si S es el secuente inferior de una regla de corte con secuentes superiores S_1 y S_2, entonces $o(S;D) = \omega_{h_1-h_0}(\mu_1\#\mu_2)$, donde
$$h_1 = h(S_1;D) = h(S_2;D), \quad h_0 = h(S;D), \quad \mu_i = o(S_i;D).$$

7. Si S es el secuente inferior de una inducción con secuente superior S', entonces
$$o(S;D) = \begin{cases} \omega^{(h_1-h_0+1)} & \text{si } o(S';D) = 0, \\ \omega_{h_1-h_0+1}(\eta+1) & \text{si } o(S';D) = \omega^\eta + \cdots, \end{cases}$$
donde $h_1 = h(S';D)$, $h_0 = h(S;D)$.

El ordinal $o(D)$ de una demostración D es el ordinal de su secuente final.

Ejemplo En la demostración del ejemplo de la página 68 todas las fórmulas son Σ_1, luego todas tienen grado 0, luego todos los secuentes tienen altura 0. Esto hace que todos los secuentes tengan ordinal 0 hasta que se aplican las reglas del particularizador, al final:

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{0}}{0}}{2} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\\ 0\end{matrix}}{2}\quad\dfrac{\begin{matrix}\vdots\\ 0\end{matrix}}{2}}{4}}{6}}{\omega}}{\omega+2}$$

■

Observación Si un secuente tiene ordinal 0, necesariamente sus fórmulas son todas de grado 0, pues los secuentes iniciales sólo tienen fórmulas Δ_0, y cualquier regla que introduce una fórmula de grado no nulo incrementa el ordinal en al menos una unidad.

Más aún, para cada fórmula α del secuente final de grado no nulo, podemos considerar sus fibras de ascendientes directos, que tienen que acabar necesariamente en un secuente inicial de ordinal 1, en la fórmula principal de una regla relevante o en la fórmula principal de una regla de debilitación. Para cada fibra ϕ, definimos $n_\phi = 1$ en los dos primeros casos y $n_\phi = 2$ en el segundo.

Definimos n_α como el mayor de los números n_ϕ (entendiendo que si α aparece tanto en el antecedente como en el consecuente del secuente final, entonces tenemos dos valores distintos de n_α) y llamemos N_D a la suma de los números n_α, para todas las fórmulas α de grado no nulo del secuente final de D. Es fácil ver que $o(D) \geq N_D$.

En particular, $o(D)$ es mayor o igual que el número de fórmulas de grado no nulo en su secuente final. ■

Observemos en primer lugar que los ordinales obtenidos por esta asignación están acotados:

Teorema 7.15 *Si D es una demostración en $\mathrm{I}\Sigma_n$ formada únicamente por fórmulas de Σ_n o Π_n, entonces $o(D) < \omega^{(n+1)}$.*

DEMOSTRACIÓN: Definimos el *rango* de un ordinal no nulo μ como el único número natural $r = r(\mu)$ tal que $\omega^{(r)} \leq \mu < \omega^{(r+1)}$, mientras que $r(0) = -1$. Tenemos que probar que el rango de $o(D)$ es $\leq n$.

Es claro que las únicas reglas de inferencia en las que el secuente inferior puede tener ordinal de rango estrictamente mayor que los de sus secuentes superiores son los cortes y las inducciones.

En el caso de un corte, tenemos que

$$r(\omega_{h_1-h_0}(\mu\#\nu)) = r(\mu\#\nu) + h_1 - h_0 = \max\{r(\mu), r(\nu)\} + h_1 - h_0.$$

Consideremos ahora una regla de inducción cuyo secuente superior tenga ordinal $\mu = \omega^{\eta_1} + \cdots$. Hay dos posibilidades:

- Si $\eta_1 = 0$, entonces μ es un número natural no nulo, luego $r(\mu) = 0$. Por otra parte, $r(\omega_{h_1-h_0}(\eta_1 + 1)) = r(\omega^{(h_1-h_0)}) = h_1 - h_0$.
- Si $\eta_1 > 0$, se cumple que $r(\eta_1+1) = r(\mu)-1$, pues si $r = r(\eta_1+1) = r(\eta_1)$, tenemos que $\omega^{(r)} \leq \eta_1 < \omega^{(r+1)}$, luego

$$\omega^{(r+1)} = \omega^{\omega^{(r)}} \leq \omega^{\eta_1} + \cdots < \omega^{\omega^{(r+1)}} = \omega^{(r+2)}.$$

Por lo tanto, $r(\omega_{h_1-h_0+1}(\eta_1 + 1)) = r(\mu) + h_1 - h_0$.

En cambio, si el secuente superior tiene ordinal $\mu = 0$, el rango del secuente inferior es $h_1 - h_0 + 1$ y el del secuente superior es -1, luego en general, para una inducción S'/S, tenemos que

$$r(o(S; D)) - r(o(S'; D)) = \begin{cases} h_1 - h_0 + 2 & \text{si } r(o(S'; D)) = -1, \\ h_1 - h_0 & \text{si } r(o(S'; D)) \geq 0. \end{cases}$$

Ahora formamos un hilo en D partiendo del secuente final y ascendiendo con el criterio de que cada vez que lleguemos al secuente inferior de una regla de corte pasemos al secuente superior con mayor ordinal. Si el hilo es

$$S_0 - S_2 - \cdots - S_p,$$

donde S_0 es un secuente inicial de D y S_p es el secuente final, entonces la sucesión de alturas $h_i = h(S_i)$ es decreciente:

$$n - 1 \geq h_0 \geq h_1 \geq \cdots \geq h_p = 0,$$

y los rangos $r_i = r(o(S_i; D))$ son crecientes:

$$-1 = r_0 \leq r_1 \leq \cdots \leq r_p = r(o(D)),$$

y, según hemos visto,

$$r_i - r_{i-1} \leq h_{i-1} - h_i,$$

salvo si $r_{i-1} = -1$, en cuyo caso puede ser $r_i - r_{i-1} \leq h_{i-1} - h_i + 2$, pero esto hace que $r_i \geq 0$, por lo que este caso se puede dar a lo sumo una vez. Por lo tanto, sumando para $i = 1, \ldots p$, resulta que

$$r(o(D)) + 1 \leq h_0 - 0 + 2,$$

donde el $+2$ final es por la posibilidad excepcional de que en el hilo haya una regla de inducción con secuente superior de rango 0. En definitiva llegamos a que $r(o(D)) \leq h_0 + 1 \leq n$. ■

Es inmediato comprobar que el teorema 7.8 sigue siendo válido para esta nueva asignación de ordinales. También podemos probar una versión de los teoremas 7.2 o 7.9 modificando ligeramente los cálculos de la demostración:

Teorema 7.16 *Sea D una demostración que contenga un secuente S_1 de modo que no haya ninguna inducción bajo S_1. Sea D_1 la subdemostración de D formada por los secuentes situados por encima de S_1 y sea D_1' otra demostración de S_1 tal que $o(S_1; D_1') < o(S_1; D)$ (resp. $o(S_1; D_1') \leq o(S_1; D)$). Sea D' la demostración que resulta de reemplazar D_1 por D_1' en D. Entonces $o(D') < o(D)$ (resp. $o(D') \leq o(D)$).*

Demostración: Vamos a probar el teorema en el caso de la desigualdad estricta. El otro caso se prueba sustituyendo en la demostración todas las desigualdades estrictas por desigualdades no estrictas. Consideremos un hilo de D que pase por S_1 y vamos a probar que cada secuente S de dicho hilo situado por debajo de S_1 cumple $o(S; D') < o(S; D)$. Luego, basta aplicar esto al secuente final de ambas pruebas.

Por hipótesis se cumple cuando $S = S_1$, y basta probar que si un secuente S' cumple la desigualdad, lo mismo sucede con el secuente S que está inmediatamente por debajo en el hilo. Esto se comprueba regla a regla. Si la regla que pasa de S' a S es de debilitación, si la fórmula principal es de grado 0, tenemos

$$o(S; D') = o(S'; D') < o(S'; D) = o(S; D).$$

y en caso contrario

$$o(S; D') = o(S'; D') + 1 < o(S'; D) + 1 = o(S; D).$$

Si la regla que pasa de S' a S es una regla lógica irrelevante y con un único secuente superior, tenemos que

$$o(S; D') = o(S'; D') < o(S'; D) = o(S; D).$$

Si se trata de la regla izquierda del disyuntor y sus secuentes superiores son S' y S'', entonces $o(S''; D') = o(S''; D)$ y

$$o(S; D') = o(S'; D') \# o(S''; D') < o(S'; D) \# o(S''; D) = o(S; D).$$

Si se trata de una regla relevante tenemos que

$$o(S;D') = o(S';D') + 2 < o(S';D) + 2 = o(S;D).$$

Si la inferencia es un corte, entonces las alturas h_0 y h_1 son las mismas en D y en D', luego, llamando S'' al segundo secuente superior, entonces tenemos que $o(S'';D') = o(S'';D)$ y

$$\begin{aligned} o(S;D') &= \omega_{h_1-h_0}(o(S';D')\#o(S'';D')) \\ &< \omega_{h_1-h_0}(o(S';D)\#o(S'';D)) = o(S;D). \end{aligned}$$ ■

La definición de la parte final de una demostración es la misma que la que hemos empleado en la sección anterior:

Definición 7.17 La *parte final* de una demostración está formada por los secuentes que no tienen por debajo ninguna regla de inferencia relevante implícita.

Lo mismo sucede con la definición de corte adecuado:

Un corte en una demostración en $\mathrm{I}\Sigma_n$ es *sustancial* si la fórmula de corte no es Δ_0. El corte es *adecuado* si además las dos fórmulas de corte tienen un ascendiente que es la fórmula principal de una regla fronteriza.

El teorema 7.11 lo hemos enunciado con la generalidad suficiente como para que sea aplicable en el contexto de esta sección.

Ya estamos en condiciones de demostrar la consistencia de $\mathrm{I}\Sigma_n$, pero, en lugar de partir de una hipotética demostración del secuente vacío, vamos a considerar en principio una situación más general que sí que puede darse y de la que extraeremos consecuencias de interés.

Vamos a considerar una demostración en $\mathrm{I}\Sigma_n$ de un secuente S^* cuyo antecedente consta únicamente de sentencias Π_1 y cuyo consecuente consta únicamente de sentencias Σ_1. Notemos que esto no excluye que S^* sea el secuente vacío.

Como el conjunto de fórmulas que son Σ_n o Π_n es cerrado para sustitución y para subfórmulas, el teorema 3.22 nos asegura que S^* admite una demostración en $\mathrm{I}\Sigma_n$ formada exclusivamente por fórmulas de tipo Σ_n o Π_n.

Como en la sección precedente, llamamos reglas de inferencia propias a la regla derecha del generalizador, la regla izquierda del particularizador y la regla de inducción.

Teorema 7.18 *Sea D una demostración en $\mathrm{I}\Sigma_n$ que conste únicamente de fórmulas Σ_n o Π_n y cuyo secuente final S^* tenga únicamente sentencias Π_1 en su antecedente y sentencias Σ_1 en su consecuente. Entonces existe otra demostración D' de S^*, formada también por fórmulas Σ_n o Π_n, tal que $o(D') \leq o(D)$ y, si se da la igualdad, D' no tiene reglas de inferencia propias ni cortes sustanciales.*

Demostración: El teorema 3.13 nos permite transformar D en una demostración regular sin alterar su ordinal. Alternativamente, podemos suponer que la demostración D es regular.

• Si en la parte final de D aparece una variable libre que no es la variable propia de ninguna regla de inferencia, por el teorema 3.11 podemos sustituirla por la constante 0, y obtenemos así una demostración (del mismo secuente S^*, pues éste no contiene variables libres) con el mismo ordinal.

Repitiendo este proceso un número finito de veces podemos suponer que en la parte final de D no hay ninguna variable libre que no esté usada como variable propia de una (única) regla de inferencia.

• Supongamos que la parte final de D contiene una regla propia y consideremos una que no tenga ninguna otra por debajo. Esto implica que todos los secuentes situados bajo ella constan únicamente de sentencias, pues, como la demostración es regular, cada variable libre es la variable propia de una regla de inferencia y sólo aparece por encima de ella. Distinguimos tres casos según el tipo de regla:

A) Generalizador derecha La fórmula principal tiene que ser una sentencia Δ_0 (o se trataría de una regla relevante), luego será de la forma:

$$\begin{array}{c} \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, y \leq t \to \alpha(y) \\ \hline \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u) \\ \vdots \\ S^* \end{array}$$

(Las letras sobre las flechas de los secuentes denotaran siempre el ordinal del secuente.) Si la fórmula principal es falsa, existe un $k \leq d(t)$ tal que $\alpha(\bar{k})$ es falsa, pero entonces $\bar{k} \leq t \to \alpha(\bar{k})$ es falsa, y por 7.8 podemos demostrar el secuente $\bar{k} \leq t \to \alpha(\bar{k}) \overset{0}{\Rightarrow}$ de modo que la prueba contiene únicamente sentencias Δ_0. Por otra parte, como y no se usa como variable propia en la demostración del secuente superior, el teorema 3.11 nos da una demostración del secuente

$$\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bar{k} \leq t \to \alpha(\bar{k}).$$

Consideramos la demostración alternativa:

$$\begin{array}{c} \begin{array}{cc} \vdots & \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bar{k} \leq t \to \alpha(\bar{k}) & \bar{k} \leq t \to \alpha(\bar{k}) \overset{0}{\Rightarrow} \end{array} \\ \hline \Gamma \overset{\mu}{\Rightarrow} \Delta \\ \hline \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u) \\ \vdots \\ S^* \end{array}$$

Si la fórmula principal en verdadera, entonces por 7.8 podemos demostrar $\stackrel{0}{\Rightarrow} \bigwedge u \leq t\, \alpha(u)$ con una demostración formada únicamente por sentencias Δ_0, y tenemos la prueba alternativa

$$\begin{array}{c} \vdots \\ \stackrel{0}{\Rightarrow} \bigwedge u \leq t\, \alpha(u) \\ \hline \Gamma \Rightarrow \Delta, \bigwedge u \leq t\, \alpha(u) \\ \vdots \\ S^* \end{array}$$

El ordinal del último secuente es igual al número de fórmulas de grado no nulo que hay en Γ y Δ, que es menor o igual que μ.

Como por debajo del secuente $\Gamma \stackrel{\mu}{\Rightarrow} \Delta, \bigwedge u \leq t\, \alpha(u)$ no hay inducciones (no hay reglas propias, en general), podemos aplicar el teorema 7.16 para sustituir la subdemostración de este secuente por la alternativa que acabamos de construir y así obtenemos una demostración D' del secuente S^* con $o(D') \leq o(D)$, pero con una variable libre menos en su parte final.

B) Particularizador izquierda Este caso es completamente análogo al anterior. La fórmula principal tiene que ser una sentencia Δ_0, de modo que tenemos

$$\begin{array}{c} \vdots \\ y \leq t \wedge \alpha(y), \Gamma \stackrel{\mu}{\Rightarrow} \Delta \\ \hline \bigvee u \leq t\, \alpha(u), \Gamma \stackrel{\mu}{\Rightarrow} \Delta \\ \vdots \\ S^* \end{array}$$

Si la fórmula principal es verdadera, entonces existe un $k \leq d(t)$ tal que $\alpha(\bar{k})$ es verdadera, luego podemos construir la demostración alternativa:

$$\begin{array}{c} \begin{array}{cc} \vdots & \vdots \\ \stackrel{0}{\Rightarrow} \bar{k} \leq t \wedge \alpha(\bar{k}) & \bar{k} \leq t \wedge \alpha(\bar{k}), \Gamma \stackrel{\mu}{\Rightarrow} \Delta \end{array} \\ \hline \Gamma \stackrel{\mu}{\Rightarrow} \Delta \\ \hline \bigvee u \leq t\, \alpha(u), \Gamma \stackrel{\mu}{\Rightarrow} \Delta \\ \vdots \\ S^* \end{array}$$

mientras que si la fórmula principal es falsa, tenemos simplemente

$$\begin{array}{c} \vdots \\ \bigvee u \leq t\, \alpha(u) \stackrel{0}{\Rightarrow} \\ \hline \bigvee u \leq t\, \alpha(u), \Gamma \Rightarrow \Delta \\ \vdots \\ S^* \end{array}$$

y llegamos igualmente a una demostración alternativa D' del secuente S^* con $o(D') \leq o(D)$ y con una variable libre menos en su parte final.

C) Inducción La regla será de la forma

$$\frac{\alpha(y),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(y') \quad (h_1)}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t) \quad (h_0)},$$

donde las fórmulas principales son sentencias.

Sea $m = d(t)$, de modo que el teorema 3.7 nos da una demostración de $\overset{0}{\Rightarrow} \bar{m} = t$ y a su vez de otra demostración E del secuente $\alpha(\bar{m}) \overset{q}{\Rightarrow} \alpha(t)$ en la que no se usan inducciones ni cortes esenciales. Como en un corte inesencial la altura de los secuentes superiores coincide con la del secuente inferior, se comprueba inmediatamente que $q = o(E)$ es un número natural.

Observemos también que una demostración sin cortes esenciales de un secuente formado por fórmulas Σ_n tiene que constar únicamente de fórmulas Σ_n, pues, tal y como razonábamos en la prueba del teorema 3.21, si una fórmula no es de tipo Σ_n, sus descendientes tampoco pueden serlo y, como ninguno puede eliminarse en un corte inesencial, si en E apareciera una fórmula no Σ_n, tendría que haber también una en el secuente final, y no es el caso.

Llamemos S al secuente superior de la regla de inducción y S_0 al inferior. Si llamamos D_0 a la subdemostración de D formada por los secuentes situados sobre S, sucede que la variable y no se usa como variable propia en D_0 (pues por la regularidad de D sólo se usa como variable propia una vez, y es en la inferencia S/S_0), luego el teorema 3.11 nos da que, para todo número natural n, al sustituir y por $\bar{n}$ en D_0 obtenemos una demostración $D_0(\bar{n})$ del secuente

$$\alpha(\bar{n}), \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\overline{n+1})$$

(notemos que y no puede aparecer en Γ o en Δ). Ahora encadenamos así las demostraciones $D_0(\bar{n})$:

$$\cfrac{\cfrac{\begin{array}{c} D_0(\bar{0}) \\ \vdots \\ \alpha(\bar{0}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\bar{1}) \end{array} \qquad \begin{array}{c} D_0(\bar{1}) \\ \vdots \\ \alpha(\bar{1}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\bar{2}) \end{array}}{\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{2})} \qquad \begin{array}{c} D_0(\bar{2}) \\ \vdots \\ \alpha(\bar{2}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(\bar{3}) \end{array}}{\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{3})}$$

hasta llegar a una demostración del secuente

$$\alpha(\bar{0}), \Gamma \Rightarrow \Delta,\, \alpha(\bar{m})$$

y, a su vez, combinando la prueba con E obtenemos:

$$\frac{\begin{array}{c} \vdots \\ \alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{m}) \end{array} \qquad \begin{array}{c} E \\ \vdots \\ \alpha(\bar{m}) \Rightarrow \alpha(t) \end{array}}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t)}$$

En suma, obtenemos una demostración alternativa D_0' del secuente S_0. Al sustituir D_0 por D_0' obtenemos una demostración D' alternativa a D en la que hemos eliminado la inducción que estamos considerando. Vamos a calcular su ordinal.

En primer lugar observamos que S tiene altura h_1 en D, lo que significa que h_1 es el máximo de los grados de los cortes situados bajo S y del grado de la fórmula de inducción $\alpha(y)$. Pero todas las fórmulas $\alpha(\bar{n})$ tienen el mismo grado que $\alpha(y)$, luego todos los cortes situados en D' entre un secuente

$$\alpha(\bar{n}), \Gamma \Rightarrow \Delta,\, \alpha(\overline{n+1})$$

y el secuente $\alpha(0)$, $\Gamma \Rightarrow \Delta$, $\alpha(t)$ tienen el grado de $\alpha(y)$, lo que se traduce en que las alturas de los cortes e inducciones contenidos en $D_0(\bar{n})$ como parte de D' son las mismas que las que tienen en D_0 como parte de D, luego el ordinal en D' de los secuentes

$$\alpha(\bar{n}), \Gamma \Rightarrow \Delta,\, \alpha(\overline{n+1})$$

sigue siendo μ. Además, todos los cortes que combinan estos secuentes en D_0' están formados por secuentes de altura h_1, por lo que el ordinal del secuente inferior cada corte es la suma formal de los de los secuentes superiores. Concretamente:

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{2}); D') = \mu\#\mu,$$

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{3}); D') = \mu\#\mu\#\mu$$

y así:

$$o(\alpha(\bar{0}),\, \Gamma \Rightarrow \Delta,\, \alpha(\bar{m}); D') = \mu * m,$$

donde $\mu * m = \mu\# \cdots \#\mu$ (m veces).

Por último, en el último corte de D_0', los secuentes superiores tienen altura h_1 en D' y el secuente inferior tiene la misma altura h_0 que en D, luego

$$o(S_0; D') = \omega_{h_1-h_0}(\mu * m + q).$$

Ahora distinguimos dos casos: si $\mu = \omega^\eta + \cdots$, entonces

$$\mu * m + q = \omega^\eta + \cdots < \omega^{\eta+1},$$

luego

$$o(S_0; D') = \omega_{h_1-h_0}(\mu * m + q) < \omega_{h_1-h_0}(\omega^{\eta+1}) = \omega_{h_1-h_0+1}(\eta+1) = o(S_0; D).$$

Si, por el contrario, $\mu = 0$, igualmente

$$o(S_0; D') = \omega_{h_1-h_0}(q) < \omega^{(h_1-h_0+1)} = o(S_0; D).$$

El teorema 7.16 nos da entonces que $o(D') < o(D)$.

Ahora podemos razonar así:

Si la parte final de D contiene una regla de inducción, aplicando repetidamente los casos anteriores a una regla propia que no tenga otra por debajo, o bien tras un número finito de aplicaciones de los casos A) y B) llegamos a una demostración D' con $o(D') \leq o(D)$ y sin variables libres en su parte final (pues en cada paso eliminamos una), o bien se da el caso C), en cuyo caso obtenemos una demostración con $o(D') < o(D)$.

Por lo tanto, a partir de aquí podemos suponer que la parte final de D está formada exclusivamente por sentencias, lo que en particular implica que en ella no hay reglas propias (y, más en particular, no hay inducciones).

• Supongamos que la parte final de D contiene una regla de inferencia relevante.

Por definición, la parte final no contiene reglas de inferencia relevantes implícitas, luego la regla tiene que ser explícita. Por otra parte, no puede ser propia, luego tiene que ser una regla derecha del particularizador o una regla izquierda del generalizador. Supongamos el primer caso, pues el segundo es análogo. La demostración será de la forma:

$$\begin{array}{c}
\vdots \\
\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(t) \\ \hline
\Gamma \overset{\mu+2}{\Rightarrow} \Delta,\, \bigvee u\, \alpha(u) \\
\vdots \\
\Gamma' \overset{\nu}{\Rightarrow} \Delta',\, \bigvee u\, \alpha(u)
\end{array}$$

Como la regla es explícita, $\alpha(t)$ es una sentencia Δ_0, luego, según el teorema 7.8, podemos demostrar $\Rightarrow \alpha(t)$ o bien $\alpha(t) \Rightarrow$ con una demostración de ordinal 0 formada por sentencias Δ_0, por lo que no contiene reglas propias ni cortes sustanciales. En el primer caso una demostración alternativa D' es

$$\begin{array}{c}
\vdots \\
\overset{0}{\Rightarrow} \alpha(t) \\ \hline
\overset{2}{\Rightarrow} \bigvee u\, \alpha(u) \\ \hline
\Gamma' \Rightarrow \Delta',\, \bigvee u\, \alpha(u)
\end{array}$$

cuyo ordinal es una unidad más que el número de fórmulas de grado no nulo del secuente final, luego es $\leq o(D)$ y D' no contiene reglas propias ni cortes sustanciales.

En el segundo caso tomamos como D' la demostración

$$\begin{array}{c}
\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(t) \qquad \alpha(t) \overset{0}{\Rightarrow} \\ \hline
\Gamma \overset{\mu}{\Rightarrow} \Delta \\ \hline
\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigvee u\, \alpha(u) \\
\vdots \\
\Gamma' \overset{\nu'}{\Rightarrow} \Delta',\, \bigvee u\, \alpha(u)
\end{array}$$

Como hemos probado el secuente $\Gamma \Rightarrow \Delta, \bigvee u\, \alpha(u)$ con ordinal $\mu < \mu + 2$, el teorema 7.16 nos da que $o(D') < o(D)$. Tras un número finito de pasos, o bien llegamos a una demostración D' de ordinal menor, o bien a una sin reglas propias ni cortes sustanciales.

Así pues, a partir de aquí podemos suponer que D no contiene reglas relevantes en su parte final.

Observemos ahora que si una sentencia α no es Δ_0 y aparece en la parte final de D, no puede ser la fórmula auxiliar de ninguna regla de inferencia salvo la de corte, pues las reglas de inferencia lógicas distintas de las de los cuantificadores darían lugar a una fórmula principal que no sería de tipo Σ_n o Π_n, y una regla de un cuantificador que tuviera a α como fórmula auxiliar sería relevante, y no hay reglas relevantes en la parte final de D. En principio, α podría ser una fórmula auxiliar de una regla de inducción, pero estamos suponiendo que no hay inducciones en la parte final. Por lo tanto, los descendientes de α tienen que ser idénticos a α.

• Supongamos ahora que la parte final de D contiene un axioma lógico $\alpha \Rightarrow \alpha$ cuya fórmula α no es Δ_0.

Si α empieza por un particularizador, entonces la fórmula del antecedente se tiene que eliminar en un corte, pues de lo contrario llegaría al secuente final sin ser Σ_1. Igualmente, si α empieza por un generalizador, es un descendiente de la fórmula del consecuente la que tiene que eliminarse en un corte. En caso de que se eliminen las dos, consideramos la que se elimina primero. Pongamos que es la del antecedente, pues el caso contrario se trata análogamente. La situación es

$$\begin{array}{c}
\begin{array}{cc} D_0 & \alpha \Rightarrow \alpha \\ \vdots & \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha & \alpha,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta' \end{array} \\ \hline
\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\ \vdots \\ S^*
\end{array}$$

donde Δ' contiene un descendiente del α situado en el consecuente del axioma. Entonces podemos simplificar D hasta una demostración D' de la forma

$$\begin{array}{c}
D_0 \\ \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha \\ \hline
\Gamma,\, \Gamma' \overset{\mu'}{\Rightarrow} \Delta,\, \Delta' \\ \vdots \\ S^*
\end{array}$$

Llamemos S al secuente $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$. Si la fórmula α contenida en Δ se mantiene hasta S^*, entonces es una sentencia Σ_1, luego su grado es 0, por lo que al pasar de D a D' hemos eliminado un corte de altura 0, luego las alturas en D de todos los secuentes de la subdemostración D_0 que acaba en $\Gamma \Rightarrow \Delta$, α son las mismas que sus alturas en D'. Si, por el contrario, α se elimina en un corte posterior (situado en los últimos puntos suspensivos), entonces se trata de un corte del mismo grado que el que hemos eliminado, por lo que también en este caso las alturas de los secuentes de D_0 no se ven alteradas.

Por consiguiente, en ambos casos:

$$\mu = o(\Gamma \Rightarrow \Delta, \alpha; D) = o(\Gamma \Rightarrow \Delta, \alpha; D') = o(S; D').$$

Más aún, como la altura de los dos secuentes superiores del corte de D es la misma que la del secuente inferior, si los secuentes superiores tienen ordinales μ y ν en D, entonces

$$o(S; D) = \mu \# \nu \geq \mu' = o(S; D'),$$

pues μ' es μ más el número de fórmulas de grado no nulo en Γ' y Δ' menos 1 (pues no hace falta introducir α) y este número es $\leq \nu$.

El teorema 7.16 nos da entonces que $o(D') \leq o(D)$. Si en D se corta antes la fórmula α del consecuente del axioma, un razonamiento totalmente análogo nos lleva a la misma conclusión.

Como en cada paso se elimina un axioma, aplicando este proceso un número finito de veces, tenemos que llegar finalmente a otra demostración con ordinal menor o igual en cuya parte final todos los secuentes iniciales constan únicamente de fórmulas Δ_0 (ya que los axiomas del igualador y los axiomas propios constan únicamente de fórmulas Δ_0 en cualquier caso).

En resumen, en este punto podemos suponer que los secuentes iniciales de la parte final de D constan únicamente de fórmulas Δ_0.

• Supongamos ahora que la parte final de D contiene una regla de debilitación implícita que introduce una fórmula α que no es Δ_0 y tomemos una que no tenga otra por debajo. Supongamos que es una regla izquierda, pero el caso de la regla derecha se trata análogamente. Como ya hemos explicado, los descendientes de α tienen que ser idénticos a α. Que la regla sea implícita significa que la fórmula introducida tiene que eliminarse posteriormente con un corte, por lo que D tiene que tener esta estructura:

$$\begin{array}{c}
\begin{array}{cc}
 & \begin{array}{c} \vdots \\ \Gamma'' \Rightarrow \Delta'' \\ \hline \alpha,\, \Gamma'' \Rightarrow \Delta'' \end{array} \\
\vdots & \vdots \\
\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha \quad (h_1) & \alpha,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta'
\end{array} \\
\hline
\Gamma,\, \Gamma' \overset{\xi}{\Rightarrow} \Delta,\, \Delta' \ \ (h_0) \\
\vdots \\
S^*
\end{array}$$

Distinguimos dos posibilidades:

A) Si α figura en el antecedente de algún secuente que se combina mediante un corte o una regla izquierda del disyuntor con otro situado bajo α, $\Gamma'' \Rightarrow \Delta''$, entonces α "aparece" aunque no usemos la regla de debilitación que la introduce en D, con lo que podemos considerar demostración alternativa D':

$$\begin{array}{c}
\begin{array}{cc}
 & \vdots \\
 & \Gamma'' \Rightarrow \Delta'' \\
\vdots & \vdots \\
\Gamma \Rightarrow \Delta,\, \alpha & \alpha,\, \Gamma' \Rightarrow \Delta'
\end{array} \\
\hline
\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\
\vdots \\
S^*
\end{array}$$

que tiene el mismo ordinal, pero una debilitación menos en su parte final.

B) Si α no figura el en antecedente de ningún secuente que se combina con alguno de los secuentes situados bajo α, $\Gamma'' \Rightarrow \Delta''$, entonces todas las reglas intermedias siguen siendo válidas si eliminamos α de los secuentes situados bajo α, $\Gamma'' \Rightarrow \Delta''$ (pues α es siempre una fórmula colateral y no hay debilitaciones que puedan volverla a introducir), con lo que ahora obtenemos la demostración alternativa D':

$$\begin{array}{c}
\vdots \\
\Gamma'' \Rightarrow \Delta'' \\
\vdots \\
\Gamma' \overset{\nu'}{\Rightarrow} \Delta' \ (h_0) \\
\hline
\Gamma,\, \Gamma' \overset{\nu''}{\Rightarrow} \Delta,\, \Delta' \ (h_0) \\
\vdots \\
S^*
\end{array}$$

La altura h_0 del secuente $\Gamma, \Gamma' \Rightarrow \Delta, \Delta'$ es la misma en D y en D', pero al haber eliminado un corte, la altura de los secuentes situados sobre él puede cambiar. Sea S un secuente en D situado sobre $\alpha, \Gamma' \Rightarrow \Delta'$ y sea S' el secuente correspondiente en D'. Sea $h = h(S, D)$ y $h' = h(S', D')$. Claramente $h' \leq h$ y, más precisamente, vamos a ver que

$$\omega_{h-h'}(o(S; D)) \geq o(S'; D'). \tag{7.2}$$

Admitiendo esto, tenemos en particular que $\omega_{h_1-h_0}(\nu) \geq \nu'$ y distinguimos dos casos:

Si en Γ y Δ todas las fórmulas son de grado 0, entonces

$$\xi = \omega_{h_1-h_0}(\mu\#\nu) \geq \omega_{h_1-h_0}(\nu) \geq \nu' = \nu''.$$

Si, por el contrario, en Γ y Δ hay fórmulas de grado no nulo, entonces ν'' es igual a ν' más el número de tales fórmulas, luego $\nu'' \leq \mu\#\nu'$. Por lo tanto, teniendo en cuenta el teorema 6.9,

$$\xi = \omega_{h_1-h_0}(\mu\#\nu) \geq \omega_{h_1-h_0}(\mu)\#\omega_{h_1-h_0}(\nu) \geq \mu\#\omega_{h_1-h_0}(\nu) \geq \mu\#\nu' \geq \nu''.$$

El teorema 7.16 nos da que $o(D') \leq o(D)$.

En cada paso del caso B) eliminamos una debilitación implícita de la parte final de las que introducen fórmulas no Δ_0, pero podemos introducir muchas otras en el último paso de D'. No obstante, el número total de secuentes iniciales de la demostración disminuye (y en el caso A no aumenta), por lo que tras un número finito de pasos llegaremos a una demostración en cuya parte final todas las fórmulas principales de las reglas de debilitación implícitas son de tipo Δ_0.

Vamos a probar (7.2). Obviamente la relación es cierta cuando S es un secuente inicial, pues los dos ordinales son iguales, luego basta probar que si la cumplen los secuentes superiores de una regla de inferencia, también la cumple el secuente inferior. Al mismo tiempo demostraremos que si un secuente tiene ordinal 0 en D, también tiene ordinal 0 en D' (notemos que esto es cierto para los secuentes iniciales). Distinguimos todos los casos posibles:

1. En el caso de una regla de debilitación S/S_0, se cumple que ambos secuentes tienen la misma altura h y los correspondientes S'/S_0' en D' también tienen la misma altura h'. Según si la fórmula principal tiene o no grado 0, el cálculo será

$$\omega_{h-h'}(o(S_0; D)) = \omega_{h-h'}(o(S; D)) \geq o(S'; D') = o(S_0'; D')$$

o bien

$$\omega_{h-h'}(o(S_0; D)) = \omega_{h-h'}(o(S; D)) + 1 \geq o(S'; D') + 1 = o(S_0'; D').$$

Además, si $o(S_0; D) = 0$, necesariamente $o(S; D) = 0$ (y esto implica que la fórmula principal tiene grado 0), luego, por hipótesis de inducción, $o(S'; D') = 0$, luego $o(S_0'; D') = 0$.

2. En el caso de una regla lógica irrelevante S/S_0 con un único secuente superior, como antes se cumple que ambos secuentes tienen la misma altura h y los correspondientes S'/S_0' en D' también tienen la misma altura h', por lo que

$$\omega_{h-h'}(o(S_0; D)) = \omega_{h-h'}(o(S; D)) \geq o(S'; D') = o(S_0'; D').$$

Además, si $o(S_0; D) = 0$, necesariamente $o(S; D) = 0$, luego, por hipótesis de inducción, $o(S'; D') = 0$, luego $o(S_0'; D') = 0$.

3. En el caso de una regla izquierda del disyuntor, los secuentes superiores S y $\bar{S}$ tienen la misma altura h que el secuente inferior S_0, y lo mismo sucede con la regla correspondiente en D'. Por lo tanto,

$$\omega_{h-h'}(o(S;D)\#o(\bar{S};D)) \geq \omega_{h-h'}(o(S;D))\#\omega_{h-h'}(o(\bar{S};D))$$
$$\geq o(S';D')\#o(\bar{S}';D')$$

salvo que alguno de los ordinales $o(S;D)$, $o(\bar{S};D)$ sea nulo, pero si, por ejemplo, lo es $o(\bar{S};D)$, por hipótesis de inducción también $o(\bar{S}';D') = 0$, luego

$$\omega_{h-h'}(o(S;D)\#o(\bar{S};D)) = \omega_{h-h'}(o(S;D))$$
$$\geq o(S';D') = o(S';D')\#o(\bar{S}';D').$$

Además, si $o(S_0;D') = 0$, necesariamente $o(S;D) = o(\bar{S};D) = 0$, luego por hipótesis de inducción $o(S';D') = o(\bar{S}';D') = 0$, luego también $o(S_0';D') = 0$.

4. En el caso de una regla lógica relevante, digamos S/S_0, ambos secuentes tienen la misma altura h, e igualmente en la regla S'/S_0' ambos secuentes tienen altura h'. Entonces

$$\omega_{h-h'}(o(S;D)+2) \geq \omega_{h-h'}(o(S;D))\#\omega_{h-h'}(2) \geq o(S';D')+2,$$

salvo a lo sumo si $o(S;D) = 0$, en cuyo caso, también $o(S';D') = 0$ y el cálculo es

$$\omega_{h-h'}(o(S;D)+2) = \omega_{h-h'}(2) \geq 2 = o(S_0';D').$$

En este caso no puede ocurrir que $o(S_0;D) = 0$.

5. Consideremos ahora un corte en D y el correspondiente en D':

$$\frac{S_1 \qquad S_2}{S_0} \qquad \frac{S_1' \qquad \bar{S}_2'}{S_0'}$$

Llamemos h_1 y h_0 a las alturas de los secuentes superiores y del secuente inferior en D, respectivamente, y h_1' y h_0' a las alturas de los secuentes correspondientes en D'. Sean $\mu_i = o(S_i;D)$ y $\mu_i' = o(S_i';D)$. Llamemos g al grado del corte y distinguimos tres casos:

   (a) Si $h_0' \leq h_0 \leq g$, entonces $h_1 = g = h_1'$, luego la hipótesis de inducción es que $\mu_i \geq \mu_i'$. A su vez,

$$\omega_{h_0-h_0'}(\omega_{h_1-h_0}(\mu_1\#\mu_2)) = \omega_{h_1-h_0'}(\mu_1\#\mu_2) \geq \omega_{h_1'-h_0'}(\mu_1'\#\mu_2').$$

   (b) Si $g \leq h_0' \leq h_0$, entonces $h_1 = h_0$ y $h_1' = h_0'$ y de nuevo la hipótesis de inducción es $\mu_i \geq \mu_i'$. Tenemos entonces que

$$\omega_{h_0-h_0'}(\mu_1\#\mu_2) \geq \mu_1\#\mu_2 \geq \mu_1'\#\mu_2'.$$

(c) Si $h'_0 \leq g \leq h_0$, entonces $h_1 = h_0$, $h'_1 = g$ y la hipótesis de inducción es $\omega_{h_0-g}(\mu_i) \geq \mu'_i$. Entonces

$$\omega_{h_0-h'_0}(\mu_1\#\mu_2) = \omega_{g-h'_0}(\omega_{h_0-g}(\mu_1\#\mu_2)) \geq$$

$$\omega_{h'_1-h'_0}(\omega_{h_0-g}(\mu_1)\#\omega_{h_0-g}(\mu_2)) \geq \omega_{h'_1-h'_0}(\mu'_1\#\mu'_2),$$

en principio salvo si algún $\mu_i = 0$, pero en tal caso, por ejemplo, si $\mu_2 = 0 = \mu'_2$, la hipótesis de inducción $\omega_{h_0-g}(\mu_1) \geq \mu'_1$ nos da $\omega_{g-h'_0}(\omega_{h_0-g}(\mu_1)) \geq \omega_{g-h'_0}(\mu_1)$, que equivale a la desigualdad que queremos probar $\omega_{h_0-h'_0}(\mu_1\#\mu_2) \geq \omega_{h'_1-h'_0}(\mu'_1\#\mu'_2)$.

Además, si $o(S_0; D) = 0$, necesariamente $h_1 = h_0$ y $\mu_1 = \mu_2 = 0$, con lo que $\mu'_1 = \mu'_2 = 0$. Además, todas las fórmulas de S_1 y S_2 tienen que tener grado 0, incluida la fórmula de corte, luego $g = 0$, luego $h'_1 = h'_0$ y, por consiguiente, $o(S'_0; D') = 0$.

6. Finalmente consideramos una regla de inducción S/S_0. Como en el caso anterior, llamamos h_1 y h_0 a las alturas del secuente superior y del secuente inferior en D, respectivamente, y h'_1 y $h' : 0$ a las alturas de los secuentes correspondientes en D'. Supongamos en primer lugar que

$$\mu = o(S; D) = \omega^\eta + \cdots, \qquad \mu' = o(S'; D') = \omega^{\eta'} + \cdots$$

Llamamos g al grado de la fórmula de inducción y distinguimos los mismos tres casos que antes:

(a) Si $h'_0 \leq h_0 \leq g$, entonces $h_1 = g = h'_1$, luego la hipótesis de inducción es que $\mu \geq \mu'$, lo que implica que $\eta \geq \eta'$. A su vez,

$$\omega_{h_0-h'_0}(\omega_{h_1-h_0+1}(\eta+1)) = \omega_{h_1-h'_0+1}(\eta+1) \geq \omega_{h'_1-h'_0+1}(\eta'+1).$$

(b) Si $g \leq h'_0 \leq h_0$, entonces $h_1 = h_0$ y $h'_1 = h'_0$ y de nuevo la hipótesis de inducción es $\mu \geq \mu'$. Tenemos entonces que

$$\omega_{h_0-h'_0}(\omega^{\eta+1}) \geq \omega^{\eta+1} \geq \omega^{\eta'+1}.$$

(c) Si $h'_0 < g \leq h_0$, entonces $h_1 = h_0$, $h'_1 = g$ y la hipótesis de inducción es $\omega_{h_0-g}(\mu) \geq \mu'$. Esto significa que

$$\omega_{h_0-g}(\omega^\eta + \cdots) = \omega^{\omega_{h_0-g-1}(\omega^\eta+\cdots)} \geq \omega^{\eta'} + \cdots,$$

luego $\omega_{h_0-g-1}(\omega^{\eta+1}) > \omega_{h_0-g-1}(\omega^\eta + \cdots) \geq \eta'$, luego

$$\omega_{h_0-g-1}(\omega^{\eta+1}) \geq \eta' + 1,$$

luego $\omega_{h_0-g}(\omega^{\eta+1}) \geq \omega^{\eta'+1}$, luego

$$\omega_{h_0-h'_0}(o(S; D)) = \omega_{h_0-h'_0}(\omega^{\eta+1}) = \omega_{g-h'_0}(\omega_{h_0-g}(\omega^{\eta+1})) \geq$$

$$\omega_{g-h'_0}(\omega^{\eta'+1}) = \omega_{h'_1-h'_0+1}(\eta'+1) = o(S'; D').$$

Si $\mu = 0$, por hipótesis de inducción también $\mu' = 0$ y, como todas las fórmulas del secuente S tienen grado 0, necesariamente $g = 0$, luego necesariamente se cumple el caso (b) precedente. La comprobación se reduce a

$$\omega_{h_0-h_0'}(\omega^{(h_1-h_0+1)}) = \omega^{(h_1-h_0'+1)} \geq \omega = \omega^{(h_1'-h_0'+1)}.$$

Si $\mu = \omega^\eta + \cdots$ y $\mu' = 0$, también $g = 0$, luego estamos de nuevo en el caso (b) y la comprobación se reduce a $\omega_{h_0-h_0'}(\omega^{\eta+1}) \geq \omega$.

En este caso no puede suceder que $o(S_0; D) = 0$.

Así pues, podemos suponer que en la parte final de D los secuentes iniciales están formados por sentencias Δ_0, que las fórmulas principales de las reglas de debilitación implícitas son Δ_0 y que no hay reglas relevantes ni reglas propias.

Si D coincide con su parte final, no puede contener cortes sustanciales, ya que los hilos que terminan en una fórmula de corte no Δ_0 no podrían iniciarse ni en axiomas, ni en reglas de debilitación, ni en reglas relevantes, con lo que la demostración D ya cumple las condiciones requeridas por el enunciado (hemos encontrado una demostración D' tal que $o(D') \leq o(D)$ sin reglas de inferencia propias ni cortes sustanciales).

En caso, contrario, podemos aplicar el teorema 7.11, según el cual en la parte final de D hay un corte adecuado.

• Consideremos un corte adecuado en la parte final de D que no tenga ningún otro por debajo. La fórmula de corte tiene que ser de la forma $\bigvee u\,\alpha(u)$ o bien $\bigwedge u\,\alpha(u)$. Podemos suponer que se da el primer caso, pues el segundo se trata de forma totalmente análoga. Tenemos la estructura siguiente:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \overset{\nu_1+2}{\Rightarrow} \Delta_1,\, \bigvee u\,\alpha(u)}\\ \vdots\end{array}}{\Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\,\alpha(u)} \quad (h_1) \quad \dfrac{\begin{array}{c}\vdots\\ \dfrac{\alpha(y),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}{\bigvee u\,\alpha(u),\, \Gamma_1' \overset{\nu_2+2}{\Rightarrow} \Delta_1'}\\ \vdots\end{array}}{\bigvee u\,\alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'}}{\begin{array}{c}\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'\\ \vdots\end{array}}$$

Como la demostración D es regular, el término t no puede contener ninguna variable propia usada en la subdemostración del secuente $\alpha(y),\, \Gamma_1' \Rightarrow \Delta_1'$, y la variable y no se usa como variable propia en dicha subdemostración, ni aparece en Γ_1' o Δ_1', luego podemos aplicar el teorema 3.11, según el cual, al sustituir y por t en toda la subdemostración obtenemos una demostración del secuente $\alpha(t),\, \Gamma_1' \Rightarrow \Delta_1'$.

Si el grado de la fórmula de corte es 0, entonces $\alpha(t)$ es Δ_0, luego, por 7.8, uno de los secuentes $\Rightarrow \alpha(t)$ o $\alpha(t) \Rightarrow$ es demostrable (mediante sentencias Δ_0)

con una demostración de ordinal 0. Pongamos que el secuente en cuestión es, concretamente, $\Rightarrow \alpha(t)$. Consideramos la demostración alternativa:

$$\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \stackrel{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \stackrel{\nu_1+1}{\Rightarrow} \Delta_1,\, \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma \stackrel{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\,\alpha(u) \qquad (h_1)\end{array} \qquad \begin{array}{c}\begin{array}{cc}\vdots & \vdots\end{array}\\ \dfrac{\dfrac{\stackrel{0}{\Rightarrow} \alpha(t) \qquad \alpha(t),\, \Gamma_1' \stackrel{\nu_2}{\Rightarrow} \Delta_1'}{\Gamma_1' \stackrel{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\,\alpha(u),\, \Gamma_1' \stackrel{\nu_2+1}{\Rightarrow} \Delta_1'}\\ \vdots\\ \bigvee u\,\alpha(u),\, \Gamma' \stackrel{\mu_2}{\Rightarrow} \Delta'\end{array}}{\begin{array}{c}\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'\\ \vdots\end{array}}$$

Puesto que

$$o(\bigvee u\,\alpha(u),\, \Gamma_1' \Rightarrow \Delta_1'; D') = \nu_2 + 1 < \nu_2 + 2 = o(\bigvee u\,\alpha(u),\, \Gamma_1' \Rightarrow \Delta_1'; D),$$

el teorema 7.16 nos da que $o(D') < o(D)$.

Si la fórmula de corte tiene grado no nulo, entonces la altura de los secuentes superiores del corte es $h_1 > 0$, por lo que podemos considerar el secuente más alto $\Gamma'' \Rightarrow \Delta''$ situado bajo $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'$ (podría ser el mismo) cuya altura h_0 es estrictamente menor que h_1:

$$\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \stackrel{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \stackrel{\nu_1+2}{\Rightarrow} \Delta_1,\, \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma \stackrel{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\,\alpha(u) \qquad (h_1)\end{array} \qquad \begin{array}{c}\vdots\\ \dfrac{\alpha(y),\, \Gamma_1' \stackrel{\nu_2}{\Rightarrow} \Delta_1'}{\bigvee u\,\alpha(u),\, \Gamma_1' \stackrel{\nu_1+2}{\Rightarrow} \Delta_1'}\\ \vdots\\ \bigvee u\,\alpha(u),\, \Gamma' \stackrel{\mu_2}{\Rightarrow} \Delta'\end{array}}{\begin{array}{c}\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'\\ \vdots\\ \Gamma'' \stackrel{\nu}{\Rightarrow} \Delta'' \quad (h_0)\\ \vdots\end{array}}$$

Ahora consideramos la demostración alternativa D' siguiente, que por razones tipográficas descomponemos en dos bloques:

$$\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \stackrel{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \stackrel{\nu_1+1}{\Rightarrow} \Delta_1,\, \alpha(t),\, \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma \stackrel{\xi_1}{\Rightarrow} \Delta,\, \alpha(t), \bigvee u\,\alpha(u) \qquad (h_1)\end{array} \quad \begin{array}{c}\vdots\\ \bigvee u\,\alpha(u),\, \Gamma' \stackrel{\xi_2}{\Rightarrow} \Delta'\end{array}}{\begin{array}{c}\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha(t)\\ \vdots\\ \Gamma'' \Rightarrow \Delta'',\, \alpha(t) \quad (h)\end{array}}$$

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \stackrel{\xi_3}{\Rightarrow} \Delta, \bigvee u\,\alpha(u) \quad (h_1)\end{array} \qquad \begin{array}{c}\vdots\\ \dfrac{\alpha(t), \Gamma'_1 \stackrel{\nu_2}{\Rightarrow} \Delta'_1}{\bigvee u\,\alpha(u), \alpha(t), \Gamma'_1 \stackrel{\nu_2+1}{\Rightarrow} \Delta'_1}\\ \vdots\\ \bigvee u\,\alpha(u), \alpha(t), \Gamma' \stackrel{\xi_4}{\Rightarrow} \Delta'\end{array}}{\alpha(t), \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}}{\begin{array}{c}\vdots\\ (h) \quad \alpha(t), \Gamma'' \Rightarrow \Delta''\end{array}}$$

Estos dos bloques se combinan en un corte:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma'' \Rightarrow \Delta'', \alpha(t) \quad (h)\end{array} \qquad \begin{array}{c}\vdots\\ (h) \quad \alpha(t), \Gamma'' \Rightarrow \Delta''\end{array}}{\Gamma'' \stackrel{\nu'}{\Rightarrow} \Delta'' \quad (h_0)}$$
$$\vdots$$

Empezamos ambos bloques sustituyendo las reglas del particularizador por reglas de debilitación sin más que conservar $\alpha(t)$ en el secuente final. Todas las reglas de inferencia siguen siendo válidas, con lo que podemos llegar a los secuentes superiores del corte original con la adición de $\alpha(t)$. Cortando dos veces $\bigvee u\,\alpha(u)$ podemos continuar la deducción manteniendo el $\alpha(t)$ adicional hasta eliminarlo justo antes de $\Gamma'' \Rightarrow \Delta''$, y a partir de ahí continuamos la deducción original.

Vamos a probar que la nueva demostración D' tiene ordinal menor que la original D. En primer lugar tenemos que

$$o(\alpha(t), \Gamma'_1 \Rightarrow \Delta'_1; D') = o(\alpha(y), \Gamma'_1 \Rightarrow \Delta'_1; D) = \nu_2,$$

pues por debajo de estos secuentes hemos añadido el corte de $\alpha(t)$, pero su grado es menor que el del corte de $\bigvee u\,\alpha(u)$, luego las alturas de los secuentes correspondientes en ambas subdemostraciones son las mismas.

Ahora observamos que los secuentes superiores de los cortes de $\bigvee u\,\alpha(u)$ en D' siguen teniendo altura h_1, pues por debajo no tienen ninguna inducción y tienen los mismos cortes, salvo un corte añadido con fórmula de corte $\alpha(t)$, pero ésta no aumenta la altura, ya que h_1 es mayor o igual que el grado de $\bigvee u\,\alpha(u)$, que es mayor que el de $\alpha(t)$. Obviamente la altura de $\Gamma'' \Rightarrow \Delta''$ en D' es la misma que en D.

Si llamamos h a la altura de los secuentes superiores del corte de $\alpha(t)$ en D', tenemos que $h = h_0$ si h_0 es mayor que el grado de $\alpha(t)$ y h es el grado de $\alpha(t)$ en caso contrario. En cualquier caso $h_0 \leq h < h_1$.

Claramente, $\xi_1 = \mu_1$, $\xi_2 < \mu_2$, $\xi_3 < \mu_1$, $\xi_4 = \mu_2$, donde las desigualdades estrictas se deben a que al pasar de D a D' hemos cambiado una regla del particularizador por una regla de debilitación.

Todos los secuentes entre Γ, $\Gamma' \Rightarrow \Delta$, Δ' y $\Gamma'' \Rightarrow \Delta''$ tienen altura h_1 en D menos el último, y lo mismo vale en las dos ramas de D'. Como uno de los secuentes anteriores a Γ, $\Gamma' \Rightarrow \Delta$, Δ' tiene ordinal estrictamente menor en D que en las ramas de D', una inducción trivial nos permite concluir que el ordinal de cada secuente bajo Γ, $\Gamma' \Rightarrow \Delta$, Δ' en D es mayor estrictamente que el ordinal del secuente correspondiente en cada una de las dos ramas correspondientes en D', salvo quizá en el caso del secuente $\Gamma'' \Rightarrow \Delta''$, cuya altura pasa de ser h_0 en D a ser h en cada rama de D'. Este posible cambio de altura sólo puede influir si la inferencia que lleva a $\Gamma'' \Rightarrow \Delta''$ en D es un corte. Cualquier otra regla nos permite concluir trivialmente que ν_1', $\nu_2' < \nu$.

Supongamos, pues que la inferencia que lleva a $\Gamma'' \Rightarrow \Delta''$ en D es un corte

$$\frac{S_1 \qquad S_2}{\Gamma'' \Rightarrow \Delta''}$$

cuyos secuentes superiores tienen ordinales ϵ_1 y ϵ_2. Entonces tenemos

$$\frac{\dfrac{S_1' \qquad S_2'}{\Gamma'' \Rightarrow \Delta'',\, \alpha(t)} \qquad \dfrac{S_1'' \qquad S_2''}{\alpha(t),\, \Gamma'' \Rightarrow \Delta''}}{\Gamma'' \Rightarrow \Delta''}$$

y los ordinales son:

$$\frac{\dfrac{\epsilon_1' \qquad \epsilon_2'}{\omega_{h_1-h}(\epsilon_1'\#\epsilon_2')} \qquad \dfrac{\epsilon_1'' \qquad \epsilon_2''}{\omega_{h_1-h}(\epsilon_1''\#\epsilon_2'')}}{\omega_{h_1-h_0}\big(\omega_{h_1-h}(\epsilon_1'\#\epsilon_2')\#\omega_{h_1-h}(\epsilon_1''\#\epsilon_2'')\big)}$$

De los ordinales ϵ_1' y ϵ_2', uno de ellos es igual al correspondiente ϵ_1 o ϵ_2 y el otro es estrictamente menor, luego $\epsilon_1'\#\epsilon_2' < \epsilon_1\#\epsilon_2$, e igualmente $\epsilon_1''\#\epsilon_2'' < \epsilon_1\#\epsilon_2$, luego[3]

$$\omega_{h-h_0}\big(\omega_{h_1-h}(\epsilon_1'\#\epsilon_2')\#\omega_{h_1-h}(\epsilon_1''\#\epsilon_2'')\big)$$
$$< \omega_{h-h_0}(\omega_{h_1-h}(\epsilon_1\#\epsilon_2)) = \omega_{h_1-h}(\epsilon_1\#\epsilon_2),$$

o, lo que es lo mismo,

$$\nu = o(\Gamma'' \Rightarrow \Delta'', D') < o(\Gamma'' \Rightarrow \Delta'', D) = \nu'.$$

El teorema 7.16 nos da entonces que $o(D') < o(D)$. ■

Ahora observamos que si existiera una demostración D del secuente vacío en $\mathrm{I}\Sigma_n$, por el teorema 3.22 existiría una formada exclusivamente por fórmulas de tipo Σ_n (que podríamos calcular explícitamente a partir de D), y podríamos aplicarle el teorema anterior, lo que nos lleva al teorema siguiente:

Teorema 7.19 *Si D es una demostración del secuente vacío en $\mathrm{I}\Sigma_n$, existe otra D' tal que $o(D') < o(D)$.*

[3] Aquí usamos que si $\eta' \leq \eta'' < \eta$, entonces $\omega^{\eta'}\#\omega^{\eta''} = \omega^{\eta''} + \omega^{\eta'} < \omega^{\eta}$.

Demostración: Suponemos tácitamente que la demostración consta únicamente de fórmulas de tipo Σ_n o Π_n. Podemos aplicarle el teorema anterior, para obtener la demostración D', pero no puede darse el caso de que D' carezca de reglas de inferencia propias y de cortes sustanciales, pues entonces sólo podría constar de fórmulas Δ_0, pues cualquier fórmula que no fuera de este tipo tendría un descendiente en el secuente final, ya que no puede ser eliminada en un corte sustancial. Además, por el teorema 3.11, podríamos convertirla en una demostración formada sólo por sentencias Δ_0, en contra del teorema 7.5.

Así pues, el teorema anterior nos proporciona concretamente una demostración que cumple $o(D') < o(D)$. ■

A su vez:

Teorema 7.20 *Si* $\mathrm{I}\Sigma_n$ *es contradictoria, existe una sucesión infinita estrictamente decreciente de ordinales menores que* $\omega^{(n+1)}$.

Por lo tanto, si la inducción transfinita vale hasta $\omega^{(n+1)}$, podemos asegurar que $\mathrm{I}\Sigma_n$ es consistente.

Nota Notemos que este teorema incluye a 7.7 y a 7.13 como casos particulares, pues si AP fuera contradictoria, también lo sería $\mathrm{I}\Sigma_n$, para algún n suficientemente grande.

En efecto, como toda fórmula es lógicamente equivalente a una fórmula en forma prenexa [LM 2.15], usando [LM 5.18] vemos que toda fórmula aritmética es equivalente en $\mathrm{I}\Sigma_1$ a una fórmula Σ_n, para un n suficientemente grande. Y es fácil ver que si en una demostración en AP aplicamos la regla de inducción con una fórmula α, siempre podemos encontrar una fórmula α' equivalente (en $\mathrm{I}\Sigma_1$) de tipo Σ_n y modificar la prueba para que la inducción se haga con α' en lugar de α. Por lo tanto, si un secuente es un teorema de AP, podemos modificar su demostración para que todos los usos de la regla de inducción usen una fórmula de tipo Σ_n, para un n suficientemente grande. En otras palabras, todo teorema de AP es un teorema de $\mathrm{I}\Sigma_n$, para algún n. ■

Capítulo VIII

Incompletitud en la aritmética de Peano

Tal y como hemos señalado en el capítulo anterior, es discutible si la prueba de Gentzen de la consistencia de la aritmética de Peano aporta algo realmente o tan sólo demuestra algo evidente. No obstante, en este capítulo vamos a mostrar cómo las técnicas de Gentzen no sólo sirven para probar que el secuente vacío no es demostrable en AP, sino que también permiten demostrar que otras sentencias verdaderas tampoco son demostrables, lo cual no es evidente en absoluto. En realidad ya nos hemos encontrado un ejemplo de esta naturaleza. Ahora sabemos que la inducción transfinita hasta ϵ_0, es decir, la fórmula

$$\bigwedge v \in E(\bigwedge v \prec u\, \phi(v) \to \phi(u)) \to \bigwedge u \in E\, \phi(u)$$

es verdadera en el modelo natural de AP cualquiera que sea la fórmula $\phi(x)$, pero no es demostrable en AP, al menos para ciertas fórmulas concretas $\phi(x)$, dado que esta fórmula (para una $\phi(x)$ adecuada, de tipo Π_1) implica la consistencia de AP.

8.1 Buenos órdenes demostrables

En el capítulo VI formalizamos aritméticamente el concepto conjuntista de ordinal menor que ϵ_0, pero la forma en que lo hemos hecho es arbitraria, en el sentido de que podríamos plantearnos la posibilidad de definir los ordinales de forma completamente diferente y, en tal caso, cabría preguntarse si dos formalizaciones aritméticas distintas de los ordinales menores que ϵ_0 son equivalentes en algún sentido que habría que precisar, así como si es posible formalizar aritméticamente ordinales mayores que ϵ_0. Vamos a introducir algunos conceptos que precisen estas ideas.

Definición 8.1 Sea $x \trianglelefteq y$ una fórmula de $\mathcal{L}_a$ de tipo Σ_1. Diremos que *representa un orden total* en un conjunto D de números naturales si se cumple:

1. $n \in D$ syss $\mathbb{N} \vDash \bar{n} \trianglelefteq \bar{n}$,
2. $\mathbb{N} \vDash (x \trianglelefteq y \rightarrow x \trianglelefteq x \wedge y \trianglelefteq y)$,
3. $\mathbb{N} \vDash (x \trianglelefteq y \wedge y \trianglelefteq x \rightarrow x = y)$,
4. $\mathbb{N} \vDash (x \trianglelefteq y \wedge y \trianglelefteq z \rightarrow x \trianglelefteq z)$,
5. $\mathbb{N} \vDash (x \trianglelefteq y \vee y \trianglelefteq x)$.

En tal caso, definimos la fórmula $x \in D \equiv x \trianglelefteq x$.

Nota Podríamos dar una definición puramente sintáctica (sin aludir al modelo natural de AP) sin más que omitir 1. y pedir que las fórmulas de los apartados siguientes sean demostrables en AP, pero entonces tenemos una definición más fuerte y nunca vamos a necesitar que tales fórmulas sean demostrables en AP. ■

Por ejemplo, tenemos que la fórmula $x \preceq y$ definida en el capítulo VI representa un orden total en el conjunto E de los ordinales (menores que ϵ_0), incluso en el sentido fuerte indicado en la nota precedente.

Si $x \trianglelefteq y$ representa un orden total en un conjunto D, representaremos también por $\trianglelefteq$ la relación que induce sobre los números naturales, de modo que

$$m \trianglelefteq n \quad \text{syss} \quad \mathbb{N} \vDash \bar{m} \trianglelefteq \bar{n}.$$

Tenemos así que $\trianglelefteq$ es una relación de orden total sobre el conjunto D. Definimos

$$x \lhd y \equiv x \trianglelefteq y \wedge x \neq y,$$

que es también una fórmula Σ_1 y claramente

$$m \trianglelefteq n \quad \text{syss} \quad \text{no } n \lhd m \quad \text{syss} \quad \mathbb{N} \vDash \neg \bar{n} \lhd \bar{m},$$

con lo que la relación $\trianglelefteq$ es en realidad Δ_1, luego recursiva [LM 7.11], al igual que lo es el conjunto D.

Más delicado es precisar en qué sentido podemos decir que una fórmula $x \trianglelefteq y$ que representa un orden total en un dominio D representa, de hecho, un buen orden en D. En principio, con ello queremos expresar que se cumple cualquiera de los hechos siguientes, equivalentes entre sí:

1. *Todo subconjunto de D no vacío tiene un mínimo elemento respecto de $\trianglelefteq$.*
2. *No existen sucesiones infinitas estrictamente decrecientes:*

$$n_0 \rhd n_1 \rhd n_2 \rhd \cdots$$

3. *Para toda propiedad $P(n)$, si para todo $n \in D$, el hecho de que todo $m \lhd n$ cumpla $P(m)$ implica $P(n)$, entonces todo $n \in D$ cumple $P(n)$.*

Sin embargo, es cuestionable que cualquiera de estas afirmaciones tenga un significado preciso fuera del marco de una teoría axiomática de conjuntos, pues no es evidente en absoluto a qué nos referimos con una propiedad que involucra a "todos los subconjuntos de un conjunto dado" o a "todas las sucesiones infinitas en un conjunto dado" o a "todas las propiedades $P(n)$".

Se trata de propiedades que, desde un punto de vista finitista —incluso no de los más estrictos— no tienen un significado preciso salvo que dispongamos de un argumento que las justifique. Así, en la sección 6.4 hemos dado un argumento que justifica que la fórmula $x \preceq y$ cumple 2. (en el sentido de que hemos argumentado que es imposible que exista cualquier clase de proceso que genere una sucesión infinita de ordinales estrictamente decreciente), y es fácil ver entonces que también cumple 1. y 3., por lo que podemos decir que representa un buen orden sobre el conjunto E de los ordinales (menores que ϵ_0).

Sin embargo, esta dificultad no nos va a afectar, porque el propósito de esta sección es estudiar las fórmulas que definen buenos órdenes, no ya en el sentido de que, de algún modo, se pueda demostrar que cumplen las propiedades anteriores, sino en el sentido más preciso de que tal cosa pueda demostrarse formalmente en AP o — más precisamente, como veremos enseguida— "casi" en AP. El "casi" se debe a que, en principio, la propiedad más cómoda de formalizar es 3., pero en la sección 6.7 vimos un ejemplo que nos previene de tratar de hacerlo equiparando las "propiedades arbitrarias $P(n)$" con las propiedades expresables mediante fórmulas aritméticas. Si tomáramos como definición que una fórmula $x \trianglelefteq y$ que define un orden total en un dominio D define un buen orden demostrable en AP si en AP se puede demostrar el esquema de inducción transfinita:

$$\bigwedge u \in D(\bigwedge v \lhd u\, \phi(v) \to \phi(u)) \to \bigwedge u \in D\, \phi(u)$$

para toda fórmula $\phi(x, x_1, \ldots, x_n)$ de $\mathcal{L}_a$, nos encontraríamos con que la fórmula $x \trianglelefteq y$ construida[1] en la prueba del teorema 6.24 sería un buen orden demostrable en AP, cuando en realidad la relación que determina no cumple 3. Para evitar este problema tenemos que salirnos "un poco" de AP:

Definición 8.2 Llamamos $\mathcal{L}_a^R$ al lenguaje formal que resulta de añadir a $\mathcal{L}_a$ un relator monádico R, y llamamos AP^R a la teoría axiomática sobre $\mathcal{L}_a^R$ determinada por los axiomas de Peano con el principio de inducción extendido a fórmulas de $\mathcal{L}_a^R$.

Diremos que una fórmula $x \trianglelefteq y$ que represente un orden total en un dominio D representa un *buen orden demostrable* (en AP)[2] si en AP^R se puede demostrar la fórmula

$$\mathrm{IT}(\trianglelefteq) \equiv \bigwedge u \in D(\bigwedge v \lhd u\, Rv \to Ru) \to \bigwedge u \in D\, Ru.$$

[1]Puesto que estamos pidiendo que la relación determine su dominio, tendríamos que considerar, más precisamente, la fórmula $x \in A \wedge y \in A \wedge x \trianglelefteq y$.

[2]Notemos el abuso de hablar de buenos órdenes demostrables en AP cuando en realidad la demostración que atestigua la definición tiene que hacerse en AP^R, pero AP^R no es más que un artificio para hablar en AP de propiedades genéricas, no necesariamente aritméticas.

En tal caso, si $\phi(x, x_1, \ldots, x_n)$ es cualquier fórmula de $\mathcal{L}_a$, en AP es demostrable la fórmula

$$\bigwedge u \in D(\bigwedge v \lhd u\, \phi(v) \to \phi(u)) \to \bigwedge u \in D\, \phi(u).$$

En efecto, si tomamos una demostración del secuente $\Rightarrow \mathrm{IT}(\unlhd)$ sustituimos cada expresión Rt por $\phi(t, x_1, \ldots, x_n)$ (con variables $x_1, \ldots, x_n$ que no aparezcan en la demostración), es claro que todas las reglas de inferencia siguen siendo válidas, y que los axiomas de AP^R se transforman en teoremas de AP (por ejemplo, un axioma $Rt \Rightarrow Rt$ se transforma en el teorema $\phi(t) \Rightarrow \phi(t)$). Por lo tanto, añadiendo demostraciones de los axiomas modificados, obtenemos una demostración del principio de inducción para ϕ.

Sin embargo, la definición que hemos dado de buen orden demostrable es más fuerte que la que habría resultado de exigir meramente que en AP puedan demostrarse las versiones aritméticas del principio de inducción transfinita. Así estamos exigiendo que $\mathrm{IT}(\unlhd)$ sea verdadero en todo modelo de AP^R, en particular en el modelo natural de AP extendido interpretando el relator R con cualquier relación que podamos considerar bien definida en $\mathbb{N}$, lo que significa que la relación $\unlhd$ satisface el principio de inducción transfinita para cualquier propiedad que pueda considerarse bien definida sobre los números naturales, aunque no pueda definirse aritméticamente.

Por ejemplo, ahora es fácil probar que la fórmula definida en el teorema 6.24 no es un buen orden demostrable en AP, pues $\mathrm{IT}(\unlhd)$ resulta ser falsa en el modelo de AP^R que resulta de extender el modelo natural de AP interpretando el relator R con la relación (Rn syss n es distinto de todos los números σ_n).

Esto no es sorprendente, puesto que, al fin y al cabo, la relación que determina la fórmula del teorema 6.24 no es un buen orden. En cambio, es más destacable que la fórmula $x \preceq y$, a pesar de que determina un buen orden en el conjunto E de los ordinales (menores que ϵ_0), no representa un buen orden demostrable en AP, ya que si lo fuera, en AP podría demostrarse el caso particular del principio de inducción transfinita que implica la consistencia de AP.

Por el contrario, para cada número natural n, la fórmula

$$x \unlhd_n y \equiv x \unlhd y \unlhd \omega^{(\bar{n})}$$

sí que representa un buen orden demostrable sobre el conjunto de los ordinales menores o iguales que $\omega^{(n)}$, pues la prueba del teorema 6.23 vale en realidad sin cambio alguno para toda fórmula ϕ de $\mathcal{L}_a^R$, en particular para la fórmula Rx.

Ejemplo (Kreisel): Un buen orden no demostrable de tipo $\boldsymbol{\omega}$ Sea $\phi(x)$ cualquier fórmula Δ_1^{AP} de $\mathcal{L}_a$ y consideremos la fórmula, también Δ_1,

$$x \unlhd y \equiv (x \leq y \land \bigwedge u \leq x\, \phi(u)) \lor (y \leq x \land \bigvee u \leq x\, \neg\phi(u)).$$

Así, si llamamos F a la relación dada por Fn syss $\mathbb{N} \vDash \phi(\bar{n})$, tenemos que si todo n cumple Fn, entonces la relación $\unlhd$ determinada por la fórmula que acabamos de definir es la relación de orden usual en los números naturales, mientras que si existe un n que no cumple Fn y n_0 es el mínimo de ellos, entonces

$$0 \lhd 1 \lhd \cdots \lhd n_0 - 1 \qquad \cdots \lhd n_0 + 2 \lhd n_0 + 1 \lhd n_0,$$

es decir, los primeros números naturales, hasta $n_0 - 1$ están ordenados con el orden usual y, a partir de n_0, el orden es el inverso al usual.

Así pues, esta fórmula $x \lhd y$ representa un orden total en cualquier caso, pero sólo representa un buen orden si todo número natural n cumple Fn. Más aún:

> *La fórmula $x \unlhd y$ representa un buen orden demostrable en* AP *si y sólo si* $\underset{\mathrm{AP}}{\vdash} \bigwedge u\, \phi(u)$.

En efecto, notemos ante todo que $\underset{\mathrm{AP}}{\vdash} \bigwedge u\, u \unlhd u$, es decir, $\underset{\mathrm{AP}}{\vdash} \bigwedge u\, u \in D$, por lo que en este caso podemos suprimir de todas partes la fórmula $x \in D$.

Si en AP se demuestra $\bigwedge u\, \phi(u)$, también se demuestra que

$$\bigwedge uv(u \unlhd v \leftrightarrow u \leq v),$$

y es fácil ver entonces que $x \unlhd y$ representa un buen orden demostrable. Recíprocamente, si $x \unlhd y$ representa un buen orden demostrable, hemos visto que en AP podemos demostrar el principio de inducción transfinita para cualquier fórmula, en particular para $\bigwedge w \leq x\, \phi(w)$, es decir:

$$\bigwedge u(\bigwedge v \lhd u \bigwedge w \leq v\, \phi(w) \to \bigwedge w \leq u\, \phi(w)) \to \bigwedge u \bigwedge w \leq u\, \phi(w).$$

Vamos a demostrar la hipótesis del principio de inducción, es decir, fijamos un número natural x, suponemos la hipótesis de inducción

$$\bigwedge v \lhd x \bigwedge w \leq v\, \phi(w)$$

y vamos a demostrar $\bigwedge w \leq x\, \phi(w)$. En caso contrario tenemos que

$$x \leq x + 1 \wedge \bigvee w \leq x\, \neg\phi(w),$$

luego $x + 1 \lhd x$, por definición de $\lhd$, luego $\bigwedge w \leq x + 1\, \phi(w)$, por la hipótesis de inducción, luego en particular $\bigwedge w \leq x\, \phi(w)$, y tenemos una contradicción.

El principio de inducción nos permite concluir que $\bigwedge u \bigwedge w \leq u\, \phi(w)$, de donde se sigue que $\bigwedge u\, \phi(u)$.

Finalmente aplicamos esto a la fórmula

$$\phi(x) \equiv \neg \overset{x}{\underset{\ulcorner\mathrm{AP}\urcorner}{\vdash}} \ulcorner 0 \neq 0 \urcorner,$$

de modo que $\bigwedge u\, \phi(u)$ es $\mathrm{Consis}\ulcorner\mathrm{AP}\urcorner$. Concluimos que la fórmula $x \unlhd y$ no representa un buen orden demostrable en AP, a pesar de que la relación de orden que determina es el buen orden usual de los números naturales. ■

El ejemplo anterior muestra que dos fórmulas $x \leq y$, $x \trianglelefteq y$ pueden determinar una misma relación de orden recursiva en el conjunto de los números naturales y, sin embargo, puede ocurrir que una represente un buen orden demostrable en AP y la otra no. En otras palabras, no tiene sentido plantearse si una buena relación de orden recursiva definida en el conjunto de los números naturales es demostrable o no en AP sin especificar la fórmula concreta con la que pretendemos representarla.

A su vez, podemos plantearnos que, del mismo modo que la inducción transfinita respecto de $x \trianglelefteq y$ no es demostrable en AP (porque implica la consistencia de AP), pero existe otra fórmula ($x \leq y$) que determina la misma relación de orden para la cual la inducción transfinita sí que es demostrable, tal vez podría existir otra fórmula $x \trianglelefteq y$ que defina la misma relación de orden que $x \preceq y$, pero que representara un buen orden demostrable en AP, para lo cual, en particular, no tendría que implicar la consistencia de AP.

En otros términos, ¿sería posible definir fórmulas Δ_1 que determinaran buenos órdenes demostrables en AP de ordinal ϵ_0 o incluso de ordinales mayores? Hay una diferencia obvia entre la fórmula $x \preceq y$ y la fórmula $x \trianglelefteq y$ del ejemplo anterior, y es que la segunda es "maliciosa", en el sentido de que lleva la consistencia de AP en su propia definición, por lo que no es extraño que la inducción transfinita respecto de ella implique dicha consistencia, mientras que la primera es "natural", en cuanto a que se limita a exigir lo necesario para obtener una relación de orden de tipo ϵ_0. Sin embargo, no existe ninguna definición objetiva que distinga lo "malicioso" de lo "natural", por lo que cabe preguntarse si el hecho de que la inducción transfinita respecto de $\preceq$ implique la consistencia de AP no podría ser un "defecto" de la definición de $\preceq$, que podría subsanarse con otra definición alternativa que permitiera formalizar en AP la inducción hasta ϵ_0 o incluso hasta ordinales mayores.

Dedicaremos la sección siguiente a probar que no es así, es decir, que ninguna fórmula permite definir un buen orden demostrable en AP de ordinal ϵ_0 o superior. Pero antes terminaremos esta sección mostrando que no perdemos generalidad si consideramos únicamente buenos órdenes demostrables cuyo dominio lo formen todos los números naturales.

Fijemos una fórmula $x \trianglelefteq y$ que determine un buen orden demostrable sobre un dominio D. Esto nos permite definir la función recursiva:

$$F(0) = 0, \quad F(n+1) = (F(n)^\frown\langle n\rangle) \cdot \chi_D(n) + F(n) \cdot (1 - \chi_D(n)),$$

de modo que $F(n)$ es la sucesión que enumera en orden creciente los elementos de D menores que n. Si D es infinito, entonces $\bigwedge m \bigvee n\, \ell(F(n)) > m$, por lo que podemos definir la función recursiva

$$N(m) = \mu n\, \ell(F(n)) > m,$$

que a su vez nos permite definir $G(m) = F(N(m)))$, y así tenemos una biyección recursiva entre $\mathbb{N}$ y D. La relación $y = G(x)$ puede expresarse mediante una fórmula $\phi(x, y)$ de tipo Δ_1^{AP}, de modo que en AP se demuestra:

$$\bigwedge u \overset{1}{\bigvee} v\, \phi(u,v), \quad \bigwedge uv(\phi(u,v) \to v \in D), \quad \bigwedge v \in D \overset{1}{\bigvee} u\, \phi(u,v).$$

Esto nos permite definir

$$x \precsim y \equiv \bigvee uv(\phi(x,u) \land \phi(y,v) \land u \trianglelefteq v),$$

y es fácil ver que la fórmula $x \precsim y$ representa un buen orden demostrable en AP cuyo dominio lo forman todos los números naturales (es decir, tal que $\bigwedge x\, x \precsim x$) y que determina una relación de orden tal que

$$m \precsim n \quad \text{syss} \quad G(m) \trianglelefteq G(n).$$

En particular, ambas relaciones determinan el mismo ordinal. Así pues, a la hora de determinar los ordinales posibles de los buenos órdenes demostrables en AP, no perdemos generalidad si nos restringimos a buenos órdenes $\trianglelefteq$ definidos sobre todos los números naturales.

Veamos también que no perdemos generalidad si suponemos que el mínimo respecto[3] de $\trianglelefteq$ es 0.

En efecto, si n_0 es el mínimo respecto de $\trianglelefteq$ y no es 0, podemos definir

$$\phi(x,y) \equiv (x \neq 0 \land x \neq \bar{n}_0 \land y = x) \lor (x = 0 \land y = \bar{n}_0) \lor (x = \bar{n}_0 \land y = 0)$$

y a su vez

$$x \precsim y \equiv \bigvee uv(\phi(x,u) \land \phi(y,v) \land u \trianglelefteq v).$$

Es claro que la fórmula $x \precsim y$ representa un buen orden demostrable (cuyo dominio lo forman todos los números naturales) y de modo que la relación que determina en $\mathbb{N}$ tiene por mínimo al 0. Concretamente, es la misma relación $\trianglelefteq$ salvo que n_0 ocupa el lugar del 0 y viceversa. En particular, ambas determinan el mismo ordinal.

Todo esto hace que no perdamos generalidad si cambiamos la definición de buen orden demostrable por ésta más restrictiva:

Definición 8.3 Diremos que una fórmula $x \trianglelefteq y$ de $\mathcal{L}_a$ de tipo Σ_1 representa un buen orden demostrable (en AP) si

1. $\mathbb{N} \vDash (x \trianglelefteq y \land y \trianglelefteq x \to x = y)$,
2. $\mathbb{N} \vDash (x \trianglelefteq y \land y \trianglelefteq z \to x \trianglelefteq z)$,
3. $\mathbb{N} \vDash (x \trianglelefteq y \lor y \trianglelefteq x)$,
4. $\mathbb{N} \vDash 0 \trianglelefteq x$.

y en AP^R se puede demostrar el *principio de inducción transfinita*

$$\mathrm{IT}(\trianglelefteq) \equiv \bigwedge u(\bigwedge v \vartriangleleft u\, Rv \to Ru) \to \bigwedge u\, Ru.$$

Notemos que de 3. se deduce que $\mathbb{N} \vDash x \trianglelefteq x$.

[3]Ya hemos señalado que si $\trianglelefteq$ es la relación definida por una fórmula que representa un buen orden demostrable, entonces todo conjunto no vacío de su dominio tiene un mínimo elemento. La prueba puede particularizarse al caso del conjunto de todos los números naturales sin necesidad de considerar conjuntos arbitrarios. En efecto, si suponemos que para todo n existe un m tal que $m \vartriangleleft n$, es fácil probar por inducción que todo número natural cumple $n \neq n$, con lo que tenemos una contradicción. Por lo tanto, existe un número natural n tal que, para todo m, se cumple $n \vartriangleleft m$.

8.2 Inducción transfinita en AP

En esta sección vamos a demostrar que todo buen orden demostrable en AP tiene necesariamente ordinal menor que ϵ_0, de modo que el hecho de que el buen orden $\preceq$ definido en el capítulo VI no sea demostrable no es debido a ningún "defecto" del modo en particular en que hemos formalizado en AP los ordinales menores que ϵ_0.

Más precisamente, vamos a demostrar el teorema siguiente, debido también a Gentzen:

Teorema 8.4 *Si $\trianglelefteq$ es un buen orden demostrable, existe un ordinal μ y una función recursiva $F : \mathbb{N} \longrightarrow \mathbb{N}$ de modo que, para todo número natural k, se cumple que $F(k) \prec \mu$ y, para todo par de números naturales k y k',*

$$k \lhd k' \quad \textit{syss} \quad F(k) \prec F(k').$$

En términos conjuntistas, esto significa que el conjunto ordenado $(\mathbb{N}, \trianglelefteq)$ es semejante a un subconjunto del conjunto de todos los ordinales menores que μ, y eso implica [TC 3.26] que tiene ordinal menor o igual que $\mu < \epsilon_0$. Si consideramos la aritmética de Peano formalizada en una teoría de conjuntos potente, como ZF o NBG, ésta es la conclusión a la que llegamos: que los buenos órdenes recursivos demostrables en AP (a través de la fórmula que sea) son los de ordinal menor que ϵ_0. Si queremos trabajar en términos estrictamente finitistas tenemos la conclusión del teorema anterior. Para obtener a partir de F una semejanza G entre $\mathbb{N}$ y un ordinal menor o igual que μ tendríamos que aplicar el teorema general de recursión transfinita, como en [TC 3.24], lo que supone definir $G(n)$ en función de la restricción de G al conjunto (en general infinito) de los m tales que $m \lhd n$, lo cual excede las técnicas finitistas.

Un cálculo secuencial para $\mathbf{AP}^R$ De acuerdo con la definición 8.3 de buen orden demostrable, que es la que adoptamos aquí, el hecho clave para que una fórmula represente un buen orden demostrable en AP es que cierta sentencia sea demostrable en AP^R. Vamos a especificar un cálculo deductivo secuencial para AP^R que nos facilite el análisis de la demostración correspondiente.

En primer lugar vamos a considerar a AP como extensión de ARP, lo que, de acuerdo con 5.1, significa que tomaremos como axiomas propios de AP los axiomas que definen los funtores de $\mathcal{L}_{\mathrm{arp}}$ (evaluados en términos arbitrarios, no sólo en variables, para que sean invariantes por sustitución) más los axiomas

$$t' = 0 \Rightarrow, \qquad s' = t' \Rightarrow s = t.$$

Las reglas de inferencia son las de LK_i más la regla de inducción para fórmulas arbitrarias de $\mathcal{L}_{\mathrm{arp}}$.

En virtud del teorema de completitud 5.6, toda sentencia atómica de $\mathcal{L}_{\mathrm{arp}}$ es demostrable o refutable en ARP, luego en AP (y siempre podemos saber cuál es el caso), por lo que podemos tomar también como axiomas propios de AP todos los secuentes $\Rightarrow \alpha$ o $\alpha \Rightarrow$ (donde α es una sentencia atómica) que sean teoremas de ARP.

A su vez, podemos considerar el lenguaje $\mathcal{L}_{\mathrm{arp}}^R$ que resulta de adjuntarle a $\mathcal{L}_{\mathrm{arp}}$ el relator monádico R y considerar el cálculo secuencial sobre este lenguaje cuyos axiomas son los de LK_i, más los axiomas propios de AP que acabamos de indicar y con la regla de inducción extendida a fórmulas de $\mathcal{L}_{\mathrm{arp}}^R$.

Más precisamente, los axiomas de LK_i correspondientes a $\mathcal{L}_{\mathrm{arp}}^R$ que no son axiomas de LK_i sobre $\mathcal{L}_{\mathrm{arp}}$ son:

1. Los axiomas lógicos $Rt \Rightarrow Rt$.
2. Los axiomas del igualador $s = t,\ Rs \Rightarrow Rt$.

Observemos que los axiomas de AP^R constan únicamente de fórmulas atómicas y son cerrados para sustitución.

Por último, vamos a añadir a AP^R una nueva regla de inferencia, que llamaremos de *sustitución* (derecha)[4]:

$$\frac{\Gamma \Rightarrow \Delta,\ Rs}{\Gamma \Rightarrow \Delta,\ Rt}$$

donde s y t son designadores tales que $\Rightarrow s = t$ es un teorema (luego un axioma) de AP. Esta regla es redundante, en el sentido de que todos los teoremas que pueden demostrarse con ella, pueden demostrarse también sin ella, pues podemos demostrarla así:

$$\frac{\Gamma \Rightarrow \Delta,\ Rs \qquad \dfrac{\Rightarrow s = t \qquad s = t,\ Rs \Rightarrow Rt}{Rs \Rightarrow Rt}}{\Gamma \Rightarrow \Delta,\ Rt}$$

Consideremos ahora una fórmula $x \trianglelefteq y$ que represente un buen orden demostrable. Entonces $x \trianglelefteq y \equiv \bigvee u\, \alpha(x, y, u)$, donde α es una fórmula Δ_0, luego, según 5.4, es equivalente en ARP (luego en AP) a una fórmula atómica. Por lo tanto, no perdemos generalidad si suponemos que α es una fórmula atómica.

La condición de que la sentencia $\mathrm{IT}(\trianglelefteq)$ considerada en la definición 8.3 sea demostrable en AP^R equivale claramente a que lo sea el secuente

$$\mathrm{IT}(\trianglelefteq) \equiv \bigwedge u(\bigwedge v \triangleleft u\, Rv \rightarrow Ru) \Rightarrow Rx$$

Demostraciones IT Llamaremos *demostraciones* IT a las demostraciones en el cálculo deductivo que resulta de añadir a los axiomas de AP^R todos los secuentes que llamaremos *secuentes de tipo* IT, que son los de la forma

$$\bigwedge v \triangleleft t\, Rv \Rightarrow Rt,$$

donde t es un término arbitrario, y cuyo secuente final sea de la forma

$$\Rightarrow R\bar{m}_1, \ldots, R\bar{m}_n,$$

donde $\bar{m}_1, \ldots \bar{m}_n$ son los numerales asociados a los números naturales $m_1, \ldots, m_n$.

[4]Podríamos introducir también una regla izquierda de sustitución de forma obvia, pero no la vamos a necesitar.

Si D es una demostración IT, definimos su *número final* $n(D)$ como el mínimo de $m_1, \ldots, m_n$ respecto del orden $\trianglelefteq$.

Notemos que, al añadir los axiomas de tipo IT, el conjunto de los axiomas sigue siendo cerrado para sustitución, pero estos axiomas contienen fórmulas no atómicas.

Es fácil ver que los teoremas 3.11 y 3.13 siguen siendo válidos para demostraciones en AP^R y para demostraciones IT. Lo único que podría invalidar las demostraciones es la presencia de la nueva regla de sustitución, pero es inmediato que ésta sigue siendo válida si en sus secuentes sustituimos cualquier variable por cualquier término, y esto basta para comprobar que las demostraciones de ambos teoremas siguen siendo válidas.

Por ejemplo, si llamamos $D(x)$ a la deducción siguiente en AP^R, que tiene como premisa el secuente IT $\bigwedge v \lhd y\, Rv \Rightarrow Ry$,

$$\dfrac{\dfrac{\dfrac{\bigwedge v \lhd y\, Rv \Rightarrow Ry}{\Rightarrow \bigwedge v \lhd y\, Rv \to Ry}}{\Rightarrow \bigwedge u(\bigwedge v \lhd u\, Rv \to Ru)} \qquad \begin{array}{c}\vdots \\ \bigwedge u(\bigwedge v \lhd u\, Rv \to Ru) \Rightarrow Rx\end{array}}{\Rightarrow Rx}$$

el teorema 3.11 nos da que, para todo número natural m, al sustituir x por $\bar{m}$ en $D(x)$ obtenemos una demostración IT, que llamaremos $D(\bar{m})$, del secuente $\Rightarrow R\bar{m}$.

El ordinal de una demostración IT Definimos el *grado* de una fórmula de $\mathcal{L}_{\mathrm{arp}}^R$ como el número de signos lógicos que contiene (entre conectores y cuantificadores). El *grado* de un corte es el grado de la fórmula de corte. El *grado* de una inducción es el grado de la fórmula de inducción. La *altura* $h(S; D)$ de un secuente S en una demostración D es el máximo de los grados de los cortes e inducciones que hay bajo S. Si no hay ninguno, la altura es 0.

A cada secuente S en una demostración IT le asociamos un ordinal $o(S; D)$ según el criterio siguiente:

1. Si S es un axioma de AP^R, entonces $o(S; D) = 1$.

2. Si S es un secuente inicial de tipo IT, entonces $o(S; D) = 6$.

3. Si S es el secuente inferior de una regla de debilitación o sustitución con secuente superior S_1, entonces $o(S; D) = o(S_1; D)$.

4. Si S es el secuente inferior de una regla izquierda del disyuntor con secuentes superiores S_1 y S_2, entonces $o(S; D) = o(S_1; D) \# o(S_2; D)$.

5. Si S es el secuente inferior de una regla de inferencia lógica con secuente superior S_1, entonces $o(S; D) = o(S_1; D) + 1$.

6. Si S es el secuente inferior de una regla de corte con secuentes superiores S_1 y S_2, entonces $o(S;D) = \omega_{h_1-h_0}(\mu_1\#\mu_2)$, donde

$$h_1 = h(S_1;D) = h(S_2;D), \quad h_0 = h(S;D), \quad \mu_i = o(S_i;D).$$

7. Si S es el secuente inferior de una inducción con secuente superior S', entonces $o(S;D) = \omega_{h_1-h_0+1}(\eta+1)$, donde

$$h_1 = h(S';D), \quad h_0 = h(S;D), \quad o(S';D) = \omega^\eta + \cdots$$

El ordinal $o(D)$ es el ordinal del secuente final de D.

El teorema 7.2 vale igualmente para demostraciones IT, de nuevo porque la presencia de la regla de sustitución no invalida la prueba. Más concretamente, basta observar que la regla de sustitución puede tratarse igual que las de sustitución.

La *parte final* de una demostración IT está formada por todos los secuentes que no tienen por debajo ninguna regla de inferencia lógica.[5] En particular, en la parte final de una demostración IT no puede haber reglas lógicas.

Ahora podemos probar el teorema clave, que es una variante del teorema 7.6:

Teorema 8.5 *Sea D una demostración* IT *cuyo número final no sea* 0*. Entonces existe otra D' tal que $o(D') \prec o(D)$ y $n(D') \trianglelefteq n(D)$.*

Demostración: El teorema 3.13 nos permite transformar D en otra demostración IT con el mismo ordinal y el mismo secuente final que además sea regular. A su vez, el teorema 3.11 nos permite sustituir por 0 cualquier variable libre en D que no sea una variable propia de una regla de inferencia.

Por lo tanto, podemos suponer que D es una demostración regular cuyas únicas variables libres son las que se usan (una única vez, por la regularidad) como variables propias de alguna regla de inferencia, y cada una sólo aparece por encima de la regla en la que actúa como variable propia.

• Si D contiene una inducción en su parte final, exactamente el mismo argumento empleado en la prueba de 7.6 nos da una demostración de ordinal menor con el mismo secuente final (en esta parte de la prueba de 7.6 no se usa que el secuente final de D es el vacío, y por eso vale sin cambio alguno en nuestro contexto).

A partir de aquí podemos suponer que la parte final de D no contiene inducciones, luego en particular está formada únicamente por sentencias.

• Supongamos ahora que la parte final de D contiene un axioma lógico, es decir, un secuente de la forma $\alpha \Rightarrow \alpha$.

[5] Podríamos decir "ninguna regla de inferencia lógica implícita" pero sería lo mismo, ya que, como el secuente final contiene únicamente fórmulas atómicas, no puede haber reglas de inferencia lógicas.

Si α no es de la forma Rt, como en la parte final no hay reglas lógicas ni inducciones y el secuente final sólo tiene fórmulas de este tipo, los descendientes de las dos fórmulas α son idénticos a α y tienen que acabar desapareciendo en un corte. Si, por el contrario, $\alpha \equiv Rt$, la fórmula del consecuente puede permanecer hasta el secuente final (tal vez sufriendo sustituciones), pero la fibra que se inicia con el α del antecedente tiene estar formada por fórmulas idénticas a α (pues no hay regla de sustitución izquierda) y acabar en un corte. Notemos que en este segundo caso α tiene grado 0.

En caso de que las dos fórmulas acaben desapareciendo en cortes, consideramos la que desaparece primero. Supondremos que es la del antecedente, pero el caso contrario se trata análogamente. La situación es:

$$\cfrac{\begin{array}{c} D_0 \\ \vdots \\ \Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha \end{array} \qquad \begin{array}{c} \alpha \Rightarrow \alpha \\ \vdots \\ \alpha,\, \Gamma' \stackrel{\nu}{\Rightarrow} \Delta' \end{array}}{\begin{array}{c} \Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\ \vdots \\ \Rightarrow R\bar{m}_1, \ldots, R\bar{m}_n \end{array}}$$

donde Δ' contiene todavía un descendiente del α situado en el consecuente del axioma. Entonces podemos simplificar D hasta una demostración D' de la forma

$$\cfrac{\begin{array}{c} D_0 \\ \vdots \\ \Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha \end{array}}{\begin{array}{c} \Gamma,\, \Gamma' \stackrel{\mu}{\Rightarrow} \Delta,\, \Delta' \\ \vdots \\ \Rightarrow R\bar{m}_1, \ldots, R\bar{m}_n \end{array}}$$

Llamemos S al secuente $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'$. Notemos que, o bien en los últimos puntos suspensivos hay otro corte que elimina la fórmula α contenida en Δ', o bien $\alpha \equiv Rt$ y tiene grado 0, luego al pasar a D' hemos eliminado un corte del grado de α, pero, si éste es no nulo, más abajo hay otro del mismo grado, luego las alturas en D de todos los secuentes de la subdemostración D_0 que acaba en $\Gamma \Rightarrow \Delta,\, \alpha$ son las mismas que sus alturas en D', luego

$$\mu = o(\Gamma \Rightarrow \Delta, \alpha; D) = o(\Gamma \Rightarrow \Delta, \alpha; D') = o(S; D').$$

Más aún, como la altura de los dos secuentes superiores del corte de D es la misma que la del secuente inferior, si los secuentes superiores tienen ordinales μ y ν en D, entonces

$$o(S; D) = \mu \# \nu \succ \mu = o(S; D').$$

El teorema 7.2 nos da entonces que $o(D') \prec o(D)$.

Así pues, a partir de aquí podemos suponer que la parte final de la demostración D no contiene ningún axioma lógico.

• Podemos suponer que D no contiene en su parte final ningún axioma del igualador de tipo

$$s = t,\ Rs \Rightarrow Rt,$$

pues en tal caso s y t tienen que ser designadores, y podemos sustituir este axioma por una de las demostraciones:

$$\dfrac{\dfrac{Rs \Rightarrow Rs}{s = t,\ Rs \Rightarrow Rs}}{s = t,\ Rs \Rightarrow Rt} \qquad \dfrac{s = t \Rightarrow}{s = t,\ Rs \Rightarrow Rt}$$

según si $\Rightarrow s = t$ o bien $s = t \Rightarrow$ es un teorema (luego un axioma) de AP. Notemos que el secuente final de ambas demostraciones tiene ordinal 1, por lo que el cambio no altera el valor de $o(D)$.

• Supongamos ahora que la parte final de D contiene una regla de debilitación y tomemos una que no tenga otra por debajo.

Si la regla es explícita, es decir, si su fórmula principal tiene un descendiente en el secuente final, tiene que ser la regla derecha y la fórmula principal tiene que ser de la forma Rt, para cierto designador t, que puede ser sustituido por otros equivalentes en los descendientes, hasta terminar en una de las sentencias $R\bar{m}_i$. No perdemos generalidad si suponemos que se trata de $R\bar{m}_n$. La situación es:

$$\begin{array}{c} \vdots \\ \dfrac{\Gamma \overset{\mu}{\Rightarrow} \Delta}{\Gamma \overset{\mu}{\Rightarrow} \Delta,\ Rt} \\ \vdots \\ \overset{\nu}{\Rightarrow} R\bar{m}_1, \ldots, R\bar{m}_n \end{array}$$

Es claro que si eliminamos Rt y todos sus desdendientes (eliminando, por consiguiente, todas las reglas de sustitución que les afecten) obtenemos otra demostración D'

$$\begin{array}{c} \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta \\ \vdots \\ \overset{\nu}{\Rightarrow} R\bar{m}_1, \ldots, R\bar{m}_{n-1}\ (R\bar{m}_n) \end{array}$$

en cuyo secuente final no estará $R\bar{m}_n$ salvo que alguna regla de corte intermedia lo vuelva a introducir. Puesto que las reglas de debilitación y de sustitución no aumentan el ordinal de un secuente, es claro que $o(D') = o(D)$, pero en la parte final de D' hay una regla de debilitación menos que en la de D.

Si la regla es implícita, es decir, si un descendiente de la fórmula que introduce desaparece en un corte, el argumento empleado en la prueba de 7.6 vale sin cambio alguno (pues no usa que el secuente final sea vacío salvo para afirmar que la regla es implícita, cuando aquí ya hemos analizado la posibilidad contraria). Concretamente, pueden darse dos casos, el caso A) es análogo al precedente, y nos permite construir una demostración D' con el mismo ordinal, el mismo secuente final y una regla de debilitación menos, mientras que el caso B) obtenemos[6] una demostración D' con el mismo secuente final tal que $o(D') \prec o(D)$.

Así, al ir considerando una regla de debilitación tras otra, o bien se dan siempre los dos primeros casos (el de que la regla sea explícita o el caso A), en cuyo caso, tras un número finito de pasos, terminamos con una demostración con el mismo ordinal, pero sin reglas de debilitación, o bien en algún momento se da el caso B), en cuyo caso terminamos con una demostración de ordinal menor.

Ahora bien, si se ha dado alguna vez el caso de que la regla sea explícita, el secuente final de la demostración resultante puede tener menos sentencias que el secuente final de D. En tal caso las añadimos de nuevo mediante reglas de debilitación. Si habíamos llegado a una demostración D' de ordinal menor, al añadir las sentencias perdidas por debilitación mantenemos el nuevo ordinal $o(D') \prec o(D)$ y el teorema ya se cumple en este caso. Si habíamos llegado a una demostración sin debilitaciones con el mismo ordinal, al añadir las sentencias perdidas obtenemos una demostración D' con el mismo ordinal tal que todas las reglas de debilitación de la parte final son explícitas y se aplican después de cualquier otra regla.

Equivalentemente, a partir de aquí podemos suponer que si la parte final de D contiene una regla de debilitación, ésta es explícita y todas las reglas que hay bajo ella son también reglas de debilitación explícitas.

En resumen, a partir de este momento tenemos que la parte final de D cumple:

1. No tiene variables libres.

2. No tiene reglas de inferencia lógicas ni inducciones.

3. No tiene axiomas lógicos ni axiomas del igualador $s = t,\ Rs \Rightarrow Rt$.

4. Si tiene una debilitación, todas las reglas subsiguientes son debilitaciones.

Así pues, las únicas reglas de inferencia que hay en la parte final son cortes, sustituciones y debilitaciones.

Al contrario de lo que sucede en la prueba de 7.6, ahora no podemos asegurar que D no coincida con su parte final (esto es tanto como afirmar que D contiene una regla de inferencia lógica). Pero sí que se cumple algo muy próximo:

> *La demostración D contiene al menos una regla de inferencia lógica o un secuente inicial de tipo* IT.

[6] La prueba de (7.1) vale igualmente sin más que contemplar un caso adicional para la regla de sustitución, que es análogo al caso de la regla de debilitación.

En efecto, si D no contiene reglas de inferencia lógicas, coincide con su parte final, luego está formado únicamente por sentencias. Si además no contiene secuentes iniciales de tipo IT, sus secuentes iniciales son necesariamente axiomas del igualador o matemáticos, los cuales constan únicamente de sentencias atómicas, y las únicas reglas de inferencia son cortes, sustituciones y debilitaciones que introducen únicamente sentencias de tipo $R\bar{m}_i$.

Por lo tanto, D consta únicamente de sentencias atómicas. Si convenimos en que toda sentencia de la forma Rt es falsa por definición, podemos dividir los secuentes en verdaderos y falsos, de modo que todos los secuentes iniciales son verdaderos y el secuente final es falso, lo cual es imposible, porque las reglas de corte, sustitución y debilitación dan lugar a secuentes verdaderos a partir de secuentes verdaderos.

Llamaremos *sentencias principales* a las fórmulas principales (sentencias, de hecho) de las reglas de inferencia lógicas fronterizas y *sentencias inductivas* a las sentencias Rt que figuran en el consecuente de un secuente inicial de tipo IT. Llamaremos *descendientes principales* (resp. *inductivos*) a los descendientes de las sentencias principales (resp. inductivas).

Como en la parte final de D no hay reglas de inferencia lógicas, los descendientes principales son siempre sentencias idénticas a la sentencia principal de la cual descienden, mientras que los descendientes de una sentencia Rt pueden transformarse en sentencias de la forma Rs, para un designador equivalente s, mediante reglas de sustitución. Las fibras de descendientes principales terminan necesariamente en fórmulas de corte (son implícitas), mientras que las de los descendientes inductivos pueden terminar también en cortes o bien llegar hasta el secuente final de D (pueden ser explícitas).

Veamos ahora lo siguiente:

> *Si un secuente S en la parte final de D contiene una sentencia α con un signo lógico, entonces S o bien un secuente situado sobre S contiene un descendiente principal o inductivo.*

En efecto, el secuente S tiene que estar por encima de todas las reglas de debilitación. Si el secuente inferior de una regla de debilitación o de sustitución tiene una sentencia con un signo lógico, el secuente superior tiene que tener esa misma fórmula (pues las reglas de debilitación de la parte final de D sólo introducen sentencias atómicas) y, si se trata del secuente inferior de un corte, entonces alguno de los dos secuentes superiores tiene que tenerla también. Por lo tanto, ascendiendo desde S, tenemos que llegar, o bien al secuente inferior de una regla fronteriza, o bien a un secuente inicial de tipo IT. En ambos casos dicho secuente contiene una sentencia principal o inductiva.

Un corte en la parte final de D es *adecuado* si las dos fórmulas de corte son descencientes principales. Ahora no podemos probar la existencia de cortes adecuados, pero tenemos lo siguiente:

> *Si la parte final de D no contiene cortes adecuados, entonces su secuente final contiene un descendiente inductivo.*

En efecto, si el secuente final no contiene descendientes inductivos, entonces el primer secuente S_0 por encima de las reglas de debilitación tampoco lo contiene y, como sus sentencias no contienen signos lógicos, tampoco contiene descendientes principales. Hemos visto que la parte final de D contiene un secuente S con un descendiente principal o inductivo, y S está sobre S_0, y entre ambos sólo hay cortes o sustituciones. Las sustituciones no eliminan ningún descendiente principal o inductivo, luego tiene que haber un corte, digamos

$$\frac{\Gamma \Rightarrow \Delta, \alpha \qquad \alpha, \Gamma' \Rightarrow \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

cuyo secuente inferior no contenga descendientes principales o inductivos, pero alguno de cuyos secuentes superiores sí que contenga uno, que necesariamente será la fórmula de corte. Para referencia posterior, llamaremos P a esta propiedad, es decir, decimos que un corte *tiene la propiedad* P si alguno de sus secuentes superiores contiene un descendiente principal o inductivo, pero el secuente inferior no contiene ninguno.

Hemos probado que la parte final de D contiene un corte con la propiedad P, luego podemos tomar uno que no tenga otro por encima. Llamemos S_1 y S_2 a los secuentes superiores. Supongamos en primer lugar que la fórmula de corte de S_1 es un descendiente principal o inductivo.

Si α contiene un signo lógico, entonces es un descendiente principal. Por la propiedad que hemos probado anteriormente, la parte final de D contiene un secuente S^* por encima de S_2 con un descendiente principal o inductivo β. Si S_2 no contiene ningún descendiente principal o inductivo, esto significa que entre S^* y S_2 tiene que haber un corte con la propiedad P, en contra de la elección del corte que estamos considerando.

Así pues, S_2 contiene un descendiente principal o inductivo, pero como el secuente inferior del corte no lo contiene, tiene que tratarse de la fórmula de corte α, luego ambas fórmulas de corte α son descendientes principales, y el corte es adecuado.

Concluimos que α no contiene signos lógicos, luego tiene que ser un descendiente inductivo, de la forma Rt. Entonces S_2 no puede contener descendientes principales o inductivos, pues, como en el secuente inferior del corte no los hay, la única posibilidad sería que lo fuera α, pero tendría que ser un descendiente inductivo y para ello tendría que estar en el consecuente de S_2 y no en el antecedente.

Más aún, por encima de S_2 no puede haber reglas de inferencia lógicas. Si las hubiera, una de ellas sería fronteriza, y su fórmula principal sería un descendiente principal en un secuente por encima de S_2, luego alguno de los cortes intermedios entre dicho secuente y S_2 tendría la propiedad P y de nuevo tenemos una contradicción.

Pero si por encima de S_2 no hay reglas de inferencia lógicas, toda la parte de la demostración D situada por encima de S_2 está en la parte final de D, luego en ella no hay axiomas lógicos, ni tampoco axiomas del igualador con fórmulas de tipo Rs en su antecedente, luego es imposible que Rt aparezca en el antecedente de S_2.

Con esto hemos probado que S_1 no contiene descendientes principales o inductivos, luego, necesariamente, la fórmula de corte α de S_2 tiene que ser un descendiente principal o inductivo, pero, al estar en el antecedente, tiene que ser un descendiente principal, luego contiene un signo lógico.

Hemos probado que en S_1 o en un secuente situado sobre él tiene que haber un descendiente principal o inductivo β, pero hemos demostrado que en S_1 no puede haber tal descendiente, luego β tiene que estar en un secuente estrictamente por encima de S_1, y esto nos lleva una vez más a que por encima de S_1 tiene que haber un corte con la propiedad P. Esta contradicción completa la prueba.

• Si la parte final de D contiene un corte adecuado, el argumento empleado en la prueba del teorema 7.6 nos permite construir otra demostración del mismo secuente final con ordinal estrictamente menor, pues en esta parte de la prueba no se usa que el secuente final de D sea vacío.

Por lo tanto, a partir de aquí podemos suponer que la parte final de D no contiene cortes adecuados, y hemos probado que en tal caso el secuente inferior contiene un descendiente inductivo, que podemos suponer que es $R\bar{m}_1$. Éste será descendiente de una sentencia inductiva Rt, de modo que el secuente $\Rightarrow t = \bar{m}_1$ es un teorema (luego un axioma) de AP.

Estamos suponiendo que $n(D)$ no es 0, así como que 0 es el mínimo de $\trianglelefteq$. Por lo tanto, podemos tomar un número natural m tal que $m \lhd n(D) \trianglelefteq m_1$. Entonces, la sentencia

$$\bar{m} \lhd t \equiv \bigvee u(\alpha(\bar{m}, t, u) \land \bar{m} \neq t)$$

es verdadera en el modelo natural de AP, luego existe un k tal que

$$\mathbb{N} \vDash \alpha(\bar{m}, t, \bar{k})$$

y, por 5.6 tenemos que el secuente $\Rightarrow \alpha(\bar{m}, t, \bar{k}) \land \bar{m} \neq t$ es demostrable en ARP, luego es un axioma de AP.

Consideremos la demostración siguiente en AP^R:

$$\begin{array}{cc}
\Rightarrow \alpha(\bar{m}, t, \bar{k}) \land \bar{m} \neq t & \\
\cline{1-1}
\Rightarrow \bar{m} \lhd t & \\
\cline{1-1}
\neg\bar{m} \lhd t \Rightarrow & R\bar{m} \Rightarrow R\bar{m} \\
\hline
\multicolumn{2}{c}{\bar{m} \lhd t \rightarrow R\bar{m} \Rightarrow R\bar{m}} \\
\hline
\multicolumn{2}{c}{\bigwedge v \lhd t Rv \Rightarrow R\bar{m}} \\
\hline
\multicolumn{2}{c}{\bigwedge v \lhd t Rv \Rightarrow Rt,\, R\bar{m}}
\end{array}$$

donde en el primer paso hemos usado la regla izquierda del particularizador y después de la regla izquierda del negador hemos usado la regla izquierda del disyuntor, teniendo en cuenta que $\bar{m} \lhd t \rightarrow R\bar{m} \equiv \neg\bar{m} \lhd t \lor R\bar{m}$.

Notemos que su ordinal es 5. La demostración D tiene como secuente inicial el secuente IT

$$\bigwedge v \lhd t\, Rv \overset{6}{\Rightarrow} Rt,$$

donde Rt inicia una fibra que termina en el secuente final como $R\bar{m}_1$. Si intercalamos el paso

$$\frac{\bigwedge v \lhd t\, Rv \overset{6}{\Rightarrow} Rt}{\bigwedge v \lhd t\, Rv \overset{6}{\Rightarrow} Rt,\ R\bar{m}}$$

y añadimos $R\bar{m}$ en los consecuentes de todos los secuentes situados por debajo, obtenemos una demostración con el mismo ordinal, pero con secuente final

$$\Rightarrow R\bar{m},\ R\bar{m}_1, \ldots, R\bar{m}_n.$$

Si ahora sustituimos los dos secuentes indicados por la demostración alternativa que hemos construido, obtenemos una demostración D' del mismo secuente final, pero con $o(D') \prec o(D)$, por el teorema 7.2, ya que hemos sustituido una demostración de ordinal 6 por otra de ordinal 5. Además, ahora $n(D') = m < n(D)$. ■

Si aplicamos el procedimiento descrito en la prueba del teorema anterior y obtenemos una demostración con $n(D') = n(D)$, podemos ir repitiendo el proceso y, como a cada paso el ordinal de la demostración desciende, tras un número finito de pasos llegaremos a una demostración D' tal que $o(D') \prec o(D)$ y $n(D') \lhd n(D)$. Recordemos que $n(D')$ podemos elegirlo como cualquier número natural k que cumpla $k \lhd n(D)$.

Definición 8.6 Si D es una demostración TI y k es un número natural tal que $k \lhd n(D)$, llamaremos *reducción* de D a k a la demostración TI obtenida aplicando repetidamente proceso descrito en la prueba teorema anterior hasta que se cumpla $n(D') = k$.

Ahora ya podemos demostrar el teorema 8.4:

Recordemos que, tras la definición del concepto de demostración IT hemos definido una demostración $D(x)$ tal que, para cada número natural k, proporciona una demostración IT $D(\bar{k})$ del secuente $\Rightarrow R\bar{k}$, que obviamente cumple $n(D(\bar{k})) = k$.

Definimos recurrentemente demostraciones IT D_k tales que $n(D_k) = k$. Distinguimos dos casos:

1. Si todo $n < k$ cumple $n \lhd k$, definimos D_k como la demostración $D(\bar{k})$ del secuente $\Rightarrow R\bar{k}$.

2. Si existe un $n < k$ tal que $k \lhd n$, sea

$$n_0 \lhd \cdots \lhd n_j = k \lhd \cdots \lhd n_k$$

la reordenación de los números $\leq k$ en orden creciente respecto de $\trianglelefteq$. Así $n_{j+1} < k$, luego está definida la demostración $D_{n_{j+1}}$, y podemos tomar como D_k la reducción de $D_{n_{j+1}}$ a k.

Es claro que la aplicación $k \mapsto o(D_k)$ es recursiva (podemos calcularla explícitamente). Por lo tanto, también es recursiva la función definida mediante $F(0) = \omega^{o(D_0)}$ y, para $k > 0$, ordenamos los números $\leq k$ en la forma

$$n_0 \lhd \cdots \lhd n_j = k \lhd \cdots \lhd n_k$$

y definimos $F(k) = F(n_{j-1}) + \omega^{o(D_k)}$. Recordemos que estamos suponiendo que 0 es el mínimo respecto de $\unlhd$, por lo que si $k > 0$ necesariamente $j > 0$, pues $n_0 = 0$.

Veamos por inducción sobre i que si

$$m_0 \lhd \cdots \lhd m_i$$

son los números naturales $\leq i$, entonces, para $0 \leq j < i$, se cumple

$$F(m_{j+1}) = F(m_j) + \omega^{o(D_{m_{j+1}})}.$$

Para $i = 0$ no hay nada que probar. Supuesto cierto para i, o bien $m_i \lhd i+1$, o bien existe un $j < i$ tal que

$$m_j \lhd i + 1 \lhd m_{j+1}.$$

Recordemos que 0 es el mínimo respecto de $\unlhd$, por lo que no puede darse el caso $i + 1 \lhd m_0 = 0$. Basta probar que se cumple

$$F(i + 1) = F(m_j) + \omega^{o(D_{i+1})}$$

(con $j = i$ en el primer caso) y que, si $j < i$,

$$F(m_{j+1}) = F(i + 1) + \omega^{o(D_{m_{j+1}})}.$$

La primera igualdad se cumple por definición de F y para la segunda usamos que $o(D_{i+1}) \prec o(D_{m_{j+1}})$ por definición de D_{i+1}, con lo que, por hipótesis de inducción,

$$\begin{aligned} F(m_{j+1}) &= F(m_j) + \omega^{o(D_{m_{j+1}})} = F(m_j) + \omega^{o(D_{i+1})} + \omega^{o(D_{m_{j+1}})} \\ &= F(i + 1) + \omega^{o(D_{m_{j+1}})}. \end{aligned}$$

Esto termina la inducción, y en particular vemos que $F(m_j) \prec F(m_{j+1})$ y, más en general, que si $0 \leq j < j' \leq i$, se cumple que $F(m_j) \prec F(m_{j'})$.

Si $k \lhd k'$, basta tomar como $i = \max\{k, k'\}$ y aplicar lo anterior para concluir que $F(k) \prec F(k')$. Esto implica que F es biyectiva y, como los órdenes son totales, también $F(k) \prec F(k')$ implica que $k \lhd k'$.

Por último, si tomamos $\mu = \omega^{o(D(x))+1}$, es claro que

$$o(D(\bar{k})) = o(D(x)) \prec o(D(x)) + 1,$$

luego $o(D_k) \prec o(D(x)) + 1$, pues $o(D_k) \preceq o(D(\bar{r}))$, para cierto r, de donde se sigue inmediatamente que $F(k) \prec \mu$. ■

8.3 Recursión transfinita

La validez de la inducción transfinita hasta ϵ_0 permite justificar la validez de ciertas definiciones por recursión transfinita. Recordemos que una función $f(x_1,\ldots,x_n)$ está definida por recursión a partir de dos funciones $g(x_1,\ldots,x_{n-1})$ y $h(x_1,\ldots,x_n,u)$ si

$$f(x_1,\ldots,x_n)=\begin{cases} g(x_1,\ldots,x_{n-1}) & \text{si } x_n=0,\\ h(x_1,\ldots,x_n,f(x_1,\ldots,x_{n-1},x_n-1)) & \text{si } x_n>0.\end{cases}$$

Si llamamos

$$r(x)=\begin{cases} 0 & \text{si } x=0,\\ x-1 & \text{si } x>0,\end{cases}$$

podemos reformular la relación precedente en la forma

$$f(x_1,\ldots,x_n)=\begin{cases} g(x_1,\ldots,x_{n-1}) & \text{si } r(x_n)\geq x_n,\\ h(x_1,\ldots,x_n,f(x_1,\ldots,x_{n-1},r(x_n))) & \text{si } r(x_n)<x_n.\end{cases}$$

A su vez, esta expresión nos lleva a la definición siguiente:

Definición 8.7 Diremos que una función $f(x_1,\ldots,x_n)$ está definida por *recursión transfinita* a partir de las funciones $g(x_1,\ldots,x_n)$, $h(x_1,\ldots,x_n,u)$ y $r(x_1,\ldots,x_n)$ si

$$f(\bar{x})=\begin{cases} g(\bar{x}) & \text{si no } r(\bar{x})\prec x_n,\\ h(\bar{x},f(x_1,\ldots,x_{n-1},r(\bar{x}))) & \text{si } r(\bar{x})\prec x_n,\end{cases}$$

donde $\bar{x}$ abrevia a $x_1,\ldots,x_n$.

Así, si no se cumple $r(\bar{x})\prec x_n$ (lo cual puede suceder si $r(\bar{x})$ o x_n no son ordinales, o si lo son pero $x_n\preceq r(\bar{x})$), entonces f se calcula directamente a partir de $\bar{x}$ mediante la función g, pero si $r(\bar{x})\prec x_n$, entonces la f se calcula en función del valor que toma en $x_1,\ldots,x_{n-1},r(\bar{x})$.

Notemos que esto determina unívocamente $f(\bar{x})$ para todo $\bar{x}$, pues, para calcularlo, tomamos $s_0=x_n$ y, en el supuesto de que $s_0\in E$, vamos calculando $s_{i+1}=r(x_1,\ldots,x_{n-1},s_i)$ hasta que deje de cumplirse $s_{i+1}\prec s_i$. Así obtenemos una sucesión decreciente

$$x_n=s_0\succ s_1\succ\cdots\succ s_l,$$

de modo que no se cumple $s_l\succ s_{l+1}$. Como no puede haber sucesiones infinitas estrictamente decrecientes de ordinales, esto debe suceder tras un número finito de pasos. Entonces podemos calcular sucesivamente $t_i=f(x_1,\ldots,x_{n-1},s_i)$ gracias a las relaciones

$$\begin{aligned} t_l &= f(x_1,\ldots,x_{n-1},s_l)=g(x_1,\ldots,x_{n-1},s_l),\\ t_i &= f(x_1,\ldots,x_{n-1},s_i)=h(\bar{x},t_{i+1})\end{aligned}$$

y así llegamos hasta $f(\bar{x})=t_0$.

Como en AP no podemos demostrar que todas las sucesiones estrictamente decrecientes de ordinales son finitas, para formalizar la recursión transfinita tenemos que añadir una restricción:

Dado un ordinal α, diremos que una función $f(x_1, \ldots, x_n)$ está definida por *recursión transfinita hasta* α a partir de $g(x_1, \ldots, x_n)$, $h(x_1, \ldots, x_n, u)$ y $r(x_1, \ldots, x_n)$ si

$$f(\bar{x}) = \begin{cases} h(\bar{x}, f(x_1, \ldots, x_{n-1}, r(\bar{x}))) & \text{si } r(\bar{x}) \prec x_n \prec \alpha, \\ g(\bar{x}) & \text{en otro caso.} \end{cases}$$

A su vez, esto nos permite extender el concepto de función recursiva primitiva:

Definición 8.8 Una función f es *recursiva primitiva respecto del ordinal* α si existe una sucesión de funciones $f_1, \ldots, f_n$ tales que f_n es f y cada f_i es una de las funciones recursivas elementales (la función 0, la función sucesor o una proyección) o bien está definida por composición, por recursión o por recursión transfinita hasta α a partir de funciones anteriores de la sucesión.

Es claro entonces que toda función recursiva primitiva es recursiva primitiva respecto de α.

Sucede que las funciones recursivas primitivas respecto de ordinales no son ni más ni menos que las funciones demostrablemente recursivas en AP. A continuación probamos la implicación más fácil:

Teorema 8.9 *Las funciones recursivas primitivas respecto de ordinales menores que* $\omega^{(k+1)}$ *son demostrablemente recursivas en* $\mathrm{I}\Sigma_k$.

DEMOSTRACIÓN: Las funciones recursivas elementales son obviamente demostrablemente recursivas en $\mathrm{I}\Sigma_k$. Es claro que basta probar que toda función definida por composición, por recursión o por recursión transfinita hasta un ordinal $\alpha \prec \omega^{(k+1)}$ a partir de funciones demostrablemente recursivas $\mathrm{I}\Sigma_k$ es demostrablemente recursiva en $\mathrm{I}\Sigma_k$.

Composición Pongamos que $f(\bar{x}) = h(g_1(\bar{x}), \ldots, g_m(\bar{x}))$, donde[7]

$$h(a_1, \ldots, a_m) = a \quad \text{syss} \quad \mathbb{N} \vDash \phi(a_1, \ldots, a_m, a)$$

$$g_i(a_1, \ldots, a_n) = a \quad \text{syss} \quad \mathbb{N} \vDash \psi_i(a_1, \ldots, a_n, a)$$

para ciertas fórmulas Σ_1 tales que

$$\underset{\mathrm{I\Sigma_k}}{\vdash} \overset{1}{\bigvee} y\, \phi(y_1, \ldots, y_m, y), \qquad \underset{\mathrm{I\Sigma_k}}{\vdash} \overset{1}{\bigvee} y\, \psi_i(x_1, \ldots, x_n, y).$$

Es fácil ver entonces que f satisface la definición de función demostrablemente recursiva con la fórmula

$$\chi(\bar{x}, y) \equiv \bigvee y_1 \cdots y_m(\psi_1(\bar{x}, y_1) \wedge \cdots \wedge \psi_m(\bar{x}, y_m) \wedge \phi(y_1, \ldots, y_m, y)).$$

[7]Por no complicar la notación, no distinguiremos entre los números naturales y sus numerales correspondientes, pues el contexto los distingue inequívocamente. En las fórmulas siguientes, por ejemplo, a la izquierda tenemos números y a la derecha numerales.

Recursión Pongamos que

$$\begin{aligned} f(\bar{x},0) &= g(\bar{x}), \\ f(\bar{x},x+1) &= h(\bar{x},x,f(\bar{x},x)) \end{aligned}$$

y que g y h satisfagan la definición de función demostrablemente recursiva con las fórmulas ϕ y ψ, respectivamente. Entonces f la satisface con

$$\chi(\bar{x},x,y) \equiv \bigvee s(\ell(s) = x+1 \land s_x = y \land \phi(\bar{x},s_n) \land \bigwedge i < x\, \psi(\bar{x},i,s_i,s_{i+1})).$$

Recursión transfinita Pongamos que

$$f(\bar{x}) = \begin{cases} h(\bar{x},f(x_1,\ldots,x_{n-1},R(\bar{x}))) & \text{si } r(\bar{x}) \prec x_n \prec \alpha \prec \omega^{(k+1)}, \\ g(\bar{x}) & \text{en otro caso} \end{cases}$$

y que g, h, r satisfacen la definición de función demostrablemente recursiva con las fórmulas ϕ, ψ y ρ, respectivamente. Entonces f la satisface con la fórmula Σ_1:

$$\chi(\bar{x},y) \equiv \bigvee stl(\ell(s) = \ell(t) = l+1 \land s_0 = x_n \land t_0 = y \land$$

$$\bigwedge i < l(\rho(x_1,\ldots,x_{n-1},s_i,s_{i+1}) \land s_{i+1} \prec s_i \prec \alpha \land \psi(\bar{x},t_{i+1},t_i)) \land$$
$$\bigvee u(\rho(x_1,\ldots,x_{n-1},s_l,u) \land \neg u \prec s_l) \land \phi(x_1,\ldots,x_{n-1},s_l,t_l)).$$

A la hora de probar $\overset{1}{\bigvee} y\, \chi(\bar{x},y)$ en $\mathrm{I}\Sigma_k$, más concretamente, a la hora de probar la existencia de al menos un y, se demuestra primero que

$$x_n \prec \alpha \rightarrow \bigvee sl(\ell(s) = l+1 \land s_0 = x_n \land$$

$$\bigwedge i < l(\rho(x_1,\ldots,x_{n-1},s_i,s_{i+1}) \land s_{i+1} \prec s_i \prec \alpha) \land$$
$$\bigvee u(\rho(x_1,\ldots,x_{n-1},s_l,u) \land \neg u \prec s_l)).$$

Para ello razonamos por inducción transfinita sobre x_n, es decir, suponemos que el resultado se cumple para todo $x_n' \prec x_n$ y lo probamos para x_n. Para ello, tomamos el único x_n' que cumple $\rho(x_1,\ldots,x_n,x_n')$ y distinguimos dos casos: si no $x_n' \prec x_n$, entonces basta tomar $s = \langle x_n \rangle$, mientras que si $x_n' \prec x_n$, la hipótesis de inducción nos da una sucesión s' que cumple lo requerido con $s_0' = x_n'$, y basta tomar $s = \langle x_n \rangle ^\frown s'$.

Como la inducción transfinita hasta α es demostrable en $\mathrm{I}\Sigma_k$, podemos concluir que la afirmación anterior se cumple para todo $x_n \prec \alpha$, pero entonces se cumple de hecho para todo x_n (incluso si no es un ordinal), pues si no $x_n \prec \alpha$, basta tomar $s = \langle x_n \rangle$.

Una vez justificada la existencia de s, es fácil probar la de t mediante una inducción ordinaria sobre la longitud de s. La unicidad no ofrece dificultad. ■

El recíproco lo deduciremos del teorema siguiente:

Teorema 8.10 *Sea $\phi(x_1,\ldots,x_n,x)$ una fórmula Δ_0 en $\mathcal{L}_a$ tal que*

$$\underset{\mathrm{I\Sigma_k}}{\vdash} \Rightarrow \bigvee u\, \phi(x_1,\ldots,x_n,u)$$

con una demostración que conste únicamente de fórmulas Σ_k o Π_k y con ordinal menor que $\alpha \prec \omega^{(k+1)}$. Entonces existe un a tal que $\underset{\mathrm{AP}(\varnothing)}{\vdash} \Rightarrow \phi(a_1,\ldots,a_n,a)$ y la función

$$f(a_1,\ldots,a_n) = \mu a \underset{\mathrm{AP}(\varnothing)}{\vdash} \Rightarrow \phi(a_1,\ldots,a_n,a)$$

es recursiva primitiva respecto de α.

Demostración: Definimos como sigue una función $r(D)$: si D es un número natural que codifica una demostración en $\mathrm{I}\Sigma_k$ formada únicamente por fórmulas Σ_k o Π_k y cuyo secuente final conste únicamente de sentencias Π_1 en su antecedente y sentencias Σ_1 en su consecuente, entonces $r(D) = D'$, donde D' es la demostración construida en el teorema 7.18. En caso contrario, $r(D) = D$. Es pura rutina comprobar que dicho teorema es formalizable en ARP, por lo que la función r es recursiva primitiva.

Sea O la función que a cada demostración D en $\mathrm{I}\Sigma_k$ le asigna su ordinal $O(D)$, y que toma el valor 0 si D no es una demostración en $\mathrm{I}\Sigma_k$. También es recursiva primitiva.

A su vez, la función

$$F_\alpha(D) = \begin{cases} F_\alpha(r(D)) & \text{si } O(r(D)) \prec O(D) \prec \alpha, \\ D & \text{en otro caso} \end{cases}$$

es recursiva primitiva respecto de α. Si D es una demostración en $\mathrm{I}\Sigma_k$ formada únicamente por fórmulas Σ_k o Π_k y cuyo secuente final conste únicamente de sentencias Π_1 en su antecedente y sentencias Σ_1 en su consecuente y $O(D) \prec \alpha$, entonces $F_\alpha(D)$ es una demostración del mismo secuente que no contiene reglas de inferencia propias ni cortes sustanciales. En efecto, para calcular $F_\alpha(D)$, hay que ir calculando la sucesión de demostraciones

$$D, \quad r(D), \quad r(r(D)), \quad r(r(r(D))), \ldots$$

mientras vayan cumpliendo

$$O(D) \succ O(r(D)) \succ O(r(r(D))) \succ O(r(r(r(D)))) \succ \cdots$$

lo cual, de acuerdo con el teorema 7.18 va sucediendo mientras las demostraciones sucesivas tengan inducciones o cortes sustanciales. Tras un número finito de pasos tenemos que llegar a una demostración D_0 que no los tenga, y entonces $F_\alpha(D)$ es la demostración resultante.

Supongamos ahora que D es una demostración en $\mathrm{I}\Sigma_k$ de $\Rightarrow \bigvee u\, \phi(\bar{a},u)$ sin reglas de inferencia propias ni cortes sustanciales, y vamos a ver cómo a partir de ella podemos calcular un a (el mínimo, de hecho) tal que $\underset{\mathrm{AP}(\varnothing)}{\vdash} \phi(\bar{a},a)$.

En primer lugar, por el teorema 3.11, podemos eliminar todas las variables libres sustituyéndolas por ceros, con lo que podemos suponer que la demostración consta únicamente de sentencias Δ_0 y de la sentencia $\bigvee u\, \phi(\bar{a}, u)$ (siempre en consecuentes), pues cualquier otra sentencia que no fuera Δ_0 no podría ser eliminada mediante cortes y tendría que aparecer en el secuente final.

Recordemos que en 3.8 vimos que podíamos definir en términos finitistas la verdad o falsedad de una sentencia Δ_0. A su vez, si un secuente

$$\gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$$

consta únicamente de sentencias Δ_0, decimos que es verdadero o falso según lo sea la sentencia

$$\neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n,$$

(entendiendo que el secuente vacío es falso). Así, podemos considerar los secuentes de D que, al quitarles la sentencia $\bigvee u\, \phi(\bar{a}, u)$, son falsos. Entre ellos está el secuente final y no puede estar ninguno de los secuentes iniciales (pues sólo contienen fórmulas atómicas y son todos verdaderos).

Por lo tanto, si partimos del secuente final y vamos ascendiendo por un hilo cualquiera, en algún momento debemos llegar a una regla cuyo secuente inferior (al quitarle la sentencia Σ_1) es falso y al menos uno de sus secuentes superiores es verdadero. Si la fórmula Σ_1 es una fórmula colateral de la regla, entonces ésta sigue siendo válida al eliminarla, y todas las reglas de inferencia dan lugar a un secuente inferior verdadero si sus secuentes superiores lo son, luego la única posibilidad es que la fórmula Σ_1 sea la fórmula principal de la regla, por lo que ésta tiene que ser de la forma

$$\frac{\Gamma \Rightarrow \Delta,\, \phi(\bar{a}, t)}{\Gamma \Rightarrow \Delta,\, \bigvee u\, \phi(\bar{a}, u),}$$

donde $\phi(\bar{a}, t)$ es verdadera (porque $\Gamma \Rightarrow \Delta$ es falso). Si $k = d(t)$, también será verdadera $\phi(\bar{a}, \bar{k})$, y a partir de k podemos calcular el mínimo $a \leq k$ tal que $\phi(\bar{a}, a)$ es verdadera. Por el teorema 3.9, en $\mathrm{AP}(\varnothing)$ se puede demostrar $\Rightarrow \phi(\bar{a}, \bar{a})$. Una vez más, todo el cálculo puede formalizarse en ARP, por lo que la función $h(D)$ que a cada demostración D en las condiciones indicadas le asigna el número a (y toma el valor 0 en otro caso) es recursiva primitiva.

Por último, si D una demostración en $\mathrm{I}\Sigma_k$ del secuente

$$\Rightarrow \bigvee u\, \phi(x_1, \ldots, x_n, u),$$

de ordinal menor que α, por el teorema 3.21 podemos suponer que consta únicamente de fórmulas de tipo Σ_k y por 3.13 podemos suponer que es regular. En particular, las variables $x_1, \ldots, x_n$ no se usan como variables propias en la demostración. En virtud del teorema 3.11, cualquier variable libre en D distinta de las x_i o de las variables propias puede sustituirse por 0 para obtener otra demostración del mismo secuente. El teorema 3.11 nos da también que al sustituir en D cada variable x_i por a_i obtenemos una demostración $D(\bar{a})$ del secuente

$$\Rightarrow \bigvee u\, \phi(\bar{a}, u)$$

con el mismo ordinal. Se trata de una demostración regular en la que las únicas variables libres son las que se usan como variables propias. Nuevamente, como la construcción de $D(\bar{a})$ a partir de D es completamente finitista, es pura rutina comprobar que puede formalizarse en ARP, por lo que la función $\bar{a} \mapsto D(\bar{a})$ (viendo a $D(\bar{a})$ como un número natural) es recursiva primitiva.

Concluimos que la función

$$f(x_1, \ldots, x_n) = h(F_\alpha(D(x_1, \ldots, x_n)))$$

es recursiva primitiva respecto de α y no es sino la función descrita en el enunciado pues, dados $a_1, \ldots, a_n$, la función $D(\bar{a})$ nos da una demostración del secuente $\Rightarrow \bigvee u\, \phi(\bar{a}, u)$ de ordinal menor que α, luego $F_\alpha(D(\bar{a}))$ nos da otra demostración del mismo secuente sin reglas de inferencia propias ni cortes sustanciales y $h(F_\alpha(D(\bar{a})))$ nos da el mínimo a tal que $\underset{\mathrm{AP}(\varnothing)}{\vdash} \Rightarrow \phi(\bar{a}, a)$. ■

Teorema 8.11 *Las funciones demostrablemente recursivas en* $\mathrm{I}\Sigma_k$ *son las funciones recursivas primitivas respecto de un ordinal* $\alpha \prec \omega^{(k+1)}$.

DEMOSTRACIÓN: Si $f(x_1, \ldots, x_n)$ es demostrablemente recursiva en $\mathrm{I}\Sigma_k$, de acuerdo con [LM 7.13], existe una fórmula $\phi(x_1, \ldots, x_n, x, y)$ de tipo Δ_0 tal que

$$f(a_1, \ldots, a_n) = a \quad \text{syss} \quad \mathbb{N} \vDash \bigvee u\, \phi(a_1, \ldots, a_n, u, a)$$

y

$$\underset{\mathrm{I}\Sigma_k}{\vdash} \overset{1}{\bigvee} v \bigvee u\, \phi(x_1, \ldots, x_n, u, v).$$

Consideramos la fórmula

$$\psi(x_1, \ldots, x_n, w) \equiv \bigvee uv \leq w(w = \langle u, v\rangle \wedge \phi(x_1, \ldots, x_n, u, v)).$$

Es de tipo Δ_0 y $\underset{\mathrm{I}\Sigma_k}{\vdash} \bigvee w\, \psi(x_1, \ldots, x_n, w)$. Podemos tomar una demostración formada por fórmulas Σ_k y Π_k y con ordinal $\alpha \prec \omega^{(k+1)}$. Por el teorema anterior, la función

$$g(a_1, \ldots, a_n) = \mu w \underset{\mathrm{AP}(\varnothing)}{\vdash} \psi(a_1, \ldots, a_n, w)$$

es recursiva primitiva respecto de α. Si $g(a_1, \ldots, a_n) = b$, entonces

$$\mathbb{N} \vDash \psi(a_1, \ldots, a_n, b),$$

lo cual se traduce en que $b = \langle c, a\rangle$ y $\mathbb{N} \vDash \phi(a_1, \ldots, a_n, c, a)$, y esto implica que $a = f(1_1, \ldots, a_n)$, luego

$$f(x_1, \ldots, x_n) = p_1^\infty(g(x_1, \ldots, x_n)),$$

lo que prueba que f es recursiva primitiva respecto de α. ■

Nota Teniendo en cuenta la prueba del teorema 8.10, hemos probado que si f es una función demostrablemente recursiva en $\mathrm{I}\Sigma_k$, entonces se puede expresar en la forma

$$f(\bar{x}) = p_1^\infty(h(F_\alpha(D(\bar{x})))),$$

o, más brevemente, en la forma

$$f(\bar{x}) = g(F_\alpha(h(\bar{x}))),$$

donde las funciones $g(x)$ y $h(x_1, \ldots, x_n)$ son recursivas primitivas y

$$F_\alpha(D) = \begin{cases} F_\alpha(r(D)) & \text{si } O(r(D)) \prec O(D) \prec \alpha, \\ D & \text{en otro caso,} \end{cases}$$

para cierto $\alpha \prec \omega^{(k+1)}$. Notemos además que α, g y h dependen de f, pero las funciones F_α, $r(D)$ y $O(D)$ no. ■

Puesto que toda función demostrablemente recursiva en AP es claramente demostrablemente recursiva en algún $\mathrm{I}\Sigma_k$, hemos demostrado:

Teorema 8.12 *Las funciones demostrablemente recursivas en* AP *son las funciones recursivas primitivas respecto de algún ordinal.*

8.4 Las funciones de Hardy

Vamos a dar otra caracterización de las funciones demostrablemente recursivas en AP que nos mostrará ejemplos concretos de funciones que son demostrablemente recursivas en AP y no son recursivas primitivas, o de funciones recursivas que no son demostrablemente recursivas en AP. Demostramos antes un resultado técnico que vamos a necesitar sobre sucesiones fundamentales:

Teorema 8.13 *Se cumple:*

1. *Si $\alpha > 1$ y $n > 0$, entonces $(\omega^\alpha)[n]$ es un ordinal límite.*

2. *Si λ es un ordinal límite y $m > 0$, existen ordinales*

$$\lambda = \lambda_1 \succ \lambda_2 \succ \cdots \succ \lambda_k \succ \lambda_{k+1} = 0$$

tales que, para $i \leq k$, se cumple que λ_i es un ordinal límite y $\lambda_{i+1} = \lambda_i[0]$ o bien $\lambda_{i+1} = \lambda_i[m]$.

3. *Si λ es un ordinal límite que no es de la forma $\lambda_0 + \omega$, dados m, $r > 1$, existen ordinales*

$$\lambda[r] = \lambda_1 \succ \lambda_2 \succ \cdots \succ \lambda_k \succ \lambda_{k+1} = \lambda[r-1]$$

tales que, para $i \leq k$, se cumple que λ_i es un ordinal límite y $\lambda_{i+1} = \lambda_i[0]$ o bien $\lambda_{i+1} = \lambda_i[m]$.

DEMOSTRACIÓN: 1) Si $\alpha = \eta + 1$, entonces $\omega^\alpha[n] = \omega^\eta \cdot n$, que ciertamente es un ordinal límite. Si α es un ordinal límite, entonces $\omega^\alpha[n] = \omega^{\alpha[n]}$, que es un ordinal límite, pues, claramente $\alpha[n] \neq 0$.

2) Si $\lambda = \beta + \omega$, entonces $\lambda[0] = \beta$ es un ordinal límite o 0 (en cambio, $\lambda[m] = \beta + m$ sería un ordinal sucesor, luego no nos serviría). Por el contrario, si $\lambda = \beta + \omega^\alpha$, con $\alpha > 1$, entonces $\lambda[m] = \beta + \omega^\alpha[m]$ es un ordinal límite por el apartado anterior (mientras que, si α es un ordinal límite, $\lambda[0] = \beta + \omega^{\alpha[0]}$ podría ser un ordinal sucesor y no serviría).

Por lo tanto, aplicando sucesivamente $[0]$ o $[m]$ según el caso, podemos generar una sucesión decreciente de ordinales límite que, tras un número finito de pasos, tiene que acabar en 0.

3) Por hipótesis $\lambda = \beta + \omega^\alpha$, con $\alpha > 1$. Si $\alpha = \eta + 1$, con $\eta > 0$, entonces

$$\lambda[r-1] = \beta + \omega^\eta(r-1), \quad \lambda[r] = \beta + \omega^\eta \cdot r = \lambda[r-1] + \omega^\eta.$$

Si $\eta = \eta_0 + 1$, entonces $\lambda[r-1] = \lambda[r][0]$ y así la sucesión del enunciado consta sólo de dos términos.

Si η es un ordinal límite, por el apartado anterior tenemos una sucesión

$$\omega^\eta = \eta_0 \succ \eta_1 \succ \cdots \succ \eta_{k+1} = 0,$$

donde cada término se obtiene del anterior mediante $[0]$ o $[m]$ y todos son ordinales límite menos el último. Basta tomar $\lambda_i = \lambda[r-1] + \eta_i$.

Supongamos ahora que α es un ordinal límite, con lo que

$$\lambda[r] = \beta + \omega^{\alpha[r]}, \qquad \lambda[r-1] = \beta + \omega^{\alpha[r-1]}.$$

Si α no es de la forma $\alpha_0 + \omega$, razonando por inducción transfinita, podemos suponer que existe una sucesión

$$\alpha[r] = \eta_0 \succ \eta_1 \succ \cdots \succ \eta_{k+1} = 0$$

donde cada término se obtiene del anterior mediante $[0]$ o $[m]$ y todos son ordinales límite menos el último. Basta tomar $\lambda_i = \beta + \omega^{\eta_i}$.

Por último, supongamos que $\alpha = \alpha_0 + \omega$. Entonces

$$\lambda[r] = \beta + \omega^{\alpha_0 + r}, \qquad \lambda[r-1] = \beta + \omega^{\alpha_0 + r - 1}.$$

Observemos que $\lambda[r][m] = \beta + \omega^{\alpha_0 + r - 1} \cdot r$, luego en el caso en que $r = 1$ tenemos que $\lambda[r][m] = \lambda[r-1]$ y tenemos la sucesión del enunciado en dos pasos. Si $r > 1$, tenemos que

$$\lambda[r][m] = \lambda[r-1] + \omega^{\alpha_0 + r - 1}(r-1).$$

Por el apartado anterior, aplicando $[0]$ o $[m]$ obtenemos una sucesión decreciente de ordinales límite que lleva de $\lambda[r][m]$ a $\lambda[r-1] + \omega^{\alpha_0 + r - 1}(r-2)$, y continuando el proceso $r-1$ veces, tras un número finito de pasos llegamos a $\lambda[r-1]$. ■

Definición 8.14 Para cada ordinal α, definimos la *función de Hardy* $h_\alpha(x)$ de modo que

$$h_0(x) = x, \qquad h_{\alpha+1}(x) = h_\alpha(x+1), \qquad h_\lambda(x) = h_{\lambda[x]}(x).$$

Observemos que, viendo a h como una función de dos variables, esta definición se ajusta a la definición 8.7 con $r(\alpha, x) = \alpha[x]$ si la expresamos así:

$$h_\alpha(x) = \begin{cases} h_{\alpha[x]}(x+1) \cdot \chi[S\alpha] + h_{\alpha[x]}(x) \cdot \chi[L\alpha] & \text{si } \alpha[x] \prec \alpha, \\ x & \text{en otro caso,} \end{cases}$$

donde $S\alpha$ y $L\alpha$ son las fórmulas que expresan, respectivamente, que α es un ordinal sucesor o un ordinal límite, y convenimos que $\alpha[x] = 0$ cuando α no es un ordinal. En particular, esto hace que, si α no es un ordinal, se cumpla por definición $h_\alpha(x) = 0$, pero sólo vamos a considerar las funciones h_α cuando α es un ordinal.

Por ejemplo,

$$\begin{aligned} h_{\omega^\omega}(2) &= h_{\omega^2}(2) = h_{\omega\cdot 2}(2) = h_{\omega\cdot 2+2}(2) = h_{\omega\cdot 2+1}(3) = h_{\omega\cdot 2}(4) \\ &= h_{\omega+4}(4) = \cdots = h_\omega(8) = h_8(8) = \cdots = h_0(16) = 16. \end{aligned}$$

A la hora de calcular funciones de Hardy es útil el resultado siguiente:

Teorema 8.15 *Si* $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_{n-1}}$ *y* $\beta = \omega^{\delta_0} + \cdots + \omega^{\delta_{m-1}}$ *con*

$$\eta_0 \succeq \cdots \succeq \eta_{n-1} \succeq \delta_0 \succeq \cdots \succeq \delta_{m-1}$$

(de modo que al calcular $\alpha + \beta$ no se cancelan términos), entonces

$$h_{\alpha+\beta}(x) = h_\alpha(h_\beta(x)).$$

Demostración: Razonamos por inducción transfinita sobre β. Para $\beta = 0$ es trivial. Si $\beta = \delta + 1$, entonces

$$h_{\alpha+\beta}(x) = h_{\alpha+\delta}(x+1) = h_\alpha(h_\delta(x+1)) = h_\alpha(h_\beta(x)).$$

Si β es un ordinal límite,

$$h_{\alpha+\beta}(x) = h_{(\alpha+\beta)[x]}(x) = h_{\alpha+\beta[x]}(x) = h_\alpha(h_{\beta[x]}(x)) = h_\alpha(h_\beta(x)).$$

■

Usaremos exponentes para indicar iteración de funciones, es decir:

$$f^0(x) = x, \quad f^{n+1}(x) = f(f^n(x)).$$

Ahora es fácil comprobar que

$$\begin{aligned} h_{\omega^0}(x) &= h_1(x) = x+1, \\ h_{\omega^{\eta+1}}(x) &= h_{\omega^\eta \cdot x}(x) = h^x_{\omega^\eta}(x), \\ h_{\omega^\lambda}(x) &= h_{\omega^{\lambda[x]}}(x). \end{aligned}$$

La segunda ecuación se sigue del teorema anterior.

Las funciones de Hardy verifican ciertas condiciones de monotonía. Empezamos probando dos de ellas:

Teorema 8.16 *Para todo ordinal α, se cumple:*

1. *La función h_α es estrictamente creciente.*

2. *Si α es un ordinal límite y $i < j \leq x$, entonces $h_{\alpha[i]}(x) \leq h_{\alpha[j]}(x)$.*

DEMOSTRACIÓN: Probamos simultáneamente las dos propiedades por inducción sobre α. Si $\alpha = 0$ ambas son triviales. Suponemos que las ambas se cumplen para todo ordinal $\alpha_0 \prec \alpha$ y veamos en primer lugar que se cumple 2).

Suponemos que α es un ordinal límite y tomamos $i < j \leq x$. No perdemos generalidad si suponemos que $j = i + 1$. Si $\alpha = \alpha_0 + \omega$, entonces

$$h_{\alpha[i]}(x) = h_{\alpha_0+i}(x) < h_{\alpha_0+i}(x+1) = h_{\alpha_0+j}(x) = h_{\alpha[j]}(x),$$

donde hemos usado que $\alpha_0 + i$ cumple 1).

Si α no es de la forma $\alpha_0+\omega$, el teorema 8.13 nos da una sucesión de ordinales límite

$$\alpha[i] = \alpha_0 \succ \alpha_1 \succ \cdots \succ \alpha_{k+1} = \alpha[j],$$

donde cada término se obtiene del anterior aplicando $[0]$ o $[x]$ (notemos que $x > i \geq 0$). Basta probar que $h_{\alpha_{s+1}}(x) \leq h_{\alpha_s}(x)$ para todo $s = 0, \ldots, k$. En efecto, si $\alpha_{s+1} = \alpha_s[0]$, por la hipótesis de inducción aplicada a α_s,

$$h_{\alpha_{s+1}}(x) = h_{\alpha_s[0]}(x) \leq h_{\alpha_s[x]}(x) = h_{\alpha_s}(x).$$

Si $\alpha_{s+1} = \alpha_s[x]$, entonces $h_{\alpha_{s+1}}(x) = h_{\alpha_s[x]}(x) = h_{\alpha_s}(x)$.

Con esto tenemos probado 2) para α. Veamos ahora que se cumple 1). Si $\alpha = \alpha_0 + 1$, es obvio. Supongamos, pues, que α es un ordinal límite. Entonces

$$h_\alpha(x) = h_{\alpha[x]}(x) < h_{\alpha[x]}(x+1) \leq h_{\alpha[x+1]}(x+1) = h_\alpha(x+1),$$

donde la primera desigualdad se cumple por hipótesis de inducción y la segunda por la propiedad 2), que ya hemos probado que se cumple para α. ■

En el teorema siguiente usamos la complejidad de un ordinal, definida en 6.12:

Teorema 8.17 *Si $\beta \prec \alpha$ y $c(\beta) \leq n$, entonces $h_\beta(n) < h_\alpha(n)$.*

DEMOSTRACIÓN: Por inducción sobre α. Si $\alpha = \alpha_0 + 1$, entonces $\beta \preceq \alpha_0$, luego

$$h_\beta(n) \leq h_{\alpha_0}(n) < h_{\alpha_0}(n+1) = h_\alpha(n).$$

Si α es un ordinal límite, como $c(\beta) \leq n$, por 6.13 tenemos que $\beta < \alpha[n]$, luego, por hipótesis de inducción, $h_\beta(n) < h_{\alpha[n]}(n) = h_\alpha(n)$. ■

Teorema 8.18 *Si $\alpha \succ 0$ y $x > 0$, entonces $x < h_\alpha(x)$.*

Demostración: Por inducción sobre α. Si $\alpha = \beta + 1$ entonces

$$h_\alpha(x) = h_\beta(x+1) \geq x + 1 > x,$$

donde la desigualdad no estricta se cumple trivialmente si $\beta = 0$ y por hipótesis de inducción en caso contrario. Análogamente, si α es un ordinal límite,

$$h_\alpha(x) = h_{\alpha[x]}(x) > x,$$

pues, como $x > 0$, tenemos que $\alpha[x] \succ \alpha[0] \succ 0$. ■

Seguidamente demostraremos que las funciones de Hardy crecen más rápidamente que muchas otras funciones. Para precisar esto diremos que una función $f(x)$ *mayora* a otra función $g(x_1, \ldots, x_n)$ si

$$g(x_1, \ldots, x_n) < f(\text{máx}\{x_1, \ldots, x_n\})$$

siempre que $\text{máx}\{x_1, \ldots, x_n\}$ es suficientemente grande. Notemos que esto equivale a que existe un número M tal que

$$g(x_1, \ldots, x_n) < \text{máx}\{f(\text{máx}\{x_1, \ldots, x_n\}), M\}$$

para todo $x_1, \ldots, x_n$.

Teorema 8.19 *Se cumple:*

1. *Si unas funciones*

$$g(x_1, \ldots, x_m), \quad h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)$$

están mayoradas por h_{ω^α}, entonces su composición $f(x_1, \ldots, x_n)$ está mayorada por $h_{\omega^\alpha \cdot 2}$.

2. *Si unas funciones*

$$g(x_1, \ldots, x_n), \quad h(x_1, \ldots, x_{n+1}, y)$$

están mayoradas por h_{ω^α}, entonces la función $f(x_1, \ldots, x_{n+1})$ definida por recursión a partir de g y h está mayorada por $h_{\omega^{\alpha+1}+1}$.

Demostración: Sea M tal que

$$g(y_1, \ldots, y_m) < \text{máx}\{h_{\omega^\alpha}(\text{máx}\{y_1, \ldots, y_m\}), M\},$$

$$h_i(x_1, \ldots, x_n) < \text{máx}\{h_{\omega^\alpha}(\text{máx}\{x_1, \ldots, x_n\}), M\}.$$

Entonces, si llamamos $x = \text{máx}\{x_1, \ldots, x_n\}$, tenemos que

$$f(x_1, \ldots, x_n) < \text{máx}\{h_{\omega^\alpha}(\text{máx}\{h_i(x_1, \ldots, x_n)\}), M\}$$

$$\leq \text{máx}\{h_{\omega^\alpha}(\text{máx}\{h_{\omega^\alpha}(x), M\}), M\} \leq \text{máx}\{h_{\omega^\alpha}(h_{\omega^\alpha}(x)), h_{\omega^\alpha}(M)\}$$

$$= \text{máx}\{h_{\omega^\alpha \cdot 2}(x), M'\}.$$

Supongamos ahora que

$$g(x_1, \ldots, x_n) < \text{máx}\{h_{\omega^\alpha}(\text{máx}\{x_1, \ldots, x_n\}), M\},$$

$$h(x_1, \ldots, x_{n+1}, y) < \text{máx}\{h_{\omega^\alpha}(\text{máx}\{x_1, \ldots, x_{n+1}, y\}), M\}$$

y vamos a probar que

$$f(x_1, \ldots, x_n, x) < h_{\omega^\alpha}^{x+1}(\text{máx}\{x_1, \ldots, x_n, x, M\}).$$

Razonamos por inducción sobre x. Para $x = 0$ es inmediato (teniendo en cuenta que $M < h_{\omega^\alpha}(M)$). Si es cierto para x, entonces

$$\begin{aligned} f(x_1, \ldots, x_n, x+1) &= h(x_1, \ldots, x_n, x, f(x_1, \ldots, x_n, x)) \\ &< \text{máx}\{h_{\omega^\alpha}(\text{máx}\{x_1, \ldots, x_n, x, f(x_1, \ldots, x_n, x)\}), M\} \\ &\leq \text{máx}\{h_{\omega^\alpha}(\text{máx}\{x_1, \ldots, x_n, x, h_{\omega^\alpha}^{x+1}(\text{máx}\{x_1, \ldots, x_n, x, M\})\}), M\} \\ &\leq h_{\omega^\alpha}(h_{\omega^\alpha}^{x+1}(\text{máx}\{x_1, \ldots, x_n, x, M\})) \leq h_{\omega^\alpha}^{x+2}(\text{máx}\{x_1, \ldots, x_n, x+1, M\}). \end{aligned}$$

Esto termina el razonamiento inductivo. Si llamamos

$$M' = \text{máx}\{x_1, \ldots, x_{n+1}, M\} + 1,$$

tenemos que

$$\begin{aligned} f(x_1, \ldots, x_{n+1}) &< h_{\omega^\alpha}^{x_{n+1}+1}(M') \leq h_{\omega^\alpha}^{M'}(M') = h_{\omega^{\alpha+1}}(M') \\ &= h_{\omega^{\alpha+1}}(\text{máx}\{x_1, \ldots, x_{n+1}, M\} + 1) = h_{\omega^{\alpha+1}+1}(\text{máx}\{x_1, \ldots, x_{n+1}, M\}) \\ &= h_{\omega^{\alpha+1}+1}(\text{máx}\{x_1, \ldots, x_{n+1}\}) \end{aligned}$$

si $\text{máx}\{x_1, \ldots, x_{n+1}\} > M$. ■

Teorema 8.20 *La función h_{ω^ω} mayora a todas las funciones recursivas primitivas.*

Demostración: La función $C(x) = 0$ está mayorada por h_0, la función $S(x) = x + 1$ está mayorada por $h_2(x) = x + 2$ y las proyecciones P_i^r están mayoradas por $h_1(x) = x + 1$. El teorema 8.17 implica que todas ellas están mayoradas por h_ω. El teorema anterior implica que si una función f está definida por composición o recursión a partir de funciones mayoradas por h_{ω^n}, entonces f está mayorada por $h_{\omega^{n+2}}$, luego una simple inducción prueba que toda función recursiva primitiva está mayorada por una función h_{ω^n}, para un n suficientemente grande, luego todas ellas están mayoradas por h_{ω^ω}. ■

En particular, las funciones h_α con $\omega^\omega \preceq \alpha$ no son recursivas primitivas. Por el contrario, las funciones h_α con $\alpha \prec \omega^\omega$ sí que lo son, ya que α es entonces suma de un número finito de potencias ω^n, luego por 8.15 basta probar que todas las funciones h_{ω^n} son recursivas primitivas, y esto se sigue inductivamente de la relación $h_{\omega^{n+1}}(x) = h^x_{\omega^n}(x)$. En efecto, si h_{ω^n} es recursiva primitiva, también lo es la función

$$F(x,0) = x, \qquad F(x, y+1) = h_{\omega^n}(F(x,y)),$$

que cumple $F(x,y) = h^y_{\omega^n}(x)$, luego también es recursiva primitiva la función

$$h_{\omega^{n+1}}(x) = F(x,x).$$

■

Notemos que, aunque no sean recursivamente primitivas, las funciones de Hardy son sin duda recursivas (sabemos calcularlas). Más aún:

Teorema 8.21 *Las funciones de Hardy son demostrablemente recursivas en* AP.

Demostración: Fijado un ordinal β, la función

$$H_\beta(\alpha,x) = \begin{cases} H(\alpha[x], x+1)\cdot\chi[S\alpha] + H(\alpha[x],x)\cdot\chi[L\alpha] & \text{si } \alpha[x] \prec \alpha \prec \beta, \\ x & \text{en otro caso,} \end{cases}$$

es recursiva primitiva respecto de β, luego por 8.12 es demostrablemente recursiva en AP, luego también lo es $h_\alpha(x) = H_{\alpha+1}(\alpha, x)$. ■

Ahora vamos a probar que toda función demostrablemente recursiva en AP está mayorada por una función de Hardy. Necesitamos un resultado técnico:

Teorema 8.22 *Si D es una demostración en $\mathrm{I}\Sigma_k$ formada por fórmulas de tipo Σ_k o Π_k, entonces su ordinal cumple $c(O(D)) < D$.*

Demostración: Si S es un secuente de D, llamemos $g(S)$ a la suma de los grados de las fórmulas que lo componen. Vamos a probar, más precisamente, que

$$c(o(S;D)) + g(S) < D_S,$$

donde D_S es la subdemostración de D formada por S y los secuentes situados sobre S en D. Razonamos inductivamente:

1. Si S es un secuente inicial, entonces

$$c(o(S;D)) + g(S) \leq 1 + 0 < D_S,$$

pues D_S codifica una aplicación que asigna el secuente S al árbol de un solo nodo y, ciertamente, tiene que ser mayor que 1.

2. Si S es el secuente inferior de una regla de debilitación, con secuente superior S_1, tenemos que

$$c(o(S;D)) + g(S) \leq c(o(S_1;D)+1) + g(S_1) + g(\alpha)$$

$$= c(o(S_1;D)) + g(S_1) + g(\alpha) + 1 < D_{S_1} + S \leq D_S,$$

pues el secuente S contiene la fórmula α, luego $g(\alpha)+1 < S$.

3. Si S es el secuente inferior de una regla lógica irrelevante con secuente superior S_1, entonces
$$c(o(S;D)) + g(S) = c(o(S_1;D)) + g(S_1) < D_{S_1} \leq D_S.$$

4. Si S es el secuente inferior de una regla izquierda del disyuntor con secuentes superiores S_1 y S_2, entonces
$$c(o(S;D)) + g(S) \leq c(o(S_1;D)) + c(o(S_2;D)) + g(S_1) + g(S_2)$$
$$< D_{S_1} + D_{S_2} < D_S.$$

5. Si S es el secuente inferior de una regla de inferencia relevante con secuente superior S_1, entonces
$$c(o(S;D)) + g(S) \leq c(o(S_1;D) + 2) + g(S_1) + 1 \leq$$
$$c(o(S_1;D)) + g(S_1) + 3 < D_{S_1} + S < D_S.$$

6. Si S es el secuente inferior de una regla de corte con secuentes superiores S_1 y S_2, fórmula de corte α y
$$h_1 = h(S_1;D) = h(S_2;D), \quad h_0 = h(S;D), \quad \mu_i = o(S_i;D),$$
entonces
$$c(o(S;D)) + g(S) \leq c(\omega_{h_1-h_0}(o(S_1;D)\# o(S_2;D))) + g(S_1) + g(S_2) - g(\alpha)$$
$$\leq c(o(S_1;D)) + c(o(S_2;D)) + h_1 - h_0 + g(S_1) + g(S_2) - g(\alpha)$$
$$< D_{S_1} + D_{S_2} \leq D.$$
Donde hemos usado que si el grado de la fórmula de corte α es $g(\alpha) \leq h_0$, entonces $h_1 - h_0 = 0$ y en caso contrario $h_1 - h_0 = g(\alpha) - h_0 \leq g(\alpha)$, por lo que, en cualquier caso,
$$h_1 - h_0 - g(\alpha) \leq 0.$$

7. Si S es el secuente inferior de una inducción con secuente superior S', $h_1 = h(S';D)$, $h_0 = h(S;D)$ y g es el grado de la regla, entonces
$$c(o(S;D)) + g(S) \leq c(o(S';D)) + h_1 - h_0 + 1 + g(S')$$
$$< D_{S'} + S \leq D_S,$$
donde usamos que, como antes, $h_1 - h_0 \leq g$, luego $h_1 - h_0 + 1 \leq S$, ya que el secuente S contiene dos fórmulas de grado g. ■

Teorema 8.23 *Toda función demostrablemente recursiva en* AP *está mayorada por una función de Hardy.*

Demostración: Sea $n \geq 2$ y llamemos $\Phi_n(x)$ a la fórmula que expresa que x es una demostración en $I\Sigma_{n-1}$ formada por fórmulas Σ_{n-1} o Π_{n-1}. Recordemos que $r(D)$ es la función recursiva primitiva tal que si se cumple $\Phi_n(D)$, entonces $r(D)$ es la demostración del mismo secuente construida en el teorema 7.18, y en caso contrario, $r(D) = D$. Teniendo en cuenta la nota tras el teorema 8.11 así como el teorema 8.19, basta probar que la función

$$F_n(D) = \begin{cases} F_n(r(D)) & \text{si } O(r(D)) \prec O(D) \prec \omega^{(n)}, \\ D & \text{en otro caso} \end{cases}$$

está mayorada por una función de la forma $h_\alpha(u(x))$, donde $u(x)$ es recursiva primitiva. Podemos suponer que $n \geq 2$. Definimos

$$|D| = \begin{cases} O(D) & \text{si } \Phi_n(D), \\ D & \text{en caso contrario.} \end{cases}$$

Claramente la función $|D|$ también es recursiva primitiva.

Como $h_{\omega^{(n)}}$ mayora a todas las funciones recursivas primitivas, existe un $M \geq 2$ tal que

$$\text{máx}\{x, \text{máx}\{(n+1)r(x), (n+1)r(r(x)), y\} + y\} \leq h_{\omega^{(n)}}(\text{máx}\{x, y\}) + M.$$

Definimos $u(x) = \text{máx}\{(n+1)x, (n+1)r(x), M\} + M$. Así,

$$\begin{aligned} \text{máx}\{x, u(r(x))\} &= \text{máx}\{x, \text{máx}\{(n+1)r(x), (n+1)r(r(x)), M\} + M\} \\ &\leq h_{\omega^{(n)}}(\text{máx}\{x, M\}) + M \\ &\leq h_{\omega^{(n)}}(\text{máx}\{x, M\} + M) \\ &\leq h_{\omega^{(n)}}(u(x)), \end{aligned}$$

donde la penúltima desigualdad se debe a que $h_{\omega^{(n)}}$ es estrictamente creciente.

Veamos ahora que $F_n(x) \leq h_{\omega^{(n)} \cdot |x|}(u(x))$.

Si no se cumple que $O(r(x)) \prec O(x) \prec \omega^{(n)}$, entonces

$$F_n(x) = x \leq u(x) \leq h_{\omega^{(n)} \cdot |x|}(u(x)),$$

porque las funciones de Hardy son crecientes. Así pues, basta probar la desigualdad con el supuesto adicional de que se cumple $\Phi_n(x)$ y que $r(x)$ es otra demostración del mismo secuente de modo que

$$|r(x)| \preceq O(r(x)) \prec O(x) = |x| \prec \omega^{(n)}$$

Razonamos por inducción transfinita sobre $|x| \prec \alpha$. Suponemos que el resultado es cierto para todo y tal que $|y| \prec |x|$. Como $|r(x)| \prec |x|$, podemos aplicar la hipótesis de inducción:

$$\begin{aligned} F_n(x) &\leq \text{máx}\{x, F_n(r(x))\} \\ &\leq \text{máx}\{x, h_{\omega^{(n)} \cdot |r(x)|}(u(r(x)))\} \\ &\leq h_{\omega^{(n)} \cdot |r(x)|}(\text{máx}\{x, u(r(x))\}) \\ &\leq h_{\omega^{(n)} \cdot |r(x)|}(h_{\omega^{(n)}}(u(x))) \\ &\leq h_{\omega^{(n)}(|r(x)|+1)}(u(x)) \\ &\leq h_{\omega^{(n)} \cdot |x|}(u(x)). \end{aligned}$$

La última desigualdad se sigue del teorema 8.17, pues, por el teorema 8.22 aplicado a $D = r(x)$ y $O(D) = |r(x)|$, tenemos que

$$c(\omega^{(n)}(|r(x)| + 1)) = (n + 1)c(|r(x)| + 1) =$$

$$(n + 1)(c(|r(x)|) + 1) \leq (n + 1)r(x) < u(x).$$

Finalmente, concluimos que $F_n(x) < h_{\omega^{(n)}\cdot\omega^{(n)}}(u(x))$. En efecto, si se cumple $\Phi_n(x)$ y $O(r(x)) \prec O(x)$, entonces, de nuevo por el teorema 8.22, tenemos que $c(\omega^{(n)}\cdot|x|) = (n+1)c(O(x)) < (n+1)x < u(x)$, luego 8.17 nos da la desigualdad. En otro caso es $F_n(x) = x$ y la desigualdad es inmediata por la monotonía de las funciones de Hardy. Así pues, tomando $\alpha = \omega^{(n)} \cdot \omega^{(n)}$, se cumple que $F_n(x) < h_\alpha(u(x))$. ■

Ahora podemos caracterizar las funciones demostrablemente recursivas en AP en términos de las funciones de Hardy:

Definición 8.24 Una función f pertenece a la *clase de Hardy* si existe una sucesión de funciones $f_1, \ldots, f_k$ de modo que f_k es f y cada f_i es la función, nula C, una proyección P_i^r, una función de Hardy h_α o bien está definida por composición o recursión a partir de funciones anteriores de la sucesión.

Teniendo en cuenta que la función sucesor es la función de Hardy h_1, es inmediato que la clase de Hardy incluye a todas las funciones recursivas primitivas, así como que toda función de la clase de Hardy es demostrablemente recursiva en AP. De hecho:

Teorema 8.25 *Las funciones demostrablemente recursivas en* AP *son las funciones de la clase de Hardy.*

Demostración: Por la nota tras el teorema 8.11, toda función demostrablemente recursiva en AP es composición de funciones recursivas primitivas y una función

$$F_n(D) = \begin{cases} F_n(r(D)) & \text{si } O(r(D)) \prec O(D) \prec \omega^{(n)}, \\ D & \text{en otro caso,} \end{cases}$$

luego basta probar que esta función está en la clase de Hardy. Para ello definimos la función recursiva primitiva

$$q(x, 0) = x, \qquad q(x, y + 1) = r(q(x, y)).$$

Con la notación del teorema 8.23, si no se cumple $\Phi_n(x)$, entonces $r(x) = x$, luego $q(x, 0) = q(x, 1)$. Por otra parte, si suponemos que

$$\Phi_n(x) \land O(x) \prec \alpha \rightarrow \bigvee u\, q(x, u) = q(x, u + 1),$$

podemos probar que $\Phi_n(x) \land O(x) = \alpha \rightarrow \bigvee u\, q(x, u) = q(x, u + 1)$. En efecto, o bien $r(x) = x$, en cuyo caso sirve $u = 0$, o bien $\Phi_n(r(x)) \land O(r(x)) \prec \alpha$, luego la hipótesis de inducción nos da un y tal que $q(r(x), y) = q(r(x), y + 1)$, pero esto es lo mismo que $q(x, y+1) = q(x, y+2)$. Por el principio de inducción transfinita hasta $\omega^{(n)}$ concluimos que

$$\Phi_n(x) \to \bigvee u\, q(x,u) = q(x, u+1),$$

luego en cualquier caso $\bigvee u\, q(x,u) = q(x,u+1)$. Esto hace que la función

$$p(x) = \mu u(q(x,u) = q(x,u+1))$$

sea demostrablemente recursiva en AP. Está representada por la fórmula

$$\phi(x,y) \equiv \bigwedge i < y\, q(x,i) \neq q(x,i+1) \wedge q(x,y) = q(x,y+1).$$

Por el teorema 8.23 existe un ordinal α tal que $p(x) < h_\alpha(x)$. Pero la función $q(x,-)$ se vuelve constante en cuanto toma dos veces el mismo valor, por lo que

$$q(x, h_\alpha(x)) = q(x, h_\alpha(x)+1),$$

de donde $F_n(D) = q(x, h_\alpha(x))$, luego F_n está en la clase de Hardy. ■

Una función recursiva no demostrablemente recursiva en AP Observemos que $F(n) = h_{\omega^{(n)}}(n)$ es un ejemplo de función recursiva que no es demostrablemente recursiva en AP, pues mayora a todas las funciones de Hardy. En efecto, para todo ordinal α, podemos tomar un n tal que $c(\alpha) \leq n$ y $\alpha \prec \omega^{(n)}$, y entonces el teorema 8.17 nos da que $h_\alpha(n) < h_{\omega^{(n)}}(n)$. ■

Ahora necesitaremos una ligera variante de las funciones de Hardy, a saber, las funciones definidas mediante:

$$\tilde{h}_0(x) = x, \qquad \tilde{h}_{\alpha+1}(x) = \tilde{h}_\alpha(x+1), \qquad \tilde{h}_\lambda(x) = \tilde{h}_{\lambda[x]}(x+1).$$

Equivalentemente,

$$\tilde{h}_\alpha(x) = \begin{cases} \tilde{h}_{\alpha[x]}(x+1) & \text{si } \alpha[x] \prec \alpha, \\ x & \text{en otro caso.} \end{cases}$$

La prueba del teorema 8.21 se adapta fácilmente para probar que las funciones $\tilde{h}_\alpha$ son demostrablemente recursivas en AP. En este caso basta considerar la función

$$\tilde{H}_\beta(\alpha, x) = \begin{cases} \tilde{H}(\alpha[x], x+1) & \text{si } \alpha[x] \prec \alpha \prec \beta, \\ x & \text{en otro caso.} \end{cases}$$

Por otra parte, se cumple que $h_\alpha(x) \leq \tilde{h}_\alpha(x)$. Basta razonar por inducción sobre α. Para $\alpha = 0$ es trivial. Si $\alpha = \beta + 1$, entonces

$$h_\alpha(x) = h_\beta(x+1) \leq \tilde{h}_\beta(x+1) = \tilde{h}_\alpha(x).$$

Por último, si α es un ordinal límite,

$$h_\alpha(x) = h_{\alpha[x]}(x) \leq h_{\alpha[x]}(x+1) \leq \tilde{h}_{\alpha[x]}(x+1) = \tilde{h}_\alpha(x).$$

En particular $h_{\omega^{(n)}}(n) \leq \tilde{h}_{\omega^{(n)}}(n)$, luego la función $\tilde{F}(n) = \tilde{h}_{\omega^{(n)}}(n)$ también mayora a todas las funciones de Hardy.

La estrategia derecha de Hércules contra la Hidra Ahora podemos probar que en AP no es posible demostrar que Hércules siempre vence a la Hidra cuando usa la estrategia derecha.

Recordemos que el número de asaltos necesarios para derrotar a la Hidra con la estrategia derecha es $N_d(\alpha) = L_\alpha(2)$, donde L es la función dada por

$$L_0(n) = 0, \qquad L_\alpha(n) = L_{\alpha[n]}(n+1) + 1.$$

La función L está estrechamente relacionada con las funciones de Hardy:

Teorema 8.26 $\tilde{h}_\alpha(n) = \tilde{h}_{L_\alpha(n)}(n) = n + L_\alpha(n)$.

DEMOSTRACIÓN: Veamos la primera igualdad por inducción sobre α. Para $\alpha = 0$ es trivial. Si α no es nulo, entonces

$$\tilde{h}_\alpha(n) = \tilde{h}_{\alpha[n]}(n+1) = \tilde{h}_{L_{\alpha[n]}(n+1)}(n+1) = \tilde{h}_{L_{\alpha[n]}(n+1)+1}(n) = \tilde{h}_{L_\alpha(n)}(n).$$

La segunda desigualdad es inmediata, pues si m es un ordinal finito, se cumple que $\tilde{h}_m(n) = n + m$. ■

En particular $N_d(\alpha) + 2 = L_\alpha(2) + 2 = \tilde{h}_\alpha(2)$.

Teorema 8.27 (Kirby, Paris) *En* AP *no es posible demostrar que Hércules derrota siempre a la Hidra cuando emplea la estrategia derecha.*

DEMOSTRACIÓN: Sea cual sea el modo en que formalicemos el problema en AP, si de algún modo hemos definido una fórmula en $\mathcal{L}_a$ tal que $\mathbb{N} \vDash \phi(\bar{\alpha}, \bar{n}, \bar{\beta})$ si y sólo si β es el ordinal tras el asalto n-simo de la hidra que inicialmente tenía ordinal α (y, por ejemplo, es $\beta = 0$ si α no es un ordinal) y se cumple que

$$\underset{\mathrm{AP}}{\vdash} \bigwedge \alpha \bigvee n\, \phi(\alpha, n, 0),$$

es decir, si podemos demostrar en AP que la Hidra siempre acaba totalmente decapitada, llamando $\psi(\alpha, n) \equiv \phi(\alpha, n, 0) \land \bigwedge m < n\, \neg\phi(\alpha, n, 0)$, tendríamos que

$$\underset{\mathrm{AP}}{\vdash} \bigwedge \alpha \overset{1}{\bigvee} n\, \psi(\alpha, n)$$

y esto probaría que la función $N_d(\alpha)$ que determina el número de combates necesarios para decapitar completamente a la hidra de ordinal α cuando Hércules sigue la estrategia derecha es demostrablemente recursiva en AP. Basta probar que no es así. Ahora bien, para todo $n \geq 2$, aplicando la definición de $\tilde{h}$, tenemos que

$$\tilde{h}_{\omega^{(n)}}(n) = \tilde{h}_{\omega^{(n)}+n \dot{-} 2}(2) = N_d(\omega^{(n)} + n \dot{-} 2).$$

Por lo tanto, si N_d fuera demostrablemente recursiva en AP, sería una función de Hardy, al igual que $N_d(\omega^{(n)} + n \dot{-} 2)$, y entonces tendría que ser mayorada por $\tilde{h}_{\omega^{(n)}}(n)$, cuando acabamos de ver que no es así. ■

8.5 El teorema de Goodstein

Vamos a demostrar un teorema que demostró Goodstein en 1944, similar hasta cierto punto con el problema de Hércules y la Hidra, pero que admite un enunciado aritmético mucho más simple y tampoco puede demostrarse en la aritmética de Peano.

Tomemos un número cualquiera, como $x = 2\,085$, y expresémoslo como suma de potencias de 2:

$$x = 2^{11} + 2^5 + 2^2 + 1,$$

ahora expresemos los exponentes como suma de potencias de 2.

$$x = 2^{2^3+2^1+1} + 2^{2^2+1} + 2^2 + 1,$$

y a su vez, los exponentes de los exponentes:

$$x = 2^{2^{2+1}+2^1+1} + 2^{2^{2^1}+1} + 2^{2^1} + 1,$$

y a su vez los exponentes de los exponentes de los exponentes:

$$x = 2^{2^{2^1+1}+2^1+1} + 2^{2^{2^1}+1} + 2^{2^1} + 1.$$

Terminamos en cuanto todos los exponentes son iguales a 1 (podríamos expresar tambiñen $1 = 2^0$, pero enseguida veremos que es irrelevante hacerlo o no). A esta expresión la llamaremos la *descomposición completa* de n_0 en base 2. La descomposición completa en base 3 es

$$x = 2 \cdot 3^{2\cdot 3^1} + 2 \cdot 3^{3^1+2} + 3^{3^1+1} + 2 \cdot 3^{3^1} + 2 \cdot 3^1.$$

Podríamos eliminar los coeficientes escribiendo:

$$x = 3^{3^1+3^1} + 3^{3^1+3^1} + 3^{3^1+2} + 3^{3^1+2} + 3^{3^1+1} + 3^{3^1} + 3^{3^1} + 3^1 + 3^1,$$

pero también sucede que en la práctica es irrelevante hacerlo, pues estas descomposiciones completas nos interesan únicamente para calcular la función $G(k, x)$ que se obtiene a partir de la descomposición completa de x en base $k+2$ sustituyendo todas las bases $k+2$ por $k+3$. Por ejemplo,

$$\begin{aligned}
G(0, 2\,085) &= 3^{3^{3^1+1}+3^1+1} + 3^{3^{3^1}+1} + 3^{3^1} + 1 \\
&= 35\,917\,545\,547\,686\,059\,365\,808\,220\,103\,027\,933\,772\,032, \\
G(1, 2\,085) &= 2 \cdot 4^{2\cdot 4^1} + 2 \cdot 4^{4^1+2} + 4^{4^1+1} + 2 \cdot 4^{4^1} + 2 \cdot 4^1 \\
&= 140\,808.
\end{aligned}$$

Es claro que haber expresado $1 = 2^0$ o $1 = 3^0$ no afecta al cálculo de G, pues al sumar 1 a la base seguimos teniendo un 1. Similarmente, convertir los coeficientes en sumas de potencias tampoco altera el cálculo de G.

La función $G(k,x)$ es recursiva primitiva y se define fácilmente en ARP mediante recursión completa. Con la notación[8] del teorema 4.22 es

$$G(k,x) = \sum_{i<N_{k+2}(x)} x_i[k+2](k+3)^{G(k,i)}.$$

Notemos que, con la definición que hemos dado, $G(n,0) = 0$.

La *sucesión de Goodstein* de un número natural n se define recurrentemente como

$$g_n(0) = n, \qquad g_n(k+1) = G(k, g_n(k)) \dot{-} 1.$$

Así, la sucesión empieza con el valor $g_n(0) = n$, para calcular $g_n(1)$ calculamos la descomposición completa de n en base 2, sustituimos todos los doses por treses y restamos 1, luego calculamos la descomposición completa de $g_n(1)$ en base 3, sustituimos todos los treses por cuatros y restamos 1 y así sucesivamente. Por ejemplo,

$$g_3(0) = 2^1 + 1, \quad g_3(1) = 3^1 = 3, \quad g_3(2) = 2, \quad g_3(3) = 1, \quad g_3(4) = 0.$$

Notemos que la descomposición de 3 en base 4 es simplemente 3 o, equivalentemente, $4^0 + 4^0 + 4^0$, pero, como ya hemos explicado, es inútil escribir 1 como potencia con exponente 0.

$k+2$	c	v	d
2	4	4	2^2
3	3^3-1	26	$2\cdot 3^2+2\cdot 3^1+2$
4	$2\cdot 4^2+2\cdot 4+1$	41	$2\cdot 4^2+2\cdot 4^1+1$
5	$2\cdot 5^2+2\cdot 5$	60	$2\cdot 5^2+2\cdot 5^1$
6	$2\cdot 6^2+2\cdot 6-1$	83	$2\cdot 6^2+6^1+5$
7	$2\cdot 7^2+7+4$	109	$2\cdot 7^2+7^1+4$
8	$2\cdot 8^2+8+3$	139	$2\cdot 8^2+8^1+3$
9	$2\cdot 9^2+9+2$	173	$2\cdot 9^2+9^1+2$
10	$2\cdot 10^2+10+1$	211	$2\cdot 10^2+10^1+1$
11	$2\cdot 11^2+11$	253	$2\cdot 11^2+11^1$
12	$2\cdot 12^2+11$	299	$2\cdot 12^2+11$
13	$2\cdot 13^2+10$	348	$2\cdot 13^2+10$
14	$2\cdot 14^2+9$	401	$2\cdot 14^2+9$
15	$2\cdot 15^2+8$	458	$2\cdot 15^2+8$
16	$2\cdot 16^2+7$	519	$2\cdot 16^2+7$
17	$2\cdot 17^2+6$	584	$2\cdot 17^2+6$
18	$2\cdot 18^2+5$	653	$2\cdot 18^2+5$
19	$2\cdot 19^2+4$	726	$2\cdot 19^2+4$
20	$2\cdot 20^2+3$	803	$2\cdot 20^2+3$
21	$2\cdot 21^2+2$	884	$2\cdot 21^2+2$
22	$2\cdot 22^2+1$	969	$2\cdot 22^2+1$
23	$2\cdot 23^2$	1 058	$2\cdot 23^2$
24	$2\cdot 24^2-1$	1 151	$24^2+23\cdot 24^1+23$
25	$25^2+23\cdot 25+22$	1 222	$25^2+23\cdot 25^1+22$

[8] Recordemos que $N_d(x) = n_d(x)+1$ si $x \neq 0$, y $N_d(0) = 0$.

La tabla de la página anterior muestra los primeros términos de la sucesión g_4. En la columna c se muestra el cálculo, en la columna v el valor y en la columna d la descomposición completa en la base correspondiente, que es el punto de partida para el cálculo del término siguiente.

El teorema de Goodstein afirma que las sucesiones de Goodstein siempre alcanzan el valor 0, es decir:

Teorema 8.28 (Goodstein) $\bigwedge n \bigvee k\, g_n(k) = 0$.

Por ejemplo, es fácil ver que $g_0(0) = g_1(1) = g_2(3) = 0$, ya hemos visto que $g_3(4) = 0$ y, para la sucesión g_4, se cumple que

$$g_4(3 \cdot (2^{402\,653\,211} - 1)) = 0.$$

La idea de la demostración del teorema de Goodstein es probar que cada sucesión de Goodstein se corresponde con una sucesión decreciente de ordinales, y si ésta llega a 0, la sucesión de Goodstein también lo hace.

Llamamos $T_k(x)$ a la función dada por $T_k(0) = 0$ y, que, para $x > 0$, en la descomposición completa de x en base $k + 2$ (con los sumandos ordenados de modo que la sucesión de exponentes sea decreciente) sustituye cada base $k + 2$ por el ordinal ω (y transforma las sumas, productos y potencias de números naturales en las correspondientes a ordinales).

Por ejemplo,

$$\begin{aligned} T_0(2\,085) &= \omega^{\omega^{\omega+1}+\omega+1} + \omega^{\omega^{\omega}+1} + \omega^{\omega} + 1, \\ T_1(2\,085) &= \omega^{\omega\cdot 2} \cdot 2 + \omega^{\omega+2} \cdot 2 + \omega^{\omega+1} + \omega^{\omega} \cdot 2 + \omega \cdot 2. \end{aligned}$$

Recíprocamente, podemos considerar la función $G_k(\alpha)$ que, en la expresión de α en forma normal, sustituye cada ω por $k+2$. Conviene observar que $G_k(\alpha)$ admite una definición recurrente muy simple:

$$G_k(0) = 0, \quad G_k(\alpha + 1) = G_k(\alpha) + 1, \quad G_k(\lambda) = G_k(\lambda[k + 2]).$$

En efecto, los dos teoremas siguientes prueban que la función definida de este modo se comporta como hemos indicado:

Teorema 8.29 *Si* $\alpha = \omega^{\eta_0} + \cdots + \omega^{\eta_{n-1}}$ *y* $\beta = \omega^{\delta_0} + \cdots + \omega^{\delta_{m-1}}$ *con*

$$\eta_0 \succeq \cdots \succeq \eta_{n-1} \succeq \delta_0 \succeq \cdots \succeq \delta_{m-1}$$

(de modo que al calcular $\alpha + \beta$ *no se cancelan términos), entonces*

$$G_k(\alpha + \beta) = G_k(\alpha) + G_k(\beta).$$

Demostración: Lo probamos por inducción transfinita sobre β. Si $\beta = 0$ es trivial. Si $\beta = \delta + 1$, entonces

$$G_k(\alpha + \beta) = G_k(\alpha + \delta) + 1 = G_k(\alpha) + G_k(\delta) + 1 = G_k(\alpha) + G_k(\beta).$$

Si β es un ordinal límite

$$G_k(\alpha + \beta) = G_k(\alpha + \beta[k + 2]) = G_k(\alpha) + G_k(\beta[k + 2]) = G_k(\alpha) + G_k(\beta).$$

■

Teorema 8.30 $G_k(\omega^\alpha) = (k+2)^{G_k(\alpha)}$.

Demostración: Por inducción transfinita sobre α. Si $\alpha = 0$ es

$$G_k(\omega^0) = G_k(1) = 1 = (k+2)^0 = (k+2)^{G_k(0)}.$$

Si $\alpha = \beta + 1$, entonces, usando el teorema anterior,

$$G_k(\omega^{\beta+1}) = G_k(\omega^\beta \cdot (k+2)) = G_k(\omega^\beta) \cdot (k+2) =$$

$$(k+2)^{G_k(\beta)} \cdot (k+2) = (k+2)^{G_k(\beta)+1} = (k+2)^{G_k(\alpha)}.$$

Si α es un ordinal límite,

$$G_k(\omega^\alpha) = G_k(\omega^{\alpha[k+2]}) = (k+2)^{G_k(\alpha[k+2])} = (k+2)^{G_k(\alpha)}.$$ ■

Así pues, en efecto, $G_k(\alpha)$ se limita a sustituir cada ω por $k+2$ en la forma normal de α. Ahora son inmediatos los hechos siguientes:

1. $G_k(\alpha) = 0$ si y sólo si $\alpha = 0$.
2. $G_k(T_k(n)) = n$.

   (Si en el ordinal que resulta de sustituir cada base $k+2$ por ω en la descomposición completa de n en base $k+2$ sustituimos de nuevo cada ω por $k+2$, recuperamos el número n.)
3. $G(k, G_k(\alpha)) = G_{k+1}(\alpha)$.

   (Si en el número que resulta de sustituir cada ω por $k+2$ en la forma normal de α, sustituimos cada $k+2$ por $k+3$, obtenemos el número que resulta de sustituir cada ω por $k+3$ en α.)

Ahora consideramos la función dada por

$$P_k(0) = 0, \quad P_k(\alpha+1) = \alpha, \quad P_k(\lambda) = P_k(\lambda[k+2]).$$

Para interpretarla observamos primero que cumple lo siguiente:

Teorema 8.31 $G_k(P_k(\alpha)) = P_k(G_k(\alpha))$.

Demostración: Notemos que $G_k(\alpha)$ es un número natural, que aquí tiene que interpretarse como un ordinal finito. Por inducción transfinita sobre α. Si $\alpha = 0$ tenemos que

$$G_k(P_k(0)) = G_k(0) = 0 = P_k(0) = P_k(G_k(0)).$$

Si $\alpha = \beta + 1$, entonces

$$G_k(P_k(\alpha)) = G_k(\beta) = P_k(G_k(\beta)+1) = P_k(G_k(\alpha)).$$

Si α es un ordinal límite, entonces

$$G_k(P_k(\alpha)) = G_k(P_k(\alpha[k+2])) = P_k(G_k(\alpha[k+2])) = P_k(G_k(\alpha)).$$ ■

Notemos que $P_k(G_k(\alpha)) = G_k(\alpha) \dot{-} 1$, por lo que el teorema anterior afirma que, para cada ordinal α no nulo, $P_k(\alpha)$ es el ordinal tal que, cuando se le sustituye cada ω por $k+2$, el número que resulta es una unidad inferior al que resulta de sustituir cada ω por $k+2$ en α. Así:

$$G(k, G_k(\alpha)) \dot{-} 1 = G_{k+1}(\alpha) \dot{-} 1 = P_{k+1}(G_{k+1}(\alpha)) = G_{k+1}(P_{k+1}(\alpha)).$$

La relación con las sucesiones de Goodstein es ahora inmediata. Observamos que:

$$\begin{array}{rcl} g_n(0) & = & n = G_0(T_0(n)), \\ g_n(1) & = & G(0, G_0(T_0(n))) \dot{-} 1 = G_1(P_1(T_0(n))), \\ g_n(2) & = & G(1, G_1(P_1(T_0(n)))) \dot{-} 1 = G_2(P_2(P_1(T_0(n)))), \\ g_n(3) & = & G(2, G_2(P_2(P_1(T_0(n))))) \dot{-} 1 = G_3(P_3(P_2(P_1(T_0(n))))), \\ & \vdots & \end{array}$$

y esto nos lleva a definir

$$Q_0(\alpha) = \alpha, \quad Q_{k+1}(\alpha) = P_{k+1}(Q_k(\alpha)),$$

con lo que una inducción obvia prueba que

$$g_n(k) = G_k(Q_k(T_0(n))).$$

Por consiguiente, $g_n(k) = 0$ es equivalente a $Q_k(T_0(n)) = 0$.

Ahora bien, una inducción transfinita trivial prueba que si $\alpha \neq 0$, entonces $P_k(\alpha) \prec \alpha$, de donde, a su vez, si $Q_k(\alpha) \neq 0$, se cumple $Q_{k+1}(\alpha) \prec Q_k(\alpha)$, con lo que la sucesión

$$Q_0(T_0(n)) \succ Q_1(T_0(n)) \succ Q_2(T_0(n)) \succ \cdots$$

decrece estrictamente mientras no alcanza el valor 0. Como no hay sucesiones infinitas de ordinales estrictamente decrecientes, tiene que existir un k tal que $Q_k(T_0(n)) = 0$, y esto equivale a que $g_n(k) = 0$, y así queda probado el teorema de Goodstein.

Veamos ahora que no es demostrable en AP. Necesitamos una versión más general de la función Q:

$$Q_{n,0}(\alpha) = \alpha, \qquad Q_{n,k+1}(\alpha) = P_{n+k+1}(Q_{n,k}(\alpha)).$$

Notemos que $Q_k(\alpha) = Q_{0,k}(\alpha)$. Sigue siendo cierto que la sucesión

$$Q_{n,0}(\alpha) \succ Q_{n,1}(\alpha) \succ Q_{n,2}(\alpha) \succ \cdots$$

es estrictamente decreciente mientras no toma el valor 0, luego, para todo n y todo α, siempre hay un k en el que vale 0. Veamos que el mínimo valor de k está relacionado con las funciones de Hardy:

Teorema 8.32 $n+3+\mu k\,(Q_{n,k}(\alpha)=0)=h_\alpha(n+3)$.

DEMOSTRACIÓN: Por inducción transfinita sobre α. Si $\alpha=0$ es

$$3+0=h_0(3),$$

lo cual es cierto. Si $\alpha=\beta+1$ y $k>0$, observemos que

$$\begin{aligned} Q_{n,k}(\alpha) &= P_{n+k}P_{n+k-1}\cdots P_{n+2}P_{n+1}(\beta+1) \\ &= P_{n+k}P_{n+k-1}\cdots P_{n+2}(\beta)=Q_{n+1,k-1}(\beta), \end{aligned}$$

luego

$$n+3+\mu k\,(Q_{n,k}(\alpha)=0)=n+3+\mu k\,(Q_{n+1,k-1}(\beta)=0)=$$

$$n+4+\mu k\,(Q_{n+1,k}(\beta)=0)=h_\beta(n+4)=h_\alpha(n+3).$$

Si α es un ordinal límite,

$$\begin{aligned} Q_{n,k}(\alpha) &= P_{n+k}P_{n+k-1}\cdots P_{n+1}(\alpha) \\ &= P_{n+k}P_{n+k-1}\cdots P_{n+1}(\alpha[n+3])=Q_{n,k}(\alpha[n+3]), \end{aligned}$$

luego

$$n+3+\mu k\,(Q_{n,k}(\alpha)=0)=n+3+\mu k\,(Q_{n,k}(\alpha[n+3])=0)=$$

$$h_{\alpha[n+3]}(n+3)=h_\alpha(n+3).$$

■

Hemos definido las funciones $Q_{n,k}$ porque el razonamiento inductivo del teorema anterior requería cambiar el valor de n en un momento dado, pero ahora podemos particularizarlo a $n=0$. Hemos probado que

$$h_\alpha(3)=3+\mu k(Q_k(\alpha)=0).$$

Teorema 8.33 (Kirby, Paris) *El teorema de Goodstein no es demostrable en la aritmética de Peano.*

DEMOSTRACIÓN: Definimos $\alpha_n=\omega^{(n)}+\omega^{(n-1)}+\cdots+\omega^{(1)}+1$,

$$a_0=1,\qquad a_{k+1}=2^{a_k},$$

$$b_n=a_n+a_{n-1}+\cdots+a_0,$$

con lo que claramente $T_0(b_n)=\alpha_n$, luego $g_{b_n}(k)=G_k(Q_k(\alpha_n))$.

Si el teorema de Goodstein fuera demostrable en AP, es decir, si

$$\underset{\mathrm{AP}}{\vdash}\bigwedge n\bigvee k\,g_n(k)=0$$

en particular

$$\underset{\mathrm{AP}}{\vdash}\bigwedge n\bigvee k\,g_{b_n}(k)=0$$

luego la función $\mu k(g_{b_n}(k)=0)=\mu k(Q_k(\alpha_n)=0)$ sería demostrablemente recursiva en AP, al igual que $h_{\alpha_n}(3)$, por la observación previa al enunciado.

Por lo tanto, basta probar que la función $h_{\alpha_n}(3)$ no es demostrablemente recursiva en AP, para lo cual basta observar que

$$h_{\alpha_n}(3) \geq h_{\omega^{(n)}}(n),$$

ya que esto implica que mayora a todas las funciones de Hardy, es decir, a todas las funciones demostrablemente recursivas en AP.

En efecto, razonamos por inducción sobre n. Para $n = 0$ es

$$h_{\alpha_0}(3) = h_1(3) = 4 \geq 1 = h_1(0) = h_{\omega^{(0)}}(0).$$

Si vale para n,

$$h_{\alpha_{n+1}}(3) = h_{\omega^{(n+1)}}(h_{\alpha_n}(3)) \geq h_{\omega^{(n+1)}}(h_{\omega^{(n)}}(n)) \geq h_{\omega^{(n+1)}}(n+1),$$

pues $h_{\omega^{(n)}}(n) > n$. ■

Capítulo IX

Lógica de segundo orden

Un lenguaje formal de primer orden está concebido para hablar de unos objetos sobre los que hay definidas unas relaciones y funciones prefijadas a las que podemos referirnos a través de los relatores y funtores del lenguaje. En cambio, un lenguaje de segundo orden dispone de variables de primer orden que pueden recorrer unos objetos y además de variables de segundo orden que pueden recorrer las relaciones y funciones definidas sobre dichos objetos. En otras palabras, mientras en un lenguaje de primer orden los cuantificadores sólo nos permiten formalizar afirmaciones del tipo "para todo objeto" o "existe un objeto tal que ", en la lógica de segundo orden podemos formalizar afirmaciones del tipo "para toda relación" o "para toda función" y "existe una relación tal que" o "existe una función tal que".

Ahora bien, cualquier teoría de conjuntos muestra que es posible hablar de relaciones y funciones entre objetos sin necesidad de salirnos de la lógica de primer orden. Más en general, sucede que cualquier teoría axiomática de segundo orden puede reformularse en términos de la lógica de primer orden. Un ejemplo de esto lo proporciona el tratamiento que dimos en la sección 10.1 de [LM] de la aritmética de Peano de segundo orden, en el que ésta quedó reducida a una teoría axiomática de primer orden.

En este capítulo veremos que el cálculo secuencial también es muy útil para estudiar la lógica de segundo orden, pero para ello es conveniente considerar lenguajes genuinos de segundo orden, sin reducirlos a lenguajes de primer orden.

9.1 Lenguajes formales de segundo orden

Definición 9.1 La definición de *lenguaje formal de segundo orden* (con o sin igualador) es la misma que la de lenguaje formal de primer orden 2.1, salvo que ahora exigimos que tenga una variable libre para cada par de números naturales r e i, que representaremos por X_i^r, e igualmente una variable ligada U_i^r. Diremos que X_i^r (resp. U_i^r) es la variable libre (resp. ligada) de *rango* r e *índice* i.

A las variables de rango 0 de un lenguaje formal $\mathcal{L}$ de segundo orden las llamaremos *variables de primer orden.* Llamaremos $x_i \equiv X_i^0$ a la variable libre de primer orden de índice i, mientras que $u_i \equiv U_i^0$ será la variable ligada de primer orden de índice i.

En la práctica sobrentenderemos que las letras x, y, z representan variables de primer orden (libres, si no se especifica lo contrario), mientras que u, v, w representarán variables ligadas de primer orden. Usaremos letras mayúsculas X, Y, Z para referirnos a variables de segundo orden (libres, si no se indica lo contrario) y, si conviene, especificaremos su rango como superíndice: X^r, $Y^r, \ldots$ Las letras U, V, W representarán variables ligadas de segundo orden.

La idea es que una variable de segundo orden X^r (libre o ligada) varíe entre las relaciones r-ádicas entre objetos (no como un relator R^r, que representa una relación r-ádica fija). Podríamos haber introducido otra serie de variables de segundo orden que variaran entre las funciones r-ádicas entre objetos, pero no necesitamos complicar tanto la teoría: toda función puede definirse a partir de una relación y toda relación puede definirse a partir de una función, por lo que no hay necesidad de considerar variables relacionales y funcionales a la vez.

Más aún, en aquellos contextos en los que es posible definir n-tuplas de objetos, no es necesario trabajar en teoría con relaciones (o funciones) r-ádicas, pues toda relación (o función) r-ádica puede definirse como una relación (o función) de rango 1 que actúa sobre r-tuplas. Ello nos lleva a la definición siguiente:

Un *lenguaje de segundo orden reducido* se define modificando la definición precedente para exigir que sólo haya variables de rangos 0 y 1 o, equivalentemente, que todas las variables de segundo orden tengan rango 1.

Términos y fórmulas Cuando relacionemos los lenguajes formales de primer orden con los de segundo orden entenderemos que las variables de un lenguaje de primer orden se corresponden con las variables de primer orden de un lenguaje de segundo orden.

Por ejemplo si decimos que la definición de *semitérmino* en un lenguaje de segundo orden es la misma que para lenguajes de primer orden, aquí hay que entender que, cuando en dicha definición se establece que las variables son semitérminos, en el caso de un lenguaje de segundo orden debemos entender que las variables de primer orden son semitérminos. En particular, los semitérminos no pueden contener variables de segundo orden.[1]

La definición de semifórmula tenemos que modificarla para incluir dos aspectos nuevos. Por una parte, que las variables de segundo orden de rango r definen fórmulas atómicas exactamente igual que los relatores de rango r y, por otra, que —al contrario que éstos— pueden ligarse mediante cuantificadores. Así, modificamos de forma obvia la definición 2.3 para que las *semifórmulas* de

[1]La situación sería completamente distinta si pretendiéramos que las variables de segundo orden representaran funciones en vez de relaciones. En tal caso las variables de segundo orden se emplearían para construir (semi)términos.

un lenguaje de segundo orden sean las cadenas de signos de una de las formas siguientes:

1. $X^r t_1 \cdots t_r$, donde X^r es un relator r-ádico o bien una variable de segundo orden (libre o ligada) de rango r y $t_1, \ldots, t_r$ son semitérminos,

2. $\neg\alpha$, donde α es una semifórmula,

3. $\alpha \vee \beta$, donde α y β son semifórmulas,

4. $\bigwedge U\alpha$, donde U es una variable ligada de primer o de segundo orden y α es una semifórmula,

5. $\bigvee U\alpha$, donde U es una variable ligada de primer o de segundo orden y α es una semifórmula.

Las semifórmulas del primer tipo se llaman semifórmulas *atómicas.* Si X es una variable de segundo orden, a menudo escribiremos $X(t_1, \ldots, t_r)$ en lugar de $Xt_1 \cdots t_r$. Esta definición de semifórmula vale igualmente para lenguajes reducidos, en cuyo caso las únicas semifórmulas atómicas asociadas a variables de segundo orden son de la forma $X(t)$.

Los conectores $\wedge$, $\rightarrow$ y $\leftrightarrow$ se definen exactamente igual que en el caso de los lenguajes de primer orden.

La definición de los conjuntos de variables libres y ligadas en una semifórmula es esencialmente la misma que para los lenguajes de primer orden:

1. Las variables que aparecen libres en $X^r t_1 \cdots t_r$ son todas las variables que aparecen en la semifórmula (tanto si son variables libres como ligadas).
2. Las variables que aparecen libres en $\neg\alpha$ son las mismas que aparecen libres en α.
3. Las variables que aparecen libres en $\alpha \vee \beta$ son las que aparecen libres en α y las que aparecen libres en β.
4. Las variables que aparecen libres en $\bigwedge u\, \alpha$ o $\bigvee u\, \alpha$ son las que aparecen libres en α y son distintas de u.
5. Las variables que aparecen libres en $\bigwedge U\, \alpha$ o $\bigvee U\, \alpha$ son las que aparecen libres en α y son distintas de U.

1. En una semifórmula atómica $X^r t_1 \cdots t_r$ ninguna variable aparece ligada.
2. Las variables que aparecen ligadas en $\neg\alpha$ son las mismas que aparecen ligadas en α.
3. Las variables que aparecen ligadas en $\alpha \vee \beta$ son las que aparecen ligadas en α y las que aparecen ligadas en β.
4. Las variables que aparecen ligadas en $\bigwedge u\, \alpha$ o $\bigvee u\alpha$ son u y las que aparecen ligadas en α.
5. Las variables que aparecen ligadas en $\bigwedge U\, \alpha$ o $\bigvee U\alpha$ son U y las que aparecen ligadas en α.

Ahora, como en el caso de los lenguajes de primer orden, podemos definir los *términos* como los semitérminos sin variables ligadas y las *fórmulas* como las semifórmulas en las que ninguna variable ligada aparece libre.

Llamaremos *fórmulas de primer orden* a las fórmulas que no tienen variables ligadas de segundo orden (pero sí que admitimos que tengan variables libres de segundo orden).

Sustitución La definición de sustitución de una variable de primer orden (libre o ligada) por un término en un semitérmino es la misma que para lenguajes de primer orden. Podríamos definir la sustitución $\mathtt{S}_x^t\alpha$ de una variable de primer orden por un término en una semiefórmula modificando de forma obvia la definición para lenguajes de primer orden, pero necesitaremos contemplar la posibilidad de que el término sea en realidad un semitérmino, lo cual nos obliga a tener en cuenta la necesidad de sustituir en α unas variables ligadas por otras para evitar que variables que estén libres en t resulten ligadas al efectuar la sustitución.[2] Esto hace que la definición correcta sea la siguiente:

1. $\mathtt{S}_x^t X^r t_1 \cdots t_r \equiv X^r S_x^t t_1 \cdots S_x^t t_r$.
2. $\mathtt{S}_x^t \neg\alpha \equiv \neg \mathtt{S}_x^t\alpha$.
3. $\mathtt{S}_x^t(\alpha \lor \beta) \equiv \mathtt{S}_x^t\alpha \lor \mathtt{S}_x^t\beta$.
4. $\mathtt{S}_x^t \bigwedge u\,\alpha \equiv \begin{cases} \bigwedge u\,\alpha & \text{si } x \text{ no está libre en } \bigwedge u\,\alpha, \\ \bigwedge u\,\mathtt{S}_x^t\,\alpha & \text{si } x \text{ está libre en } \bigwedge u\,\alpha \text{ y } u \text{ no está en } t, \\ \bigwedge v\,\mathtt{S}_x^t\mathtt{S}_u^v\alpha & \text{si } x \text{ está libre en } \bigwedge u\,\alpha,\ u \text{ está en } t \text{ y } v \text{ es la} \\ & \text{menor variable que no está en } \bigwedge u\,\alpha \text{ ni en } t. \end{cases}$
5. $\mathtt{S}_x^t \bigvee u\,\alpha \equiv \begin{cases} \bigvee u\,\alpha & \text{si } x \text{ no está libre en } \bigvee u\,\alpha, \\ \bigvee u\,\mathtt{S}_x^t\,\alpha & \text{si } x \text{ está libre en } \bigvee u\,\alpha \text{ y } u \text{ no está en } t, \\ \bigvee v\,\mathtt{S}_x^t\mathtt{S}_u^v\alpha & \text{si } x \text{ está libre en } \bigvee u\,\alpha,\ u \text{ está en } t \text{ y } v \text{ es la} \\ & \text{menor variable que no está en } \bigvee u\,\alpha \text{ ni en } t. \end{cases}$
6. $\mathtt{S}_x^t \bigwedge U\,\alpha \equiv \bigwedge U\,\mathtt{S}_x^t\alpha$.
7. $\mathtt{S}_x^t \bigvee U\,\alpha \equiv \bigvee U\,\mathtt{S}_x^t\alpha$.

Exactamente igual se define la sustitución $\mathtt{S}_X^Y\alpha$ de una variable de segundo orden X por otra variable Y del mismo rango (o incluso por un relator Y del mismo rango) en una semifórmula α:

1. $\mathtt{S}_X^Y Z t_1 \cdots t_r \equiv \begin{cases} Y t_1 \cdots t_r & \text{si } X \equiv Z, \\ Z t_1 \cdots t_r & \text{si } X \not\equiv Z. \end{cases}$
2. $\mathtt{S}_X^Y \neg\alpha \equiv \neg\mathtt{S}_X^Y\alpha$.
3. $\mathtt{S}_X^Y(\alpha \lor \beta) \equiv \mathtt{S}_X^Y\alpha \lor \mathtt{S}_X^Y\beta$.
4. $\mathtt{S}_X^Y \bigwedge u\,\alpha \equiv \bigwedge u\,\mathtt{S}_X^Y\,\alpha$.
5. $\mathtt{S}_X^Y \bigvee u\,\alpha \equiv \bigvee u\,\mathtt{S}_X^Y\,\alpha$.

[2]Véase la discusión al respecto en la sección 1.5 de [LM].

6. $\mathsf{S}_X^Y \bigwedge U\alpha \equiv \begin{cases} \bigwedge U\,\alpha & \text{si } X \text{ no está libre en } \bigwedge U\alpha, \\ \bigwedge U\,\mathsf{S}_X^Y\alpha & \text{si } X \text{ está libre en } \bigwedge U\alpha \text{ y } Y \not\equiv U, \\ \bigwedge V \mathsf{S}_X^Y \mathsf{S}_U^V \alpha & \text{si } X \text{ está libre en } \bigwedge U\alpha,\ Y \equiv U \text{ y } V \not\equiv X \text{ es} \\ & \text{la menor variable del mismo rango que no} \\ & \text{está en } \bigwedge U\alpha. \end{cases}$

7. $\mathsf{S}_X^Y \bigvee U\alpha \equiv \begin{cases} \bigvee U\,\alpha & \text{si } X \text{ no está libre en } \bigvee U\alpha, \\ \bigvee U\,\mathsf{S}_X^Y\alpha & \text{si } X \text{ está libre en } \bigvee U\alpha \text{ e } Y \not\equiv U, \\ \bigvee V \mathsf{S}_X^Y \mathsf{S}_U^V \alpha & \text{si } X \text{ está libre en } \bigvee U\alpha,\ Y \equiv U \text{ y } V \not\equiv X \text{ es} \\ & \text{la menor variable del mismo rango que no} \\ & \text{está en } \bigvee U\alpha. \end{cases}$

Como es habitual, usaremos la notación $\alpha(x_1, \ldots, x_n)$ para señalar unas variables (de primer o segundo orden, libres o ligadas, que pueden estar o no en α) de modo que $\alpha(t_1, \ldots, t_n)$ (donde t_i es un semitérmino si la variable x_i es de primer orden o un relator o una variable de segundo orden del mismo rango que x_i si ésta es de segundo orden) representa la sustitución simultánea de x_i por t_i en α, definida análogamente a como lo hemos hecho para lenguajes de primer orden (evitando que una variable libre en un t_i pueda ser sustituida).

Es claro que si sustituimos una variable libre de primer orden por un término en una fórmula obtenemos una fórmula, al igual que si sustituimos una variable libre de segundo orden por otra o por un relator. Si hemos contemplado la posibilidad de que t sea un semitérmino (o de que Y sea una variable ligada) es porque necesitábamos esta posibilidad en la definición recurrente de otro tipo de sustitución que no tiene equivalente en la lógica de primer orden:

En efecto, ahora vamos a definir la sustitución $\mathsf{S}_X^{\alpha(\bar{x})}\beta$, donde β es una semifórmula, X es una variable de segundo orden (libre o ligada) de rango r y $\alpha(\bar{x}) \equiv \alpha(x_1, \ldots, x_r)$ es una semifórmula en la que hemos señalado r variables de primer orden distintas entre sí (libres o ligadas, que pueden estar o no en α).

1. $\mathsf{S}_X^{\alpha(\bar{x})} Y t_1 \cdots t_n \equiv \begin{cases} \alpha(t_1, \ldots, t_r) & \text{si } X \equiv Y \text{ (luego } n = r), \\ Y t_1 \cdots t_n & \text{si } X \not\equiv Y. \end{cases}$
2. $\mathsf{S}_X^{\alpha(\bar{x})} \neg\beta \equiv \neg \mathsf{S}_X^{\alpha(\bar{x})}\beta$.
3. $\mathsf{S}_X^{\alpha(\bar{x})}(\beta \vee \gamma) \equiv \mathsf{S}_X^{\alpha(\bar{x})}\beta \vee \mathsf{S}_X^{\alpha(\bar{x})}\gamma$.
4. $\mathsf{S}_X^{\alpha(\bar{x})} \bigwedge u\,\beta \equiv \begin{cases} \bigwedge u\,\beta & \text{si } X \text{ no está libre en } \bigwedge u\,\beta, \\ \bigwedge u\,\mathsf{S}_X^{\alpha(\bar{x})}\,\beta & \text{si } X \text{ está libre en } \bigwedge u\,\beta \text{ y } u \text{ no está libre} \\ & \text{en } \alpha(\bar{x}), \\ \bigwedge v \mathsf{S}_X^{\alpha(\bar{x})} \mathsf{S}_u^v \beta & \text{si } X \text{ está libre en } \bigwedge u\,\beta,\ u \text{ está libre en} \\ & \alpha(\bar{x}) \text{ y } v \text{ es la menor variable que no está} \\ & \text{en } \alpha(\bar{x}) \text{ ni en } \bigwedge u\,\beta. \end{cases}$
5. $\mathsf{S}_X^{\alpha(\bar{x})} \bigvee u\,\beta \equiv \begin{cases} \bigvee u\,\beta & \text{si } X \text{ no está libre en } \bigvee u\,\beta, \\ \bigvee u\,\mathsf{S}_X^{\alpha(\bar{x})}\,\beta & \text{si } X \text{ está libre en } \bigvee u\,\beta \text{ y } u \text{ no está libre} \\ & \text{en } \alpha(\bar{x}), \\ \bigvee v \mathsf{S}_X^{\alpha(\bar{x})} \mathsf{S}_u^v \beta & \text{si } X \text{ está libre en } \bigvee u\,\beta,\ u \text{ está libre en} \\ & \alpha(\bar{x}) \text{ y } v \text{ es la menor variable que no está} \\ & \text{en } \alpha(\bar{x}) \text{ ni en } \bigvee u\,\beta. \end{cases}$

6. $\mathtt{S}_X^{\alpha(\bar{x})}\bigwedge U\beta \equiv \begin{cases} \bigwedge U\,\beta & \text{si } X \text{ no está libre en } \bigwedge U\beta, \\ \bigwedge U\,\mathtt{S}_X^{\alpha(\bar{x})}\beta & \text{si } X \text{ está libre en } \bigwedge U\beta \text{ y } U \text{ no está} \\ & \text{libre en } \alpha(\bar{x}), \\ \bigwedge V\,\mathtt{S}_X^{\alpha(\bar{x})}\mathtt{S}_U^V\beta & \text{si } X \text{ está libre en } \bigwedge U\beta,\ U \text{ está libre en} \\ & \alpha(\bar{x}) \text{ y } V \text{ es la menor variable del mismo} \\ & \text{rango que no está en } \bigwedge U\beta \text{ ni en } \alpha(\bar{x}). \end{cases}$

7. $\mathtt{S}_X^{\alpha(\bar{x})}\bigvee U\beta \equiv \begin{cases} \bigvee U\,\beta & \text{si } X \text{ no está libre en } \bigvee U\beta, \\ \bigvee U\,\mathtt{S}_X^{\alpha(\bar{x})}\beta & \text{si } X \text{ está libre en } \bigvee U\beta \text{ y } U \text{ no está} \\ & \text{libre en } \alpha(\bar{x}), \\ \bigvee V\,\mathtt{S}_X^{\alpha(\bar{x})}\mathtt{S}_U^V\beta & \text{si } X \text{ está libre en } \bigvee U\beta,\ U \text{ está libre en} \\ & \alpha(\bar{x}) \text{ y } V \text{ es la menor variable del mismo} \\ & \text{rango que no está en } \bigvee U\beta \text{ ni en } \alpha(\bar{x}). \end{cases}$

Notemos que la idea de esta sustitución está contenida en el primer caso (en el cual no podíamos exigir que $t_1, \ldots, t_n$ fueran términos). Los demás casos establecen lo necesario para que calcular $\mathtt{S}_X^{\alpha(\bar{x})}\beta$ sea en esencia aplicar el primer caso siempre que sea posible y cambiar las variables ligadas de β por otras cuando entren en conflicto con variables libres de $\alpha(\bar{x})$.

Notemos que todas las definiciones que hemos dado se particularizan trivialmente al caso de lenguajes reducidos.

9.2 El cálculo secuencial de segundo orden

Sobre un lenguaje $\mathcal{L}$ de segundo orden podemos considerar secuentes y cálculos secuenciales exactamente igual que sobre lenguajes de primer orden.

Definición 9.2 Si $\mathcal{L}$ es un lenguaje formal de segundo orden, llamaremos $\mathrm{B}_{\mathcal{L}}$ (o simplemente B) al cálculo secuencial cuyas axiomas son los de LK, es decir, los secuentes $\alpha \Rightarrow \alpha$, y cuyas reglas de inferencia son las de LK más las cuatro reglas siguientes:

$$\textstyle\bigwedge_2 \textbf{ izquierda} \quad \frac{\alpha(X),\,\Gamma \Rightarrow \Delta}{\bigwedge U\,\alpha(U),\,\Gamma \Rightarrow \Delta}, \qquad \bigwedge_2 \textbf{ derecha} \quad \frac{\Gamma \Rightarrow \Delta, \alpha(Y)}{\Gamma \Rightarrow \Delta, \bigwedge U\,\alpha(U)},$$

$$\textstyle\bigvee_2 \textbf{ izquierda} \quad \frac{\alpha(Y),\,\Gamma \Rightarrow \Delta}{\bigvee U\,\alpha(U),\,\Gamma \Rightarrow \Delta}, \qquad \bigvee_2 \textbf{ derecha} \quad \frac{\Gamma \Rightarrow \Delta,\,\alpha(X)}{\Gamma \Rightarrow \Delta,\,\bigvee U\,\alpha(U)},$$

donde X e Y son variables libres del mismo rango que la variable U y la variable propia Y no aparece en el secuente inferior.

Observemos que a cualquier lenguaje de primer orden le podemos añadir variables de segundo orden (de rango 1 o de todos los rangos) y, dada cualquier teoría axiomática sobre dicho lenguaje, podemos considerar la teoría de segundo orden que resulta de añadirle los axiomas lógicos para fórmulas con variables de segundo orden y estas cuatro reglas de inferencia. Así, todos los teoremas de la teoría original siguen siéndolo de la teoría de segundo orden asociada.

Por ejemplo, si partimos de la aritmética de Peano, al añadir variables de segundo orden de rango 1 podemos hablar de conjuntos arbitrarios de números naturales. Por ejemplo, la fórmula siguiente:

$$\bigvee U \bigwedge u(U(u) \leftrightarrow \bigvee v\, u = 2v)$$

afirma la existencia del conjunto de los números pares. Sin embargo, esta fórmula no es demostrable en B. De hecho, la lógica de segundo orden B sirve de poco si no se completa con axiomas de comprensión que garanticen que las fórmulas —o algunas de ellas— definen conjuntos (o, más en general, relaciones).

Definición 9.3 Sea $\mathcal{L}$ un lenguaje formal de segundo orden y sea

$$\alpha(x_1, \ldots, x_r, y_1, \ldots, y_m, Y_1, \ldots, Y_n)$$

una fórmula de $\mathcal{L}$ cuyas variables libres estén entre las indicadas. El *axioma de comprensión* asociado a α es la sentencia

$$\bigwedge \bar{V} \bigwedge \bar{v} \bigvee U \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow \alpha(\bar{u}, \bar{v}, \bar{V})).$$

Este axioma afirma la existencia de una relación r-ádica U que es satisfecha por las r-tuplas de objetos que cumplen la fórmula α con parámetros $\bar{v}$ y $\bar{V}$.

Vamos a probar que, al igual que sucede con el principio de inducción en la aritmética de Peano, los axiomas de comprensión son equivalentes a una regla de inferencia. Para ello necesitamos un resultado previo:

Teorema 9.4 *Sea $\mathcal{L}$ un lenguaje de segundo orden, sea $\alpha(X)$ una fórmula de $\mathcal{L}$, donde X es una variable de rango r, sean $T_1 \equiv \beta(x_1, \ldots, x_r)$, $T_2 \equiv \gamma(x_1, \ldots, x_r)$ dos fórmulas con r variables de primer orden señaladas. Entonces el secuente siguiente es un teorema de* B:

$$\bigwedge u_1 \cdots u_r(\beta(u_1, \ldots, u_r) \leftrightarrow \gamma(u_1, \ldots, u_r)),\ \alpha(T_1) \Rightarrow \alpha(T_2).$$

DEMOSTRACIÓN: Razonamos, por inducción sobre el número de signos lógicos de α, que tanto la fórmula del enunciado como

$$\bigwedge u_1 \cdots u_r(\beta(u_1, \ldots, u_r) \leftrightarrow \gamma(u_1, \ldots, u_r)),\ \alpha(T_2) \Rightarrow \alpha(T_1)$$

son teoremas de B.

Si $\alpha(X) \equiv Yt_1 \cdots t_n$, donde Y es un relator o una variable libre, o bien $Y \not\equiv X$, en cuyo caso $\alpha(T_1) \equiv \alpha(T_2) \equiv \alpha(X)$ y los secuentes se siguen del axioma $\alpha(X) \Rightarrow \alpha(X)$ por debilitación, o bien $\alpha(X) \equiv Xt_1 \cdots t_r$, en cuyo caso

$$\alpha(T_1) \equiv \beta(t_1, \ldots, t_r), \qquad \alpha(T_2) \equiv \gamma(t_1, \ldots, t_r).$$

Tenemos que probar que

$$\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\ \beta(t_1, \ldots, t_r) \Rightarrow \gamma(t_1, \ldots, t_r)$$

ahora bien, abreviando $\beta \equiv \beta(t_1,\ldots,t_r)$, $\gamma \equiv \gamma(t_1,\ldots,t_r)$, tenemos la demostración

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\beta \Rightarrow \beta}{\beta \Rightarrow \beta,\, \gamma} \qquad \dfrac{\gamma \Rightarrow \gamma}{\beta,\, \gamma \Rightarrow \gamma}}{\beta \to \gamma,\, \beta \Rightarrow \gamma}}{\beta \to \gamma,\, \gamma \to \beta,\, \beta \Rightarrow \gamma}}{\beta \leftrightarrow \gamma,\, \beta \Rightarrow \gamma}}{\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \beta \Rightarrow \gamma}$$

donde en el último paso hemos aplicado r veces la regla izquierda del generalizador de primer orden. Análogamente se prueba el teorema con β intercambiado con γ.

Si $\alpha(X) \equiv \neg\delta(X)$, por hipótesis de inducción podemos demostrar

$$\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \delta(T_1) \Rightarrow \delta(T_2), \qquad \bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \delta(T_2) \Rightarrow \delta(T_1),$$

y aplicando dos veces la regla del negador en cada caso de aquí obtenemos

$$\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \neg\delta(T_2) \Rightarrow \neg\delta(T_1), \quad \bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \neg\delta(T_1) \Rightarrow \neg\delta(T_2).$$

(Pero notemos que para probar el teorema con T_1 en el antecedente necesitamos la hipótesis de inducción con T_1 en el consecuente, y viceversa. Por eso necesitamos tratar simultáneamente los dos casos.)

Si $\alpha(X) \equiv \delta(X) \vee \epsilon(X)$, por hipótesis de inducción tenemos los teoremas

$$\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \delta(T_1) \Rightarrow \delta(T_2), \qquad \bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \epsilon(T_1) \Rightarrow \epsilon(T_2),$$

y es fácil llegar a la conclusión usando las reglas del disyuntor.

Si $\alpha(X) \equiv \bigwedge u\, \delta(u, X)$, por hipótesis de inducción

$$\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \delta(y, T_1) \Rightarrow \delta(y, T_2)$$

y basta aplicar las reglas del generalizador (primero la izquierda y luego la derecha). El caso en que $\alpha(X) \equiv \bigvee u\, \delta(u, X)$ es análogo.

Si $\alpha(X) \equiv \bigwedge U \delta(U, X)$, por hipótesis de inducción tenemos

$$\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \delta(Y, T_1) \Rightarrow \delta(Y, T_2),$$

y de nuevo basta aplicar las reglas del generalizador, en este caso las de segundo orden. El caso en que $\alpha(X) \equiv \bigvee U\, \delta(U, X)$ es análogo. ■

Ahora podemos probar que, en un cálculo secuencial de segundo orden que tenga al menos los axiomas y las reglas de inferencia de B, admitir como axioma el axioma de comprensión asociado a una fórmula $\alpha(x_1,\ldots,x_r,\bar{y},\bar{Y})$ equivale a admitir como regla de inferencia

$$\frac{\Gamma \Rightarrow \Delta,\, \gamma(T)}{\Gamma \Rightarrow \Delta,\, \bigvee U\, \gamma(U)}$$

para toda fórmula $\gamma(X)$, donde X es una variable de rango r y $T \equiv \alpha(x_1, \ldots, x_r)$.

En efecto, si admitimos esta regla, podemos demostrar como sigue el axioma de comprensión:

$$\dfrac{\dfrac{\dfrac{\dfrac{\alpha(\bar{x}) \Rightarrow \alpha(\bar{x}) \qquad \alpha(\bar{x}) \Rightarrow \alpha(\bar{x})}{\Rightarrow \alpha(\bar{x}) \leftrightarrow \alpha(\bar{x})}}{\Rightarrow \bigwedge \bar{u}(\alpha(\bar{u}) \leftrightarrow \alpha(\bar{u}))}}{\Rightarrow \bigvee U \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow \alpha(\bar{u}))}}{\Rightarrow \bigwedge \bar{V} \bigwedge \bar{v} \bigvee U \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow \alpha(\bar{u}))}$$

donde en el tercer paso hemos aplicado la regla nueva con

$$\gamma(X) \equiv \bigwedge \bar{u}(X(\bar{u}) \leftrightarrow \alpha(\bar{u})),$$

pues $\gamma(T) \equiv \bigwedge \bar{u}(\alpha(\bar{u}) \leftrightarrow \alpha(\bar{u}))$.

Recíprocamente, si suponemos el axioma de comprensión para α, por el teorema anterior tenemos que[3]

$$\bigwedge \bar{u}(X(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \gamma(T_2),$$

donde $T_1 \equiv T \equiv \alpha(\bar{x})$ y $T_2 \equiv X(\bar{x})$, pero claramente $\gamma(T_2) \equiv \gamma(X)$. A partir de ahí podemos razonar:

$$\dfrac{\dfrac{\dfrac{\bigwedge \bar{u}(X(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \gamma(X)}{\bigwedge \bar{u}(X(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \bigvee U \gamma(U)}}{\bigvee U \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \bigvee U \gamma(U)}}{\bigwedge \bar{V} \bigwedge \bar{v} \bigvee U \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \bigvee U \gamma(U)}$$

Como la primera fórmula del último secuente es el axioma de comprensión para α, podemos cortarla y obtenemos

$$\gamma(T) \Rightarrow \bigvee U \gamma(U),$$

luego cortando con $\Gamma \Rightarrow \Delta,\ \gamma(T)$ obtenemos $\Gamma \Rightarrow \Delta,\ \bigvee U \gamma(U)$. ∎

A su vez, esta regla derecha del particularizador implica una regla izquierda del generalizador:

$$\dfrac{\gamma(T),\ \Gamma \Rightarrow \Delta}{\bigwedge U \gamma(U),\ \Gamma \Rightarrow \Delta}$$

En efecto:

$$\dfrac{\dfrac{\gamma(T),\ \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta,\ \bigvee U \neg\gamma(U)} \qquad \dfrac{\dfrac{\gamma(X) \Rightarrow \gamma(X)}{\neg\gamma(X),\ \gamma(X) \Rightarrow}}{\bigvee U \neg\gamma(U),\ \bigwedge U \gamma(U)}}{\bigwedge U \gamma(U),\ \Gamma \Rightarrow \Delta}$$

Esto nos lleva a la definición siguiente:

[3] En realidad tendríamos que poner $\bigwedge \bar{u}(\alpha(\bar{u}) \leftrightarrow X(\bar{u}))$, pero es claro que con este cambio obtenemos un secuente equivalente.

Definición 9.5 Sea $\mathcal{L}$ un lenguaje formal de segundo orden y sea Φ una familia de fórmulas de $\mathcal{L}$ *cerrada para sustitución,* es decir, tal que

1. Si $\alpha(x)$ es una fórmula de Φ y t es un término, entonces $\alpha(t)$ también es una fórmula de ϕ.

2. Si $\alpha(X)$ es una fórmula se Φ, donde X tiene rango r, y $T \equiv \beta(x_1, \ldots, x_r)$ es otra fórmula de Φ, entonces $\alpha(T)$ también está en Φ.

Llamaremos $\mathrm{B}(\Phi)$ al cálculo secuencial sobre $\mathcal{L}$ cuyos axiomas son los axiomas lógicos $\alpha \Rightarrow \alpha$ y cuyas reglas de inferencia son las de LK más las cuatro reglas siguientes:

$$\textstyle\bigwedge_2 \textbf{ izquierda} \quad \frac{\alpha(T),\, \Gamma \Rightarrow \Delta}{\bigwedge U\, \alpha(U),\, \Gamma \Rightarrow \Delta}, \qquad \bigwedge_2 \textbf{ derecha} \quad \frac{\Gamma \Rightarrow \Delta, \alpha(Y)}{\Gamma \Rightarrow \Delta, \bigwedge U\, \alpha(U)},$$

$$\textstyle\bigvee_2 \textbf{ izquierda} \quad \frac{\alpha(Y),\, \Gamma \Rightarrow \Delta}{\bigvee U\, \alpha(U),\, \Gamma \Rightarrow \Delta}, \qquad \bigvee_2 \textbf{ derecha} \quad \frac{\Gamma \Rightarrow \Delta,\, \alpha(T)}{\Gamma \Rightarrow \Delta,\, \bigvee U\, \alpha(U)},$$

donde $T \equiv \beta(x_1, \ldots, x_r, \bar{y}, \bar{Y})$ es una fórmula de Φ y la variable propia Y es una variable libre del mismo rango que U y que no aparece en el secuente inferior.

Observemos que la regla izquierda del generalizador y la regla derecha del particularizador aplicadas al caso en que $T \equiv X^r(x_1, \ldots, x_r)$ son simplemente las reglas correspondientes de B. Por lo tanto, si Φ contiene a las fórmulas atómicas, las reglas de inferencia de $\mathrm{B}(\Phi)$ incluyen a las de B, y hemos demostrado que $\mathrm{B}(\Phi)$ es equivalente (en el sentido de que tiene los mismos teoremas) que el cálculo deductivo que resulta de añadirle a B todos los axiomas de comprensión correspondientes a fórmulas de Φ.

Llamaremos *lógica de segundo orden plena* B^2 al cálculo secuencial $\mathrm{B}(\Phi)$ que resulta de tomar como Φ el conjunto de todas las fórmulas de $\mathcal{L}$ y *lógica de segundo orden predicativa* B_0 al cálculo secuencial que resulta de tomar como Φ el conjunto de todas las fórmulas de primer orden.[4]

En ambos casos podemos considerar la variante reducida que admite únicamente variables de rangos 0 y 1 y el caso general con variables de todos los rangos posibles.

Los axiomas del igualador Sea $\mathcal{L}$ un lenguaje de segundo orden con igualador y Φ un conjunto de fórmulas de $\mathcal{L}$ cerrado para sustitución que contenga las fórmulas atómicas. Consideremos la fórmula

$$I_1 \equiv \textstyle\bigwedge W \bigwedge uv(u = v \land W(u) \to W(v)).$$

[4]Recordemos que las fórmulas de primer orden pueden tener variables libres de segundo orden.

Vamos a probar que de I_1 (es decir, del secuente $\Rightarrow I_1$) se deducen en $\mathrm{B}(\Phi)$ todos los secuentes

$$s = t,\, \alpha(s) \Rightarrow \alpha(t),$$

donde s y t son términos de $\mathcal{L}$ y $\alpha(x)$ es una fórmula de Φ. En efecto:

$$\dfrac{\dfrac{s = t \land \alpha(s) \to \alpha(t) \Rightarrow s = t \land \alpha(s) \to \alpha(t)}{\bigwedge uv(u = v \land \alpha(u) \to \alpha(v)) \Rightarrow s = t \land \alpha(s) \to \alpha(t)}}{\bigwedge W \bigwedge uv(u = v \land W(u) \to W(v)) \Rightarrow s = t \land \alpha(s) \to \alpha(t)}$$

donde hemos usado la regla izquierda del generalizador con $T \equiv \alpha(x)$ y

$$\gamma(X) \equiv \bigwedge uv(u = v \land X(u) \to X(v)),$$

pues entonces $\gamma(T) \equiv \bigwedge uv(u = v \land \alpha(u) \to \alpha(v))$.

Cortando con la premisa llegamos a

$$\Rightarrow s = t \land \alpha(s) \to \alpha(t)$$

y aplicando las reglas inversas del implicador y del conjuntor llegamos al secuente que queríamos probar.

Recíprocamente, a partir de un caso particular de estos secuentes, a saber, a partir de:

$$x = y,\, Z(x) \Rightarrow Z(y)$$

podemos probar I_1:

$$\dfrac{\dfrac{\dfrac{\dfrac{x = y,\, Z(x) \Rightarrow Z(y)}{x = y \land Z(x) \Rightarrow Z(y)}}{\Rightarrow x = y \land Z(x) \to Z(y)}}{\Rightarrow \bigwedge uv(u = v \land Z(u) \to Z(v))}}{\Rightarrow \bigwedge W \bigwedge uv(u = v \land W(u) \to W(v))}$$

Con esto podemos probar que todos los axiomas del igualador pueden reducirse a una sentencia de primer orden y otra de segundo orden:

Teorema 9.6 *Sea $\mathcal{L}$ un lenguaje formal de segundo orden con igualador y sea Φ un conjunto de fórmulas de $\mathcal{L}$ cerrado para sustitución y que contenga a las fórmulas atómicas. Sea $I_1 \equiv \bigwedge W \bigwedge uv(u = v \land W(u) \to W(v))$. Entonces:*

1. *De I_1 se deducen (en* $\mathrm{B}(\Phi)$*) todos los axiomas del igualador de tipo* I3:

$$s_1 = t_1, \ldots, s_n = t_n,\, Rs_1 \cdots s_n \Rightarrow Rt_1 \cdots t_n.$$

2. *De $\bigwedge u\, u = u$ se deducen todos los axiomas del igualador de tipo* I1:

$$\Rightarrow t = t.$$

3. *De I_1 y $\bigwedge u\, u = u$ se deducen todos los axiomas del igualador de tipo* I2:

$$s_1 = t_1, \ldots s_n = t_n \Rightarrow fs_1 \cdots s_n = ft_1 \cdots t_n.$$

Demostración: 1) Según acabamos de probar, tomando $\alpha(x) \equiv Rxt_2 \cdots t_n$, de I_1 se deduce el secuente

$$s_1 = t_1,\ Rs_1 \cdots s_n \Rightarrow Rt_1 s_2 \cdots s_n.$$

Ahora tomamos $\alpha(x) \equiv Rt_1 x s_3 \cdots s_n$ y obtenemos

$$s_2 = t_2,\ Rt_1 s_2 \cdots s_n \Rightarrow Rt_1 t_2 s_3 \cdots s_n,$$

y cortando los dos secuentes queda

$$s_1 = t_1,\ s_2 = t_2,\ Rs_1 \cdots s_n \Rightarrow Rt_1 t_2 s_3 \cdots s_n$$

tras un número finito de pasos llegamos al axioma del igualador.

2) se comprueba sin dificultad.

3) Basta considerar la fórmula $\alpha(x) \equiv fs_1 \cdots s_n = fxs_2 \cdots s_n$, de la que obtenemos

$$s_1 = t_1,\ fs_1 \cdots s_n = fs_1 \cdots s_n \Rightarrow fs_1 \cdots s_n = ft_1 s_2 \cdots s_n.$$

Cortando con un axioma de tipo I1 obtenemos

$$s_1 = t_1 \Rightarrow fs_1 \cdots s_n = ft_1 s_2 \cdots s_n.$$

Ahora tomamos $\alpha(x) \equiv ft_1 s_2 \cdots s_n = ft_1 x s_3 \cdots s_n$, con lo que obtenemos

$$s_2 = t_2 \Rightarrow ft_1 s_2 \cdots s_n = ft_1 t_2 s_3 \cdots s_n.$$

Los axiomas I3 (que ya sabemos que se deducen de I) implican la transitividad de la igualdad, en particular el secuente

$$fs_1 \cdots s_n = ft_1 s_2 \cdots s_n,\ ft_1 s_2 \cdots s_n = ft_1 t_2 s_3 \cdots s_n$$
$$\Rightarrow fs_1 \cdots s_n = ft_1 t_2 s_3 \cdots s_n,$$

luego cortando este secuente con los dos anteriores obtenemos

$$s_1 = t_1,\ s_2 = t_2 \Rightarrow fs_1 \cdots s_n = ft_1 t_2 s_3 \cdots s_n.$$

Prosiguiendo de este modo, tras un número finito de pasos obtenemos el axioma del igualador. ■

Por último, si X e Y son dos variables o relatores del mismo rango r, podemos definir

$$X = Y \equiv \bigwedge u_1 \cdots u_r (Xu_1 \cdots u_r \leftrightarrow Yu_1 \cdots u_r),$$

y un caso particular del teorema 9.4 nos da que, para toda fórmula $\alpha(Z)$, donde Z es una variable de rango r, se cumple

$$X = Y,\ \alpha(X) \Rightarrow \alpha(Y).$$

De aquí se sigue fácilmente que

$$\Rightarrow X = X, \qquad X = Y \Rightarrow Y = X, \qquad X = Y,\ Y = Z \Rightarrow X = Z.$$

9.3 Eliminación de cortes

La prueba del teorema de eliminación de cortes 2.24 se adapta con pequeños cambios al caso de la lógica de segundo orden predicativa:

Teorema 9.7 (de eliminación de cortes) *Sea $\mathcal{L}$ un lenguaje formal de segundo orden (sin igualador). Todo secuente demostrable en* B_0 *admite una demostración sin cortes.*

Como en el caso de 2.24, basta probar el teorema siguiente:

Teorema 9.8 *Si un secuente es demostrable en* B_0 *con una prueba que contiene un único corte como última inferencia, entonces es demostrable sin cortes.*

DEMOSTRACIÓN: Consideremos una demostración D que termina así:

$$\frac{\Gamma \Rightarrow \Delta,\, \alpha \qquad \alpha,\, \Gamma' \Rightarrow \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}.$$

Llamamos S al secuente inferior y S_1 y S_2 a los dos secuentes superiores. Llamaremos hilos izquierdos de D a los hilos que contengan a S_1 e hilos derechos a los que contengan a S_2.

Definimos el *rango* de un hilo izquierdo (derecho) H como el número de secuentes consecutivos, contados a partir de S_1 (o S_2) que contienen a α en su consecuente (antecedente). Lo representaremos por $\operatorname{rang} H$. Como α está en S_1 y en S_2, el rango de un hilo es siempre ≥ 1.

Definimos el *rango izquierdo (derecho)* de la demostración D como el máximo de los rangos de los hilos izquierdos (derechos) de D. Representaremos por $\operatorname{rang}_i(D)$ y $\operatorname{rang}_d(D)$ a los rangos izquierdo y derecho de D. El *rango* de D lo definimos como

$$\operatorname{rang} D = \operatorname{rang}_i(D) + \operatorname{rang}_d(D) \geq 2.$$

Llamaremos *grado* de una fórmula α (y lo abreviaremos $g(\alpha)$) al número de signos lógicos que contiene ($\neg$, $\vee$, $\bigwedge$ o $\bigvee$). Llamaremos $g(D)$ al grado de la fórmula de corte de (el único) corte de D.

El *grado de segundo orden* de una fórmula α (lo representaremos por $s(\alpha)$) es el número de cuantificadores de segundo orden que contiene, es decir, de cuantificadores que van seguidos de una variable de segundo orden. Llamaremos $s(D)$ al grado de segundo orden de la fórmula de corte de (el único) corte de D.

Vamos a probar el teorema por inducción sobre el grado de segundo orden de D, es decir, suponemos que $s(D) = s$ y que el teorema es cierto para demostraciones D' con $s(D') < s$.

A su vez, razonamos por inducción sobre $g(D)$, es decir, suponemos que $g(D) = g$ y que el teorema es cierto para demostraciones D' con $g(D') < g$.

Finalmente, razonamos por inducción cobre el rango r de D, con lo que suponemos que el resultado es cierto para demostraciones de grado g y rango menor que r.

Caso 1: $\operatorname{rang} D = 2$, es decir, $\operatorname{rang}_i(D) = \operatorname{rang}_d(D) = 1$.

Subcaso 1.1: Uno de los secuentes S_1 o S_2 es un secuente inicial, necesariamente $\alpha \Rightarrow \alpha$, donde α es la fórmula de corte.

Supongamos que S_1 es $\alpha \Rightarrow \alpha$ (el caso de S_2 es análogo). Entonces la demostración D termina así:

$$\dfrac{\alpha \Rightarrow \alpha \qquad \begin{array}{c}\vdots\\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{array}}{\alpha, \Gamma' \Rightarrow \Delta'}$$

con lo que el corte puede suprimirse, obviamente. A partir de aquí suponemos que ninguno de los secuentes S_1 o S_2 es inicial.

Subcaso 1.2: Uno de los secuentes S_1 o S_2 se obtiene por debilitación.

Pongamos que S_1 se obtiene por debilitación (el caso de S_2 es análogo). Como estamos suponiendo que $\operatorname{rang}_i(D) = 1$, la fórmula de corte no puede aparecer en el consecuente del secuente anterior a S_1, luego tiene que ser la fórmula principal de la regla de debilitación, y la demostración D termina así:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta\end{array}}{\Gamma \Rightarrow \Delta,\, \alpha} \qquad \begin{array}{c}\vdots\\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

Vemos entonces que podemos pasar de $\Gamma \Rightarrow \Delta$ al secuente final sin más que aplicar la regla de debilitación.

Subcaso 1.3: Tanto S_1 como S_2 se obtienen mediante reglas de inferencia lógicas.

Nuevamente, debido a que $\operatorname{rang}_i(D) = \operatorname{rang}_d(D) = 1$, la fórmula de corte α tiene que ser la fórmula principal de ambas reglas de inferencia.

Si $\alpha \equiv \neg\beta$, entonces la demostración D acaba así:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \beta,\, \Gamma \Rightarrow \Delta\end{array}}{\Gamma \Rightarrow \Delta,\, \neg\beta} \qquad \dfrac{\begin{array}{c}\vdots\\ \Gamma' \Rightarrow \Delta',\, \beta\end{array}}{\neg\beta,\, \Gamma' \Rightarrow \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

y una demostración alternativa es

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma' \Rightarrow \Delta',\, \beta\end{array} \qquad \begin{array}{c}\vdots\\ \beta,\, \Gamma \Rightarrow \Delta\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

donde ahora el corte tiene grado una unidad menor y podemos aplicar la hipótesis de inducción.

Si $\alpha \equiv \beta \vee \gamma$, tenemos:

$$\dfrac{\dfrac{\vdots}{\Gamma \Rightarrow \Delta,\, \beta,\, \gamma}}{\Gamma \Rightarrow \Delta,\, \beta \vee \gamma} \qquad \dfrac{\beta,\, \Gamma' \Rightarrow \Delta' \qquad \gamma,\, \Gamma' \Rightarrow \Delta'}{\beta \vee \gamma,\, \Gamma' \Rightarrow \Delta'}$$
$$\overline{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

La alternativa es:

$$\dfrac{\dfrac{\Gamma \Rightarrow \Delta,\, \beta,\, \gamma \qquad \beta,\, \Gamma' \Rightarrow \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \gamma} \qquad \gamma,\, \Gamma' \Rightarrow \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

El corte de β tiene grado menor que el de D, por lo que por hipótesis de inducción podemos demostrar sin cortes el secuente $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \gamma$ y obtenemos así una demostración de S con un único corte cuya fórmula de corte es γ y, de nuevo por hipótesis de inducción, llegamos a una prueba sin cortes.

Si $\alpha \equiv \bigwedge u\, \beta(u)$, tenemos:

$$\dfrac{\dfrac{\Gamma \Rightarrow \Delta,\, \beta(y)}{\Gamma \Rightarrow \Delta,\, \bigwedge u\, \beta(u)} \qquad \dfrac{\beta(t),\, \Gamma' \Rightarrow \Delta'}{\bigwedge u\, \beta(u),\, \Gamma' \Rightarrow \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

Ahora observamos que los teoremas 2.25 y 2.27 siguen siendo válidos para B_0, es decir, que si en una demostración sustituimos una variable libre x por un término t que no contenga variables propias, el resultado sigue siendo una demostración (sólo tenemos que comprobar que las cuatro reglas de segundo orden siguen siendo válidas cuando se realiza la sustitución), así como que, sin más que cambiar unas variables libres por otras, podemos exigir que en una demostración cada variable de primer orden sólo se emplee una vez como variable propia y sólo aparezca por encima del secuente en el que se emplea como tal.

Por consiguiente, por 2.27 podemos suponer que la demostración del secuente $\Gamma \Rightarrow \Delta,\, \beta(y)$ es regular (y sin cortes), lo que en particular implica que la variable y no es la variable propia de ninguna regla anterior a la que lleva a S_2. Más aún, podemos elegir todas las variables propias de la demostración, por lo que podemos exigir que ninguna esté en t. Por lo tanto, el teorema 2.25 nos da una demostración sin cortes del secuente $\Gamma \Rightarrow \Delta,\, \beta(t)$ (aquí usamos que y no está en Γ o Δ). Por consiguiente, una demostración alternativa es

$$\dfrac{\Gamma \Rightarrow \Delta,\, \beta(t) \qquad \beta(t),\, \Gamma' \Rightarrow \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

cuyo corte tiene grado menor que el de D, luego por hipótesis de inducción existe otra demostración sin cortes.

Si $\alpha \equiv \bigvee u\, \beta(u)$, tenemos:

$$\cfrac{\cfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t)\end{array}}{\Gamma \Rightarrow \Delta,\, \bigvee u\, \beta(u)} \qquad \cfrac{\begin{array}{c}\vdots\\ \beta(y),\, \Gamma' \Rightarrow \Delta'\end{array}}{\bigvee u\, \beta(u),\, \Gamma' \Rightarrow \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

y en perfecta analogía con el caso anterior podemos llegar a una demostración:

$$\cfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t)\end{array} \qquad \begin{array}{c}\vdots\\ \beta(t),\, \Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

cuyo corte tiene grado menor que el de D, luego por hipótesis de inducción existe otra demostración sin cortes.

Si $\alpha \equiv \bigwedge U \beta(U)$, tenemos:

$$\cfrac{\cfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(Y)\end{array}}{\Gamma \Rightarrow \Delta,\, \bigwedge U\, \beta(U)} \qquad \cfrac{\begin{array}{c}\vdots\\ \beta(T),\, \Gamma' \Rightarrow \Delta'\end{array}}{\bigwedge U\, \beta(U),\, \Gamma' \Rightarrow \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

Ahora observamos que los equivalentes para variables de segundo orden de los teoremas 2.25 y 2.27 también son válidos, es decir, que en una demostración podemos sustituir una variable de segundo orden X por una fórmula $T \equiv \alpha(\bar{x})$ con tal de que en ella no aparezcan variables que se empleen como variables propias (de primer o segundo orden) en la demostración, por lo que podemos suponer que ni Y ni ninguna variable propia de la demostración de $\Gamma \Rightarrow \Delta,\, \beta(Y)$ está en T, lo que a su vez nos permite obtener una demostración (sin cortes) del secuente $\Gamma \Rightarrow \Delta,\, \beta(T)$, con la que podemos construir la demostración

$$\cfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(T)\end{array} \qquad \begin{array}{c}\vdots\\ \beta(T),\, \Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

Observemos que T puede tener cuantificadores, por lo que ahora no es cierto que el grado de $\beta(T)$ sea menor que el de $\bigwedge U \beta(U)$, pero, como T es una fórmula de primer orden (por definición de B_0), tenemos que $s(\beta(T)) < s(\bigwedge U \beta(U))$, luego por hipótesis de inducción existe otra demostración sin cortes.

Si $\alpha \equiv \bigvee U \beta(U)$ el razonamiento es análogo.

Caso 2: $\operatorname{rang}(D) > 2$, luego $\operatorname{rang}_i(D) > 1$ o bien $\operatorname{rang}_d(D) > 1$.

Supongamos concretamente que $\operatorname{rang}_i(D) > 1$. El otro caso se trata análogamente. Notemos que esto implica que S_1 no es un secuente inicial.

Subcaso 2.1: S_2 contiene a α en su consecuente.

Entonces tenemos:

$$\dfrac{\begin{matrix}\vdots \\ \Gamma \Rightarrow \Delta,\, \alpha\end{matrix} \qquad \begin{matrix}\vdots \\ \alpha,\, \Gamma' \Rightarrow \Delta',\, \alpha\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha}$$

y el secuente inferior puede obtenerse del superior izquierdo por debilitación, sin necesidad del corte. A partir de aquí suponemos que α no está en el consecuente de S_2.

Subcaso 2.2 El secuente S_1 se obtiene por debilitación o bien por una regla lógica cuya fórmula principal no es α.

Entonces tenemos

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ \Gamma'' \Rightarrow \Delta'',\, \alpha\end{matrix} \qquad \begin{matrix}\vdots \\ \Gamma''' \Rightarrow \Delta''',\, \alpha\end{matrix}}{\Gamma \Rightarrow \Delta,\, \alpha} \qquad \begin{matrix}\vdots \\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

si es que la regla que proporciona S_1 tiene dos secuentes superiores. El caso en que sólo haya uno es más simple. Adelantamos el corte:

$$\dfrac{\begin{matrix}\vdots \\ \Gamma'' \Rightarrow \Delta'',\, \alpha\end{matrix} \qquad \begin{matrix}\vdots \\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma'',\, \Gamma' \Rightarrow \Delta'',\, \Delta'} \qquad \dfrac{\begin{matrix}\vdots \\ \Gamma''' \Rightarrow \Delta''',\, \alpha\end{matrix} \qquad \begin{matrix}\vdots \\ \alpha,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma''',\, \Gamma' \Rightarrow \Delta''',\, \Delta'}$$

El rango de estas demostraciones es una unidad menor, luego por hipótesis de inducción existen demostraciones sin cortes de los secuentes finales, y usando la misma regla que proporcionaba S_1 en la prueba original (ahora con más fórmulas colaterales), podemos probar sin cortes

$$\dfrac{\begin{matrix}\vdots \\ \Gamma'',\, \Gamma' \Rightarrow \Delta''\, \Delta'\end{matrix} \qquad \begin{matrix}\vdots \\ \Gamma''',\, \Gamma' \Rightarrow \Delta'''\, \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

Subcaso 2.3 El secuente S_1 se obtiene de una regla lógica cuya fórmula principal es α.

Tenemos cuatro posibilidades. Si $\alpha \equiv \neg\beta$, la situación es

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ \beta,\, \Gamma \Rightarrow \Delta\end{matrix}}{\Gamma \Rightarrow \Delta,\, \neg\beta} \qquad \begin{matrix}\vdots \\ \neg\beta,\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

pero $\neg\beta$ tiene que estar en Δ, por la hipótesis sobre el rango izquierdo. Esto nos permite adelantar el corte:

$$\dfrac{\begin{array}{c}\vdots\\ \beta,\,\Gamma \Rightarrow \Delta,\,\neg\beta\end{array} \qquad \begin{array}{c}\vdots\\ \neg\beta,\,\Gamma' \Rightarrow \Delta'\end{array}}{\beta,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}$$

Esta demostración tiene rango una unidad menor, luego por hipótesis de inducción el secuente inferior puede demostrarse sin cortes y, como Δ contiene a $\neg\beta$, podemos eliminar β del antecedente mediante la regla del negador.

Si $\alpha \equiv \beta \vee \gamma$, la situación es

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta,\,\gamma\end{array}}{\Gamma \Rightarrow \Delta,\,\beta \vee \gamma} \qquad \begin{array}{c}\vdots\\ \beta \vee \gamma,\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}$$

y de nuevo $\beta \vee \gamma$ tiene que estar en Δ y podemos adelantar el corte:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta,\,\gamma,\,\beta \vee \gamma\end{array} \qquad \begin{array}{c}\vdots\\ \beta \vee \gamma,\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta',\,\beta,\,\gamma}$$

Por hipótesis de inducción el secuente inferior puede probarse sin cortes y aplicando a continuación la regla del disyuntor[5] eliminamos β y γ.

Si $\alpha \equiv \bigwedge u\,\beta(u)$, donde la variable u es de primer o de segundo orden, tenemos

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta(y)\end{array}}{\Gamma \Rightarrow \Delta,\,\bigwedge u\,\beta(u)} \qquad \begin{array}{c}\vdots\\ \bigwedge u\,\beta(u),\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'}$$

para cierta variable propia y que podemos sustituir por otra para asegurar que no esté en Γ' ni en Δ'. Como Δ contiene $\bigwedge u\,\beta(u)$, también podemos adelantar el corte:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\,\beta(y),\,\bigwedge u\,\beta(u)\end{array} \qquad \begin{array}{c}\vdots\\ \bigwedge u\,\beta(u),\,\Gamma' \Rightarrow \Delta'\end{array}}{\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta',\,\beta(y)}$$

Por hipótesis de inducción existe una prueba sin cortes del secuente final, y aplicando la regla derecha del generalizador eliminamos $\beta(y)$.

[5] En el caso análogo en que el rango derecho es mayor que 1 estaríamos aplicando la regla izquierda del disyuntor, que tiene dos secuentes superiores, y la hipótesis de inducción nos da demostraciones sin cortes de los secuentes $\beta,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'$ y $\gamma,\,\Gamma,\,\Gamma' \Rightarrow \Delta,\,\Delta'$, y a continuación podemos aplicar la regla izquierda del disyuntor.

Si $\alpha \equiv \bigvee u\, \beta(u)$, donde la variable u es de primer o de segundo orden, tenemos

$$\dfrac{\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t)\end{matrix}}{\Gamma \Rightarrow \Delta,\, \bigvee u\, \beta(u)} \qquad \begin{matrix}\vdots\\ \bigvee u\, \beta(u),\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}$$

pero Δ contiene $\bigvee u\, \beta(u)$, con lo que también podemos adelantar el corte:

$$\dfrac{\begin{matrix}\vdots\\ \Gamma \Rightarrow \Delta,\, \beta(t),\, \bigvee u\, \beta(u)\end{matrix} \qquad \begin{matrix}\vdots\\ \bigvee u\, \beta(u),\, \Gamma' \Rightarrow \Delta'\end{matrix}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \beta(t)}$$

Por hipótesis de inducción existe una prueba sin cortes del secuente final, y aplicando la regla derecha del particularizador eliminamos $\beta(t)$. ■

Como consecuencia:

Teorema 9.9 B$_0$ *es una extensión conservativa de* LK, *es decir, si* $\mathcal{L}$ *es un lenguaje de primer orden y* $\mathcal{L}^2$ *es el lenguaje que resulta de añadirle variables de segundo orden (de rango* 1 *o de todos los rangos) y un secuente de* $\mathcal{L}$ *es demostrable en* B$_0$, *entonces es demostrable en* LK.

Demostración: Basta considerar una demostración sin cortes y observar que no puede contener variables de segundo orden, pues si un secuente superior de una regla de inferencia distinta de la de corte tiene variables de segundo orden, el secuente inferior también las tiene, luego si hubiera una variable de segundo orden en algún secuente de la demostración, las habría también en el secuente final. En particular, todos los secuentes iniciales son axiomas de LK y todas las reglas de inferencia son de LK, luego la demostración es una demostración de LK. ■

Observemos que la demostración es constructiva, es decir, nos proporciona un algoritmo para construir una demostración en LK de un secuente dado a partir de una demostración en B$_0$. Lo mismo se aplica al teorema siguiente, para el cual necesitamos una definición:

Definición 9.10 Si K es un cálculo secuencial sobre un lenguaje formal de primer orden $\mathcal{L}$ que consta de los axiomas y reglas de inferencia de LK$_i$ más quizá otros axiomas propios, llamaremos *extensión predicativa* de K al cálculo secuencial K_0 sobre el lenguaje formal $\mathcal{L}^2$ que resulta de añadir a $\mathcal{L}$ variables de segundo orden (de rango 1 o de todos los rangos) cuyas reglas de inferencia son las de B y cuyos axiomas son los de B, más los de K, más los axiomas de comprensión asociados a todas las fórmulas de primer orden. Si admitimos los axiomas de comprensión para todas las fórmulas de $\mathcal{L}^2$ tenemos la *extensión plena* K_2 de K.

Teorema 9.11 *En las condiciones de la definición anterior,* K_0 *es una extensión conservativa de* K, *es decir, todo secuente de* $\mathcal{L}$ *demostrable en* K_0 *es demostrable en* K.

Demostración: Sea $S \equiv \Gamma \Rightarrow \Delta$ un secuente de $\mathcal{L}$ demostrable en K_0. Hemos probado que los teoremas de K_0 son los mismos que los de la teoría que resulta de sustituir los axiomas de comprensión por las reglas de inferencia de B_0, luego podemos considerar una demostración de S en estas condiciones. Sean $S_1, \ldots, S_n$ los axiomas propios de K que se usan en la demostración. Podemos suponer que no son vacíos. Sea $\bar{S}_i$ la fórmula asociada a S_i, es decir, la disyunción de las negaciones de las fórmulas de su antecedente y las fórmulas de su consecuente. Es claro que de $\Rightarrow \bar{S}_i$ se deduce S_i, aplicando las reglas inversas del disyuntor y del negador. Por lo tanto, podemos formar una demostración de S en K_0 cuyos axiomas propios sean $\Rightarrow \bar{S}_i$ en lugar de S_i.

Si añadimos $\bar{S}_1, \ldots, \bar{S}_n$ en los antecedentes de todos los secuentes de la demostración, obtenemos una demostración del secuente

$$\bar{S}_1, \ldots, \bar{S}_n, \Gamma \Rightarrow \Delta$$

en la que los axiomas propios se han convertido en $\bar{S}_1, \ldots, \bar{S}_n \Rightarrow \bar{S}_i$, que a su vez son deducibles por debilitación de los axiomas lógicos $\bar{S}_i \Rightarrow \bar{S}_i$. En suma, tenemos una demostración en B_0 del secuente indicado. Por el teorema anterior dicho secuente es demostrable en LK. Cortando con los secuentes $\Rightarrow \bar{S}_i$ obtenemos una deducción en LK que tiene por premisas estos secuentes, los cuales a su vez pueden ser demostrados a partir de los secuentes S_i mediante las reglas del negador y del disyuntor. Con ello obtenemos una demostración en K de S. ■

Así, a cualquier teoría de primer orden le podemos añadir variables de segundo orden para obtener una teoría de segundo orden “equivalente” a la inicial en el sentido de que sus teoremas sin variables de segundo orden son los mismos.

En realidad, al pasar de una teoría de primer orden a su extensión predicativa es posible dar un pequeño paso adicional sustituyendo los infinitos axiomas del igualador por los dos axiomas considerados en el teorema 9.6. Vamos a probar que con ello obtenemos también una extensión conservativa, para lo cual necesitamos un resultado técnico que constituye una nueva aplicación del teorema de eliminación de cortes:

Teorema 9.12 *Sea $\mathcal{L}$ un lenguaje formal de segundo orden. Sea $\Gamma \Rightarrow \Delta$ un secuente en $\mathcal{L}$ formado por fórmulas de primer orden y consideremos unas fórmulas de primer orden $\alpha_1(X_1^{r_1}), \ldots, \alpha_m(X_m^{r_m})$ cada una de las cuales tenga a $X_i^{r_i}$ como única variable libre (de rango r_i). Entonces, el secuente*

$$\bigwedge U_1^{r_1} \alpha_1(U_1^{r_1}), \ldots, \bigwedge U_m^{r_m} \alpha_m(U_m^{r_m}), \Gamma \Rightarrow \Delta$$

es demostrable en B_0 *si y sólo si existen fórmulas $T_{ij} \equiv \beta_{ij}(x_{ij1}, \ldots, x_{ijr_i})$ de primer orden, para $i = 1, \ldots, m$ y $j = 1, \ldots, n_i$, tales que el secuente*

$$\{\bigwedge \bar{v}_{ij}\, \alpha_i(T_{ij})\}, \Gamma \Rightarrow \Delta$$

(donde las llaves indican que en el antecedente están todas las fórmulas correspondientes a todo i y todo j) es demostrable en B *sin hacer uso de las reglas de inferencia de segundo orden. Aquí $\bar{v}_{ij}$ representa una sucesión de variables ligadas que cuantifican todas las variables libres de primer orden de $\alpha_i(T_{ij})$.*

DEMOSTRACIÓN: Observemos que en B_0 se demuestra

$$\bigwedge U_i^{r_i}\alpha_i(U_i^{r_i}) \Rightarrow \bigwedge \bar{v}_{ij}\,\alpha_i(T_{ij})$$

Basta partir del axioma $\alpha_i(T_{ij}) \Rightarrow \alpha_i(T_{ij})$, aplicar la regla izquierda del generalizador de segundo orden y luego repetidas veces la regla derecha del generalizador de primer orden. Por lo tanto, prolongando una demostración de $\{\bigwedge \bar{v}_{ij}\,\alpha_i(T_{ij})\}$, $\Gamma \Rightarrow \Delta$ mediante cortes con los secuentes anteriores obtenemos una demostración del primer secuente del enunciado.

Recíprocamente, supongamos que dicho secuente es demostrable en B_0. Por el teorema de eliminación de cortes podemos tomar una demostración D sin cortes. Probamos el teorema por inducción sobre el número de inferencias de D.

Si D no contiene inferencias es que no tiene más que un axioma $\alpha \Rightarrow \alpha$, para una cierta fórmula atómica α, luego tiene que ser $m = 0$ y la conclusión es trivial.

Ahora distinguimos casos según cuál sea la última regla de inferencia de D.

Si se trata de una regla de segundo orden, necesariamente será la regla izquierda del generalizador, luego la demostración acaba así:

$$\frac{\alpha_1(T),\, \bigwedge U_2^{r_2}\alpha_2(U_2^{r_2}), \ldots, \bigwedge U_m^{r_m}\alpha_m(U_m^{r_m}),\, \Gamma \Rightarrow \Delta}{\bigwedge U_1^{r_1}\alpha_1(U_1^{r_1}), \ldots, \bigwedge U_m^{r_m}\alpha_m(U_m^{r_m}),\, \Gamma \Rightarrow \Delta}$$

Podemos aplicar la hipótesis de inducción al secuente superior, lo que nos da una demostración de

$$\{\bigwedge \bar{v}_{ij}\,\alpha_i(T_{ij})\},\, \alpha_1(T),\, \Gamma \Rightarrow \Delta,$$

donde $i = 2, \ldots, m$, y basta definir $T_{1,1} \equiv T$ y aplicar la regla izquierda del cuantificador de primer orden para cambiar $\alpha_1(T_{1,1})$ por $\bigwedge \bar{v}_{1,1}\,\alpha_1(T_{1,1})$.

Los demás casos son triviales. Consideremos, por ejemplo, el de la regla izquierda del disyuntor. Omitiendo por brevedad los superíndices, tenemos:

$$\frac{\bigwedge U_1\alpha_1(U_1), \ldots, \bigwedge U_m\alpha_m(U_m),\, \alpha,\, \Gamma' \Rightarrow \Delta \qquad \bigwedge U_1\alpha_1(U_1), \ldots, \bigwedge U_m\alpha_m(U_m),\, \beta,\, \Gamma' \Rightarrow \Delta}{\bigwedge U_1\alpha_1(U_1), \ldots, \bigwedge U_m\alpha_m(U_m),\, \alpha \vee \beta,\, \Gamma' \Rightarrow \Delta}$$

donde Γ' resulta de eliminar $\alpha \vee \beta$ en Γ. La hipótesis de inducción nos da demostraciones de los secuentes

$$\{\bigwedge \bar{v}_{ij}\,\alpha_i(T_{ij})\},\, \alpha,\, \Gamma' \Rightarrow \Delta, \qquad \{\bigwedge \bar{v}'_{ij}\,\alpha_i(T'_{ij})\},\, \beta,\, \Gamma' \Rightarrow \Delta$$

y basta aplicar la regla izquierda del disyuntor (renumerando las fórmulas T_{ij} y T'_{ij} para formar una única sucesión). Es este caso el que hace que no podamos considerar una única fórmula T_i para cada $\alpha_i(X_i)$. ■

Teorema 9.13 *En las condiciones de la definición* 9.10, *sea* $\tilde{K}$ *la teoría que resulta de eliminar en* K_0 *los axiomas del igualador y sustituirlos por los axiomas*

$$\bigwedge u\, u = u, \qquad I_n \equiv \bigwedge U^n \bigwedge \bar{u}\bar{v}(u_1 = v_1 \wedge \cdots \wedge u_n = v_n \wedge U^n(\bar{u}) \to U^n(\bar{v})).$$

Entonces $\tilde{K}$ *es una extensión conservativa de* K*, es decir, una fórmula sin variables de segundo orden es demostrable en* K *si y sólo si es demostrable en* $\tilde{K}$.

Demostración: Según el teorema 9.6, a partir de $\bigwedge u = u$ e I_1 se pueden probar todos los axiomas del igualador de primer orden,[6] luego todo teorema de K_0 (en particular todo teorema de K) lo es también de $\tilde{K}$.

Supongamos ahora que δ es una fórmula sin variables de segundo orden demostrable en $\tilde{K}$. Hemos probado que los axiomas de comprensión de $\tilde{K}$ pueden eliminarse si a cambio admitimos las reglas de inferencia de B_0 y los axiomas propios de $\tilde{K}$ (que son los mismos que los de K) pueden sustituirse por versiones equivalentes de la forma $\Rightarrow \alpha$, para fórmulas α sin variables de segundo orden (la disyunción de las negaciones de las fórmulas del antecedente y las fórmulas del consecuente).

Por lo tanto, podemos partir de una demostración de $\Rightarrow \delta$ que use las reglas de inferencia de B_0 y cuyos secuentes iniciales sean:

1. Axiomas lógicos $\alpha \Rightarrow \alpha$ (para fórmulas de primer o segundo orden).
2. Los secuentes $\Rightarrow I_n$.
3. El secuente $\Rightarrow \bigwedge uu = u$ y los secuentes de la forma $\Rightarrow \alpha$ equivalentes a los axiomas de K.

Llamamos Γ al conjunto finito de axiomas de tipo 3 que aparecen en la demostración de $\Rightarrow \delta$. Observemos que ninguno de ellos tiene variables de segundo orden. Es claro entonces que existe un n tal que en B_0 se demuestra

$$I_1, \ldots, I_n, \Gamma \Rightarrow \delta.$$

Ahora observamos que $\mathrm{I}_i \equiv \bigwedge U^i\, \alpha_i(U^i)$, donde $\alpha_i(X^i)$ es una fórmula de primer orden, por lo que podemos aplicar el teorema anterior, según el cual en B podemos demostrar un secuente de la forma

$$\{\alpha_i(T_{ij})\}, \Gamma \Rightarrow \delta$$

sin usar reglas de inferencia de segundo orden.

Ahora comprobamos que, si en la demostración sustituimos cada semifórmula atómica $X^l(t_1, \ldots, t_l)$ por la fórmula $\bigwedge u\, u = u$, el resultado sigue siendo una demostración de un secuente de la misma forma (a lo sumo se modificarán

[6] El hecho de que sólo se necesite $I \equiv I_1$ hace que este teorema valga igualmente si consideramos únicamente variables de segundo orden de rango 1.

las fórmulas T_i) en el que no hay variables de segundo orden. Basta observar que los axiomas (lógicos) siguen siéndolo con este cambio, y que todas las reglas de inferencia siguen siendo válidas (y aquí es fundamental que ninguna regla de inferencia es de segundo orden). Como ya no hay variables de segundo orden, lo que tenemos es una demostración en LK. Finalmente observamos que

$$\alpha_{ij}(T_i) \equiv \bigwedge \bar{u}\bar{v}(u_1 = v_1 \land \cdots \land u_i = v_i \land \beta_{ij}(\bar{u}) \to \beta_{ij}(\bar{v}))$$

es un teorema de LK_i (por el teorema 2.14), luego también de K. Lo mismo sucede con las fórmulas de Γ, que son axiomas lógicos o teoremas de K (equivalentes a axiomas). Por lo tanto, aplicando la regla de corte, podemos prolongar la demostración que tenemos en LK hasta una demostración de $\Rightarrow \delta$ en K. ■

Nota En vista del teorema anterior, cuando hablemos de la extensión predicativa de una teoría de primer orden, consideraremos en ella los axiomas del igualador de segundo orden. ■

9.4 Reducción a la lógica de primer orden

Vamos a probar ahora que todo cálculo deductivo T de segundo orden (cuyas reglas de inferencia sean las de B) puede reducirse a otro de primer orden en el sentido de que determinar si una sentencia α es o no un teorema de T equivale a determinar si otra sentencia $\tilde{\alpha}$ de primer orden es o no un teorema de otra teoría de primer orden $\tilde{T}$.

Definición 9.14 Si $\mathcal{L}$ es un lenguaje formal de segundo orden, llamaremos $\tilde{\mathcal{L}}$ al lenguaje de primer orden cuyos signos eventuales son los de $\mathcal{L}$ más una sucesión de relatores $R_0, R_1, R_2, \ldots$ de rango 1 y otra sucesión de relatores $S_1, S_2, S_3 \ldots$ de modo que S_r tenga rango $r+1$. Usaremos la notación

$$t_0(t_1, \ldots, t_r) \equiv S_r(t_0, \ldots, t_r).$$

La idea subyacente es que R_0x pretende significar "x es un objeto", mientras que R_rX, para $r \geq 1$, pretende significar que "X es una relación de rango r" y $X(x_1, \ldots, x_r)$ que "los objetos $x_1, \ldots, x_r$ cumplen la relación X".

Decimos "pretende significar" porque, mientras la sintaxis de segundo orden de $\mathcal{L}$ prohíbe escribir incoherencias como $X^3(y, z)$, nos encontramos con que

$$R_3X \land X(y, z)$$

es una fórmula acorde con la sintaxis de primer orden de $\tilde{\mathcal{L}}$, a pesar de que contradice el uso pretendido de los relatores R_3 y S_2. Vamos a definir ahora las fórmulas de $\tilde{\mathcal{L}}$ que, además de cumplir los requisitos de la sintaxis de $\tilde{\mathcal{L}}$, es coherente con el significado pretendido de los relatores adicionales.

Podemos identificar las variables de $\tilde{\mathcal{L}}$ con las variables de $\mathcal{L}$, de modo que cada variable de $\tilde{\mathcal{L}}$ tiene asignado un rango que es irrelevante en lo que respecta a la sintaxis de $\mathcal{L}$, pero que podemos tener en cuenta para relacionar $\mathcal{L}$ y $\tilde{\mathcal{L}}$.

Por ejemplo, usaremos las abreviaturas:

$$\bigwedge_r U\,\alpha \equiv \bigwedge U(R_r U \to \alpha), \qquad \bigvee_r U\,\alpha \equiv \bigvee U(R_r U \land \alpha),$$

donde U es una variable de $\tilde{L}$ de rango r.

Con la identificación de variables, podemos considerar que todo semitérmino de $\mathcal{L}$ lo es también de $\tilde{\mathcal{L}}$. Llamaremos *semitérminos estructurados* de $\tilde{\mathcal{L}}$ a los semitérminos que no contengan variables de segundo orden (a los que llamaremos semitérminos de rango 0 y que coinciden con los semitérminos de $\mathcal{L}$) y a las variables de rango $r \geq 1$ (a los que llamaremos semitérminos estructurados de rango r).

Definimos las *semifórmulas estructuradas* de $\tilde{\mathcal{L}}$ como las construidas según las reglas siguientes:

1. Si R^r es un relator de $\mathcal{L}$ de rango r y $t_1, \ldots, t_r$ son semitérminos estructurados de rango 0, entonces $R^r t_1 \cdots t_r$ es una semifórmula estructurada.
2. Si X es una variable de rango r (libre o ligada) y $t_1, \ldots, t_r$ son semitérminos estructurados de rango 0, entonces $X(t_1, \ldots, t_r) \equiv S_r X t_1 \cdots t_r$ es una semifórmula estructurada.
3. Si α y β son semifórmulas estructuradas y U es una variable ligada de rango r, también lo son

$$\neg\alpha, \quad \alpha \lor \beta, \quad \bigwedge_r U\,\alpha, \quad \bigvee_r U\,\alpha.$$

Las *semifórmulas estructuradas de primer orden* son las semifórmulas estructuradas cuyas variables ligadas son todas de rango 0.

Observemos que todos los semitérminos de $\mathcal{L}$ son semitérminos estructurados de rango 0 de $\tilde{\mathcal{L}}$. Para cada semifórmula α de $\mathcal{L}$ definimos como sigue una semifórmula estructurada $\tilde{\alpha}$ de $\tilde{\mathcal{L}}$:

1. $\widetilde{R^r t_1 \cdots t_r} \equiv R^r t_1 \cdots t_r$, para todo relator R^r de $\mathcal{L}$ de rango r.
2. $\widetilde{X(t_1, \ldots, t_r)} \equiv X(t_1, \ldots, t_r) \equiv S_r X t_1 \cdots t_r$, donde X es una variable de rango r y $t_1, \ldots, t_r$ son semitérminos de $\mathcal{L}$.
3. $\widetilde{\neg\alpha} \equiv \neg\tilde{\alpha}$, $\widetilde{\alpha \lor \beta} \equiv \tilde{\alpha} \lor \tilde{\beta}$.
4. $\widetilde{\bigwedge U\alpha} \equiv \bigwedge_r U\,\tilde{\alpha}$, $\widetilde{\bigvee U\alpha} \equiv \bigvee_r U\,\tilde{\alpha}$, donde U es una variable de rango r.

Necesitaremos considerar una clase de fórmulas mucho más amplia que la de las fórmulas estructuradas. Llamaremos *semifórmulas cuasiestructuradas* a las semifórmulas de $\tilde{\mathcal{L}}$ cuyos cuantificadores aparezcan todos en la forma $\bigwedge_r U$ o $\bigvee_r U$.

Las fórmulas cuasiestructuradas pueden traducirse a fórmulas de $\mathcal{L}$:

Para cada semifórmula cuasiestructurada α de $\tilde{\mathcal{L}}$, definimos una fórmula α^* de $\mathcal{L}$ con el criterio siguiente:

1. $(t_1 = t_2)^* \equiv \begin{cases} t_1 = t_2 & \text{si los } t_i \text{ tienen ambos rango } 0, \\ \bigwedge \bar{u}(t_1(\bar{u}) \leftrightarrow t_2(\bar{u})) & \text{si los } t_i \text{ tienen ambos rango } r \geq 1, \\ \bigwedge u\, u = u & \text{si los } t_i \text{ son ambos no estructurados} \\ \bigvee u\, u \neq u & \text{en otro caso.} \end{cases}$

2. Si R^r es un relator r-ádico de $\mathcal{L}$ distinto del igualador, entonces

$$(R^r t_1 \cdots t_r)^* \equiv \begin{cases} R^r t_1 \cdots t_r & \text{si los } t_i \text{ son estructurados de rango } 0, \\ \bigvee u\, u \neq u & \text{en caso contrario.} \end{cases}$$

3. $(R_r t)^* \equiv \begin{cases} \bigwedge u\, u = u & \text{si } t \text{ es estructurado de rango } r, \\ \bigvee u\, u \neq u & \text{en caso contrario.} \end{cases}$

4. $(S_r T t_1 \cdots t_r)^* \equiv \begin{cases} T(t_1, \ldots, t_r) & \text{si } T \text{ es una variable de rango } r \\ & \text{y los } t_i \text{ son estructurados de rango } 0, \\ \bigvee u\, u \neq u & \text{en caso contrario.} \end{cases}$

5. $(\neg\alpha)^* \equiv \neg\alpha^*$, $(\alpha \vee \beta)^* \equiv \alpha^* \vee \beta^*$,

6. $(\bigwedge_r U\, \alpha)^* \equiv \bigwedge U\, \alpha^*$, $\quad (\bigvee_r U\, \alpha)^* \equiv \bigvee U\, \alpha^*$.

Es fácil ver que si α es una semifórmula de $\mathcal{L}$, entonces $\tilde{\alpha}^* \equiv \alpha$, y si α es una semifórmula estructurada de $\tilde{\mathcal{L}}$, entonces $\widetilde{(\alpha^*)} \equiv \alpha$. En particular, las fórmulas estructuradas de $\tilde{\mathcal{L}}$ son exactamente las fórmulas de la forma $\tilde{\alpha}$, para cierta fórmula α de $\mathcal{L}$. Observemos además que las fórmulas de primer orden de $\mathcal{L}$ se corresponden con las fórmulas estructuradas de primer orden de $\tilde{\mathcal{L}}$.

Lenguajes reducidos Hasta aquí hemos considerado el caso en que el lenguaje de partida $\mathcal{L}$ tiene variables de segundo orden de todos los rangos. Todo lo dicho se adapta fácilmente al caso de lenguajes reducidos, pero, de hecho, puede simplificarse un poco más. En principio, si $\mathcal{L}$ es un lenguaje reducido, entonces $\tilde{\mathcal{L}}$ tiene únicamente tres relatores adicionales, los relatores monádicos R_0 y R_1 y el relator diádico S_1. Sin embargo, en este caso podemos eliminar el relator R_0 y adoptar la notación

$$R_0 t \equiv \neg R_1 t, \qquad \operatorname{cto} t \equiv R_1 t, \qquad t \in X \equiv S_1 X t,$$

de modo que R_0 es ahora una mera notación para la negación de R_1. En estos términos, $\operatorname{cto} X$ pretende significar "X es un conjunto" y $x \in X$ pretende significar que x es uno de los elementos del conjunto X.

Notemos que la definición de $(R_0 t)^*$ que hemos dado en general ahora no es una definición, pero sigue siendo válida, porque se deduce de la definición que hemos dado de R_0. ■

Definición 9.15 Sea T un cálculo secuencial sobre un lenguaje formal $\mathcal{L}$ con igualador cuyas reglas de inferencia sean las de B y cuyos axiomas incluyan los axiomas lógicos $\alpha \Rightarrow \alpha$ y además:

1. Los axiomas del igualador:

$$\bigwedge u\, u = u, \qquad I_n \equiv \bigwedge U^n \bigwedge \bar{u}\bar{v}(u_1 = v_1 \land \cdots \land u_n = v_n \land U^n(\bar{u}) \to U^n(\bar{v})).$$

2. Un conjunto adicional (tal vez vacío) de axiomas propios, todos los cuales son sentencias de $\mathcal{L}$.

Llamaremos $\tilde{T}$ a la teoría axiomática sobre $\tilde{\mathcal{L}}$ cuyas reglas de inferencia son las de LK y cuyos axiomas son los axiomas lógicos $\alpha \Rightarrow \alpha$ más:

1. Los axiomas del igualador de LK_i.

2. Los axiomas de extensionalidad (para todo $r \geq 1$):

$$\bigwedge_r UV(\bigwedge_0 \bar{u}(U(\bar{u}) \leftrightarrow V(\bar{u})) \to U = V).$$

3. $\bigwedge_0 \bar{u}\, R_0 t(\bar{u})$, para todo término estructurado $t(x_1, \ldots, x_n)$.

4. $\bigvee_r U\, R_r U$, para todo $r \geq 0$.

5. Las traducciones de los axiomas de T distintos de los axiomas lógicos y los axiomas del igualador.

Nota Aunque en la elección concreta de los axiomas de $\tilde{T}$ hemos usado los rangos asignados a sus variables, notemos que $\tilde{T}$ es una teoría axiomática de primer orden, por lo que dichos rangos son irrelevantes, en el sentido de que si en cualquier axioma sustituimos unas variables por otras cualesquiera (respetando la distinción entre variables libres y ligadas) obtenemos un teorema de $\tilde{T}$ o, equivalentemente, que si omitimos toda referencia a los rangos de las variables en la definición de $\tilde{T}$ obtenemos una teoría equivalente (con los mismos teoremas), pero con la elección que hemos hecho de los axiomas éstos resultan ser todos fórmulas cuasiestructuradas, lo cual nos ayudará a relacionar T con $\tilde{T}$. ■

Teorema 9.16 *En las condiciones anteriores, si una fórmula cuasiestructurada es demostrable en $\tilde{T}$, entonces admite una demostración formada únicamente por fórmulas cuasiestructuradas.*

DEMOSTRACIÓN: Todos los axiomas de $\tilde{T}$ son de la forma $\Rightarrow \delta$, donde δ es una sentencia estructurada, salvo los axiomas de LK_i. Los axiomas del igualador son equivalentes (en LK) a secuentes de la forma $\Rightarrow \delta$, donde δ es una fórmula sin cuantificadores, luego cuasiestructurada.

Consideremos ahora una demostración en $\tilde{T}$ de un secuente $S \equiv \Gamma \Rightarrow \Delta$ formado por fórmulas cuasiestructuradas. Podemos extenderla para demostrar sus secuentes iniciales que no sean axiomas lógicos a partir de secuentes de la forma $\Rightarrow \delta$, donde δ es una fórmula cuasiestructurada. Llamamos Θ al conjunto de todas las fórmulas δ que aparecen en los consecuentes de los secuentes iniciales de la demostración que no son axiomas lógicos.

Si añadimos Θ a los antecedentes de todos los secuentes de la demostración, todas las reglas de inferencia siguen siendo válidas, y los secuentes iniciales que no son axiomas lógicos tienen ahora una fórmula en el antecedente idéntica a la de su consecuente, luego pueden deducirse de un axioma lógico por debilitación. Así obtenemos una demostración en LK del secuente $\Theta, \Gamma \Rightarrow \Delta$, el cual consta únicamente de fórmulas cuasiestructuradas.

Por el teorema de eliminación de cortes 2.24, existe una demostración de $\tilde{S}$ sin cortes. Ahora bien, es obvio que si los secuentes superiores de una regla de inferencia que no sea la de corte contienen una fórmula no cuasiestructurada, el secuente inferior también contiene una (pues la fórmula contiene un cuantificador mal acotado y eso no lo arregla ninguna regla de inferencia). Como no hay cortes y en el secuente final todas las fórmulas son cuasiestructuradas, todas las fórmulas de la demostración tienen que ser cuasiestructuradas.

Finalmente deducimos cada secuente $\Rightarrow \delta$ que no sea un axioma de $\tilde{T}$ del axioma del igualador correspondiente y luego aplicamos la regla de corte, con lo que llegamos a una demostración en $\tilde{T}$ del secuente S formada únicamente por fórmulas cuasiestructuradas. ■

El objeto de esta sección es demostrar el teorema siguiente:

Teorema 9.17 *En las condiciones de la definición* 9.15*, una sentencia α de $\mathcal{L}$ es un teorema de T si y sólo si su traducción $\tilde{\alpha}$ es un teorema de $\tilde{T}$. En particular, se cumple que T es consistente si y sólo si lo es $\tilde{T}$.*

Demostración: Si $S \equiv \Gamma \Rightarrow \Delta$ es un secuente de $\mathcal{L}$ en el que aparecen libres las variables $X_1, \ldots, X_n$ de rangos $r_1, \ldots, r_n$ (incluyendo las de primer orden), llamaremos $\Theta_S \equiv \{R_{r_1}X_1, \ldots R_{r_n}X_n\}$. A su vez definimos $\tilde{S} = \Theta_S, \tilde{\Gamma} \Rightarrow \tilde{\Delta}$, donde $\tilde{\Gamma}$ y $\tilde{\Delta}$ son los conjuntos formados por las traducciones de las fórmulas de Γ y Δ, respectivamente.

Vamos a probar que si S es demostrable en T, entonces $\tilde{S}$ es demostrable en $\tilde{T}$. En particular, si $S \equiv \Rightarrow \alpha$, donde α es una sentencia de $\mathcal{L}$, entonces Θ_S es vacío y $\tilde{S} \equiv \Rightarrow \tilde{\alpha}$, luego podremos concluir que $\tilde{\alpha}$ es un teorema de $\tilde{T}$.

Veamos en primer lugar que si S es un axioma de T, entonces $\tilde{S}$ es un teorema de $\tilde{T}$. De hecho, esto es cierto incluso sin incluir Θ_S en $\tilde{S}$, pero siempre podemos añadirlo por debilitación. En efecto, esto es trivial para los axiomas lógicos. La traducción de $\bigwedge u\, u = u$ es

$$\bigwedge u(R_0 u \rightarrow u = u),$$

que claramente es un teorema de lógico (Notemos que $\tilde{T}$ contiene todos los axiomas y reglas de inferencia de LK_i, por lo que todos los teoremas lógicos son teoremas de $\tilde{T}$). La traducción de los axiomas del igualador de segundo orden es

$$\bigwedge_n U \bigwedge_0 \bar{u}\bar{v}(u_1 = v_1 \land \cdots \land u_n = v_n \land U(\bar{u}) \rightarrow U(\bar{v})),$$

que también es un teorema lógico.

Las traducciones de los axiomas restantes de T (sin el Θ_S añadido) son axiomas de $\tilde{T}$ por definición de $\tilde{T}$.

Veamos ahora que la traducción de una regla de inferencia de B es una regla de inferencia válida (no necesariamente primitiva) de LK. Esto es inmediato salvo lo sumo para las reglas de los cuantificadores. Distinguimos cada caso. En todos ellos llamamos S_1 al secuente superior de la regla y S_2 al secuente inferior.

Generalizador izquierda La traducción de la regla de primer orden es

$$\frac{\Theta_{S_1},\ \tilde{\alpha}(t),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}{\Theta_{S_2},\ \bigwedge_0 u\, \tilde{\alpha}(u),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}.}$$

Para probarla, razonamos como sigue:

$$\frac{\dfrac{\Theta_{S_1},\ \tilde{\alpha}(t),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta} \qquad R_0 t \Rightarrow R_0 t}{\Theta_{S_1},\ R_0 t,\ R_0 t \rightarrow \tilde{\alpha}(t),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}}{\Theta_{S_1},\ R_0 t,\ \bigwedge_0 u\, \tilde{\alpha}(u),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

Ahora usamos que $\Theta_{S_1} \Rightarrow R_0 t$ (por el axioma 3 de $\tilde{T}$), por lo que la regla de corte nos permite eliminar $R_0 t$ del secuente inferior. Para cada variable x que esté libre en S_1, pero no en S_2, podemos aplicar la regla izquierda del particularizador con x como variable propia para transformar la fórmula $R_0 x$ que está en Θ_{S_1} en $\bigvee u\, R_0 u$, que es un teorema de $\tilde{T}$ (se deduce del axioma 3), luego podemos eliminarla del secuente inferior mediante un corte. Así llegamos al secuente $\Theta_{S_2},\ \bigwedge_0 u\, \tilde{\alpha}(u),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}$.

La regla de segundo orden se prueba análogamente. En este caso en lugar del término t tenemos una variable X de rango r.

Generalizador derecha En este caso la prueba es mucho más simple:

$$\frac{\dfrac{\Theta_{S_1},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \tilde{\alpha}(Y)}{\Theta_{S_2},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ R_r Y \rightarrow \tilde{\alpha}(Y)}}{\Theta_{S_2},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \bigwedge_r U\, \tilde{\alpha}(U)}$$

donde hemos usado que la única variable libre de S_1 que deja de estarlo en S_2 es Y, con lo que $\Theta_{S_1} = \Theta_{S_2} \cup \{R_r Y\}$.

Particularizador izquierda La traducción de la regla se demuestra así:

$$\frac{\dfrac{\Theta_{S_1},\ \tilde{\alpha}(Y),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}{\Theta_{S_2},\ R_r Y \wedge \tilde{\alpha}(Y),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}}{\Theta_{S_2},\ \bigvee_r U\, \tilde{\alpha}(U),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

Particularizador derecha Para la regla de primer orden, por los mismos argumentos empleados en la prueba de la regla izquierda del generalizador, tenemos:

$$\frac{\dfrac{\Theta_{S_1},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \tilde{\alpha}(t) \qquad \Theta_{S_1} \Rightarrow R_0 t}{\Theta_{S_1},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ R_0 t \wedge \tilde{\alpha}(t)}}{\Theta_{S_1},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \bigvee_0 u\, \tilde{\alpha}(u)}$$

A partir de aquí, podemos transformar Θ_{S_1} en Θ_{S_2} igual que en el caso del generalizador. La regla de segundo orden se demuestra análogamente.

Es claro entonces que cada demostración de un secuente S en T se traduce a una demostración de $\tilde{S}$ en $\tilde{T}$.

Para probar el recíproco basta ver que si una fórmula cuasiestructurada α es un teorema de $\tilde{T}$, entonces α^* es un teorema de T. En efecto, admitiendo esto, si $\tilde{\alpha}$ es un teorema de $\tilde{T}$, tenemos que $\tilde{\alpha}^* \equiv \alpha$ es un teorema de T.

Por el teorema anterior, podemos tomar una demostración de α en $\tilde{T}$ formada únicamente por fórmulas cuasiestructuradas. Ahora razonamos igual que en el caso anterior. En primer lugar probamos que los axiomas de $\tilde{T}$ se traducen a teoremas de T.

1. Para los axiomas lógicos es inmediato.
2. Consideremos ahora los axiomas del igualador.
   (a) Supongamos en primer lugar que es tipo I1, es decir, $\Rightarrow t = t$.
      i. Si t es un término estructurado de rango 0, su traducción es $\Rightarrow t = t$, que es ciertamente un teorema de T.
      ii. Si t es un término estructurado de rango $r \geq 1$, su traducción es
      $$\Rightarrow \bigwedge \bar{u}(t(\bar{u}) \leftrightarrow t(\bar{u})),$$
      que claramente es un teorema de T.
      iii. Si t no es un término estructurado, la traducción es $\Rightarrow \bigwedge u\, u = u$, que también es un teorema de T.
   (b) Consideremos un axioma de tipo I2, es decir:
   $$s_1 = t_1, \ldots, s_n = t_n \Rightarrow fs_1 \cdots s_n = ft_1 \cdots t_n.$$
      i. Si todos los términos son estructurados de rango 0, su traducción es él mismo, y es un teorema de T (se deduce de los axiomas del igualador de T).
      ii. Si todos los s_i son estructurados de rango 0, pero algún t_i no lo es (o viceversa), entonces $s_i = t_i$ se traduce en $\bigvee u\, u \neq u$, luego $(s_i = t_i)^* \Rightarrow$ es un teorema de T y de él se deduce por debilitación la traducción del axioma.
      iii. Si existen s_i y t_j que no son términos estructurados de rango 0 entonces ambos miembros del consecuente son términos no estructurados, luego su traducción es $\bigwedge u\, u = u$, y la traducción del axioma se deduce por debilitación del teorema $\Rightarrow \bigwedge u\, u = u$.
   (c) Consideremos ahora un axioma de tipo I3 correspondiente a un relator de $\mathcal{L}$ distinto del igualador:
   $$s_1 = t_1, \ldots, s_n = t_n,\ Rs_1 \cdots s_n \Rightarrow Rt_1 \cdots t_n.$$

i. Si todos los términos son estructurados de rango 0, la traducción es el mismo secuente y es claramente un teorema de T.

ii. Si algún s_i no es un término estructurado de rango 0, entonces la traducción de $Rs_1\cdots s_n$ es $\bigvee u\, u\neq u$, con lo que la traducción del axioma se demuestra por debilitación.

iii. Si todos los s_i son términos estructurados de rango 0 pero algún t_i no lo es, entonces es $s_i = t_i$ el que se traduce en $\bigvee u\, u\neq u$ y concluimos igualmente.

(d) El caso del igualador es:

$$s_1 = t_1,\ s_2 = t_2,\ s_1 = s_2 \Rightarrow t_1 = t_2.$$

i. Si todos los términos son estructurados de rango 0, la traducción es el mismo secuente y es claramente un teorema de T.

ii. Si s_1 y s_2 tienen ambos rango 0, y un t_i no, entonces $s_i = t_i$ se traduce en $\bigvee u\, u\neq u$ y la traducción del axioma se sigue por debilitación.

iii. Supongamos que s_1 no es un término estructurado. Si s_2 sí que lo es, razonamos como antes a partir de $s_1 = s_2$. Por lo tanto, podemos suponer que s_1 y s_2 son ambos no estructurados. Si algún t_i es estructurado, concluimos a partir de $s_i = t_i$. Si ambos son no estructurados, entonces $t_1 = t_2$ se traduce en $\bigwedge u\, u = u$ y la traducción del axioma se obtiene por debilitación a partir de $\Rightarrow \bigwedge u\, u = u$.

iv. Supongamos que s_1 tiene rango $r\geq 1$. Si s_2 no tiene también rango r concluimos a partir de $s_1 = s_2$, así que podemos suponer que ambos tienen rango r. Si algún t_i no tiene rango r concluimos igualmente a partir de $s_i = t_i$, luego nos reducimos al caso en el que todos los términos tienen rango r, es decir, son variables. El axioma es entonces

$$X_1 = Y_1,\ X_2 = Y_2,\ X_1 = X_2 \Rightarrow Y_1 = Y_2,$$

cuya traducción es

$$\bigwedge\bar{u}(X_1(\bar{u})\leftrightarrow Y_1(\bar{u})),\ \bigwedge\bar{u}(X_2(\bar{u})\leftrightarrow Y_2(\bar{u})),\ \bigwedge\bar{u}(X_1(\bar{u})\leftrightarrow X_2(\bar{u}))$$
$$\Rightarrow \bigwedge\bar{u}(Y_1(\bar{u})\leftrightarrow Y_2(\bar{u})),$$

y es fácil ver que es un teorema de B.

(e) Consideremos ahora I3 para el relator R_r:

$$s = t,\ R_r s \Rightarrow R_r t.$$

i. Si s y t no tienen el mismo rango o uno es estructurado y el otro no, entonces $s = t$ se traduce en $\bigvee u\, u\neq u$, y concluimos como siempre.

ii. En caso contrario, $R_r s$ y $R_r t$ tienen la misma traducción, por lo que la traducción del axioma se sigue por debilitación de un axioma lógico.

(f) Finalmente, consideramos I3 para el relator S_r:

$$S_0 = T_0,\, s_1 = t_1, \ldots, s_r = t_r,\, S_0(s_1, \ldots, s_r) \Rightarrow T_0(t_1, \ldots, t_r).$$

i. Si S_0 no tiene rango r o algún s_i no tiene rango 0, la última fórmula del antecedente se traduce en $\bigvee u\, u \neq u$ y la conclusión es inmediata. Suponemos, pues, que S_0 tiene rango r y que todos los s_i tienen rango 0.

ii. T_0 no tiene rango r o algún t_i no tiene rango 0, concluimos a partir de $S_0 = T_0$ o de $s_i = t_i$.

iii. Si S_0 y T_0 tienen rango r (es decir, son variables X e Y de rango r) y los demás términos tienen rango 0, la traducción es

$$\bigwedge \bar{u}(X(u) \leftrightarrow Y(u)),\, s_1 = t_1, \ldots, s_r = t_r,\, X(s_1, \ldots, s_r) \Rightarrow Y(t_1, \ldots, t_r)$$

y es fácil ver que se trata de un teorema de B.

3. Consideremos el axioma de extensionalidad para rango r:

$$\bigwedge\nolimits_r UV(\bigwedge\nolimits_0 \bar{u}(U(\bar{u}) \leftrightarrow V(\bar{u})) \rightarrow U = V).$$

Su traducción es

$$\bigwedge UV(\bigwedge \bar{u}(U(\bar{u}) \leftrightarrow V(\bar{u})) \rightarrow \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow V(\bar{u}))),$$

que claramente es un teorema de B.

4. La traducción de $\bigwedge_0 \bar{u}\, R_0 t(\bar{u})$ es $\bigwedge \bar{u} \bigwedge u\, u = u$, que claramente es un teorema de B.

5. La traducción de $\bigvee_r U\, R_r U$ es $\bigvee U \bigwedge u\, u = u$, y también es un teorema de B.

6. Los últimos axiomas de $\tilde{T}$ son los de la forma $\tilde{\alpha}$, donde α es un axioma propio de T. Su traducción es $\tilde{\alpha}^* \equiv \alpha$, que ciertamente es un teorema de T.

Fijemos ahora una demostración en $\tilde{T}$ de un secuente $\Rightarrow \delta$. Por el teorema anterior podemos tomarla formada únicamente por fórmulas cuasiestructuradas. Todos los axiomas de $\tilde{T}$ son sentencias excepto los axiomas lógicos y los del igualador, y la sustitución de una variable libre por otra en cualquiera de estos axiomas es de nuevo un axioma. Por lo tanto, podemos aplicar el teorema 3.13 para transformar la demostración en una demostración regular. Más aún, como podemos sustituir cada variable propia por otra que no aparezca en la demostración, podemos exigir que cada variable propia de una regla cuya fórmula principal sea $\bigwedge_r U\, \alpha(U)$ o $\bigvee_r U\, \alpha(U)$ tenga precisamente rango r.

Ahora basta probar que la traducción de cada regla de inferencia de la demostración es una regla de inferencia válida en B (no necesariamente primitiva). Las únicas reglas para las que esto no es inmediato son las asociadas a los cuantificadores.

Generalizador izquierda Puesto que las fórmulas tienen que ser cuasiestructuradas, tiene que ser de la forma

$$\frac{R_r t \rightarrow \alpha(t),\, \Gamma \Rightarrow \Delta}{\bigwedge_r U \alpha(U),\, \Gamma \Rightarrow \Delta},$$

donde la variable U tiene rango r. Si t es un término estructurado de rango r, la traducción es

$$\frac{\bigwedge u\, u = u \rightarrow \alpha^*(t),\, \Gamma^* \Rightarrow \Delta^*}{\bigwedge U\, \alpha^*(U),\, \Gamma^* \Rightarrow \Delta^*}$$

y esta regla es válida en B, pues claramente $\alpha^*(t) \Rightarrow \bigwedge u\, u = u \rightarrow \alpha^*(t)$ es un teorema de B, y basta cortarlo con el secuente superior y aplicar la regla izquierda del generalizador.

Si t no es un término estructurado de rango r, la traducción es

$$\frac{\bigvee u\, u \neq u \rightarrow \alpha^*(t),\, \Gamma^* \Rightarrow \Delta^*}{\bigwedge U\, \alpha^*(U),\, \Gamma^* \Rightarrow \Delta^*},$$

pero $\Rightarrow \bigvee u\, u \neq u \rightarrow \alpha^*(t)$ es un teorema de B, luego del secuente superior se deduce $\Gamma^* \Rightarrow \Delta^*$ y por debilitación obtenemos el secuente inferior.

Generalizador derecha La regla es de la forma

$$\frac{\Gamma \Rightarrow \Delta,\, R_r Y \rightarrow \alpha(Y)}{\Gamma \Rightarrow \Delta,\, \bigwedge_r U \alpha(U).}$$

y hemos tomado la demostración de modo que el rango de Y sea precisamente r. La traducción es

$$\frac{\Gamma^* \Rightarrow \Delta^*,\, \bigwedge u\, u = u \rightarrow \alpha^*(Y)}{\Gamma^* \Rightarrow \Delta^*,\, \bigwedge U\, \alpha^*(U).}$$

Teniendo en cuenta que $\bigwedge u\, u = u \rightarrow \alpha^*(Y) \Rightarrow \alpha^*(Y)$ es un teorema de B, basta cortar este secuente con el secuente superior de la traducción y luego aplicar la regla derecha del generalizador.

Particularizador izquierda La regla tiene que ser de la forma

$$\frac{R_r Y \wedge \alpha(Y),\, \Gamma \Rightarrow \Delta}{\bigvee_r U \alpha(U),\, \Gamma \Rightarrow \Delta}$$

donde la variable propia Y tiene rango r. La traducción es

$$\frac{\bigwedge u\, u = u \wedge \alpha^*(Y),\, \Gamma^* \Rightarrow \Delta^*}{\bigvee U \alpha^*(U),\, \Gamma^* \Rightarrow \Delta^*}$$

Basta tener en cuenta que $\alpha^*(Y) \Rightarrow \bigwedge u\, u = u \wedge \alpha^*(Y)$ es un teorema de B.

Particularizador derecha La regla tiene que ser de la forma

$$\frac{\Gamma \Rightarrow \Delta,\ R_r t \wedge \alpha(t)}{\Gamma \Rightarrow \Delta,\ \bigvee_r U \alpha(U)},$$

donde la variable U tiene rango r. Si t es un término estructurado de rango r, la traducción es

$$\frac{\Gamma^* \Rightarrow \Delta^*,\ \bigwedge u\, u = u \wedge \alpha^*(t)}{\Gamma^* \Rightarrow \Delta^*,\ \bigvee U \alpha^*(U)},$$

y esta regla es válida en B, pues claramente $\bigwedge u\, u = u \wedge \alpha^*(t) \Rightarrow \alpha^*(t)$ es un teorema de B, y basta cortarlo con el secuente superior y aplicar la regla derecha del particularizador.

Si t no es un término estructurado de rango r, la traducción es

$$\frac{\Gamma^* \Rightarrow \Delta^*,\ \bigvee u\, u \neq u \wedge \alpha^*(t)}{\Gamma^* \Rightarrow \Delta^*,\ \bigvee U \alpha^*(U)},$$

pero $\bigvee u\, u \neq u \wedge \alpha^*(t) \Rightarrow$ es un teorema de B, luego del secuente superior se deduce $\Gamma^* \Rightarrow \Delta^*$ y por debilitación obtenemos el secuente inferior. ■

Nota La demostración del teorema anterior muestra que el teorema sigue siendo válido si a $\tilde{T}$ le añadirmos cualquier axioma cuasiestructurado cuya traducción sea un teorema de T. Por ejemplo, también podemos considerar como axiomas de $\tilde{T}$ las sentencias

$$\bigwedge_r U\, \neg R_s U,$$

para todo $r \neq s$.

En el caso de que el lenguaje r sea reducido, es decir, que sólo disponga de variables de segundo orden de rango 1, tenemos por definición que

$$\bigwedge U (R_0 U \vee R_1 U),$$

es decir, que todo objeto es un objeto de la teoría inicial o bien un conjunto de objetos. También podríamos considerar lenguajes de segundo orden que sólo tuvieran variables de segundo orden de rangos entre 0 y n, en cuyo caso podríamos definir $R_0 X \equiv \neg(R_1 X \vee \cdots \vee R_n X)$ y también se cumpliría

$$\bigwedge U (R_0 U \vee \cdots \vee R_n U).$$

Sin embargo, cuando consideramos variables de todos los rangos, no podemos expresar mediante una fórmula que todo objeto tenga un rango asignado. ■

Uno de los motivos por los que tiene interés traducir la lógica de segundo orden a lógica de primer orden es que para la lógica de primer orden disponemos del teorema de completitud semántica, que nos asegura que cualquier razonamiento puramente lógico a partir de unos axiomas dados (es decir, que no presuponga nada que no afirmen realmente los axiomas) es formalizable, por lo que en la práctica no es necesario preocuparse por encontrar formalizaciones de los argumentos considerados.

En particular, si T es una teoría axiomática sobre un lenguaje de primer orden $\mathcal{L}$, podemos considerar sus extensiones predicativa y plena T_0 y T_2 definidas en 9.10, y a su vez podemos considerar las teorías de primer orden $\tilde{T}_0$ y $\tilde{T}_2$. Conviene particularizar la definición de estas teorías a partir de T sin pasar por las teorías de segundo orden:

Definición 9.18 Sea T una teoría axiomática sobre un lenguaje formal de primer orden $\mathcal{L}$. Sea $\tilde{\mathcal{L}}$ un lenguaje formal de primer orden cuyos signos eventuales son los mismos que los de $\mathcal{L}$ más una familia R_0, R_1, $R_2, \ldots$ de relatores de rango 1 y otra familia S_1, S_2, $S_3, \ldots$ de relatores S_r de rango $r+1$. Usaremos las abreviaturas:

$$X(x_1, \ldots, x_r) \equiv S_r X x_1, \ldots, x_n,$$

$$\textstyle\bigwedge_r U\alpha \equiv \bigwedge U(R_r U \to \alpha), \qquad \bigvee_r U\,\alpha \equiv \bigvee U(R_r U \land \alpha).$$

Diremos que una semifórmula α de $\tilde{\mathcal{L}}$ está *estructurada* si a cada una de sus variables (libre o ligada) se le puede asignar un rango de modo que:

1. Las subfórmulas atómicas asociadas a relatores de $\mathcal{L}$ y a R_0 contengan únicamente variables de rango 0,

2. En las subfórmulas $R_r T$ con $r \geq 1$ el término T sea una mera variable de rango r,

3. En las subfórmulas $T(t_1, \ldots, t_r)$ el término T sea una mera variable de rango r y los términos t_i sólo contengan variables de rango 0. Todos los cuantificadores aparezca en la forma $\bigwedge_r U\,\alpha$ o $\bigvee_r U\,\alpha$, donde r es el rango de la variable U.

La semifórmula es de primer orden si todas sus variables ligadas son de rango 0.

Identificando las variables de $\mathcal{L}$ con las de $\tilde{\mathcal{L}}$, podemos ver a cada término t de $\mathcal{L}$ como término de $\tilde{\mathcal{L}}$. A cada semifórmula α de $\mathcal{L}$ le podemos asignar una semifórmula estructurada de primer orden $\tilde{\alpha}$ de $\tilde{\mathcal{L}}$ con el criterio siguiente:

1. $\widetilde{Rt_1 \cdots t_r} \equiv Rt_1 \cdots t_r$,

2. $\widetilde{\neg\alpha} \equiv \neg\tilde{\alpha}$, $\quad \widetilde{\alpha \lor \beta} \equiv \tilde{\alpha} \lor \tilde{\beta}$,

3. $\widetilde{\bigwedge u\,\alpha} \equiv \bigwedge_0 u\,\tilde{\alpha}$, $\quad \widetilde{\bigvee u\,\alpha} \equiv \bigvee_0 u\,\tilde{\alpha}$.

La estructuración se obtiene sin más que asignar a todas las variables el rango 0.

Definimos la *extensión predicativa de segundo orden* $\tilde{T}_0$ de T como la teoría axiomática sobre $\tilde{\mathcal{L}}$ cuyos axiomas propios son:

Extensionalidad Para cada $r \geq 1$:

$$\textstyle\bigwedge_r UV(\bigwedge_0 u_1 \cdots u_r(U(u_1, \ldots, u_r) \leftrightarrow V(u_1, \ldots, u_r)) \to U = V).$$

Comprensión Para cada semifórmula estructurada de primer orden $\alpha(\bar{u}, \bar{v})$ en la que las variables u_i tengan rango 0 y las variables v_i tengan rango r_i:

$$\bigwedge_{r_1} v_1 \cdots \bigwedge_{r_n} v_n \bigvee_r U \bigwedge_0 u_1 \cdots u_r (U(u_1, \ldots, u_r) \leftrightarrow \alpha(\bar{u}, \bar{v})).$$

Axiomas estructurales Son las sentencias:

1. $\bigwedge_0 u_1 \cdots u_n \, R_0 t(u_1, \ldots u_n)$, para todo término t de $\tilde{\mathcal{L}}$,
2. $\bigvee_0 u \, R_0 u$,
3. $\bigwedge_r U \, \neg R_s U$, para $r \neq s$.

Axiomas propios Son las traducciones $\tilde{\alpha}$, donde α es la clausura universal de un axioma propio de T.

Si extendemos el axioma de comprensión eliminando la restricción de que α sea de primer orden tenemos la *extensión plena de segundo orden* $\tilde{T}_2$ de T.

Notemos que no hemos incluido como axioma $\bigvee_r U \, R_r U$ para $r \geq 1$ porque esto se sigue del axioma de comprensión.

También podemos definir *extensiones restringidas* en las que $\tilde{\mathcal{L}}$ sólo tenga los relatores adicionales R_1 y S_1, de modo que $R_0 t \equiv \neg R_1 t$, en cuyo caso es más conveniente la notación

$$\operatorname{cto} X \equiv R_1 X, \qquad x \in X \equiv X(x).$$

Combinando los teoremas 9.11 y 9.17, obtenemos el enunciado siguiente:

Teorema 9.19 *Si T es una teoría axiomática sobre un lenguaje de primer orden $\mathcal{L}$, entonces su extensión predicativa de segundo orden $\tilde{T}_0$ es una extensión conservativa de T, es decir, que si una sentencia α de $\mathcal{L}$ es demostrable en T si y sólo si su traducción $\tilde{\alpha}$ es demostrable en $\tilde{T}_0$. En particular, T es consistente si y sólo si lo es $\tilde{T}_0$.*

Informalmente, la extensión predicativa $\tilde{T}_0$ nos permite hablar de los objetos de los que habla la teoría T (identificados con los objetos que cumplen $R_0 x$), pero además incorpora relaciones de cualquier rango (o sólo de rango 1) entre dichos objetos, definibles mediante fórmulas de primer orden.

El teorema anterior nos permite ver el paso de T a $\tilde{T}_0$ como un mero artificio técnico para trabajar con más comodidad, pues este uso formal de relaciones arbitrarias (siempre suponiéndolas definibles mediante fórmulas de primer orden) es prescindible, en el sentido de que todo teorema de $\tilde{T}_0$ que hable exclusivamente de objetos de la teoría original (es decir, que no tenga variables de segundo orden) es demostrable en T, es decir, sin hacer referencia en ningún momento a variables de segundo orden.

Esto ya no es así si consideramos la extensión plena, que en general permite demostrar traducciones de fórmulas de $\mathcal{L}$ que no son demostrables en T. La aritmética de Peano y la teoría de conjuntos ZF que estudiaremos en las secciones siguientes muestran ejemplos de ello.

9.5 La aritmética de Peano de segundo orden

La aritmética de Peano de segundo orden AP_2 se define como la teoría sobre el lenguaje $\mathcal{L}_a$ de la aritmética extendido con variables de segundo orden de rango 1 y cuyos axiomas son:

1. Los axiomas lógicos $\alpha \Rightarrow \alpha$,
2. Los axiomas del igualador:
$$\bigwedge u\, u = u, \qquad \bigwedge W \bigwedge uv(u = v \land W(u) \to W(v)),$$
3. Los axiomas de comprensión para toda fórmula $\alpha(x, \bar{y}, \bar{Y})$:
$$\bigwedge \bar{V} \bigwedge \bar{v} \bigvee U \bigwedge u(U(u) \leftrightarrow \alpha(u, \bar{v}, \bar{V})),$$
4. Los axiomas de Peano salvo los axiomas de inducción,
5. El axioma de inducción de segundo orden:
$$\bigwedge U(U(0) \land \bigwedge u(U(u) \to U(u')) \to \bigwedge u\, U(u)),$$

y cuyas reglas de inferencia son las de B.

Las fórmulas de primer orden de $\mathcal{L}_a$ reciben el nombre de *fórmulas aritméticas,* por lo que la teoría que resulta de restringir el axioma de comprensión a fórmulas aritméticas se conoce como[7] ACA_0.

Notemos que ACA_0 y AP_2 no son exactamente lo que hemos definido como las extensiines predicativa y plena de AP debido a que no sólo hemos sustituido los axiomas del igualador de primer orden por sus versiones de segundo orden, sino que también hemos sustituido los axiomas de inducción de primer orden por un único axioma de segundo orden.

Observemos que aplicando este axioma de segundo orden al conjunto U dado por el axioma de comprensión para una fórmula α obtenemos el axioma de inducción de primer orden asociado a α, luego todo teorema de AP es también un teorema de ACA_0. Más aún:

Teorema 9.20 *La teoría* ACA_0 *es una extensión conservativa de* AP, *es decir, una fórmula sin variables de segundo orden es demostrable en* AP *si y sólo si es demostrable en* ACA_0.

Demostración: El argumento es exactamente el mismo empleado en la prueba del teorema 9.13. Las únicas diferencias consisten en que, en lugar de los axiomas $I_1, \ldots, I_n$ ahora tenemos únicamente $\mathrm{I} \equiv \mathrm{I}_1$ y el axioma de inducción de segundo orden, pero están exactamente en las mismas condiciones. ■

[7] ACA (sin el subíndice) es la teoría que mantiene el principio de inducción como esquema axiomático, pero admitiendo todas las fórmulas, incluso las de segundo orden.

A su vez, podemos considerar las teorías de primer orden equivalentes a AP_2 y a ACA_0. Para ello añadimos al lenguaje $\mathcal{L}_a$ de la aritmética de primer orden un nuevo relator cto de rango 1 y un relator $\in$ de rango 2. Definimos

$$\operatorname{Nat} x \equiv \neg \operatorname{cto} x$$

y usaremos letras minúsculas para representar variables restringidas con $\operatorname{Nat} u$ y mayúsculas para indicar variables restringidas con $\operatorname{cto} U$, es decir,

$$\bigwedge u\,\alpha \equiv \bigwedge_0 u\,\alpha \equiv \bigwedge u(\operatorname{Nat} u \to \alpha), \quad \bigwedge U\,\alpha \equiv \bigwedge_1 U\,\alpha \equiv \bigwedge U(\operatorname{cto} U \to \alpha),$$

$$\bigvee u\,\alpha \equiv \bigvee_0 u\,\alpha \equiv \bigvee u(\operatorname{Nat} u \land \alpha), \quad \bigvee U\alpha \equiv \bigvee_1 U\alpha \equiv \bigvee U(\operatorname{cto} U \land \alpha).$$

Llamamos $\widetilde{\mathrm{AP}}_2$ a la teoría determinada por los axiomas siguientes:

Axiomas de Peano de primer orden			
1	$\operatorname{Nat} 0$	5	$\bigwedge u(u+0=u)$
2	$\bigwedge u \operatorname{Nat} u'$	6	$\bigwedge uv(u+v'=(u+v)')$
3	$\bigwedge u\, u' \neq 0$	7	$\bigwedge u\, u\cdot 0 = 0$
4	$\bigwedge uv(u'=v' \to u=v)$	8	$\bigwedge uv(u\cdot v' = u\cdot v + u)$
Inducción	$\bigwedge U(0\in U \land \bigwedge u(u\in U \to u'\in U) \to \bigwedge u\, u\in U)$		
Extensionalidad	$\bigwedge UV(\bigwedge u(u\in U \leftrightarrow u\in V) \to U=V)$		
Comprensión	$\bigwedge U_1\cdots U_r \bigwedge u_1\cdots u_s \bigvee U \bigwedge u(u\in U \leftrightarrow \phi(u))$ $(*)$		

$(*)$ para toda semifórmula estructurada $\phi(u, u_1, \ldots, u_s, U_1, \ldots, U_r)$ cuyas variables libres sean las indicadas.

La teoría $\widetilde{\mathrm{ACA}}_0$ es la que resulta de restringir el axioma de comprensión a semifórmulas aritméticas, es decir, semifórmulas estructuradas que no contengan variables ligadas de segundo orden.

Observemos que hemos sustituido el primer axioma estructural por los dos primeros axiomas de Peano (que son dos casos particulars), pues una simple inducción demuestra

$$\bigwedge uv \operatorname{Nat}(u+v), \qquad \bigwedge uv \operatorname{Nat}(u\cdot v)$$

y a su vez esto implica $\bigwedge \bar{u} \operatorname{Nat} t(\bar{u})$ por inducción sobre la longitud de t. El segundo axioma estructural es consecuencia del axioma $\operatorname{Nat} 0$ y el tercero se cumple trivialmente por definición de Nat.

Las teorías $\widetilde{\mathrm{AP}}_2$ y $\widetilde{\mathrm{ACA}}_0$ son esencialmente las mismas[8] que en [LM 10.1] llamábamos AP_2 y ACA_0, por lo que el teorema siguiente, que es consecuencia inmediata de 9.20 y 9.19, es esencialmente el mismo que [LM 10.2]:

Teorema 9.21 *La teoría $\widetilde{\mathrm{ACA}}_0$ es una extensión conservativa de* AP*, es decir, una sentencia α de $\mathcal{L}_a$ es demostrable en* AP *si y sólo si su traducción $\tilde{\alpha}$ es demostrable en $\widetilde{\mathrm{ACA}}_0$.*

[8]Las únicas diferencias consisten en que aquí estamos considerando lenguajes formales sin descriptor, distinguimos entre variables libres y ligadas y hemos tomado como signos lógicos primitivos el negador, el disyuntor y los cuantificadores, pero nada de esto es relevante.

En [LM 10.2] dimos una demostración completamente distinta de este mismo resultado. La prueba que hemos dado aquí es muy técnica (pues depende del teorema de eliminación de cortes), pero tiene la ventaja de que es finitista y nos da un algoritmo para transformar una demostración en ACA_0 en una demostración en AP. Por el contrario, la demostración de [LM] no es finitista en sentido estricto, pues se basa en el teorema de completitud semántica, pero deja mucho más clara la razón de fondo por la cual es cierto el teorema: lo que sucede es que todo modelo de AP puede extenderse hasta un modelo de ACA_0, de donde se sigue que todo teorema de ACA_0 sin variables de segundo orden es verdadero en todo modelo de AP, luego es un teorema de AP.

Por otro lado, el teorema [LM 10.7] prueba que AP_2 no es una extensión conservativa de AP, ya que en ella puede probarse la consistencia de AP.

9.6 La teoría de von Neumann-Bernays

Vamos a estudiar ahora las extensiones de segundo orden de la teoría de conjuntos ZFC. En realidad sólo son relevantes los axiomas básicos, por lo que podemos considerar la teoría ZF^* definida sobre el lenguaje formal de la teoría de conjuntos $\mathcal{L}_{\mathrm{tc}}$ cuyo único signo eventual es un relator diádico $\in$ y cuyos axiomas propios son [LM 12.1]:

Extensionalidad	$\bigwedge vw(\bigwedge u(u \in v \leftrightarrow u \in w) \rightarrow v = w)$
Par	$\bigwedge ab \bigvee v \bigwedge u(u \in v \leftrightarrow u = a \vee u = b)$
Unión	$\bigwedge a \bigvee b \bigwedge u(u \in b \leftrightarrow \bigvee v(u \in v \wedge v \in a))$
Reemplazo	$\bigwedge uv_1v_2(\phi(u, v_1) \wedge \phi(u, v_2) \rightarrow v_1 = v_2)$
	$\rightarrow \bigwedge a \bigvee b \bigwedge v(v \in b \leftrightarrow \bigvee u \in a\, \phi(u, v))$ $(*)$

$(*)$ para toda fórmula $\phi(x, y)$, tal vez con más variables libres, distintas de b.

Vemos así que los axiomas propios de ZF^* son tres axiomas más un esquema axiomático y vamos a ver que, al igual que sucede con el principio de inducción en AP, al pasar a la extensión predicativa podemos sustituirlo por un único axioma de segundo orden.

Como estamos trabajando sin descriptores, no podemos definir los pares ordenados (x, y), pero sí que podemos definir una fórmula $z = (x, y)$ de modo que, a partir de los tres primeros axiomas, se demuestra:

$$\bigwedge uvwu'v'w'(w = (u, v) \wedge w' = (u', v') \rightarrow (w = w' \leftrightarrow u = u' \wedge v = v')).$$

Definimos la *teoría (restringida) de von Neumann-Bernays* NB^* como la teoría sobre el lenguaje que resulta de añadir a $\mathcal{L}_{\mathrm{tc}}$ variables de segundo orden de rango 1 determinada por los axiomas y reglas de inferencia de B más los axiomas propios siguientes:

1. Los axiomas del igualador:

$$\bigwedge u\, u = u, \qquad \bigwedge W \bigwedge uv(u = v \wedge W(u) \rightarrow W(v)),$$

2. Los axiomas de comprensión, para toda fórmula de primer orden $\alpha(x, \bar{y}, \bar{Y})$:

$$\bigwedge \bar{V} \bigwedge \bar{v} \bigvee U \bigwedge u (U(u) \leftrightarrow \alpha(u, \bar{v}, \bar{V})),$$

3. Los axiomas de extensionalidad, par y unión de ZF*

4. El axioma de reemplazo de segundo orden:[9]

$$\bigwedge U(\mathrm{Un}\, U \to \bigwedge a \bigvee b \bigwedge v(v \in b \leftrightarrow \bigvee uw(u \in a \land w = (u,v) \land U(w)))),$$

donde

$$\mathrm{Un}\, X \equiv \bigwedge uvwv'w'(w = (u,v) \land w' = (u,v') \land X(w) \land X(w') \to v = v').$$

Así, NB* es la extensión predicativa de segundo orden de ZF* salvo por el hecho de que hemos sustituido los axiomas del igualador y de reemplazo de primer orden por dos axiomas de segundo orden.

En NB* se demuestra que la fórmula $z = (x, y)$ cumple la misma relación de unicidad que hemos señalado para ZF* (con exactamente la misma prueba). Si $\phi(x, y)$ es cualquier fórmula sin variables de segundo orden, aplicando el axioma de reemplazo de segundo orden a la relación U determinada por el axioma de comprensión para la fórmula

$$\alpha(x) \equiv \bigvee uv(x = (u, v) \land \phi(u, v))$$

obtenemos el axioma de reemplazo de primer orden correspondiente a ϕ, por lo que todo teorema de ZF* es un teorema de NB*. Esto implica que todo teorema de la extensión predicativa de ZF* (en particular, todo teorema de ZF*) es demostrable en NB*. Pero también se da el recíproco:

Teorema 9.22 *La teoría* NB* *es una extensión conservativa de* ZF*, *es decir, una fórmula sin variables de segundo orden es demostrable en* ZF* *si y sólo si lo es en* NB*.

Demostración: El argumento es exactamente el mismo empleado en la prueba del teorema 9.13. Las únicas diferencias consisten en que, en lugar de los axiomas $I_1, \ldots, I_n$ ahora tenemos únicamente $\mathrm{I} \equiv \mathrm{I}_1$ y el axioma de reemplazo de segundo orden, pero están exactamente en las mismas condiciones. ■

Nota Observemos que este teorema se extiende automáticamente a cualquier teoría que resulte de añadir axiomas a ZF*. Por ejemplo, ZFC es la teoría que resulta de añadir a ZF* los axiomas de infinitud, partes, regularidad y elección [LM 12.1], y se corresponde con la teoría NB que resulta de añadir a NB* estos

[9] Si admitiéramos variables de segundo orden de rango 2 el axioma de reemplazo admitiría un enunciado más simple:

$$\bigwedge U(\bigwedge uv_1v_2(U(u,v_1) \land U(u,v_2) \to v_1 = v_2) \to \bigwedge a \bigvee b \bigwedge v(v \in b \leftrightarrow \bigvee u \in a\, U(u,v))).$$

mismos axiomas. Si llamamos γ a la conjunción de los nuevos axiomas, tenemos que una fórmula δ sin variables de segundo orden es un teorema de ZFC si y sólo si $\gamma \rightarrow \delta$ es un teorema de ZF*, si y sólo si lo es de NB*, si y sólo si δ es un teorema de NB. Lo mismo vale para cualquier otra combinación de axiomas que añadamos a ZF*. ■

La teoría de conjuntos NBG La teoría NB*, como cualquier otra teoría axiomática de segundo orden, es equivalente a una teoría de primer orden. Sin embargo, en este caso podemos diseñar una muchísimo más simple que la que resulta de particularizar la construcción general descrita en la definición 9.18.

Informalmente, la idea básica es, como siempre, interpretar las variables de segundo orden de NB* como conjuntos de objetos, pero como los objetos descritos por ZF* son ya conjuntos, conviene referirse a los "conjuntos de conjuntos" recorridos por las variables de segundo orden de NB* como "clases". Con esto queremos decir que podemos pensar que cada variable de segundo orden X representa una clase cuyos elementos son los conjuntos x que cumplen $X(x)$. Ahora bien, el axioma de comprensión aplicado a la fórmula $\alpha(x) \equiv x \in y$ es

$$\bigwedge u \bigvee U \bigwedge v(U(v) \leftrightarrow v \in u),$$

y esto —siempre informalmente— significa que, para cada conjunto u, existe una clase U cuyos elementos son exactamente los de u. En otras palabras, las clases vuelven redundantes a los conjuntos. La teoría de conjuntos de von Neumann-Bernays-Gödel (NBG) aprovecha esta idea para formalizar NB sin más conceptos primitivos que el de clase y la pertenencia entre clases, es decir, sin necesidad de introducir desde el principio una distinción entre clases y conjuntos análoga a la que la teoría de primer orden $\widehat{\mathrm{ACA}}_0$ establece entre conjuntos y números naturales.

Para precisar esta idea extendemos la relación de pertenencia a clases arbitrarias mediante la definición:

$$X \in Y \equiv \bigvee v(Y(v) \wedge \bigwedge u(X(u) \leftrightarrow u \in v)).$$

Así, una clase X pertenece a otra clase Y si sus elementos son los mismos que los de uno de los conjuntos que pertenecen a Y. A su vez, definimos

$$\operatorname{cto} X \equiv \bigvee U\, X \in U$$

En otras palabras: una clase es un conjunto si pertenece a otra clase. Ésta es la definición más conveniente desde un punto de vista técnico, porque se corresponde con la definición de conjunto que daremos en NBG, pero es equivalente a otra más natural:

Teorema 9.23 *En* NB* *se demuestra*

$$\operatorname{cto} X \leftrightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v),$$

es decir, una clase es un conjunto si y sólo si tiene los mismos elementos que un conjunto.

Demostración: Según la definición que hemos dado:

$$\operatorname{cto} X \equiv \bigvee Uv(U(v) \land \bigwedge u(X(u) \leftrightarrow u \in v)).$$

Se trata de probar que $U(v)$ es redundante. Para ello razonamos como sigue:

$$\begin{array}{c}
\begin{array}{cc} \begin{array}{c} \Rightarrow y = y \\ \hline \Rightarrow y = y,\, Y(y) \end{array} & Y(y) \Rightarrow Y(y) \end{array} \\ \hline
y = y \to Y(y) \Rightarrow Y(y) \\ \hline
Y(y) \leftrightarrow Y(y) \Rightarrow Y(y)
\end{array}$$

Aplicando la regla derecha del conjuntor a este secuente y al axioma

$$\bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigwedge u(X(u) \leftrightarrow u \in y)$$

obtenemos

$$\bigwedge u(X(u) \leftrightarrow u \in y),\ (Y(y) \leftrightarrow y = y) \Rightarrow Y(y) \land \bigwedge u(X(u) \leftrightarrow u \in y)$$

Aplicando la regla derecha del particularizador para ligar y e Y obtenemos

$$\begin{array}{c}
\bigwedge u(X(u) \leftrightarrow u \in y),\ (Y(y) \leftrightarrow y = y) \Rightarrow \operatorname{cto} X \\ \hline
\bigwedge u(X(u) \leftrightarrow u \in y),\ \bigwedge u(Y(u) \leftrightarrow u = y) \Rightarrow \operatorname{cto} X \\ \hline
\bigwedge u(X(u) \leftrightarrow u \in y),\ \bigvee U \bigwedge u(U(u) \leftrightarrow u = y) \Rightarrow \operatorname{cto} X \\ \hline
\bigwedge u(X(u) \leftrightarrow u \in y),\ \bigwedge v \bigvee U \bigwedge u(U(u) \leftrightarrow u = v) \Rightarrow \operatorname{cto} X \\ \hline
\bigvee v \bigwedge u(X(u) \leftrightarrow u \in v),\ \bigwedge v \bigvee U \bigwedge u(U(u) \leftrightarrow u = v) \Rightarrow \operatorname{cto} X
\end{array}$$

pero la segunda fórmula del antecedente es un axioma de comprensión, luego podemos cortarlo y queda

$$\begin{array}{c}
\bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \Rightarrow \operatorname{cto} X \\ \hline
\Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \to \operatorname{cto} X
\end{array}$$

La implicación contraria es más sencilla:

$$\begin{array}{c}
\bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigwedge u(X(u) \leftrightarrow u \in y) \\ \hline
y \in Y, \bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigwedge u(X(u) \leftrightarrow u \in y) \\ \hline
y \in Y \land \bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigwedge u(X(u) \leftrightarrow u \in y) \\ \hline
y \in Y \land \bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \\ \hline
\bigvee v(v \in Y \land \bigwedge u(X(u) \leftrightarrow u \in v)) \Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \\ \hline
\operatorname{cto} X \Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \\ \hline
\Rightarrow \operatorname{cto} X \to \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v)
\end{array}$$

La regla derecha del conjuntor nos da la coimplicación ■

Pasamos ya a analizar la versión de primer orden de NB*, que no es sino la teoría de conjuntos (restringida) de von Neumann-Bernays-Gödel (NBG*). Se trata [LM 12.1] de la teoría axiomática de primer orden sobre el lenguaje $\mathcal{L}_{\rm tc}$ cuyos axiomas son:

Extensionalidad	$\bigwedge UV(\bigwedge u(u\in U\leftrightarrow u\in V)\rightarrow U=V)$
Comprensión	$\bigvee U\bigwedge u(u\in U\leftrightarrow \phi(u))\qquad (*)$
Vacío	$\bigvee v\bigwedge u\, u\notin v$
Par	$\bigwedge ab\bigvee v\bigwedge u(u\in v\leftrightarrow u=a\vee u=b)$
Unión	$\bigwedge a\bigvee b\bigwedge u(u\in b\leftrightarrow \bigvee v(u\in v\wedge v\in a))$
Reemplazo	$\bigwedge F(\mathrm{Un}\, F\rightarrow \bigwedge a\bigvee b\bigwedge v(v\in b\leftrightarrow$ $\bigvee uw(u\in a\, w=(u,v)\wedge w\in F)))$

$(*)$ para toda semifórmula primitiva $\phi(u)$ tal vez con más variables libres (distintas de U),

donde estamos adoptando los convenios siguientes:

1. $\mathrm{cto}\, X\equiv \bigvee U\, X\in U$,
2. Las variables ligadas minúsculas representan conjuntos, es decir,
$$\bigwedge u\,\alpha\equiv\bigwedge U(\mathrm{cto}\, U\rightarrow\alpha),\quad \bigvee u\,\alpha\equiv\bigvee U(\mathrm{cto}\, U\wedge\alpha),$$
3. Las semifórmulas primitivas son las que tienen todas las variables ligadas restringidas a conjuntos,
4. La fórmula $w=(x,y)$ es la definición usual de par ordenado en teoría de conjuntos,
5. La definición de clase unívoca es:
$$\mathrm{Un}\, F\equiv\bigwedge uvwv'w'(w=(u,v)\wedge w'=(u,v')\wedge w\in V\wedge w'\in F\rightarrow v=v').$$

Vamos a probar que NBG* es esencialmente la misma teoría que NB*. Para ello, fijada una biyección entre las variables (de primer y segundo orden) del lenguaje de de NB* y las variables de $\mathcal{L}_{\rm tc}$, a cada fórmula α del primero le asociamos la fórmula $\tilde{\alpha}$ de $\mathcal{L}_{\rm tc}$ dada por:

1. $\widetilde{x=y}\equiv X=Y$,
2. $\widetilde{x\in y}\equiv X\in Y$,
3. $\widetilde{X(y)}\equiv Y\in X$,
4. $\widetilde{\neg\alpha}\equiv\neg\tilde{\alpha}$,
5. $\widetilde{\alpha\vee\beta}\equiv\tilde{\alpha}\vee\tilde{\beta}$,
6. $\widetilde{\bigwedge u\,\alpha(u)}\equiv\bigwedge U(\mathrm{cto}\, U\rightarrow\tilde{\alpha}(U))\equiv\bigwedge u\tilde{\alpha}(u)$,
7. $\widetilde{\bigwedge U\,\alpha(U)}\equiv\bigwedge U\,\tilde{\alpha}(U)$,
8. $\widetilde{\bigvee u\,\alpha(u)}\equiv\bigvee U(\mathrm{cto}\, U\wedge\tilde{\alpha}(U))\equiv\bigvee u\,\tilde{\alpha}(u)$,
9. $\widetilde{\bigvee U\,\alpha(U)}\equiv\bigvee U\,\tilde{\alpha}(U)$.

Es claro entonces que las fórmulas de primer orden se traducen en fórmulas primitivas.

Teorema 9.24 *Si una fórmula α es demostrable en* NB* *y no tiene variables libres de primer orden, entonces $\tilde{\alpha}$ es demostrable en* NBG*.

DEMOSTRACIÓN: Si $S \equiv \Gamma \Rightarrow \Delta$ es un secuente del lenguaje de NB* en cuyas fórmulas aparecen libres las variables de primer orden $x_1, \ldots, x_n$, correspondientes a las variables $X_1, \ldots, X_n$ de $\mathcal{L}_{\text{tc}}$, llamaremos

$$\Theta_S \equiv \{\operatorname{cto} X_1, \ldots, \operatorname{cto} X_n\}$$

y definimos $\tilde{S} \equiv \Theta_S, \tilde{\Gamma} \Rightarrow \tilde{\Delta}$, donde $\tilde{\Gamma}$ y $\tilde{\Delta}$ son los conjuntos de traducciones de las fórmulas de Γ y Δ.

Una comprobación rutinaria muestra que si S es un axioma de NB*, entonces $\tilde{S}$ es un teorema de NBG* (de hecho, la adición de Θ_S no aporta nada en este caso, pero siempre se puede añadir por debilitación). Veamos ahora que al traducir cada regla de inferencia de B obtenemos una regla de inferencia válida de LK. Las únicas reglas para las que esto no es inmediato son las asociadas a los cuantificadores de primer orden. Llamemos S_1 al secuente superior y S_2 al inferior.

Generalizador izquierda La traducción de la regla es

$$\frac{\Theta_{S_1}, \tilde{\alpha}(Y), \tilde{\Gamma} \Rightarrow \tilde{\Delta}}{\Theta_{S_2}, \bigwedge u\, \tilde{\alpha}(u), \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

Notemos que $\Theta_{S_1} = \Theta_{S_2} \cup \{\operatorname{cto} Y\}$, por lo que la regla se deduce así:

$$\cfrac{\cfrac{\Theta_{S_2}, \operatorname{cto} Y, \tilde{\alpha}(Y), \tilde{\Gamma} \Rightarrow \tilde{\Delta} \qquad \operatorname{cto} Y \Rightarrow \operatorname{cto} Y}{\Theta_{S_2}, \operatorname{cto} Y, \operatorname{cto} Y \rightarrow \tilde{\alpha}(Y), \tilde{\Gamma} \Rightarrow \tilde{\Delta}}}{\Theta_{S_2}, \operatorname{cto} Y, \bigwedge u\, \tilde{\alpha}(u), \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

Si la variable y está libre en S_2, entonces podemos suprimir $\operatorname{cto} Y$ del secuente inferior, pues ya está en Θ_{S_2}. En caso contrario, la variable Y sólo aparece en la fórmula $\operatorname{cto} Y$, luego sirve como variable crítica para aplicar la regla izquierda del particularizador, con lo que la transformamos en $\bigvee U \operatorname{cto} U$ y, como esto es un teorema de NBG*, podemos cortarla e igualmente acabamos eliminando $\operatorname{cto} Y$. El resultado es el secuente $\tilde{S}_2$.

Generalizador derecha La traducción de la regla se demuestra así:

$$\cfrac{\cfrac{\Theta_{S_2}, \operatorname{cto} Y, \tilde{\Gamma} \Rightarrow \tilde{\Delta}, \tilde{\alpha}(Y)}{\Theta_{S_2}, \tilde{\Gamma} \Rightarrow \tilde{\Delta}, \operatorname{cto} Y \rightarrow \tilde{\alpha}(Y)}}{\Theta_{S_2}, \tilde{\Gamma} \Rightarrow \tilde{\Delta}, \bigwedge u\, \tilde{\alpha}(u)}$$

donde usamos que la variable y era crítica en la regla de partida, por lo que Y sólo aparece en la fórmula auxiliar del segundo secuente, y sirve como variable crítica.

Particularizador izquierda La traducción de la regla se demuestra así:

$$\cfrac{\cfrac{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\alpha}(Y),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}{\Theta_{S_2},\ \mathrm{cto}\,Y \wedge \tilde{\alpha}(Y),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}}{\Theta_{S_2},\ \bigvee u\, \tilde{\alpha}(u),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

donde la variable Y sirve como variable propia por la misma razón que en el caso anterior.

Particularizador derecha Ahora tenemos:

$$\cfrac{\cfrac{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \tilde{\alpha}(Y) \qquad \mathrm{cto}\,Y \Rightarrow \mathrm{cto}\,Y}{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \mathrm{cto}\,Y \wedge \tilde{\alpha}(Y)}}{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \bigvee u\, \tilde{\alpha}(u)}$$

Si la variable y está libre en S_2, podemos suprimir $\mathrm{cto}\,Y$ del secuente inferior. En caso contrario, podemos usar Y como variable propia para sustituirla por $\bigvee U\, \mathrm{cto}\, U$ y, como esto es un teorema de NBG*, podemos cortarlo y así llegamos a $\tilde{S}_2$.

Por consiguiente, es claro que cada demostración de α en NB* se traduce en una demostración de $\tilde{\alpha}$ en NBG*. ■

Recíprocamente, si α es una fórmula de $\mathcal{L}_{\mathrm{tc}}$, podemos traducirla a una fórmula $\bar{\alpha}$ del lenguaje de segundo orden de NB* considerando a todas sus variables como variables de segundo orden e interpretando la igualdad y la pertenencia como

$$X = Y \equiv \bigwedge u(X(u) \leftrightarrow Y(u)), \qquad X \in Y \equiv \bigvee v(Y(v) \wedge \bigwedge u(X(u) \leftrightarrow u \in v)).$$

Teorema 9.25 *Si α es una fórmula de $\mathcal{L}_{\mathrm{tc}}$, entonces α es un teorema de* NBG* *si y sólo si $\bar{\alpha}$ es un teorema de* NB**.*

Demostración: De nuevo es pura rutina comprobar que las traducciones de los axiomas de NBG* (incluyendo los axiomas lógicos y los axiomas del igualador) son teoremas de NB*, y en este caso es inmediato que cada regla de inferencia de LK se traduce en una regla de inferencia válida en B. (Las reglas de los cuantificadores de LK se corresponden exactamente con las reglas de los cuantificadores de segundo orden de B.) Por lo tanto, concluimos que si α es un teorema de NBG*, entonces $\bar{\alpha}$ es un teorema de NB*.

Para probar el recíproco observamos que si $\bar{\alpha}$ es un teorema de NB*, como no tiene variables libres de primer orden, por 9.24 sabemos que $\tilde{\bar{\alpha}}$ es un teorema de NBG*, y basta ver que esta fórmula equivale a α en NBG*.

En efecto, razonamos por inducción sobre la longitud de α. Si $\alpha \equiv X = Y$, entonces

$$\bar{\alpha} \equiv \bigwedge u(X(u) \leftrightarrow Y(u)), \qquad \tilde{\bar{\alpha}} \equiv \bigwedge u(u \in X \leftrightarrow u \in Y),$$

y claramente $\tilde{\bar{\alpha}}$ equivale a α por el axioma de extensionalidad.

Si $\alpha \equiv X \in Y$, entonces

$$\bar{\alpha} \equiv \bigvee u(u \in Y \land \bigwedge v(X(v) \leftrightarrow v \in u)), \quad \bar{\tilde{\alpha}} \equiv \bigvee u(u \in Y \land \bigwedge v(v \in X \leftrightarrow v \in u)),$$

y, de nuevo por el axioma de extensionalidad, $\bar{\tilde{\alpha}}$ equivale a $\bigvee u \in Y\, u = X$, que a su vez equivale a $X \in Y$, es decir, a α.

Esto cubre todos los casos en que α es atómica, y los casos restantes se siguen de la hipótesis de inducción por razonamientos lógicos elementales. ■

Por otra parte:

Teorema 9.26 *Si α es una fórmula del lenguaje de segundo orden de* NB* *sin variables libres de primer orden, entonces α es un teorema de* NB* *si y sólo si $\tilde{\alpha}$ es un teorema de* NBG*.

DEMOSTRACIÓN: Una implicación es el teorema 9.24. Si $\tilde{\alpha}$ es un teorema de NBG*, el teorema anterior nos da que $\bar{\tilde{\alpha}}$ es un teorema de NB*, luego basta probar que esta fórmula es equivalente a α en NB*.

Más en general, supongamos que la fórmula α tiene variables libres de primer orden $x_1, \ldots, x_n$, que al calcular $\tilde{\alpha}$ se corresponden con las variables $X_1, \ldots, X_n$ de $\mathcal{L}_{\mathrm{tc}}$, las cuales se corresponden a su vez con variables de segundo orden $X_1, \ldots, X_n$ al calcular $\bar{\tilde{\alpha}}$. Podemos definir las correspondencias entre variables de modo que $X_1, \ldots, X_n$ no aparezcan en α.

Si x es una variable de primer orden y X otra de segundo orden, definimos

$$I(x, X) \equiv \bigwedge u(X(u) \leftrightarrow u \in x).$$

Vamos a probar que, en NB*,

$$I(x_1, X_1), \ldots, I(x_n, X_n) \Rightarrow \alpha \leftrightarrow \bar{\tilde{\alpha}}.$$

En particular, si α no tiene variables libres de primer orden, tenemos la equivalencia requerida.

Razonamos por inducción sobre α.

Si $\alpha \equiv x_1 = x_2$, entonces $\tilde{\alpha} \equiv X_1 = X_2$ y $\bar{\tilde{\alpha}} \equiv \bigwedge u(X_1(u) \leftrightarrow X_2(u))$. Es pura rutina demostrar el secuente siguiente (que es, de hecho, un teorema del cálculo proposicional):

$$X_1(y) \leftrightarrow y \in x_1,\ X_2(y) \leftrightarrow y \in x_2,\ X_1(y) \leftrightarrow X_2(y) \Rightarrow y \in x_1 \leftrightarrow y \in x_2.$$

Aplicando las reglas del generalizador obtenemos

$$I(x_1, X_1),\ I(x_2, X_2),\ \bigwedge u(X_1(u) \leftrightarrow X_2(u)) \Rightarrow \bigwedge u(u \in x_1 \leftrightarrow u \in x_2).$$

Aplicando la regla izquierda del implicador a este secuente y a

$$x_1 = x_2 \Rightarrow x_1 = x_2$$

obtenemos

$$I(x_1, X_1),\ I(x_2, X_2),\ \bigwedge u(X_1(u) \leftrightarrow X_2(u)),\ \bigwedge u(u \in x_1 \leftrightarrow u \in x_2) \rightarrow x_1 = x_2$$
$$\Rightarrow x_1 = x_2.$$

Con la regla izquierda del generalizador convertimos la última fórmula del consecuente en el axioma de extensionalidad, que a su vez podemos cortarlo y así llegamos a

$$I(x_1, X_1),\ I(x_2, X_2),\ \bigwedge u(X_1(u) \leftrightarrow X_2(u)) \Rightarrow x_1 = x_2,$$

de donde a su vez resulta

$$I(x_1, X_1),\ I(x_2, X_2) \Rightarrow \bigwedge u(X_1(u) \leftrightarrow X_2(u)) \rightarrow x_1 = x_2,$$

Similarmente, podemos probar

$$X_1(y) \leftrightarrow y \in x_1,\ X_2(y) \leftrightarrow y \in x_2,\ y \in x_1 \leftrightarrow y \in x_2 \Rightarrow X_1(y) \leftrightarrow X_2(y)$$

De los axiomas del igualador se sigue que

$$x_1 = x_2 \Rightarrow y \in x_1 \leftrightarrow y \in x_2$$

y cortando ambos secuentes llegamos a

$$X_1(y) \leftrightarrow y \in x_1,\ X_2(y) \leftrightarrow y \in x_2,\ x_1 = x_2 \Rightarrow X_1(y) \leftrightarrow X_2(y)$$

Las reglas del generalizador nos llevan a

$$I(x_1, X_1),\ I(x_2, X_2),\ x_1 = x_2 \Rightarrow \bigwedge u(X_1(u) \leftrightarrow X_2(u)),$$

de donde

$$I(x_1, X_1),\ I(x_2, X_2) \Rightarrow x_1 = x_2 \rightarrow \bigwedge u(X_1(u) \leftrightarrow X_2(u)),$$

y combinando las dos implicaciones que hemos probado con la regla derecha del conjuntor queda

$$I(x_1, X_1),\ I(x_2, X_2) \Rightarrow x_1 = x_2 \leftrightarrow \bigwedge u(X_1(u) \leftrightarrow X_2(u)),$$

donde el consecuente es $\alpha \leftrightarrow \bar{\tilde{\alpha}}$.

Si $\alpha \equiv x_1 \in x_2$, entonces

$$\tilde{\alpha} \equiv X_1 \in X_2, \qquad \bar{\tilde{\alpha}} \equiv \bigvee v(X_2(v) \wedge \bigwedge u(X_1(u) \leftrightarrow u \in v)).$$

No detallamos la formalización de la equivalencia, que es similar a la anterior, pero la idea es que $I(x_1, X_1)$ hace que la parte final de $\bar{\tilde{\alpha}}$ equivalga a $v = x_1$, luego $\bar{\tilde{\alpha}}$ equivale a $X_2(x_1)$ y por $I(x_2, X_2)$ esto equivale a $x_1 \in x_2$.

Los casos $\alpha \equiv \neg\beta$, $\alpha \equiv \beta \vee \gamma$, $\alpha \equiv \bigwedge U\beta(U)$ y $\alpha \equiv \bigvee U\beta(U)$ se siguen fácilmente de la hipótesis de inducción.

Supongamos ahora que $\alpha \equiv \bigwedge u\, \beta(u)$. Entonces

$$\tilde{\alpha} \equiv \bigwedge U(\mathrm{cto}\, U \rightarrow \tilde{\beta}(U)), \qquad \bar{\tilde{\alpha}} \equiv \bigwedge U(\mathrm{cto}\, U \rightarrow \bar{\tilde{\beta}}(U)).$$

Si llamamos $\Gamma \equiv \{I(x_1, X_1), \ldots, I(x_n, X_n)\}$, la hipótesis de inducción es que

$$\Gamma,\, I(x_{n+1}, X_{n+1}) \Rightarrow \beta(x_{n+1}) \leftrightarrow \bar{\tilde{\beta}}(X_{n+1}).$$

Partiendo de aquí y del teorema 9.23 podemos razonar como sigue:

$$\dfrac{\dfrac{\dfrac{I(x_{n+1}, X_{n+1}) \Rightarrow \mathrm{cto}\, X_{n+1}}{I(x_{n+1}, X_{n+1}) \Rightarrow \mathrm{cto}\, X_{n+1},\, \beta(x_{n+1})} \quad \Gamma,\, I(x_{n+1}, X_{n+1}),\, \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \beta(x_{n+1})}{\Gamma,\, I(x_{n+1}, X_{n+1}),\, \mathrm{cto}\, X_{n+1} \rightarrow \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \beta(x_{n+1})}}{\Gamma,\, I(x_{n+1}, X_{n+1}),\, \bigwedge U(\mathrm{cto}\, U \rightarrow \bar{\tilde{\beta}}(U)) \Rightarrow \beta(x_{n+1})}$$

Recordemos que

$$I(x_{n+1}, X_{n+1}) \equiv \bigwedge u(X_{n+1}(u) \leftrightarrow u \in x_{n+1}).$$

Como la variable X_{n+1} no aparece en ninguna otra parte del último secuente al que hemos llegado, podemos aplicar la regla izquierda del particularizador de segundo orden y luego la del generalizador de primer orden para convertirla en

$$\bigwedge v \bigvee U \bigwedge u(U(u) \leftrightarrow u \in v),$$

que es un axioma de comprensión, luego podemos eliminarlo con un corte. A su vez, al haber eliminado la variable x_{n+1} del antecedente, podemos aplicar la regla derecha del generalizador, con lo que obtenemos

$$\Gamma,\, \bigwedge U(\mathrm{cto}\, U \rightarrow \bar{\tilde{\beta}}(U)) \Rightarrow \bigwedge u\, \beta(u),$$

y a su vez

$$\Gamma \Rightarrow \bigwedge U(\mathrm{cto}\, U \rightarrow \bar{\tilde{\beta}}(U)) \rightarrow \bigwedge u\, \beta(u).$$

Por otra parte, de la hipótesis de inducción se sigue fácilmente el secuente inicial del razonamiento siguiente:

$$\dfrac{\dfrac{\Gamma,\, I(x_{n+1}, X_{n+1}),\, \beta(x_{n+1}) \Rightarrow \bar{\tilde{\beta}}(X_{n+1})}{\Gamma,\, I(x_{n+1}, X_{n+1}),\, \bigwedge u\, \beta(u) \Rightarrow \bar{\tilde{\beta}}(X_{n+1})}}{\Gamma,\, \bigvee v \bigwedge u(X_{n+1}(u) \leftrightarrow u \in v),\, \bigwedge u\, \beta(u) \Rightarrow \bar{\tilde{\beta}}(X_{n+1})}$$

Por otro lado, el teorema 9.23) nos da el secuente:

$$\mathrm{cto}\, X_{n+1} \Rightarrow \bigvee v \bigwedge u(X_{n+1}(u) \leftrightarrow u \in v)$$

y la regla de corte nos permite concluir

$$\begin{array}{c}
\Gamma,\ \bigwedge u\,\beta(u),\ \mathrm{cto}\,X_{n+1} \Rightarrow \bar{\tilde{\beta}}(X_{n+1}) \\ \hline
\Gamma,\ \bigwedge u\,\beta(u) \Rightarrow \mathrm{cto}\,X_{n+1} \rightarrow \bar{\tilde{\beta}}(X_{n+1}) \\ \hline
\Gamma,\ \bigwedge u\,\beta(u) \Rightarrow \bigwedge U(\mathrm{cto}\,U \rightarrow \bar{\tilde{\beta}}(U)) \\ \hline
\Gamma \Rightarrow \bigwedge u\,\beta(u) \rightarrow \bigwedge U(\mathrm{cto}\,U \rightarrow \bar{\tilde{\beta}}(U))
\end{array}$$

Combinando las dos implicaciones con la regla del conjuntor concluimos:

$$\Gamma \Rightarrow \bigwedge u\,\beta(u) \leftrightarrow \bigwedge U(\mathrm{cto}\,U \rightarrow \bar{\tilde{\beta}}(U)).$$

El caso en que $\alpha \equiv \bigvee u\,\beta(u)$ es similar. La hipótesis de inducción es la misma, de la que se deduce el secuente inicial del razonamiento siguiente

$$\begin{array}{c}
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \beta(x_{n+1}) \\ \hline
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \bigvee u\,\beta(u) \\ \hline
\Gamma,\ \bigvee v \bigwedge u(X_{n+1}(u) \leftrightarrow u \in v),\ \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \bigvee u\,\beta(u)
\end{array}$$

El teorema 9.23 y la regla de corte nos permiten pasar a:

$$\begin{array}{c}
\Gamma,\ \mathrm{cto}\,X_{n+1},\ \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \bigvee u\,\beta(u) \\ \hline
\Gamma,\ \mathrm{cto}\,X_{n+1} \wedge \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \bigvee u\,\beta(u) \\ \hline
\Gamma,\ \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U)) \Rightarrow \bigvee u\,\beta(u) \\ \hline
\Gamma \Rightarrow \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U)) \rightarrow \bigvee u\,\beta(u)
\end{array}$$

Para la implicación opuesta partimos de

$$\Gamma,\ I(x_{n+1}, X_{n+1}),\ \beta(x_{n+1}) \Rightarrow \bar{\tilde{\beta}}(X_{n+1}),$$

que, junto con $I(x_{n+1}, X_{n+1}) \Rightarrow \mathrm{cto}\,X_{n+1}$, nos da

$$\begin{array}{c}
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \beta(x_{n+1}) \Rightarrow \mathrm{cto}\,X_{n+1} \wedge \bar{\tilde{\beta}}(X_{n+1}) \\ \hline
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \beta(x_{n+1}) \Rightarrow \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U)) \\ \hline
\Gamma,\ \bigvee U \bigwedge u(U(u) \leftrightarrow u \in x_{n+1}),\ \beta(x_{n+1}) \Rightarrow \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U)) \\ \hline
\Gamma,\ \bigwedge v \bigvee U \bigwedge u(U(u) \leftrightarrow u \in v),\ \beta(x_{n+1}) \Rightarrow \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U))
\end{array}$$

La segunda fórmula del antecedente es un axioma de compresión, luego podemos cortarlo y pasar a:

$$\begin{array}{c}
\Gamma,\ \beta(x_{n+1}) \Rightarrow \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U)) \\ \hline
\Gamma,\ \bigvee u\,\beta(u) \Rightarrow \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U)) \\ \hline
\Gamma \Rightarrow \bigvee u\,\beta(u) \rightarrow \bigvee U(\mathrm{cto}\,U \wedge \bar{\tilde{\beta}}(U))
\end{array}$$

Combinando las dos implicaciones con la regla del conjuntor obtenemos la coimplicación. ■

En particular:

Teorema 9.27 *Una sentencia α de $\mathcal{L}_{\mathrm{tc}}$ es un teorema de* ZF* *si y sólo si $\tilde{\alpha}$ es un teorema de* NBG*.

Demostración: Por 9.22 sabemos que α es un teorema de ZF* si y sólo si lo es de NB* y como no tiene variables libres, por el teorema anterior esto sucede si y sólo si $\tilde{\alpha}$ es un teorema de NBG*. ■

Nota Por el mismo argumento empleado en la nota tras el teorema 9.22, el teorema anterior vale para cualquier extensión de ZF*. Por ejemplo, NBG es la teoría que resulta de añadir a NBG* los axiomas de infinitud, partes, regularidad y elección, y ahora podemos asegurar que una sentencia α de $\mathcal{L}_{\mathrm{tc}}$ es un teorema de ZFC si y sólo si $\tilde{\alpha}$ es un teorema de NBG. ■

En [LM 10.19] vimos una demostración alternativa de este mismo resultado. La prueba que hemos visto aquí tiene la ventaja de ser constructiva, pues de ella se puede obtener un algoritmo para obtener una demostración en ZF* a partir de una demostración en NBG*. Sin embargo, la prueba de [LM 10.19] es más conceptual, pues se basa en que todo modelo de ZF* se puede extender a un modelo de NBG*.

La teoría de Morse-Kelley Si en NB* extendemos el axioma de comprensión a fórmulas cualesquiera, no necesariamente primitivas, obtenemos una extensión de la extensión plena de ZF* de segundo orden (es una extensión porque hemos sustituido los esquemas axiomáticos de primer orden del igualador y de reemplazo por axiomas de segundo orden), y los teoremas 9.24 y 9.25 valen con la misma prueba para esta extensión si sustituimos también NBG* por la teoría (restringida) de Morse-Kelley MK* que resulta de extender igualmente el axioma de comprensión a fórmulas arbitrarias. A su vez, el teorema 9.26 vale exactamente con la misma prueba para dichas extensiones. En otras palabras, extender el axioma de comprensión en NB* (o NB) a fórmulas arbitrarias es equivalente a hacerlo en NBG* (o NBG). Ahora bien, según [LM 10.23] sucede que MK* no es una extensión conservativa de ZF* (y, según el apartado siguiente a [LM 10.23], tampoco lo es MK de NBG). ■

Bibliografía

[1] Beckmann, A. y Buss, S.R. *Corrected upper bounds for free-cut elimination* Theor. Comput. Sci.(2011) 5433–5445

[2] Buss, S.R. (editor) *Handbook of Proof Theory,* Elsevier, Amsterdam, 1998.

[3] Goodstein, R.L. *Logic-Free Formalisations of Recursive Arithmetic,* Math. Scand. 2 (1954) 247–261.

[4] Takeuti, G. *Proof Theory,* North Holland (1987)

[5] Troelstra, A.S. *Basic Proof Theory,* Cambridge University Press (1996)

Índice de Materias