Carlos Ivorra Castillo

EL CÁLCULO SECUENCIAL DE GENTZEN

El hecho de que todas las matemáticas son lógica simbólica es uno de los mayores descubrimientos de nuestra era; y, una vez establecido este hecho, el resto de los principios de las matemáticas consiste en el análisis de la propia lógica simbólica.

Bertrand Russell

Índice General

Introducción

En nuestro libro de *Lógica Matemática* [LM], o en *La lógica del finitismo* [LF], 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 razonamiento formal presentado en el capítulo II de [LM]:

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

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

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 $K_{\mathcal{L}}$ 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 $K_{\mathcal{L}}$ (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 $K_{\mathcal{L}}$ se esforzara por detallar hasta el más mínimo detalle un argumento, llegaría sin saberlo a una demostración en $K_{\mathcal{L}}$.

Aquí vamos a estudiar un cálculo deductivo que, en principio cumple exactamente la misma función que $K_{\mathcal{L}}$, es decir, la de formalizar el concepto matemático de deducción lógica y que, por lo tanto, es equivalente a $K_{\mathcal{L}}$, 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 22. 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.

Más concretamente, aquí probaremos varios resultados que en [LF] no es posible demostrar con las técnicas expuestas allí, 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.

El capítulo I de este libro requiere conocer al menos el capítulo III de [LF] y, a partir de ahí conviene leer este libro a medida que va siendo necesario en [LF]. Así, a partir de la sección 1.4 se necesita el capítulo IV de [LF], a partir de la subsección 1.5.3 se necesita el capítulo VI de [LF], el capítulo II requiere el capítulo VII de [LF] y a partir del capítulo III conviene haber completado ya la lectura de [LF].

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

Finalmente, en el apéndice A estudiamos la teoría de conjuntos NBG (von Neumann-Bernays-Gödel) que no estudiamos en [LF], sino en el capítulo X de [LM]. Concretamente, aquí daremos una prueba constructiva de [LM 10.2].

Capítulo I

El cálculo secuencial

En el capítulo III de [LF] hemos definido lo que es un lenguaje formal de primer orden y, para cada uno de estos lenguajes $\mathcal{L}$, hemos presentado un sistema deductivo formal al que hemos llamado $K_{\mathcal{L}}$, es decir, una forma de extraer conclusiones de unas premisas expresadas como fórmulas de $\mathcal{L}$, con la garantía de que si las premisas son verdaderas con respecto a cierta interpretación de los signos de $\mathcal{L}$ (técnicamente, en un modelo M de $\mathcal{L}$), la conclusión es necesariamente verdadera, pero de tal modo que la deducción es puramente formal, en el sentido de que el hecho de que una sucesión de fórmulas de $\mathcal{L}$ constituya una deducción lógica puede determinarse sin hacer referencia en ningún momento al posible significado de las fórmulas consideradas.

El sistema deductivo formal $K_{\mathcal{L}}$ es lo que se conoce como un cálculo deductivo "a la Hilbert", lo que significa que las deducciones en $K_{\mathcal{L}}$ son sucesiones de fórmulas de $\mathcal{L}$ de forma que cada una de ellas es un axioma de una lista prefijada o bien se deduce de fórmulas anteriores en virtud de unas reglas de inferencia prefijadas. Esta concepción puramente formal del razonamiento matemático fue introducida por Hilbert en 1899 en sus *Fundamentos de la geometría,* y posteriormente aplicada a la teoría de conjuntos y a la matemática en general. Fue en 1917 cuando Hilbert introdujo lo que hoy en día se conoce como "lógica de primer orden".

Aquí vamos a estudiar un cálculo deductivo "a la Gentzen", pues fue introducido por Gerhard Gentzen en 1934, y es equivalente a $K_{\mathcal{L}}$ en el sentido de que permite deducir las mismas consecuencias lógicas de las mismas fórmulas, pero que resulta ser muy superior a la hora de obtener resultados teóricos, que además resultan ser totalmente constructivos.

Todo el contenido de este capítulo puede formalizarse —y puede considerarse formalizado— en la aritmética recursiva primitiva descrita en el capítulo I de [LF]. Para ello vamos a necesitar el concepto de árbol, cuya formalización no ofrece ninguna dificultad, pero que vamos a discutir aquí brevemente:

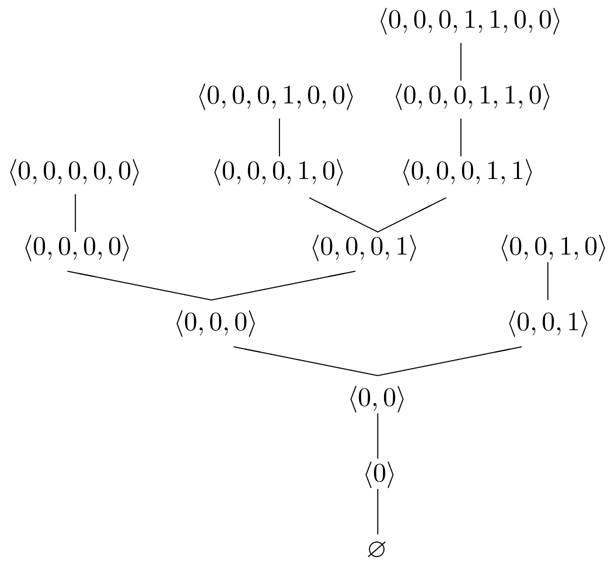
Definición 1.1 Un *árbol de nodos* es un conjunto (finito) no vacío A tal que

$$\bigwedge s \in A \bigwedge i < \ell(s)\, s|_i \in A.$$

Un ejemplo de árbol de nodos es:

$$A = \{0, \langle 0\rangle, \langle 0,0\rangle, \langle 0,0,0\rangle, \langle 0,0,1\rangle, \langle 0,0,0,0\rangle, \langle 0,0,1,0\rangle, \langle 0,0,0,1\rangle,$$
$$\langle 0,0,0,0,0\rangle, \langle 0,0,0,1,0\rangle, \langle 0,0,0,1,1\rangle, \langle 0,0,0,1,0,0\rangle, \langle 0,0,0,1,1,0\rangle$$
$$\langle 0,0,0,1,1,0,0\rangle\}.$$

Esto se comprueba mejor si lo representamos como muestra la figura siguiente, en la que hemos puesto cada nodo sobre sus restricciones:



Es claro que todo árbol está parcialmente ordenado por la relación $s \sqsubseteq t$ que se cumple cuando t extiende a s. La *altura* de un nodo es su longitud. Todo árbol contiene necesariamente la sucesión nula 0, que es el único nodo de altura 0, y se llama *raíz* o *nodo final* del árbol. Un nodo t es un *sucesor* de otro nodo s si $s \subseteq t \wedge \ell(t) = \ell(s) + 1$. Los nodos sin sucesores se llaman *iniciales.*

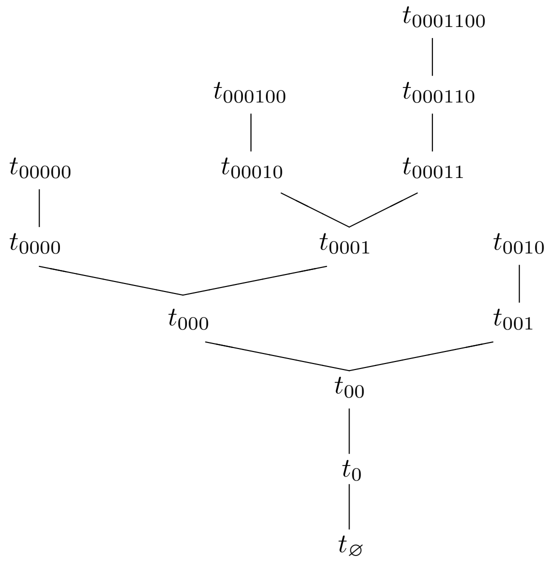
Un árbol de nodos es *binario* si cada nodo tiene a lo sumo dos sucesores. Esto sucede en particular si exigimos que el árbol cumpla

$$\bigwedge s \in A \bigwedge i < \ell(s)\, s_i \in \{0, 1\}.$$

En tal caso diremos que el árbol de nodos es *propiamente binario.*

Más en general, un *árbol* es una aplicación $t : A \longrightarrow B$ cuyo dominio A sea un árbol de nodos.

Por ejemplo, la página siguiente muestra un árbol cuyo dominio es el árbol de nodos del ejemplo precedente. Los conjuntos t_s pueden ser cualesquiera. Lo que importa es que los tenemos ordenados en forma de árbol.



Es fácil definir operaciones para construir nuevos árboles a partir de otros dados. Por ejemplo, si s es un nodo inicial del dominio de un árbol $t : A \longrightarrow B$ y $t' : A' \longrightarrow B'$ es otro árbol tal que $t'_\varnothing = t_s$, podemos prolongar el árbol t hasta el árbol de nodos

$$A \cup \{s^\frown s' \mid s' \in A'\}$$

mediante $t_{s^\frown s'} = t'_{s'}$, lo que supone "injertar" el árbol t' sobre el nodo s del árbol t.

1.1 El cálculo secuencial de primer orden

En esta sección consideraremos lenguajes sin igualador (luego, sin descriptor), y pospondremos hasta la sección siguiente el tratamiento secuencial del igualador. En principio vamos a considerar lenguajes formales en el sentido de la definición [LF 3.2] (sin igualador ni descriptor) con los cinco conectores lógicos $\neg, \vee, \wedge, \rightarrow, \leftrightarrow$ y los dos cuantificadores $\bigwedge, \bigvee$, pero veremos que no perdemos generalidad si consideramos que los únicos conectores primitivos son $\neg, \vee$, igual que en la sección [LF 3.2] vimos que en el caso de $K_\mathcal{L}$ sucede lo mismo.

La primera diferencia entre el cálculo secuencial y un cálculo "a la Hilbert" es que en él las deducciones no son sucesiones de fórmulas, sino árboles de secuentes, en el sentido que introducimos a continuación:

Definición 1.2 Si $\mathcal{L}$ es un lenguaje formal de primer orden, un *secuente* en $\mathcal{L}$ es un par ordenado de conjuntos finitos Γ y Δ de fórmulas de $\mathcal{L}$, y lo expresaremos[1] en la forma $\Gamma \Rightarrow \Delta$. El conjunto Γ recibe el nombre de *antecedente,* del secuente mientras que Δ es el *consecuente.*

[1]Si usamos la notación formal de ARP, estamos diciendo que $\Gamma \Rightarrow \Delta \equiv \langle \Gamma, \Delta \rangle$.

Si Γ está formado por las fórmulas $\gamma_1, \ldots, \gamma_m$ y Δ está formado por las fórmulas $\delta_1, \ldots, \delta_n$, en lugar de $\Gamma \Rightarrow \Delta$ escribiremos también

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

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, así como 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. Al último lo llamaremos *secuente vacío.*

En general, 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

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

Ahora bien, ¿qué significa un secuente? La idea básica es que un secuente $S \equiv \gamma_1, \ldots, \gamma_m \Rightarrow \delta_1, \ldots, \delta_n$ no vacío pretende significar lo mismo que la fórmula

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

Decimos "pretende significar" porque, en principio, las fórmulas de un lenguaje formal no tienen ningún significado asociado, pero, supuesto que tengan alguno, el significado pretendido de un secuente no vacío S es el mismo que el de la fórmula $\bar{S}$.

Nota Para precisar esta idea tenemos que considerar modelos del lenguaje $\mathcal{L}$, en el sentido de la definición [LF 3.3] y, como hemos hecho a partir de ese punto de [LF], usaremos este tipo de letra cuando hagamos afirmaciones no formalizables en ARP. Como en [LF], anticipamos el concepto de modelo únicamente para mostrar que la construcción del cálculo secuencial no es arbitraria, sino que da lugar a un cálculo deductivo correcto en el sentido de que extrae consecuencias verdaderas de premisas verdaderas, pero todo cuanto digamos sobre modelos puede omitirse y posponerse hasta el momento en que dispongamos de la teoría axiomática adecuada para formalizar el concepto. ■

Diremos que un modelo M de $\mathcal{L}$ *satisface* un secuente no vacío 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

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

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 1.3 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[2] 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.

Así pues, a diferencia de lo que sucede con las teorías axiomáticas consideradas en [LF], las deducciones en un cálculo secuencial no son sucesiones finitas, sino árboles (y no de fórmulas, sino de secuentes).

A continuación vamos a definir un cálculo secuencial alternativo a $K_{\mathcal{L}}$ (para lenguajes sin igualador).

El cálculo secuencial LK Dado un lenguaje formal $\mathcal{L}$ (sin descriptor), llamaremos $\mathrm{LK}_{\mathcal{L}}$, o simplemente[3] 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 recogidas en la tabla de la página siguiente.

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.

[2]Para formalizar este concepto en ARP es necesario entender que la fórmula $\mathfrak{S} \overset{d}{\underset{\mathrm{K}}{\vdash}} S$ incluye una variable d que hace referencia a la deducción que la justifica, pero normalmente no la mostraremos explícitamente (compárese con [LF 3.13]).

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

Reglas de inferencia de LK

Debilitación izquierda $\dfrac{\Gamma \Rightarrow \Delta}{\alpha, \Gamma \Rightarrow \Delta}$, **Debilitación derecha** $\dfrac{\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \alpha}$,

Corte $\dfrac{\Gamma \Rightarrow \Delta, \alpha \qquad \alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta}$,

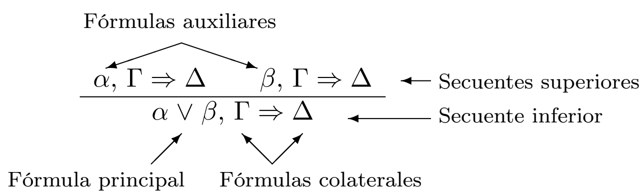
$\neg$	$\dfrac{\Gamma \Rightarrow \Delta, \alpha}{\neg\alpha, \Gamma \Rightarrow \Delta}$,	$\dfrac{\alpha, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\alpha}$,
$\lor$	$\dfrac{\alpha,\, \Gamma \Rightarrow \Delta \qquad \beta,\, \Gamma \Rightarrow \Delta}{\alpha \lor \beta,\, \Gamma \Rightarrow \Delta}$,	$\dfrac{\Gamma \Rightarrow \Delta,\, \alpha,\, \beta}{\Gamma \Rightarrow \Delta,\, \alpha \lor \beta}$,
$\land$	$\dfrac{\alpha,\, \beta,\, \Gamma \Rightarrow \Delta}{\alpha \land \beta,\ \Gamma \Rightarrow \Delta}$,	$\dfrac{\Gamma \Rightarrow \Delta,\, \alpha \quad \Gamma \Rightarrow \Delta,\, \beta}{\Gamma \Rightarrow \Delta, \alpha \land \beta}$,
$\rightarrow$	$\dfrac{\Gamma \Rightarrow \Delta, \alpha \qquad \beta, \Gamma \Rightarrow \Delta}{\alpha \rightarrow \beta,\ \Gamma \Rightarrow \Delta}$,	$\dfrac{\alpha, \Gamma \Rightarrow \Delta, \beta}{\Gamma \Rightarrow \Delta, \alpha \rightarrow \beta}$,
$\leftrightarrow$	$\dfrac{\alpha,\, \beta,\, \Gamma \Rightarrow \Delta \qquad \Gamma \Rightarrow \Delta,\, \alpha,\, \beta}{\alpha \leftrightarrow \beta,\ \Gamma \Rightarrow \Delta}$,	$\dfrac{\alpha, \Gamma \Rightarrow \Delta, \beta \qquad \beta, \Gamma \Rightarrow \Delta, \alpha}{\Gamma \Rightarrow \Delta, \alpha \leftrightarrow \beta}$,
$\bigwedge$	$\dfrac{\alpha(t),\, \Gamma \Rightarrow \Delta}{\bigwedge u\, \alpha(u),\, \Gamma \Rightarrow \Delta}$,	$\dfrac{\Gamma \Rightarrow \Delta, \alpha(y)}{\Gamma \Rightarrow \Delta, \bigwedge u\, \alpha(u)}$,
$\bigvee$	$\dfrac{\alpha(y),\, \Gamma \Rightarrow \Delta}{\bigvee u\, \alpha(u),\, \Gamma \Rightarrow \Delta}$,	$\dfrac{\Gamma \Rightarrow \Delta,\, \alpha(t)}{\Gamma \Rightarrow \Delta,\, \bigvee u\, \alpha(u)}$,

con la condición de que, en la regla derecha del generalizador y en la izquierda del particularizador, la variable y no aparezca[4] fuera de la fórmula auxiliar (y se dice entonces que y es la *variable propia* de la regla).

---

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.*



---

[4]Hay que entender que $\alpha(u) \equiv \mathtt{S}_y^u \alpha$, donde u es una variable que puede sustituir a y en α, lo que implica que y no está en $\alpha(u)$.

Notemos que, puesto que las reglas de inferencia de LK tienen siempre uno o dos secuentes superiores (y así sucederá también con todos los cálculos secuenciales que vamos a considerar), en la definición de deducción no perdemos generalidad si suponemos que los árboles de nodos son estrictamente binarios.

Si quisiéramos mantenernos en el plano puramente formal tendríamos que considerar que los axiomas y las reglas de inferencia de LK son arbitrarios, pero, si atendemos al posible significado de las fórmulas, la situación es muy distinta:

Teorema 1.4 (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: Fijemos una deducción d de S a partir de $\mathfrak{S}$ en LK. De acuerdo con las definiciones que hemos dado, cualquier axioma $\alpha \Rightarrow \alpha$ es verdadero en M si y sólo si lo es la fórmula $\neg\alpha \lor \alpha$, lo cual es obviamente cierto. Por hipótesis, las premisas de la deducción también son verdaderas en M. Es claro entonces que basta comprobar que si los secuentes superiores de una regla de inferencia de LK son verdaderos en M, el secuente inferior también lo es.

Fijamos una valoración v en M y distinguimos dos casos:

1) Si Γ y Δ no son ambos vacíos y

$$M \vDash \gamma_1 \lor \cdots \lor \neg\gamma_m \lor \delta_1 \lor \cdots \lor \delta_n[v],$$

entonces el secuente inferior de cualquiera de las reglas también es satisfecho.

2) Supongamos en segundo lugar que Γ y Δ son ambos vacíos o bien que no lo son y que no se cumple

$$M \vDash \gamma_1 \lor \cdots \lor \neg\gamma_m \lor \delta_1 \lor \cdots \lor \delta_n[v]$$

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 nos dan que $M \vDash \alpha[v]$ y que $M \vDash \neg\alpha[v]$, luego este caso tampoco puede darse.

La regla izquierda del negador afirma que si $M \vDash \alpha[v]$, entonces $M \vDash \neg\neg\alpha[v]$, mientras que la regla derecha afirma que si $M \vDash \neg\alpha[v]$ entonces $M \vDash \neg\alpha[v]$.

La regla izquierda del disyuntor afirma que si $M \vdash \neg\alpha[v]$ y $M \vDash \neg\beta[v]$, entonces $M \vDash \neg(\alpha \lor \beta)[v]$, mientras que la regla derecha afirma que si $M \vDash \alpha[v]$ o $M \vDash \beta[v]$, entonces $M \vDash \alpha \lor \beta[v]$.

La regla izquierda del conjuntor afirma que si $M \vDash \neg\alpha[v]$ o $M \vDash \neg\beta[v]$, entonces $M \vDash \neg(\alpha \land \beta)[v]$, mientras que la regla derecha afirma que si $M \vDash \alpha[v]$ y $M \vDash \beta[v]$, entonces $M \vDash \alpha \land \beta[v]$.

La regla izquierda del implicador afirma que si $M \vDash \alpha[v]$ y $M \vDash \neg\beta[v]$, entonces $M \vDash (\alpha \to \beta)[v]$, mientras que la regla derecha afirma que si $M \vDash \neg\alpha[v]$ o $M \vDash \beta[v]$, entonces $M \vDash (\alpha \to \beta)[v]$.

La regla izquierda del coimplicador afirma que si una de las fórmulas α o β no es satisfecha y otra sí, entonces $\alpha \leftrightarrow \beta$ no es satisfecha, mientras que la regla derecha afirma que si ambas son satisfecha o ninguna lo es, entonces $\alpha \leftrightarrow \beta$ es satisfecha.

Si el secuente superior de la regla izquierda del generalizador es satisfecho en M, tenemos que

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

Por el teorema [LF 3.12], esto 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 $M \vDash \bigwedge u\, \alpha(u)[v]$, o a que se cumpla $M \vDash \neg\bigwedge u\, \alpha(u)[v]$, y esto hace que el secuente inferior sea satisfecho en M.

Si el secuente superior de la regla derecha es verdadero en M, tenemos que, para todo a en M, se cumple

$$M \vDash (\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n \vee \alpha(y))[v_y^a],$$

y esto equivale a que

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

o bien $M \vDash \alpha(y))[v_y^a]$. Como la variable propia y no aparece en ninguna de las fórmulas γ_i o δ_j, por el teorema [LF 3.9], la primera posibilidad equivale a

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

que estamos suponiendo que no se cumple, luego tenemos $M \vDash \alpha(y))[v_y^a]$, y esto vale para todo a en M, luego se cumple $M \vDash \bigwedge u\, \alpha(u)[v]$, y esto hace que el secuente inferior sea verdadero en M.

En el caso del particularizador, si el secuente superior de la regla izquierda es verdadero en M, tenemos que, para todo a en M, se cumple

$$M \vDash (\neg\alpha(y) \vee \neg\gamma_1 \vee \cdots \vee \neg\gamma_m \vee \delta_1 \vee \cdots \vee \delta_n)[v_y^a],$$

y esto equivale a que $M \vDash \neg\alpha(y)[v_y^a]$, o bien

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

pero, como en el caso precedente, la segunda opción contradice el caso 2) que estamos suponiendo. Por lo tanto, $M \vDash \neg\alpha(y)[v_y^a]$, es decir, que ningún a en M cumple $M \vDash \alpha(y)[v_y^a]$. Esto significa que no se cumple $M \vDash \bigvee u\, \alpha(u)[v]$, luego $M \vDash \neg\bigvee u\, \alpha(u)[v]$, y esto hace que el secuente inferior de la regla sea verdadero en M.

Si el secuente superior de la regla derecha es verdadero en M, tenemos que $M \vDash \alpha(t)[v]$, que por [LF 3.12] equivale a $M \vDash \alpha(u)[v_u^{M(t)[v]}]$. A su vez, esto implica que $M \vDash \bigvee u\, \alpha(u)[v]$, luego el secuente inferior es verdadero en M. ■

Más precisamente, la prueba del teorema anterior permite transformar cualquier deducción en LK en un argumento informal que justifica que si las premisas de $\mathfrak{S}$ son verdaderas en un modelo entonces S también tiene que serlo.

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 en Δ.

Por ejemplo, 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 en el que el relator $=$ se interprete como la igualdad, pero al aplicar la "regla" resulta

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

que no es verdadero en modelos en los que el relator $=$ se interprete como la igualdad y haya más de un objeto en su universo, y 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 1.5 *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[5] 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:

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

[5]Para formalizar el argumento en ARP observamos que la prueba permite construir un funtor F que a cada fórmula que incumpla el teorema le asigna otra de longitud menor. Si existiera una fórmula α_0 que no cumpliera el teorema, podríamos definir $G(\alpha, 0) = \alpha$, $G(\alpha, n+1) = F(G(\alpha, n))$, y entonces $F(\alpha_0, \ell(\alpha_0) + 1)$ sería una fórmula de longitud < 0.

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 $\alpha \equiv \beta \land \gamma$, el razonamiento es similar, usando ahora:

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

Si $\alpha \equiv \beta \rightarrow \gamma$, usamos

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

Para $\alpha \equiv \beta \leftrightarrow \gamma$ usamos[6]

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

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:

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

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

$$\dfrac{\dfrac{\beta(y) \Rightarrow \beta(y)}{\beta(y) \Rightarrow \bigvee u\, \beta(u)}}{\bigvee u\, \beta(u) \Rightarrow \bigvee u\, \beta(u)}$$

■

Conviene observar que la demostración de teorema anterior muestra que un secuente $\alpha \Rightarrow \alpha$ siempre puede demostrarse sin usar la regla de corte. Esta regla es necesaria cuando se necesita eliminar algún signo lógico presente en las premisas que no tiene que estar en la conclusión. En efecto, las reglas lógicas

[6] Notemos que en todos los casos las deducciones que estamos presentando se encuentran fácilmente razonando de abajo hacia arriba. En este caso, para que en el antecedente del secuente final aparezca $\beta \leftrightarrow \gamma$ aplicamos la regla izquierda del bicondicionador, y en cada uno de sus secuentes superiores aplicamos la regla derecha, con lo que llegamos a secuentes que se deducen inmediatamente de $\beta \Rightarrow \beta$ y $\gamma \Rightarrow \gamma$ por debilitación.

aumentan la complejidad de la fórmula auxiliar, luego si en las premisas aparece, por ejemplo, $\neg\alpha$ y en la conclusión no hay ningún negador, necesariamente $\neg\alpha$ tendrá que eliminarse mediante la regla de corte. Las deducciones del apartado siguiente ilustran este principio general.

Reglas inversas Las reglas lógicas deducen la fórmula principal de las fórmulas auxiliares introduciendo signos lógicos. Ahora probamos las reglas inversas que permiten eliminar signos lógicos:

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

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

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

$$\frac{\Gamma \Rightarrow \Delta, \bigwedge u\, \alpha(u)}{\Gamma \Rightarrow \Delta, \alpha(t)}, \quad \frac{\bigvee u\, \alpha(u),\, \Gamma \Rightarrow \Delta}{\alpha(t),\, \Gamma \Rightarrow \Delta}.$$

Demostración: La primera regla inversa del negador se prueba así:

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

Pensándola de abajo hacia arriba, como sabemos que tiene que aplicarse la regla de corte con $\neg\alpha$, empezamos aplicándola, y de los secuentes superiores que obtenemos es fácil llegar en un caso a $\alpha \Rightarrow \alpha$ (que es un teorema por 1.5) y en el otro caso a la premisa. La segunda regla inversa del negador se prueba análogamente. Para el disyuntor tenemos:

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

La versión para β se prueba análogamente y la tercera se obtiene con:

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

Para el conjuntor tenemos:

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

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

Las reglas inversas de las del implicador se obtienen así:

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

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

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

Para la regla del generalizador tenemos:

$$\dfrac{\dfrac{\Gamma \Rightarrow \Delta,\, \bigwedge u\, \alpha(u)}{\Gamma \Rightarrow \Delta,\, \alpha(t),\, \bigwedge u\, \alpha(u)} \qquad \dfrac{\dfrac{\alpha(t) \Rightarrow \alpha(t)}{\alpha(t),\, \Gamma \Rightarrow \Delta,\, \alpha(t)}}{\bigwedge u\, \alpha(u),\, \Gamma \Rightarrow \Delta,\, \alpha(t)}}{\Gamma \Rightarrow \Delta,\, \alpha(t)}$$

y, por último, para el particularizador:

$$\dfrac{\dfrac{\dfrac{\alpha(t) \Rightarrow \alpha(t)}{\alpha(t),\, \Gamma \Rightarrow \Delta,\, \alpha(t)}}{\alpha(t),\, \Gamma \Rightarrow \Delta,\, \bigvee u\, \alpha(u)} \qquad \dfrac{\bigvee u\, \alpha(u),\, \Gamma \Rightarrow \Delta}{\bigvee u\, \alpha(u),\, \alpha(t),\, \Gamma \Rightarrow \Delta}}{\alpha(t),\, \Gamma \Rightarrow \Delta}$$

■

Las pruebas precedentes ilustran una característica del cálculo secuencial: si el lector pretende probar en $K_{\mathcal{L}}$ que una fórmula es consecuencia de otras dadas, la única forma de determinar qué reglas de inferencia conviene aplicar en cada momento es pensar una prueba informal detallada que nos convenza de que la conclusión es realmente una consecuencia lógica de las premisas y usarla como guía para obtener la deducción formal, mientras que, en casos sencillos como los del teorema anterior, en los que no hace falta introducir ninguna idea original en el razonamiento, podemos encontrar la deducción sin necesidad de considerar en ningún momento el posible significado de los secuentes involucrados, sino atendiendo exclusivamente a su forma. Por ejemplo, en la última deducción, el mero hecho de saber que la fórmula $\bigvee u\, \alpha(u)$ de la premisa tiene que desaparecer, nos lleva a empezar (de abajo arriba) con un corte, y en el lado izquierdo aplicamos la regla izquierda del particularizador porque es la única que puede aplicarse de forma natural, y con esto llegamos inmediatamente a la premisa o bien a "casi axiomas" de tipo $\alpha \Rightarrow \alpha$.

Podría decirse que las deducciones en $K_{\mathcal{L}}$ "están en prosa", mientras que las deducciones en LK "están en verso", en el sentido de que, si hacemos abstracción completamente del posible significado de las fórmulas consideradas, las deducciones en $K_{\mathcal{L}}$ tienen un aspecto caótico, mientras que las deducciones en LK muestran relaciones sencillas entre sus secuentes, hasta el punto de que, en casos simples, bastan para construirlas, sin consideraciones semánticas de ningún tipo. Esto es anecdótico, pero es una consecuencia anecdótica del hecho de que LK pone en primer plano la estructura formal de las deducciones, a lo cual le podremos sacar mucho partido.

No hemos enunciado reglas inversas a las reglas del bicondicionador. El lector puede enunciarlas y demostrarlas como ejercicio, pero en la práctica resulta más conveniente considerar las reglas que transforman las implicaciones en coimplicaciones y viceversa:

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

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

La primera regla la probamos en la página siguiente, por razones de espacio. La segunda se prueba así:

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

La prueba de la tercera regla es análoga. Para la cuarta:

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

Y la quinta se prueba así:

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

Definición de conectores Combinando las reglas precedentes con las reglas del conjuntor y sus inversas obtenemos inmediatamente estas variantes:

$$\frac{\alpha \leftrightarrow \beta, \Gamma \Rightarrow \Delta}{(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha), \Gamma \Rightarrow \Delta}, \qquad \frac{\Gamma \Rightarrow \Delta, \alpha \leftrightarrow \beta}{\Gamma \Rightarrow \Delta, (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)},$$

$$\frac{(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha), \Gamma \Rightarrow \Delta}{\alpha \leftrightarrow \beta, \Gamma \Rightarrow \Delta}, \qquad \frac{\Gamma \Rightarrow \Delta, (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)}{\Gamma \Rightarrow \Delta, \alpha \leftrightarrow \beta}.$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\alpha\Rightarrow\alpha}{\alpha,\beta\to\alpha,\Gamma\Rightarrow\Delta,\beta,\alpha}\qquad\dfrac{\beta\Rightarrow\beta}{\alpha,\beta,\beta\to\alpha,\Gamma\Rightarrow\Delta,\beta}}{\alpha,\alpha\to\beta,\beta\to\alpha,\Gamma\Rightarrow\Delta,\beta}\qquad\dfrac{\dfrac{\beta\Rightarrow\beta}{\beta,\alpha\to\beta,\Gamma\Rightarrow\Delta,\alpha,\beta}\qquad\dfrac{\alpha\Rightarrow\alpha}{\alpha,\beta,\alpha\to\beta,\Gamma\Rightarrow\Delta,\alpha}}{\beta,\alpha\to\beta,\beta\to\alpha,\Gamma\Rightarrow\Delta,\alpha}}{\alpha\to\beta,\beta\to\alpha,\Gamma\Rightarrow\Delta,\alpha\leftrightarrow\beta}\qquad\dfrac{\alpha\leftrightarrow\beta,\Gamma\Rightarrow\Delta}{\alpha\leftrightarrow\beta,\alpha\to\beta,\beta\to\alpha,\Gamma\Rightarrow\Delta}}{\alpha\to\beta,\beta\to\alpha,\Gamma\Rightarrow\Delta}$$

Y esto se traduce en que si consideramos que los lenguajes formales no tienen coimplicador, eliminamos sus dos reglas de la definición de LK y definimos

$$\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \land (\beta \to \alpha),$$

podemos demostrar exactamente los mismos secuentes, salvo que las fórmulas que contengan coimplicaciones serán cadenas de caracteres distintas.
Por una parte, las reglas del coimplicador pueden demostrarse a partir de las otras y de la definición de $\alpha \leftrightarrow \beta$, aplicando primero las reglas del implicador y luego las del conjuntor, y, por otra parte, si transformamos $\alpha \leftrightarrow \beta$ en $(\alpha \to \beta) \land (\beta \to \alpha)$ usando que, por definición, son lo mismo, cuando el coimplicador es un conector primitivo ese paso se justifica por las reglas que acabamos de enunciar.
Del mismo modo podemos eliminar el conjuntor de entre los conectores primitivos y definirlo como

$$\alpha \land \beta \equiv \neg(\neg\alpha \lor \neg\beta).$$

Por una parte, es fácil probar las cuatro reglas

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

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

que prueban que podemos pasar de una fórmula a la otra tanto si las consideramos fórmulas distintas como si consideramos que son la misma, y, por otra parte, podemos eliminar las reglas del conjuntor de la definición de PK, puesto que se demuestran inmediatamente a partir de las reglas del negador y del disyuntor (y de la definición del conjuntor).

Por último, también es fácil probar las reglas

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

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

que nos permiten definir análogamente

$$\alpha \to \beta \equiv \neg\alpha \lor \beta$$

y eliminar de la definición de LK las reglas del implicador.

También podríamos definir $\bigvee u\, \alpha \equiv \neg \bigwedge u \,\neg\alpha$ demostrando las cuatro reglas oportunas, pero no conviene hacer tal cosa, pues vamos a usar los cuantificadores para medir la complejidad de las fórmulas y para ello es necesario que ambos sean primitivos. En conclusión:

> *En lo sucesivo convendremos en que los únicos conectores lógicos primitivos de los lenguajes formales son* $\neg, \vee$*, y que las únicas reglas de inferencia lógicas de* LK *son las cuatro correspondientes a estos conectores y las cuatro correspondientes a los cuantificadores.*

Para referencias posteriores, enunciamos aquí la definición de la versión reducida de LK:

Definición 1.6 Llamaremos LK al cálculo secuencial sobre un lenguaje formal de primer orden $\mathcal{L}$ (sin igualador) cuyos axiomas son los secuentes $\alpha \Rightarrow \alpha$, para toda fórmula atómica α y cuyas reglas de inferencia son las siguientes:

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

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

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

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

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

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

con la condición de que, en la regla derecha del generalizador y en la regla izquierda del particularizador, la variable propia y no aparezca en las fórmulas de Γ y Δ.

A partir de estas reglas y de las definiciones

$$\alpha \wedge \beta \equiv \neg(\neg\alpha \vee \neg\beta), \quad \alpha \rightarrow \beta \equiv \neg\alpha \vee \beta, \quad \alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha).$$

se demuestran fácilmente las seis reglas adicionales incluidas en la tabla de la página 7.

Variantes Algunas reglas admiten variantes equivalentes de interés. Por ejemplo, la regla de corte es equivalente a

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

Esta variante incluye a la regla original como caso particular y, recíprocamente, puede 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.

Lo mismo vale para todas las reglas con dos secuentes superiores. Concretamente, 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 conjuntor es equivalente a

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

Otra variante de interés consiste en que 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

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

■

Ejemplo Veamos una demostración del secuente:

$$\Rightarrow \bigvee u(Cu \to \bigwedge v\, Cv),$$

que puede interpretarse como que existe alguien que, si vivirá hasta los 100 años, entonces todos viviremos hasta los 100 años.(Compárese con el último ejemplo de la subsección [LF 3.4.2].) La idea de la prueba es distinguir dos casos, correspondientes a los secuentes

$$\neg\bigvee v\,\neg Cv \Rightarrow \bigvee u(Cu \to \bigwedge v\, Cv), \qquad \bigvee v\,\neg Cv \Rightarrow \bigvee u(Cu \to \bigwedge v\, Cv),$$

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.

$$\dfrac{\begin{array}{c} Cy \Rightarrow Cy \\ \hline Cx,\, Cy \Rightarrow Cy \\ \hline Cx \Rightarrow Cy,\, \neg Cy \\ \hline Cx \Rightarrow Cy,\, \bigvee v\,\neg Cv \\ \hline Cx \Rightarrow \bigwedge v\, Cv,\, \bigvee v\,\neg Cv \\ \hline \Rightarrow Cx \to \bigwedge v\, Cv,\, \bigvee v\,\neg Cv \\ \hline \Rightarrow \bigvee u(Cu \to \bigwedge v\, Cv),\, \bigvee v\,\neg Cv \end{array} \qquad \begin{array}{c} Cy \Rightarrow Cy \\ \hline Cy \Rightarrow Cy,\, \bigwedge v\, Cv \\ \hline \neg Cy,\, Cy \Rightarrow \bigwedge v\, Cv \\ \hline \neg Cy \Rightarrow Cy \to \bigwedge v\, Cv \\ \hline \neg Cy \Rightarrow \bigvee u(Cu \to \bigwedge v\, Cv) \\ \hline \bigvee v\,\neg Cv \Rightarrow \bigvee u(Cu \to \bigwedge v\, Cv) \end{array}}{\Rightarrow \bigvee u(Cu \to \bigwedge v\, Cv)}$$

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. ■

Eliminación de cortes La razón principal por la que el cálculo secuencial es mucho más potente que los cálculos "a la Hilbert" a la hora de probar metateoremas sobre demostraciones es que muchos cálculos secuenciales satisfacen los llamados teoremas de eliminación de cortes, según los cuales todo teorema puede demostrarse sin usar la regla de corte, o bien usándola únicamente con fórmulas de corte con una estructura determinada. En el caso concreto de LK puede probarse que todo teorema puede demostrarse sin cortes (lo cual no significa que la regla de corte sea redundante, pues el teorema sólo vale para demostraciones (deducciones sin premisas).

Aunque ya podríamos demostrar este hecho, no lo haremos porque la demostración es laboriosa y más adelante probaremos un teorema más general junto con otra versión para la lógica de segundo orden. No obstante, vamos a ver cómo podemos eliminar el corte de la demostración del ejemplo precedente. La idea es que si rastreamos de dónde vienen las fórmulas de corte, vemos que la izquierda proviene del Cy situado en el antecedente del secuente inicial izquierdo, mientras que la derecha proviene del Cy del consecuente del secuente inicial derecho. Así, en lugar de mantener estas dos fórmulas y transformarlas hasta convertirlas en las fórmulas de corte, podemos cortarlas al principio, es decir, podemos cortar los dos secuentes iniciales eliminando los Cy cuyos "descendientes" son las fórmulas de corte, y así obtenemos un único secuente inicial $Cy \Rightarrow Cy$. El resultado es:

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{Cy \Rightarrow Cy}{Cx, Cy \Rightarrow Cy,\ \bigwedge v\, Cv,}}{Cx \Rightarrow Cy,\ Cy \rightarrow \bigwedge v\, Cv}}{Cx \Rightarrow Cy,\ \bigvee u(Cu \rightarrow \bigwedge v\, Cv)}}{Cx \Rightarrow \bigwedge v\, Cv,\ \bigvee u(Cu \rightarrow \bigwedge v\, Cv)}}{\Rightarrow Cx \rightarrow \bigwedge v\, Cv,\ \bigvee u(Cu \rightarrow \bigwedge v\, Cv)}}{\Rightarrow \bigvee u(Cu \rightarrow \bigwedge v\, Cv)}$$

donde en el último paso hemos aplicado la regla derecha del particularizador, que nos da la misma fórmula repetida. ■

1.2 El cálculo secuencial con igualador

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

Definición 1.7 Si $\mathcal{L}$ es un lenguaje formal con igualador (pero sin descriptor), 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 $\mathcal{L}$ (considerando ahora modelos de $\mathcal{L}$ en los que el igualador se interpreta necesariamente como la identidad), por lo que el teorema de corrección 1.4 es válido también para LK_i.

Veamos unas consecuencias inmediatas de estos axiomas:

Teorema 1.8 *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 =	$t_1 = t_2,\ t_2 = t_3 \Rightarrow t_1 = t_3$

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 1.5, a partir de estos axiomas pueden probarse versiones más generales:

Teorema 1.9 *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[7] 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 izquierda. ■

[7] La inducción del apartado precedente puede formalizarse en ARP como una simple inducción sobre t. En este caso podemos construir un funtor F tal que si α incumple el teorema, entonces $F(\alpha)$ es otra fórmula que lo incumple de longitud menor. Al iterar este funtor obtenemos una contradicción.

Ejemplo Como ilustración vamos a demostrar el secuente

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

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

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

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 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 de 1.9, tomando $\alpha(y) \equiv z = yy'$. ■

1.3 Conexión con $K_{\mathcal{L}}$

Dedicamos esta última sección a probar que las deducciones en LK_i se corresponden con las deducciones en el sistema deductivo formal $K_{\mathcal{L}}$ definido en la sección [LF 3.3]. Por una parte tenemos lo siguiente:

Teorema 1.10 *Sea $\mathcal{L}$ un lenguaje formal con igualador (pero sin descriptor), sea $\mathfrak{S}$ un conjunto de secuentes en $\mathcal{L}$ y sea Θ el conjunto de las fórmulas $\bar{S}$ asociadas*[8] *a los secuentes S de $\mathfrak{S}$. Entonces, para todo secuente T, si $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} T$, entonces $\Theta \underset{K_{\mathcal{L}}}{\vdash} \bar{T}$.*

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 obvio si S es una premisa, 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 (en $K_{\mathcal{L}}$) 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

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

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.

[8]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 $\epsilon \wedge \neg\epsilon$.

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, 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 $\bigwedge u\neg\alpha(u)$, por la regla de introducción del generalizador, y $\neg\bigvee u\, \alpha(u)$ por la negación del particularizador. Como y no está libre en ζ, podemos aplicar el teorema de deducción y concluir que $\neg\zeta \rightarrow \neg\bigvee u\, \alpha(u)$. De aquí se sigue a su vez $\bigvee u\, \alpha(u) \rightarrow \zeta$, 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 $\neg\zeta \rightarrow \bigvee u\, \alpha(u)$, 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 $\mathfrak{S}$. Por otra parte:

Teorema 1.11 *Sea $\mathcal{L}$ un lenguaje formal con igualador, sea Θ un conjunto de fórmulas de $\mathcal{L}$ 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 $\Theta \underset{K_{\mathcal{L}}}{\vdash} \alpha$ si y sólo si $\mathfrak{S} \underset{\mathrm{LK_i}}{\vdash} \Rightarrow \alpha$.*

Demostración: Tenemos una deducción $\alpha_1, \ldots, \alpha_m \equiv \alpha$ de α a partir de Θ. 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 $K_{\mathcal{L}}$ basta comprobar que $\Rightarrow \alpha_i$ es un teorema de LK_i. Para los primeros axiomas la comprobación es mecánica. Vamos a analizar el caso de los tres axiomas sobre los cuantificadores y el del igualador.

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

En la prueba del segundo axioma y es una variable libre que no aparezca en las fórmulas consideradas. Esto se usa al aplicar la regla derecha del generalizador. En la prueba siguiente y es de nuevo una variable libre que no aparezca en las fórmulas consideradas:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\alpha(y)\Rightarrow\alpha(y)}{\alpha(y),\neg\alpha(y)\Rightarrow}}{\alpha(y),\bigwedge u\,\neg\alpha(u)\Rightarrow}}{\bigvee u\,\alpha(u),\bigwedge u\neg\alpha(u)\Rightarrow}}{\bigvee u\,\alpha(u)\Rightarrow\neg\bigwedge u\,\neg\alpha(u)}\qquad\dfrac{\dfrac{\dfrac{\dfrac{\alpha(y)\Rightarrow\alpha(y)}{\alpha(y)\Rightarrow\bigvee u\,\alpha(u)}}{\Rightarrow\neg\alpha(y),\bigvee u\,\alpha(u)}}{\Rightarrow\bigwedge u\,\neg\alpha(u),\bigvee u\,\alpha(u)}}{\neg\bigwedge u\neg\alpha(u)\Rightarrow\bigvee u\,\alpha(u)}}{\Rightarrow\bigvee u\,\alpha(u)\leftrightarrow\neg\bigwedge u\neg\alpha(u)}$$

Por último:

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

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 $\Rightarrow\alpha_i$. Finalmente, 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 $\Theta \underset{K_{\mathcal{L}}}{\vdash} \alpha$. ■

Es fácil ver que, sin más que eliminar toda referencia al igualador, la prueba del teorema anterior se adapta para lenguajes sin igualador, cambiando LK_i por LK.

Así pues, en teoría es indistinto usar $K_{\mathcal{L}}$ o LK_i para estudiar las consecuencias de unas premisas dadas. En la práctica $K_{\mathcal{L}}$ es mucho más cómodo de manejar, pero en este libro demostraremos algunos resultados clave planteados en [LF] que requieren del cálculo secuencial para ser demostrados.

1.4 Cálculos secuenciales aritméticos

El primer paso para aplicar el cálculo secuencial al estudio de las teorías aritméticas consideradas en [LF] es fijar teorías equivalentes adecuadas. En principio, el teorema 1.11 nos dice que un cálculo secuencial equivalente, por ejemplo, a AP es el que tiene por axiomas los de LK_i más los secuentes de la forma $\Rightarrow \alpha$, donde α es un axioma de AP, y como reglas de inferencia, las de LK. Este cálculo secuencial es equivalente en el sentido de que una fórmula γ de $\mathcal{L}_a$ es un teorema de AP si y sólo si el secuente $\Rightarrow \gamma$ es demostrable en el cálculo que acabamos de describir. Sin embargo, esta formulación secuencial "trivial" de AP no es adecuada para nuestros fines y vamos a encontrar alternativas mejores. En primer lugar conviene formular el principio de inducción en términos de una regla de inferencia:

Teorema 1.12 *Sea T un cálculo secuencial que incluya los axiomas y las reglas de inferencia de* LK *sobre un lenguaje formal $\mathcal{L}$ que incluya una constante* 0 *y un funtor "sucesor" x'. Sea Φ una clase de fórmulas Entonces, el cálculo secuencial T_1 que resulta de añadir a T los axiomas* $\mathrm{IND}(\Phi)$ *de la forma*

$$\mathrm{Ind}(\alpha) \equiv \alpha(0) \wedge \bigwedge u(\alpha(u) \rightarrow \alpha(u')) \rightarrow \bigwedge u\, \alpha(u),$$

para cada fórmula $\alpha(x)$ en Φ (que puede tener más variables libres), es equivalente a (es decir, tiene los mismos teoremas que) el cálculo secuencial T_2 que resulta de añadirle a T la regla de inferencia[9] Φ-IND*:*

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

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 otra fórmula distinta de las dos en las que aparece explícitamente.

[9]Consideraremos que esta regla tiene dos fórmulas auxiliares, $\alpha(y)$, $\alpha(y')$ y dos fórmulas principales $\alpha(0)$ y $\alpha(t)$.

Demostración: Para probar que todo teorema de T_1 lo es de T_2 basta ver que todos los axiomas $\mathrm{Ind}(\alpha)$, con $\alpha \in \Phi$, son teoremas de T_2. En efecto, razonando “de abajo hacia arriba” obtenemos fácilmente la demostración siguiente, en la que la regla Φ-IND se aplica en el cuarto paso (desde abajo):

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

Recíprocamente, para probar que todo teorema de T_2 lo es de T_1 basta probar que el secuente inferior de la regla Φ-IND puede deducirse en T_1 del secuente superior. Por razones tipográficas partimos la prueba en tres bloques (el primero parte del secuente superior de la regla Φ-IND):

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

El segundo parte del axioma de inducción correspondiente:

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

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

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

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

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

En [LF 4.32] definimos una extensión de AP o de cualquier teoría $\mathrm{I}\Sigma_n$ resultante de añadirle un relator $\leq$ junto con unos axiomas que lo regulan (y modificando la jerarquía de Kleene para que las fórmulas Δ_0 tengan los cuantificadores acotados por el relator $\leq$ y no por la fórmula $x \leq y \equiv \bigvee u\, u + x = y$), y en [LF 4.33] probamos que se trata de una extensión intrascendente. Esto justifica que en este capítulo trabajemos siempre con las teorías extendidas de este modo. Por otro lado, al contrario que en [LF], aquí suponemos que todos los lenguajes formales considerados carecen de descriptor, lo que a efectos teóricos es irrelevante en virtud del teorema [LF 3.29], según el cual (con el convenio de que $u|u = u \equiv 0$) toda fórmula de $\mathcal{L}_a$ es lógicamente equivalente a otra sin descriptores, y que todo teorema sin descriptores se puede demostrar sin descriptores.

Definición 1.13 Si Φ es un conjunto de fórmulas de $\mathcal{L}_a$, llamaremos AP(Φ) al cálculo secuencial sobre el lenguaje $\mathcal{L}_a$ cuyas reglas de inferencia son las de LK más la regla Φ-IND y cuyos axiomas son los de LK$_i$ más los secuentes:

(O1)	$\Rightarrow x \leq x$	(O4)	$\Rightarrow x \leq y,\ y \leq x$
(O2)	$x \leq y,\ y \leq x \Rightarrow x = y$	(O5)	$\Rightarrow x \leq x'$
(O3)	$x \leq y,\ y \leq z \Rightarrow x \leq z$		

(AP1)	$x' = 0 \Rightarrow$	(AP4)	$\Rightarrow x + y' = (x + y)'$
(AP2)	$x' = y' \Rightarrow x = y$	(AP5)	$\Rightarrow x \cdot 0 = 0$
(AP3)	$\Rightarrow x + 0 = x$	(AP6)	$\Rightarrow xy' = xy + x$

Cuando Φ es la clase de todas las fórmulas de $\mathcal{L}_a$ tenemos la aritmética de Peano AP, mientras que si Φ es la clase de todas las fórmulas Σ_n obtenemos IΣ_n. Más aún, en estos casos, el cálculo secuencial AP(Φ) es equivalente a la aritmética de Peano con la inducción restringida a fórmulas de Φ, en el sentido de que una fórmula γ (sin descriptores) de $\mathcal{L}_a$ es demostrable en esta teoría si y sólo si el secuente $\Rightarrow \gamma$ es demostrable en AP(Φ).

En efecto, por [LF 4.33] γ es demostrable en la aritmética de Peano con la inducción restringida a fórmulas de Φ si y sólo si lo es en la teoría descrita en [LF 4.32] con el principio de inducción restringido a fórmulas de Φ. Por [LF 3.29] sabemos que esto sucede si y sólo si γ es demostrable en la versión sin descriptor de esta teoría, cuyos axiomas propios (aparte de los de $K_{\mathcal{L}}$) son:

1. Los axiomas de Peano distintos del de inducción:

   (AP1) $x' \neq 0$
   (AP2) $x' = y' \rightarrow x = y$
   (AP3) $x + 0 = x$
   (AP4) $x + y' = (x + y)'$
   (AP5) $x \cdot 0 = 0$
   (AP6) $xy' = xy + x$

2. Los axiomas de ordenación:

   (a) $x \leq x$
   (b) $x \leq y \land y \leq x \rightarrow x = y$

(c) $x \leq y \land y \leq z \rightarrow x \leq z$

(d) $x \leq y \lor y \leq x$

(e) $x \leq x + 1$

3. Los axiomas de inducción $\mathrm{Ind}(\alpha)$, con α en Φ,

El teorema 1.11 nos asegura que esto sucede si y sólo si el secuente $\Rightarrow \gamma$ es demostrable en LK_i extendido con los axiomas de la forma $\Rightarrow \alpha$, donde α es uno de los axiomas precedentes. El teorema 1.12 nos asegura que esto sucede si y sólo si $\Rightarrow \gamma$ es demostrable si quitamos los axiomas de tipo 3 y añadimos la regla Φ-IND, y lo único que queda por ver es que cada axioma de tipo 1, 2 implica en LK el axioma correspondiente de $\mathrm{AP}(\Phi)$ y viceversa, pero esto se prueba sin dificultad usando las reglas del implicador y del conjuntor y sus inversas.

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

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

$$\dfrac{\dfrac{\dfrac{\dfrac{\Rightarrow 0 = 0}{\Rightarrow 0 = 0,\ \bigvee u\, 0 = u'}}{\Rightarrow 0 = 0 \lor \bigvee u\, 0 = u'} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Rightarrow y' = y'}{\Rightarrow \bigvee u\, y' = u'}}{\Rightarrow y' = 0,\ \bigvee u\, y' = u'}}{y = 0 \lor \bigvee u\, y = u' \Rightarrow y' = 0,\ \bigvee u\, y' = u'}}{y = 0 \lor \bigvee u\, y = u' \Rightarrow y' = 0 \lor \bigvee u\, y' = u'}}{0 = 0 \lor \bigvee u\, 0 = u' \Rightarrow x = 0 \lor \bigvee u\, x' = u'}}{\Rightarrow x = 0 \lor \bigvee u\, x = u'}}{\Rightarrow x = 0,\ \bigvee u\, x = u'}$$

■

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

$$\begin{array}{llll}
(\mathrm{O1}) & \Rightarrow s \leq s & (\mathrm{O4}) & \Rightarrow s \leq t,\ t \leq s \\
(\mathrm{O2}) & s \leq t,\ t \leq s \Rightarrow s = u & (\mathrm{O5}) & \Rightarrow s \leq s' \\
(\mathrm{O3}) & s \leq t,\ t \leq u \Rightarrow s \leq u & &
\end{array}$$

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

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

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

■

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:

$$\begin{array}{c} \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\stackrel{\text{AM}}{\Rightarrow \eta} \qquad \stackrel{\text{AI}}{\eta,\, \beta_6 \Rightarrow \zeta}}{\beta_6 \Rightarrow \zeta} \qquad \stackrel{\text{AI}}{\zeta \Rightarrow \epsilon}}{\beta_6 \Rightarrow \epsilon} \qquad \dfrac{\stackrel{\text{AM}}{\Rightarrow \theta} \qquad \stackrel{\text{AI}}{\theta,\, \epsilon \Rightarrow \alpha_4}}{\epsilon \Rightarrow \alpha_4}}{\beta_6 \Rightarrow \alpha_4}}{\beta_6 \Rightarrow \alpha_3,\, \alpha_4 \quad (\vee)}}{\beta_6 \Rightarrow \alpha_2} \\ (*) \end{array}$$

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

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

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:

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

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:

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

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. ■

Definición 1.15 El cálculo secuencial ARP^+ es el cálculo secuencial sobre el lenguaje $\mathcal{L}_{\mathrm{arp}}$ cuyas reglas de inferencia son las de LK más la regla de inducción para fórmulas abiertas (sin cuantificadores) y cuyos axiomas son los de LK_i más:

1. Los secuentes $\Rightarrow \alpha$, donde α recorre las definiciones de los funtores de $\mathcal{L}_{\mathrm{arp}}$ (definición [LF 1.8]),
2. El secuente $Sx = 0 \Rightarrow$,
3. El secuente $Sx = Sy \Rightarrow x = y$.

Exactamente el mismo argumento que hemos empleado con $\mathrm{AP}(\Phi)$ nos permite concluir que una fórmula γ de $\mathcal{L}_{\mathrm{arp}}$ es demostrable en la teoría ARP^+ definida en [LF 4.1] si y sólo si el secuente $\Rightarrow \gamma$ es demostrable en el cálculo secuencial al que acabamos de dar el mismo nombre. Más aún, análogamente a como hemos probado el teorema 1.14, podemos probar que los secuentes que resultan de sustituir las variables en los axiomas por términos arbitrarios son teoremas de ARP^+, por lo que podemos incluirlos como axiomas sin alterar los teoremas.

De este modo, los axiomas de ARP^+ constan únicamente de fórmulas atómicas y son cerrados para sustitución, en el sentido de que si sustituimos una variable por un término en un axioma, obtenemos otro axioma del mismo tipo.

1.5 Eliminación de cortes

En la sección [LF 4.1] hemos dejado pendiente la demostración del teorema [LF 4.8], según el cual una fórmula de $\mathcal{L}_{\text{arp}}$ es demostrable en ARP si y sólo si lo es en ARP$^+$. Posteriormente, en [LF 4.23] hemos definido la teoría IΣ_1, y hemos probado que al añadirle los funtores de $\mathcal{L}_{\text{arp}}$ junto con sus definiciones, obtenemos una extensión intrascendente IΣ_1^+, pero hemos dejado pendiente demostrar que una fórmula de tipo Π_2 de $\mathcal{L}_{\text{arp}}$ es demostrable en ARP$^+$ si y sólo si es demostrable en IΣ_1^+ (si y sólo si su traducción a $\mathcal{L}_a$ es demostrable en IΣ_1).

Todos estos hechos son metateoremas no triviales cuya prueba requiere el uso del cálculo secuencial (también pueden demostrarse mediante modelos, pero las pruebas basadas en el cálculo secuencial son constructivas, en el sentido de que nos dicen cómo obtener explícitamente una demostración en ARP a partir de una demostración en ARP$^+$, etc.) Dedicamos esta sección a demostrar estos hechos y otros más. Las demostraciones se basan esencialmente en un teorema de eliminación de cortes libres cuya prueba pospondremos hasta el capítulo III para demostrarlo juntamente con una versión para el cálculo secuencial de segundo orden.

Para no repetir la introducción de los conceptos necesarios para formular el teorema ni la descripción detallada de sus hipótesis, invitamos al lector a que estudie la sección 3.1 omitiendo los pocos párrafos que hacen referencia a la lógica de segundo orden. Con ello debería entender el enunciado del teorema de eliminación de cortes libres para la lógica de primer orden:

Teorema 3.3 *En un cálculo secuencial que conste de los axiomas y reglas de inferencia de* LK *más un conjunto* $\mathfrak{S}$ *de axiomas propios cerrado para sustitución (y, en el caso de que el lenguaje formal sea* $\mathcal{L}_a$ *o* $\mathcal{L}_{\text{arp}}$*, admitimos también la regla* Φ-IND*, para un conjunto de fórmulas* Φ *cerrado para sustitución), todo teorema admite una demostración sin cortes libres.*

En particular tenemos el teorema de eliminación de cortes 3.5, que afirma simplemente que todo teorema de LK puede demostrarse sin usar la regla de corte.

Veamos una primera consecuencia no trivial de la eliminación de cortes libres, pero antes necesitamos una definición:

Definición 1.16 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 1.17 *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 el cálculo secuencial sobre* LK *con los axiomas propios de $\mathfrak{S}$ (más la regla* Φ-IND *si el lenguaje formal es $\mathcal{L}_a$ o $\mathcal{L}_{\mathrm{arp}}$) admite una demostración 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. ■

En particular:

Teorema 1.18 *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.*

A continuación mostramos varias aplicaciones no triviales del teorema de eliminación de cortes:

1.5.1 ARP como teoría de primer orden

Ya estamos en condiciones de probar que ARP^+ es una extensión conservativa de ARP. El teorema siguiente es consecuencia de [LF 4.2], pero no obstante lo demostramos de nuevo con una precisión adicional:

Teorema 1.19 *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$^+$ (y α es una fórmula atómica). 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 1.9) 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 1.9), 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). ■

En [LF 4.4] hemos asociado a cada fórmula α de $\mathcal{L}_{\mathrm{arp}}^+$ de tipo Δ_0^* una fórmula atómica (es decir, de tipo Δ_0) α^* con la propiedad (teorema [LF 4.5]) de que en ARP$^+$ se demuestra $\alpha \leftrightarrow \alpha^*$. En particular, si α^* es demostrable en ARP, entonces α es demostrable en ARP$^+$. Ahora podemos probar el recíproco:

Teorema 1.20 *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 suponer 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 1.17 nos da 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. Por lo tanto, 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 las fórmulas siguientes:

I1. $t = t$.

I2. $t_1 = t_1' \wedge \ldots \wedge t_n = t_n' \rightarrow Ft_1 \cdots t_n = Ft_1' \cdots t_n'$.

I3. $t_1 = t_1' \wedge t_2 = t_2' \wedge t_1 = t_2 \rightarrow t_1' = t_2'$.

Es fácil comprobar que todas ellas son demostrables en ARP. Las fórmulas asociadas a los axiomas asociados a los funtores son axiomas de ARP, luego obviamente son teoremas. Finalmente, las fórmulas asociadas a los axiomas matemáticos son

$$St \neq 0, \qquad Ss = St \rightarrow s = t,$$

que son teoremas de ARP (teorema [LF 1.18]). 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

$$\alpha(x) \land \gamma_1 \land \cdots \land \gamma_m \to \delta_1 \lor \cdots \lor \delta_n \lor \alpha(Sx),$$

y tenemos que demostrar

$$\alpha(0) \land \gamma_1 \land \cdots \land \gamma_m \to \delta_1 \lor \cdots \lor \delta_n \lor \alpha(t).$$

Distinguimos dos casos: si se cumple $\neg\gamma_1 \lor \cdots \neg\gamma_m \lor \delta_1 \lor \cdots \delta_n$, entonces la conclusión es inmediata. Si se cumple lo contrario (o no hay fórmulas colaterales), entonces tenemos $\alpha(x) \to \alpha(Sx)$ 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 $\alpha(0) \to \alpha(t)$, de la que se sigue trivialmente la fórmula asociada al secuente inferior de la inducción. ■

En particular, si α es una fórmula de $\mathcal{L}_{\mathrm{arp}}$, también podemos verla como fórmula atómica de $\mathcal{L}_{\mathrm{arp}}^+$ y $\alpha^* \equiv \alpha$, luego, por el teorema anterior:

Teorema 1.21 (LF 4.8) *Si una fórmula de $\mathcal{L}_{\mathrm{arp}}$ es demostrable en* ARP$^+$, *de hecho puede demostrarse en* ARP.

Nota Al igual que hemos convenido al final de la sección [LF 4.1], a partir de aquí llamaremos ARP a la teoría que hasta ahora hemos llamado ARP$^+$. ■

1.5.2 IΣ_1 como extensión de ARP

Demostramos ahora que IΣ_1 también es una extensión conservativa de ARP. Empezamos probando el teorema siguiente, que viene a decir que si, a partir de una fórmula Δ_0, en IΣ_1 podemos probar un teorema de existencia, la demostración es necesariamente constructiva:

Teorema 1.22 *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 1.18 existe una demostración D de este secuente formada únicamente por fórmulas Δ_0 y Σ_1 (en sentido estricto, es decir, con un único 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[10] 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

$$\underset{\text{ARP}}{\vdash} \bigwedge u_1 \ldots u_{r'}(\gamma_1 \wedge \cdots \wedge \gamma_r \wedge \gamma'_1 \wedge \cdots \wedge \gamma'_{r'} \rightarrow \delta_1 \vee \cdots \vee \delta_s \vee \tilde{\delta}'_1 \vee \cdots \vee \tilde{\delta}'_{s'}),$$

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 $y_1, \ldots, y_l$. Similarmente, la conclusión se expresa en la forma

$$\underset{\text{ARP}}{\vdash} \bigwedge \bar{u}(\gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y}) \rightarrow \delta_j(\bar{y}) \vee \delta'_{j'}(F_{j'}(\bar{y}, \bar{u}), \bar{y})).$$

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

$$\bigwedge \bar{u}(\gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y}) \rightarrow \delta_j(\bar{y}) \vee \delta'_{j'}(F_{j'}(\bar{y}, \bar{u}), \bar{y})).$$

[10]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.

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:

$$\bigwedge \bar{u}(\gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y}) \rightarrow \delta_j(\bar{y}) \vee \delta'_{j'}(F^1_{j'}(\bar{y}, \bar{u}), \bar{y}) \vee \alpha(F^*(\bar{y}, \bar{u}), \bar{y}))$$
$$\bigwedge \bar{u}w(\alpha(w, \bar{y}) \wedge \gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y}) \rightarrow \delta_j(\bar{y}) \vee \delta'_{j'}(F^2_{j'}(\bar{y}, \bar{u}, w), \bar{y})).$$

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 $\gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y})$ y distingamos dos casos:

Si $\neg\alpha(F^*(\bar{y}, \bar{u}), \bar{y})$, entonces se cumple $\delta_j(\bar{y}) \vee \delta'_{j'}(F^1_{j'}(\bar{y}, \bar{u}), \bar{y})$.

Si $\alpha(F^*(\bar{y}, \bar{u}), \bar{y})$, se cumple $\delta_j(\bar{y}) \vee \delta'_{j'}(F^2_{j'}(\bar{y}, \bar{u}, F^*(\bar{y}, \bar{u})), \bar{y})$.

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 $(\alpha(\bar{y}) \lor \beta(\bar{y})) \land \gamma_i(\bar{y}) \land \gamma'_{i'}(u_{i'},\bar{y})$ y distinguimos dos casos:

Si se cumple $\alpha(\bar{y})$, por la hipótesis de inducción $\delta_j(\bar{y}) \lor \delta'_{j'}(F^1_{j'}(\bar{y},\bar{u}),\bar{y})$.

Si no se cumple $\alpha(\bar{y})$, entonces se cumple $\beta(\bar{y})$ y la hipótesis de inducción nos da $\delta_j(\bar{y}) \lor \delta'_{j'}(F^2_{j'}(\bar{y},\bar{u}),\bar{y})$.

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 $\delta_j(\bar{y}) \lor \delta'_{j'}(F^3_{j'}(\bar{y},\bar{u}),\bar{y})$.

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 $y \leq t(\bar{y}) \land \alpha(y,\bar{u})$ 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 $y \leq t(\bar{y}) \land \alpha(y,\bar{y})$, 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

$$\bigwedge \bar{u}(\bigvee u' \leq t(\bar{y})\, \alpha(u',\bar{y}) \wedge \gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'},\bar{y}) \rightarrow \delta_j(\bar{y}) \vee \delta'_{j'}(F^2_{j'}(\bar{y},\bar{u}),\bar{y})).$$

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:

$$\bigwedge u'\bar{u}(\alpha(u',y,\bar{y}) \wedge \gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'},\bar{y})$$

$$\rightarrow \delta_j(\bar{y}) \vee \delta'_{j'}(F_{j'}(y,\bar{y},u',\bar{u}),\bar{y}) \vee \alpha(F'(y,\bar{y},u',\bar{u}),y+1,\bar{y})).$$

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

$$\alpha(u', 0, \bar{y}) \wedge \gamma_i(\bar{y}) \wedge \gamma'_{i'}(u_{i'}, \bar{y}).$$

Queremos probar

$$\delta_j(\bar{y}) \vee \delta'_{j'}(F^2_{j'}(\bar{y}, u', \bar{u}), \bar{y}) \vee \alpha(F''(\bar{y}, u', \bar{u}), t(\bar{y}), \bar{y}).$$

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

$$\begin{array}{rcl} F^1_{j'}(w, \bar{y}, G(w, \bar{y}, u', \bar{u})) & = & F^1_{j'}(G_{j'}(\bar{y}, u', \bar{u}), \bar{y}, G(G_{j'}(\bar{y}, u', \bar{u}), \bar{y}, u', \bar{u})) \\ & = & F^2_{j'}(\bar{y}, u', \bar{u}), \end{array}$$

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 1.23 *Sea $\phi(x_1,\ldots,x_n,x)$ 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

$$\phi'(x_1,\ldots,x_n,v) \equiv \bigvee v_0 v_1 \leq v\, (v=(v_0,v_1) \land \chi(v_0,x_1,\ldots,x_n,v_1)).$$

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 1.24 *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 $\mathrm{I}\Sigma_1$. 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 $\mathrm{I}\Sigma_1$ es una extensión conservativa de ARP para fórmulas de tipo Π_2 (o una extensión conservativa de la versión original de ARP, sin cuantificadores).

1.5.3 Satisfacción de fórmulas aritméticas

En [LF 6.11] hemos definido unas fórmulas

$$\mathbb{N} \vDash_{\Sigma_n} \alpha[v], \qquad \mathbb{N} \vDash_{\Pi_n} \alpha[v]$$

de tipo Σ_n y Π_n, respectivamente, en $\mathcal{L}_a$ que formalizan el concepto de satisfacción de una fórmula $\alpha \in \mathrm{Form}(\ulcorner \mathcal{L}_a \urcorner)$ de tipo Σ_n o Π_n, respectivamente. A su vez, podemos definir el concepto de fórmula verdadera de tipo Σ_n:

$$\mathbb{N} \vDash_{\Sigma_n} \alpha \equiv \bigwedge v(\mathrm{Val}(v, \alpha) \to \mathbb{N} \vDash_{\Sigma_n} \alpha[v]).$$

Notemos que se trata de una fórmula de tipo Π_{n+1}.

Teorema 1.25 $\underset{\mathrm{I}\Sigma_{n+1}}{\vdash} \bigwedge \alpha \in \Sigma_n(\underset{\ulcorner \mathrm{I}\Sigma_n \urcorner}{\vdash} \alpha \to \mathbb{N} \vDash_{\Sigma_n} \alpha)$.

Demostración: Supongamos que α es una fórmula de tipo Σ_n en $\ulcorner \mathcal{L}_a \urcorner$ tal que $\underset{\ulcorner \mathrm{I}\Sigma_n \urcorner}{\vdash} \alpha$. El teorema 1.11 nos dice que esto es equivalente a que el secuente $\Rightarrow \alpha$ sea demostrable en LK_i a partir de los secuentes $\Rightarrow \delta$, donde δ es un axioma de $\ulcorner \mathrm{I}\Sigma_n \urcorner$. Según hemos visto tras la definición 1.13, esto equivale a que $\Rightarrow \alpha$ sea demostrable en el cálculo secuencial $\mathrm{AP}(\Sigma_n)$. Fijemos una demostración D, de modo que D es un árbol de secuentes tal que $D_\varnothing = \Rightarrow \alpha$. Por el teorema 1.18, podemos suponer que todas las fórmulas que aparecen en los secuentes de D son de tipo $\mathrm{I}\Sigma_n$.

Sea V el conjunto (finito) de todas las variables (libres o ligadas) que aparecen en las fórmulas de los secuentes de D y escribiremos $\mathrm{Val}(v, V)$ para indicar que v es una aplicación con dominio V. Vamos a probar que

$$\bigwedge v(\mathrm{Val}(v, V) \to \bigwedge s \in \mathcal{D}D(\bigvee \gamma \in (D_s)_1 \neg \mathbb{N} \vDash_{\Sigma_n} \gamma[v] \vee \bigvee \delta \in (D_s)_2 \mathbb{N} \vDash_{\Sigma_n} \delta[v]).$$

Si llamamos h a la altura de D, es decir, la máxima altura de sus nodos, y, para cada $s \in D$, llamamos $r(s) = h - \ell(s)$, probaremos esta fórmula por inducción sobre $r(s)$, es decir, fijada v tal que $\mathrm{Val}(v, V)$, vamos a probar que

$$\bigwedge m \bigwedge v(\mathrm{Val}(v, V) \to \bigwedge s \in \mathcal{D}D(r(s) = m \to$$
$$(\bigvee \gamma \in (D_s)_1 \neg \mathbb{N} \vDash_{\Sigma_n} \gamma[v] \vee \bigvee \delta \in (D_s)_2 \mathbb{N} \vDash_{\Sigma_n} \delta[v]))).$$

Para ello observamos que la fórmula tras el $\bigwedge m$ es de tipo Π_{n+1}, luego podemos razonar por inducción sobre m en $\mathrm{I}\Sigma_{n+1}$. En la práctica, basta probar que s cumple lo requerido supuesto que se cumpla para los nodos situados por encima de s en D.

A partir de este punto la demostración es una comprobación rutinaria: sólo hay que ver que los axiomas de $\ulcorner \mathrm{I}\Sigma_\mathrm{n} \urcorner$ son satisfechos (es decir, que cumplen la conclusión) y que si un secuente D_s se deduce de secuentes anteriores por alguna de las reglas de inferencia (secuenciales) de $\mathrm{I}\Sigma_n$ (para los cuales se cumple la conclusión por hipótesis de inducción), también se cumple para D_s.

Notemos que, una vez probada esta fórmula, en particular podemos aplicarla a $s = \varnothing$, es decir, al secuente $\Rightarrow \alpha$, para el que la conclusión es precisamente (dado que su antecedente es vacío) que $\mathbb{N} \vDash_{\Sigma_n} \alpha[v]$. En principio, hemos probado esto para toda v que cumpla $\mathrm{Val}(v, V)$, pero esto implica que se cumple para toda valoración que cumpla $\mathrm{Val}(v, \alpha)$, ya que esto sólo depende de la restricción de v a las variables libres de α. Por lo tanto, tenemos $\mathbb{N} \vDash \alpha$, como queremos probar.

Todos los axiomas de $\mathrm{I}\Sigma_n$ son secuentes formados por fórmulas atómicas, y todos se prueban trivialmente a partir de los dos primeros apartados del teorema [LF 6.8] y del teorema [LF 6.9]. Por ejemplo, consideremos un axioma de la forma

$$S = (\{s = t\} \Rightarrow \{Ss = St\}).$$

Se trata de comprobar que, fijada una valoración v,

$$\neg \mathbb{N} \vDash_0 (s = t)[v] \vee \mathbb{N} \vDash_0 (Ss = St)[v],$$

que a su vez, aplicando las definiciones correspondientes, 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.

En cuanto a las reglas de inferencia, vamos a comprobar, por ejemplo, la validez de la regla izquierda del disyuntor y de la regla de inducción. Para la primera 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 $S = (\{\alpha \vee \beta\} \cup \Gamma \Rightarrow \Delta)$.

Como la demostración D consta exclusivamente de fórmulas Σ_n en sentido estricto, en particular lo son α, β y $\alpha \vee \beta$, 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,

$$\neg\mathbb{N} \vDash_0 (\alpha \vee \beta)[v] \vee \bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash_{\Sigma_n} \gamma[v] \vee \bigvee\delta \in \Delta\, \mathbb{N} \vDash_{\Sigma_n} \delta[v].$$

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.

Para 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 que, para toda valoración v,

$$\bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash_{\Sigma_n} \gamma[v] \vee \bigvee\delta \in \Delta\ \mathbb{N} \vDash_{\Sigma_n} \delta[v] \vee \neg\mathbb{N} \vDash_{\Sigma_n} \mathtt{S}_y^0\alpha[v] \vee \mathbb{N} \vDash_{\Sigma_n} \mathtt{S}_y^t\alpha[v].$$

Para ello 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

$$\bigvee\gamma \in \Gamma \neg\mathbb{N} \vDash_{\Sigma_n} \gamma[v_y^a] \vee \bigvee\delta \in \Delta\ \mathbb{N} \vDash_{\Sigma_n} \delta[v_y^a],$$

luego, por la hipótesis de inducción, 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[11] 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 $\mathbb{N} \vDash_{\Sigma_n} \mathtt{S}_y^t\alpha[v]$, como había que probar. ■

Para comprender la relevancia de este resultado remitimos al lector al teorema [LF 6.16] y siguientes. Terminamos probando esta variante:

[11]Se trata de formalizar para $\mathbb{N} \vDash$ el teorema [LF 5.11] (que puede probarse, concretamente, en $\mathrm{I}\Sigma_1$). Ello supone demostrarlo primero para $\mathbb{N} \vDash_0$ y de ahí generalizarlo a $\mathbb{N} \vDash_{\Sigma_n}$ y $\mathbb{N} \vDash_{\Pi_n}$. Los argumentos son todos elementales.

Teorema 1.26 $\underset{\mathrm{I}\Sigma_1}{\vdash} \bigwedge \alpha \in \Delta_0(\underset{\ulcorner \mathrm{Q} \urcorner}{\vdash} \alpha \rightarrow \mathbb{N} \vDash_0 \alpha)$.

DEMOSTRACIÓN: Fijemos una fórmula α de tipo Δ_0, sean $x_1, \ldots, x_r$ sus variables libres y sea v definida sobre ellas. Llamemos $n_i = v(x_i)$. Suponemos $\underset{\ulcorner \mathrm{Q} \urcorner}{\vdash} \alpha$, con lo que también $\underset{\ulcorner \mathrm{Q} \urcorner}{\vdash} \alpha(0^{(n_1)}, \ldots, 0^{(n_r)})$.

Ahora usamos [LF 6.21], que nos da que la sentencia $\alpha(0^{(n_1)}, \ldots, 0^{(n_r)})$ es equivalente en Q a otra sentencia $\bar{\alpha}$ sin cuantificadores. Entonces también $\underset{\ulcorner \mathrm{Q} \urcorner}{\vdash} \bar{\alpha}$.

Ahora consideramos la extensión intrascendente Q^* de Q definida en [LF 6.5], cuyos axiomas son todos fórmulas sin cuantificadores. Considerando como axiomas todas las fórmulas que resultan de sustituir variables por términos en los axiomas de Q^* obtenemos una teoría con los mismos teoremas y cuyos axiomas son cerrados para sustitución. Obviamente $\underset{\ulcorner \mathrm{Q}^* \urcorner}{\vdash} \bar{\alpha}$.

Así tenemos una fórmula sin cuantificadores demostrable en una teoría cuyos axiomas no tienen cuantificadores (y son cerrados para sustitución), y esto permite aplicar el teorema 1.17, que nos da una demostración D de $\bar{\alpha}$ en $\ulcorner \mathrm{Q}^* \urcorner$ en la que sólo aparecen fórmulas sin cuantificadores. En particular, todas son de tipo Δ_0, y todo el argumento del teorema anterior es aplicable para concluir que, para toda valoración v, se cumple (con la notación del teorema):

$$\bigwedge v(\mathrm{Val}(v, V) \rightarrow \bigwedge s \in \mathcal{D}D(\bigvee \gamma \in (D_s)_1 \neg \mathbb{N} \vDash_0 \gamma[v] \vee \bigvee \delta \in (D_s)_2 \mathbb{N} \vDash_0 \delta[v]),$$

donde usamos que $\mathbb{N} \vDash_0$ puede definirse para fórmulas de $\ulcorner \mathcal{L}_a^* \urcorner$, y la única comprobación adicional es que los axiomas de Q^* que definen el funtor pre son verdaderos, lo cual es trivial. La conclusión es que $\mathbb{N} \vDash_0 \bar{\alpha}$. Por la nota posterior a [LF 6.21], esto implica que $\mathbb{N} \vDash_0 \alpha(0^{(n_1)}, \ldots, 0^{(n_r)})$, que a su vez es equivalente a $\mathbb{N} \vDash_0 \alpha[v]$, lo que, por definición, significa que $\mathbb{N} \vDash_0 \alpha$. ■

Capítulo II

Lógica de segundo orden

En la sección [LF 7.1] hemos visto cómo podemos extender cualquier teoría axiomática de primer orden a teorías de segundo orden que incorporan en su lenguaje variables que representen relaciones n-ádicas entre los objetos de los que habla la teoría (en particular, conjuntos), de modo que sea posible cuantificar sobre ellas. En la sección [LF 7.2] hemos introducido extensiones más precisas para el caso de las teorías aritméticas $\mathrm{I}\Sigma_1$ y AP. Como es habitual, los resultados más delicados que relacionan cada teoría de primer orden con su extensión de segundo orden se demuestran usando el cálculo secuencial, y a ello dedicamos este capítulo.

Hay una diferencia esencial entre el tratamiento de la lógica de segundo orden que vamos a considerar aquí y el considerado en [LF], y es que allí los lenguajes de segundo orden los hemos definido como una clase particular de lenguajes de primer orden, de modo que el cálculo deductivo de segundo orden es el mismo que el de primer orden, sólo que con algunos axiomas estructurales específicos. Aquí, por el contrario, vamos a definir lenguajes de segundo orden propiamente dichos y luego definiremos un cálculo secuencial de segundo orden con reglas de inferencia adicionales que regulen la cuantificación de variables de segundo orden.

Al igual que los capítulos precedentes, todo el contenido de este capítulo es formalizable en ARP.

2.1 Lenguajes formales de segundo orden

Definición 2.1 La definición de *lenguaje formal de segundo orden* (con o sin igualador) es la misma que la de lenguaje formal de primer orden [LF 3.2], 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. Como siempre, aquí consideramos únicamente lenguajes sin descriptor y sólo consideraremos como conectores primitivos el negador y el disyuntor.

A las variables de rango 0 de un lenguaje formal $\mathcal{L}$ de segundo orden las llamaremos *variables de primer orden,* mientras que a las de rango mayor que 0 las llamaremos *variables de segundo 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 (como es el caso de $\mathrm{I}\Sigma_1$ o AP), 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 Los semitérminos de un lenguaje formal de segundo orden se definen igual[1] que los de los lenguajes de primer orden (sin descriptor), entendiendo que el equivalente en un lenguaje de segundo orden a las variables de un lenguaje de primer orden son las variables de primer orden:

Definición 2.2 Si $\mathcal{L}$ es un lenguaje formal de segundo orden, una cadena de signos t es un *semitérmino* de $\mathcal{L}$ si cumple una de las condiciones siguientes:

1. t es una variable de primer orden (libre o ligada),
2. t es una constante,
3. $t \equiv f^n t_1 \cdots t_n \equiv f^n(t_1, \ldots, t_n)$, donde f^n es un funtor n-ádico y $t_1, \ldots, t_n$ son semitérminos.

[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.

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, las *semifórmulas* de un lenguaje de segundo orden sean las cadenas de signos de una de las formas siguientes:

1. $X^r(t_1, \ldots, t_r) \equiv X^r t_1 \cdots, t_r$, 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.* 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 por un semitérmino en una semiexpresión es la misma que para la lógica de primer orden, salvo que se simplifica un poco por el hecho de que aquí estamos considerando lenguajes sin descriptor. Esto nos permite definir separadamente la sustitución en semitérminos y en semifórmulas. Para semitérminos definimos:

1. $\mathtt{S}_x^t x_0 \equiv \begin{cases} t & \text{si } x \equiv x_0, \\ x_0 & \text{si } x \not\equiv x_0, \end{cases}$ donde las variables pueden ser libres o ligadas.
2. $\mathtt{S}_x^t c \equiv x$.
3. $\mathtt{S}_x^t f^n(t_1, \ldots, t_n) \equiv f^n(\mathtt{S}_x^t t_1, \ldots, \mathtt{S}_x^t t_n)$.

Para semifórmulas tenemos que definir primero cuándo una variable x puede sustituirse por un semitérmino t en una semifórmula:

1. Si α es atómica, entonces la sustitución es posible.
2. La sustitución en $\neg\alpha$ o $\alpha \vee \beta$ es posible si y sólo si lo es en α y en β (luego lo mismo vale para $\alpha \rightarrow \beta, \alpha \wedge \beta$ y $\alpha \leftrightarrow \beta$).
3. La sustitución en $\bigwedge u\,\alpha$ o en $\bigvee u\,\alpha$ es posible salvo si $x \not\equiv u$ y no es posible sustituir x por t en α o la variable u aparece libre en t.
4. La sustitución en $\bigwedge U\,\alpha$ o en $\bigvee U\,\alpha$ es posible si y sólo si x se puede sustituir por t en α.

Notemos que la sustitución siempre es posible cuando las variables libres de t no están ligadas en α, en particular cuando t es un término.

Si x es una variable de primer orden que puede sustituirse por un semitérmino t en una semifórmula, la sustitución se define así:

1. $\mathtt{S}_x^t X^n(t_1, \ldots, t_n) \equiv X^n(\mathtt{S}_x^t t_1, \ldots, \mathtt{S}_x^t t_n)$, donde X^n es una variable de segundo orden de rango n o un relator de rango n.
2. $\mathtt{S}_x^t(\neg\alpha) \equiv \neg\mathtt{S}_x^t\alpha$.

3. $\mathsf{S}_x^t(\alpha \lor \beta) \equiv \neg\mathsf{S}_x^t\alpha \lor \mathsf{S}_x^t\beta$.

4. $\mathsf{S}_x^t(\bigwedge u\,\alpha) \equiv \begin{cases} \bigwedge u\,\alpha & \text{si } u \equiv x, \\ \bigwedge u\,\mathsf{S}_x^t\alpha & \text{si } u \not\equiv x. \end{cases}$

5. $\mathsf{S}_x^t(\bigvee u\,\alpha) \equiv \begin{cases} \bigvee u\,\alpha & \text{si } u \equiv x, \\ \bigvee u\,\mathsf{S}_x^t\alpha & \text{si } u \not\equiv x. \end{cases}$

6. $\mathsf{S}_x^t \bigwedge U\,\alpha \equiv \bigwedge U\,\mathsf{S}_x^t\alpha$.

7. $\mathsf{S}_x^t \bigvee U\,\alpha \equiv \bigvee U\,\mathsf{S}_x^t\alpha$.

Es claro entonces que

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

así como que $\mathsf{S}_x^t\alpha \equiv \alpha$ siempre que x no está libre en α.

Diremos que una variable de segundo orden X se puede sustituir por otra variable o por un relator del mismo rango Y en una semifórmula si se cumple uno de los casos siguientes (tanto X como Y pueden ser variables libres o ligadas):

1. Si α es atómica, la sustitución es posible.
2. La sustitución en $\neg\alpha$ o $\alpha \lor \beta$ es posible si y sólo si lo es en α y en β (luego lo mismo vale para $\alpha \to \beta, \alpha \land \beta$ y $\alpha \leftrightarrow \beta$).
3. La sustitución en $\bigwedge u\,\alpha$ o $\bigvee u\,\alpha$ es posible si y sólo si lo es en α.
4. La sustitución en $\bigwedge U\,\alpha$ o $\bigvee U\,\alpha$ es posible salvo si $X \not\equiv U$ y no es posible sustituir X por Y en α o $U \equiv Y$.

En particular, la sustitución siempre es posible cuando Y es una variable libre. Si se da esta situación, definimos la sustitución de X por Y en una fórmula mediante las reglas siguientes:

1. $\mathsf{S}_X^Y X^n(t_1, \dots t_n) \equiv \begin{cases} Y(t_1, \dots, t_n) & \text{si } X \equiv X^n, \\ X^n(t_1, \dots, t_n) & \text{si } X \not\equiv X^n. \end{cases}$

2. $\mathsf{S}_X^Y(\neg\alpha) \equiv \neg S_X^Y\alpha$.

3. $\mathsf{S}_X^Y(\alpha \lor \beta) \equiv \mathsf{S}_X^Y\alpha \lor \mathsf{S}_X^Y\beta$.

4. $\mathsf{S}_X^Y(\bigwedge u\,\alpha) \equiv \bigwedge u\,\mathsf{S}_X^Y\alpha$.

5. $\mathsf{S}_X^Y(\bigvee u\,\alpha) \equiv \bigvee u\,\mathsf{S}_X^Y\alpha$.

6. $\mathsf{S}_X^Y(\bigwedge U\,\alpha) \equiv \begin{cases} \bigwedge U\,\alpha & \text{si } U \equiv X, \\ \bigwedge U \mathsf{S}_X^U\alpha & \text{si } U \not\equiv X. \end{cases}$

7. $\mathsf{S}_X^Y(\bigvee U\,\alpha) \equiv \begin{cases} \bigvee U\,\alpha & \text{si } U \equiv X, \\ \bigvee U \mathsf{S}_X^U\alpha & \text{si } U \not\equiv X. \end{cases}$

De nuevo tenemos que

$$\mathtt{S}_X^Y(\alpha \rightarrow \beta) \equiv \mathtt{S}_X^Y\alpha \rightarrow \mathtt{S}_X^Y\beta, \qquad \mathtt{S}_X^Y(\alpha \wedge \beta) \equiv \mathtt{S}_X^Y\alpha \wedge \mathtt{S}_X^Y\beta,$$

$$\mathtt{S}_X^Y(\alpha \leftrightarrow \beta) \equiv \mathtt{S}_X^Y\alpha \leftrightarrow \mathtt{S}_X^Y\beta,$$

así como que $\mathtt{S}_X^Y\alpha \equiv \alpha$ si X no está libre en α.

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:

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

donde las variables z_i son variables libres del rango que corresponda y que no estén en α ni en los términos t_i.

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.

Ahora introducimos otro tipo de sustitución que no tiene equivalente en la lógica de primer orden:

Sea α una fórmula y sean $x_1, \ldots, x_n$ variables libres de primer orden distintas entre sí (que pueden estar o no en α). Abreviaremos $\bar{x}$ en lugar de $x_1, \ldots, x_n$. Diremos que una variable libre de segundo orden X de rango n puede sustituirse por $\alpha(\bar{x})$ en una semifórmula β si se cumple uno de los casos siguientes:

1. Si $\beta \equiv X^r(t_1, \ldots, t_r)$ la sustitución es posible salvo si $X \equiv X^r$ y alguna variable x_i no puede sustituirse por el semitérmino t_i en α.
2. La sustitución en $\neg\alpha$ o $\alpha \vee \beta$ es posible si y sólo si lo es en α y en β (luego lo mismo vale para $\alpha \rightarrow \beta, \alpha \wedge \beta$ y $\alpha \leftrightarrow \beta$).
3. La sustitución en $\bigwedge u\, \alpha$ o $\bigvee u\, \alpha$ es posible si y sólo si lo es en α.
4. La sustitución en $\bigwedge U\, \alpha$ o $\bigvee U\, \alpha$ es posible si y sólo si lo es en α.

En estas condiciones, la sustitución se define así:

1. $\mathtt{S}_X^{\alpha(\bar{x})} X^r(t_1, \ldots, t_r)) \equiv \begin{cases} \alpha(t_1, \ldots, t_n) & \text{si } X \equiv X^r \text{ (luego } r = n), \\ X^r(t_1, \ldots, t_r) & \text{si } X \not\equiv X^r. \end{cases}$
2. $\mathtt{S}_X^{\alpha(\bar{x})} \neg\beta \equiv \neg\mathtt{S}_X^{\alpha(\bar{x})}\beta$.
3. $\mathtt{S}_X^{\alpha(\bar{x})}(\beta \vee \gamma) \equiv \mathtt{S}_X^{\alpha(\bar{x})}\beta \vee \mathtt{S}_X^{\alpha(\bar{x})}\gamma$.
4. $\mathtt{S}_X^{\alpha(\bar{x})}(\bigwedge u\, \beta) \equiv \bigwedge u\, \mathtt{S}_X^{\alpha(\bar{x})}\beta$.

5. $\mathsf{S}_X^{\alpha(\bar{x})}(\bigvee u\,\beta) \equiv \bigvee u\,\mathsf{S}_X^{\alpha(\bar{x})}\beta$.
6. $\mathsf{S}_X^{\alpha(\bar{x})}(\bigwedge U\,\beta) \equiv \bigwedge U\,\mathsf{S}_X^{\alpha(\bar{x})}\beta$.
7. $\mathsf{S}_X^{\alpha(\bar{x})}(\bigvee U\,\beta) \equiv \bigvee U\,\mathsf{S}_X^{\alpha(\bar{x})}\beta$.

De nuevo tenemos que

$$\mathsf{S}_X^{\alpha(\bar{x})}(\beta \rightarrow \gamma) \equiv \mathsf{S}_X^{\alpha(\bar{x})}\beta \rightarrow \mathsf{S}_X^{\alpha(\bar{x})}\gamma, \qquad \mathsf{S}_X^{\alpha(\bar{x})}(\beta \wedge \gamma) \equiv \mathsf{S}_X^{\alpha(\bar{x})}\beta \wedge \mathsf{S}_X^{\alpha(\bar{x})}\gamma,$$

$$\mathsf{S}_X^{\alpha(\bar{x})}(\beta \leftrightarrow \gamma) \equiv \mathsf{S}_X^{\alpha(\bar{x})}\beta \leftrightarrow \mathsf{S}_X^{\alpha(\bar{x})}\gamma,$$

así como que $\mathsf{S}_X^{\alpha(\bar{x})}\beta \equiv \beta$ si X no está libre en β. Notemos además que $\mathsf{S}_X^{\alpha(\bar{x})}\beta$ se puede calcular siempre que β y α no tienen variables ligadas en común.

Observemos que si las fórmulas α y β no tienen variables ligadas en común, entonces cualquier variable x_i podrá sustituirse en α por cualquier semitérmino contenido en β, por lo que será posible sustituir X^r por $\alpha(\bar{x})$.

Notemos que todas las definiciones que hemos dado se particularizan trivialmente al caso de lenguajes reducidos. Por ejemplo:

Definición 2.3 Definimos el *lenguaje de la aritmética de segundo orden* $\mathcal{L}_a^2$ como el lenguaje reducido de segundo orden que resulta de añadir variables de segundo orden al lenguaje $\mathcal{L}_a$ (sin descriptor) y dotado del relator de orden $\leq$.

Las fórmulas de primer orden de $\mathcal{L}_a^2$ (es decir, las fórmulas que no tienen cuantificadores de segundo orden, pero sí pueden tener variables libres de segundo orden) se llaman habitualmente *fórmulas aritméticas.*

Definimos las semifórmulas de tipo Δ_0^0 en $\mathcal{L}_a^2$ como las dadas por las reglas siguientes:

1. Si t_1, t_2 son semitérminos, entonces $t_1 = t_2$ y $t_1 \leq t_2$ son semifórmulas Δ_0^0.
2. Si t es un semitérmino y X es una variable de segundo orden (libre o ligada), entonces $X(t)$ es una semifórmula Δ_0^0.
3. Si α y β son semifórmulas Δ_0^0, también lo son $\neg\alpha$ y $\alpha \vee \beta$.
4. Si t es un semitérmino y α es una semifórmula Δ_0^0, también lo son $\bigwedge u \leq t\,\alpha$ y $\bigvee u \leq t\,\alpha$.

Las fórmulas Δ_0^0 son las semifórmulas Δ_0^0 que son fórmulas. Claramente no pueden tener variables ligadas de segundo orden, pero sí variables libres de segundo orden. De hecho las fórmulas Δ_0^0 sin variables de segundo orden son precisamente las fórmulas Δ_0 de $\mathcal{L}_a$.

Las fórmulas Σ_n^0 y Π_n^0 (en sentido estricto) de $\mathcal{L}_a^2$ se definen exactamente igual que las fórmulas Σ_n y Π_n de $\mathcal{L}_a$ salvo que partimos de fórmulas Δ_0^0 en el lugar de las fórmulas Δ_0.

2.2 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 2.4 Si $\mathcal{L}$ es un lenguaje formal de segundo orden, llamaremos $B_{\mathcal{L}}$ (o simplemente B) al cálculo secuencial cuyas axiomas son los secuentes $\alpha \Rightarrow \alpha$, para todas las fórmulas atómicas α de $\mathcal{L}$, 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.

Es claro que todas las reglas derivadas de LK (como las reglas inversas) valen también para B aunque se apliquen a secuentes con fórmulas de segundo orden, pues las demostraciones valen igualmente. También podemos razonar como en el teorema 1.5 que todos los secuentes $\alpha \Rightarrow \alpha$, para fórmulas no necesariamente atómicas, son teoremas.

En principio, el igualador sólo puede relacionar términos de primer orden, pero podemos definir como sigue la igualdad de segundo orden:

Si X e Y son dos variables o relatores del mismo rango r, definimos

$$X = Y \equiv \textstyle\bigwedge u_1 \cdots u_r (X(u_1, \ldots, u_r) \leftrightarrow Y(u_1, \ldots, u_r)).$$

Es fácil probar:

$$\Rightarrow X = X, \qquad X = Y \Rightarrow Y = X, \qquad X = Y,\ Y = Z \Rightarrow X = Z.$$

De la propia definición se sigue además que

$$X = Y, X(t_1, \ldots, t_r) \Rightarrow Y(t_1, \ldots, t_r).$$

Para acabar de comprobar que esta igualdad se comporta como una auténtica igualdad nos falta probar que

$$X = Y, \alpha(X) \Rightarrow \alpha(Y).$$

El teorema siguiente prueba algo más general:

Teorema 2.5 *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 libres de primer orden señaladas tales que X pueda sustituirse por T_1 y T_2 en $\alpha(X)$. Entonces en B se demuestra:*

$$\textstyle\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\ \alpha(T_1) \Rightarrow \alpha(T_2).$$

DEMOSTRACIÓN: Razonamos, por inducción sobre la longitud[2] de α, que tanto la fórmula del enunciado como

$$\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})),\, \alpha(T_2) \Rightarrow \alpha(T_1)$$

son teoremas de B.

Si $\alpha(X) \equiv Y(t_1, \ldots, t_n)$, 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 $\alpha(X) \equiv X(t_1, \ldots, t_r)$, 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

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\beta \Rightarrow \beta}{\beta \Rightarrow \beta, \gamma} \qquad \dfrac{\gamma \Rightarrow \gamma}{\beta, \gamma \Rightarrow \gamma}}{\beta \rightarrow \gamma, \beta \Rightarrow \gamma}}{\beta \rightarrow \gamma, \gamma \rightarrow \beta, \beta \Rightarrow \gamma}}{\beta \leftrightarrow \gamma, \beta \Rightarrow \gamma}}{\bigwedge \bar{u}(\beta(\bar{u}) \leftrightarrow \gamma(\bar{u})), \beta \Rightarrow \gamma}}{}$$

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.

[2]Técnicamente esto supone definir un funtor tal que $F(\alpha, n)$ sea una función de dominio el conjunto $S_n(\alpha)$ de las fórmulas de longitud n que resultan de sustituir las variables ligadas que estén libres por variables libres en una subsemifórmula de α y que a cada una le asignan un par de demostraciones de los dos secuentes considerados.

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. ■

Tomando $T_1 \equiv X(x_1, \ldots, x_r)$ y $T_2 \equiv Y(x_1, \ldots, x_r)$ obtenemos la propiedad de la igualdad indicada antes del teorema.

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. Sin embargo, las variables de segundo orden serían inútiles sin algunos axiomas adicionales más que las relacionen con la lógica de primer orden.

Definición 2.6 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 de segundo orden $\mathcal{L}^2$ que resulta de añadirle a $\mathcal{L}$ variables de segundo orden, cuyas reglas de inferencia son las de B y cuyos axiomas son:

1. Los axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica α de $\mathcal{L}^2$,
2. Los axiomas propios de K,
3. $\Rightarrow x = x$,
4. $x_1 = y_1, \ldots, x_r = y_r, X^r(x_1, \ldots, x_r) \Rightarrow X^r(y_1, \ldots, y_r)$,
5. Comprensión: $\Rightarrow \bigvee U^r \bigwedge \bar{u}(U^r(u_1, \ldots, u_r) \leftrightarrow \alpha(u_1, \ldots, u_r))$,
   para toda fórmula de primer orden $\alpha(x_1, \ldots, x_r)$, que puede tener otras variables libres, de primer o segundo orden.

Si en el esquema de comprensión admitimos fórmulas arbitrarias, entonces tenemos la *extensión plena* de K, a la que nos referiremos como K^2.

Las *extensiones predicativa y plena reducidas* se definen análogamente, pero considerando el lenguaje de segundo orden reducido que resulta de añadir únicamente variables de rango 1 y particularizando los esquemas 4) y 5) a variables de rango 1.

Demostraremos (teorema 2.22) que K_0 es una extensión conservativa de K, es decir, que toda fórmula de $\mathcal{L}$ demostrable en K_0 es, de hecho, demostrable en K, pero antes necesitamos estudiar estas teorías.

Del mismo modo que al estudiar las teorías aritméticas de primer orden ha sido fundamental sustituir el esquema de inducción por la regla de inferencia de inducción, ahora será igualmente necesario sustituir el esquema de comprensión por una regla de inferencia adecuada:

Teorema 2.7 *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 $\alpha(x_1,\ldots,x_r)$ equivale a admitir como regla de inferencia*

$$\frac{\Gamma \Rightarrow \Delta,\ \gamma(T)}{\Gamma \Rightarrow \Delta,\ \bigvee U\,\gamma(U)}$$

para $T \equiv \alpha(x_1,\ldots,x_r)$ y toda fórmula $\gamma(X)$, donde X es una variable de rango r sustituible por T en α.

Demostración: Si admitimos esta regla, podemos demostrar como sigue el axioma de comprensión:

$$\cfrac{\cfrac{\cfrac{\alpha(\bar{x}) \Rightarrow \alpha(\bar{x}) \qquad \alpha(\bar{x}) \Rightarrow \alpha(\bar{x})}{\Rightarrow \alpha(\bar{x}) \leftrightarrow \alpha(\bar{x})}}{\Rightarrow \bigwedge \bar{u}(\alpha(\bar{u}) \leftrightarrow \alpha(\bar{u}))}}{\Rightarrow \bigvee U \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow \alpha(\bar{u}))}$$

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 2.5 tenemos que

$$\bigwedge \bar{u}(X(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \gamma(T_2),$$

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:

$$\cfrac{\cfrac{\bigwedge \bar{u}(X(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \gamma(X)}{\bigwedge \bar{u}(X(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \bigvee U \gamma(U)}}{\bigvee U \bigwedge \bar{u}(U(\bar{u}) \leftrightarrow \alpha(\bar{u})),\ \gamma(T_1) \Rightarrow \bigvee U \gamma(U)}$$

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:

$$\frac{\gamma(T),\,\Gamma \Rightarrow \Delta}{\bigwedge U\gamma(U),\,\Gamma \Rightarrow \Delta}$$

En efecto:

$$\dfrac{\dfrac{\dfrac{\gamma(T),\,\Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg\gamma(T)}}{\Gamma \Rightarrow \Delta,\, \bigvee U \neg\gamma(U)} \qquad \dfrac{\dfrac{\dfrac{\gamma(X) \Rightarrow \gamma(X)}{\neg\gamma(X),\, \gamma(X) \Rightarrow}}{\neg\gamma(X),\, \bigwedge U\,\gamma(U) \Rightarrow}}{\bigvee U\neg\gamma(U),\, \bigwedge U\gamma(U) \Rightarrow}}{\bigwedge U\gamma(U),\,\Gamma \Rightarrow \Delta}$$

Esto nos lleva a la definición siguiente:

Definición 2.8 Dado un lenguaje formal de segundo orden $\mathcal{L}$ y un conjunto Ψ de fórmulas de $\mathcal{L}$, llamaremos *lógica de segundo orden* con Ψ-comprensión al cálculo secuencial B_0 cuyos axiomas son los axiomas lógicos $\alpha \Rightarrow \alpha$, para todas las fórmulas atómicas α de $\mathcal{L}$, y cuyas reglas de inferencia son las de LK más las cuatro reglas siguientes:

$\bigwedge_2$ **izquierda** $\quad \dfrac{\alpha(T),\,\Gamma \Rightarrow \Delta}{\bigwedge U\,\alpha(U),\,\Gamma \Rightarrow \Delta}, \qquad$ $\bigwedge_2$ **derecha** $\quad \dfrac{\Gamma \Rightarrow \Delta, \alpha(Y)}{\Gamma \Rightarrow \Delta, \bigwedge U\,\alpha(U)},$

$\bigvee_2$ **izquierda** $\quad \dfrac{\alpha(Y),\,\Gamma \Rightarrow \Delta}{\bigvee U\,\alpha(U),\,\Gamma \Rightarrow \Delta}, \qquad$ $\bigvee_2$ **derecha** $\quad \dfrac{\Gamma \Rightarrow \Delta,\, \alpha(T)}{\Gamma \Rightarrow \Delta,\, \bigvee U\,\alpha(U)},$

donde $T \equiv \beta(x_1,\ldots,x_r,\bar{y},\bar{Y})$ es una fórmula de Ψ, la variable X puede sustituirse por T en $\alpha(X)$ y la variable propia Y es una variable libre del mismo rango que U y que no aparece en el secuente inferior.

Si tomamos como Ψ el conjunto de las fórmulas de primer orden de $\mathcal{L}$, tenemos la *lógica de segundo orden predicativa,* que representaremos por B_0, mientras que si Ψ es el conjunto de todas las fórmulas de $\mathcal{L}$, tenemos la *lógica de segundo orden plena* B^2.

Podemos considerar tanto la variante reducida de $B(\Psi)$, que admite únicamente variables de rangos 0 y 1, como el caso general, con variables de todos los rangos posibles.

Siempre que consideremos una lógica de tipo $B(\Psi)$, supondremos que el conjunto Ψ contiene todas las fórmulas atómicas. Así, teniendo en cuenta que la regla izquierda del generalizador y la regla derecha del particularizador aplicadas a las fórmulas atómicas $T \equiv X(x_1,\ldots,x_r)$ son simplemente las reglas correspondientes de B, concluimos que las reglas de inferencia de $B(\Psi)$ incluyen a las de B.

El teorema 2.7 implica que $B(\Psi)$ es equivalente al cálculo deductivo que resulta de añadirle a B todos los axiomas de comprensión correspondientes a fórmulas de Ψ.

En particular, vemos que en la definición 2.6 podemos eliminar el esquema de comprensión y tomar como reglas de inferencia las de B_0 o las de B^2, según si consideramos la extensión predicativa o la extensión plena de K.

Notemos que en $B(\Psi)$ vale la regla inversa del generalizador

$$\frac{\Gamma \Rightarrow \Delta, \bigwedge U^r\, \alpha(U^r)}{\Gamma \Rightarrow \Delta,\, \alpha(T)},$$

donde $T \equiv \alpha(x_1, \ldots, x_r)$ es una fórmula de Ψ. En efecto, la prueba es:

$$\frac{\Gamma \Rightarrow \Delta, \bigwedge U^r\, \alpha(U^r) \qquad \dfrac{\alpha(T) \Rightarrow \alpha(T)}{\bigwedge U^r\, \alpha(U^r) \Rightarrow \alpha(T)}}{\Gamma \Rightarrow \Delta,\, \alpha(T)}$$

Ahora observamos que, de los axiomas I1, I2, I3 de LK_i, en la definición 2.6 sólo hemos incluido I1 como parte de los axiomas de K_0 o K^2. Esto se debe a que los restantes pueden deducirse del axioma 4. y más concretamente, de su restricción a variables de rango 1.

Para probarlo, conviene ver antes algunos hechos generales sobre el esquema 4. En primer lugar observamos que puede sustituirse por los axiomas $\Rightarrow I_r$, donde

$$I_r \equiv \bigwedge U \bigwedge \bar{u}\bar{v}(u_1 = v_1 \land \cdots \land u_r = v_r \land U(u_1\, \ldots, u_r) \to U(v_1, \ldots, v_r)).$$

En efecto, si partimos del axioma

$$x_1 = y_1, \ldots, x_r = y_r, X(x_1, \ldots, x_r) \Rightarrow X(y_1, \ldots, y_r),$$

aplicando las reglas obvias podemos llegar a I_r y, recíprocamente, de $\Rightarrow I_r$ podemos deducir el secuente

$$\Rightarrow \bigwedge \bar{u}\bar{v}(u_1 = v_1 \land \cdots \land u_r = v_r \land X(u_1\, \ldots, u_r) \to X(v_1, \ldots, v_r)),$$

por la regla inversa del generalizador de segundo orden, y aplicando a su vez la regla inversa del generalizador de primer orden y las del conjuntor y el implicador llegamos a 4).

En segundo lugar, vamos a probar que, en $B(\Psi)$, el secuente $\Rightarrow I_1$, es decir,

$$\Rightarrow \bigwedge U \bigwedge uv(u = v \land U(u) \to U(v)),$$

equivale al esquema

$$s = t,\ \alpha(s) \Rightarrow \alpha(t)$$

para fórmulas de Ψ.

En efecto,

$$\cfrac{\cfrac{s = t \land \alpha(s) \to \alpha(t) \Rightarrow s = t \land \alpha(s) \to \alpha(t)}{\bigwedge uv(u = v \land \alpha(u) \to \alpha(v)) \Rightarrow s = t \land \alpha(s) \to \alpha(t)}}{\bigwedge U \bigwedge uv(u = v \land U(u) \to U(v)) \Rightarrow s = t \land \alpha(s) \to \alpha(t)}$$

donde hemos usado la regla izquierda del generalizador con $T \equiv \alpha(x)$ (lo cual requiere que α esté en Ψ) y

$$\gamma(X) \equiv \bigwedge uv(u = v \wedge X(u) \to X(v)),$$

pues entonces $\gamma(T) \equiv \bigwedge uv(u = v \wedge \alpha(u) \to \alpha(v))$. Cortando con $\Rightarrow I_1$ llegamos a

$$\Rightarrow s = t \wedge \alpha(s) \to \alpha(t)$$

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:

$$x = y,\ Z(x) \Rightarrow Z(y)$$

(recordemos que estamos suponiendo que Ψ contiene las fórmulas $Z(x)$) podemos probar I_1 aplicando las reglas lógicas de forma obvia.

Con esto podemos probar que todos los axiomas del igualador pueden reducirse a una sentencia de primer orden y otra de segundo orden:

Teorema 2.9 *Si $\mathcal{L}$ es un lenguaje de segundo orden con igualador y Ψ es un conjunto de fórmulas de $\mathcal{L}$ que contiene a todas las fórmulas atómicas:*

1. *De I_1 se deducen en $B(\Psi)$ 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 I_1 y $x = x$ se deducen en $B(\Psi)$ 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) Es claro que de $\Rightarrow x = x$ se deduce $\Rightarrow \bigwedge u\, u = u$ y de ahí $\Rightarrow t = t$ para todo término t, es decir, que tenemos todos los axiomas de tipo I1. Ahora 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_1) implican la transitividad de la igualdad, y 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. ■

Así pues, la extensión predicativa de una teoría de primer orden no sólo extiende a LK, sino también a LK$_i$.

Intercambio de variables ligadas Terminamos esta sección con un resultado técnico que vamos a necesitar. Es válido igualmente para el cálculo secuencial de primer y de segundo orden.

Sea $\mathcal{L}$ un lenguaje formal de primer orden y pongamos que a cada variable ligada U le hacemos corresponder otra U^* del mismo rango (incluyendo el caso de rango 0). Para cada fórmula α, sea α^* la fórmula que resulta de cambiar en α cada variable ligada U por la variable U^*. Entonces, en B podemos demostrar los secuentes

$$\alpha \Rightarrow \alpha^*, \qquad \alpha^* \Rightarrow \alpha.$$

En efecto, la definición de α^* vale también para semifórmulas (entendiendo que sólo sustituimos las variables ligadas que aparecen ligadas). Vamos a probar que si $\alpha(\bar{U}, \bar{X})$ es una semifórmula cuyas variables que aparecen libres (de primer o segundo orden) son las indicadas, en B podemos demostrar

$$\alpha(\bar{Y}, \bar{X}) \Rightarrow \alpha^*(\bar{Y}, \bar{X}), \qquad \alpha^*(\bar{Y}, \bar{X}) \Rightarrow \alpha(\bar{Y}, \bar{X}),$$

donde $\bar{Y}$ son variables libres distintas de todas las que hay en α. Cuando esto se aplica al caso en que α es una fórmula, tenemos el resultado requerido.

Lo probamos por inducción sobre la longitud de α (o, más precisamente, lo suponemos cierto para las subsemifórmulas de α y lo probamos para α).

Si $\alpha \equiv X(t_1, \ldots, t_n)$, donde X es una variable (libre o ligada) o un relator, entonces α no tiene variables ligadas, luego $\alpha^* \equiv \alpha$ y la conclusión es trivial.

Si $\alpha \equiv \neg\beta$, tenemos que $\neg\alpha \equiv \neg\beta^*$, y basta aplicar las reglas del negador a la hipótesis de inducción. Lo mismo sucede si $\alpha \equiv \beta \vee \gamma$.

Si $\alpha \equiv \bigwedge u\, \beta(u, \bar{U}, \bar{X})$, entonces $\alpha^* \equiv \bigwedge u^* \beta^*(u^*, \bar{U}, \bar{X})$, y por hipótesis de inducción

$$\beta(y, \bar{Y}, \bar{X}) \Rightarrow \beta^*(y, \bar{Y}, \bar{X}), \qquad \beta^*(y, \bar{Y}, \bar{X}) \Rightarrow \beta(y, \bar{Y}, \bar{X}).$$

Aplicando las reglas del generalizador (primero la izquierda y luego la derecha, para que se cumplan las condiciones sobre la variable propia) obtenemos

$$\bigwedge u \beta(u, \bar{Y}, \bar{X}) \Rightarrow \bigwedge u^* \beta^*(u^*, \bar{Y}, \bar{X}), \quad \bigwedge u^* \beta^*(u^*, \bar{Y}, \bar{X}) \Rightarrow \bigwedge u \beta(u, \bar{Y}, \bar{X}).$$

El argumento vale tanto si las variables son de primer o de segundo orden y para los particularizadores. ■

Diremos que dos fórmulas son iguales salvo por sus variables ligadas si una se obtiene de otra cambiándole unas variables ligadas por otras. Lo que acabamos de probar implica que en cualquier demostración podemos cambiar cualquier fórmula de cualquier secuente por otra igual salvo por sus variables ligadas, sin más que cortar con el secuente $\alpha \Rightarrow \alpha^*$ o $\alpha^* \Rightarrow \alpha$, según el lado en el que esté la fórmula.

Por ello, podemos relajar las reglas de inferencia de cualquier cálculo secuencial que extienda a B admitiendo que en cada aplicación de una regla de inferencia una fórmula del secuente superior se diferencie en sus variables ligadas de la que debería estar en el secuente inferior, o que las dos fórmulas de corte se diferencien en sus variables ligadas, etc. En efecto, si tenemos una demostración en estas condiciones, siempre se puede convertir en una demostración en la que las reglas se aplican estrictamente introduciendo las variaciones de las fórmulas mediante cortes oportunos.

2.3 Reducción a la lógica de primer orden

En [LF 7.1] definimos los lenguajes de segundo orden como una clase particular de lenguajes de primer orden. Vamos a ver que (en el caso de lenguajes sin descriptor) la definición es equivalente a la que hemos adoptado aquí. Por comodidad repetimos la definición:

Definición 2.10 Un *lenguaje formal de segundo orden* es un lenguaje formal de primer orden con igualador dotado de 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 $r+1$. (Nos referiremos a estos relatores como *relatores estructurales.*) Usaremos la notación

$$t_0(t_1, \ldots, t_r) \equiv S_r(t_0, \ldots, t_r).$$

Llamaremos variable libre de índice i y rango r de $\mathcal{L}$ a la variable $X_i^r \equiv X_{\langle r,i\rangle}$, mientras que la variable ligada de índice i y rango r será $U_i^r \equiv U_{\langle r,i\rangle}$, donde $\langle r, i\rangle$ es el par definido en [LF 2.3]. A las variables de rango 0 las llamaremos *variables de primer orden,* mientras que a las de rango no nulo las llamaremos *variables de segundo orden.*

Tenemos así dos definiciones distintas de "lenguaje de segundo orden" que ahora vamos a relacionar. Si $\mathcal{L}$ es un lenguaje de segundo orden en el sentido de la definición 2.1, podemos considerarlo como lenguaje de primer orden sin más que "olvidar" la clasificación en rangos de sus variables, y a su vez, a partir de este lenguaje de primer orden podemos formar un lenguaje $\tilde{\mathcal{L}}$ de segundo orden recuperando dicha clasificación en rangos y añadiéndole relatores estructurales. Recíprocamente, partiendo de un lenguaje $\tilde{\mathcal{L}}$ en el sentido de la definición precedente, podemos obtener un lenguaje de segundo orden $\mathcal{L}$ en el sentido de 2.1 sin más que eliminar los relatores estructurales.

Por ejemplo, en esta situación, si X^r es una variable de rango r y $x_1, \ldots, x_r$ son variables de rango 0, la cadena de signos $X^r x_1 \cdots x_r$ es una fórmula de $\mathcal{L}$, pero no de $\tilde{\mathcal{L}}$, pero en $\tilde{\mathcal{L}}$ podemos considerar la fórmula $S_r(X^r, x_1, \ldots, x_r)$, y ambas las representamos como $X^r(x_1, \ldots, x_r)$.

Siguiendo con [LF 7.1], definimos las fórmulas de $\tilde{\mathcal{L}}$:

$$\textstyle\bigwedge_r U\,\alpha \equiv \bigwedge U(R_r U \rightarrow \alpha), \qquad \bigvee_r U\,\alpha \equiv \bigvee U(R_r U \land \alpha),$$

donde U es una variable de rango r.

Llamaremos *semitérminos estructurados* de $\tilde{\mathcal{L}}$ a los semitérminos de $\mathcal{L}$ que no contengan variables de segundo orden (a los que llamaremos *semitérminos estructurados de primer orden, o de rango* 0) 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 no estructural 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

$$\textstyle\neg\alpha, \quad \alpha \lor \beta, \quad \bigwedge_r U\,\alpha, \quad \bigvee_r U\,\alpha.$$

Claramente, si α y β son semifórmulas estructuradas, también lo son

$$\alpha \rightarrow \beta, \qquad \alpha \land \beta, \qquad \alpha \leftrightarrow \beta.$$

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. $\widetilde{\neg\alpha} \equiv \neg\tilde{\alpha}$, $\widetilde{\alpha \vee \beta} \equiv \tilde{\alpha} \vee \tilde{\beta}$.

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.

Es fácil ver que las fórmulas estructuradas de $\tilde{\mathcal{L}}$ son precisamente las traducciones de las fórmulas de $\mathcal{L}$.

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 $\bigvee_r U$. Vamos a ver que cada una de ellas admite una traducción a $\mathcal{L}$:

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,
$$(R^r t_1 \cdots t_r)^* \equiv \begin{cases} R^r t_1 \cdots t_r & \text{si los } t_i \text{ son estructurados de rango } 0, \\ \bigvee u\, u \neq u & \text{en caso contrario.} \end{cases}$$

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. $(\bigwedge_r U\, \alpha)^* \equiv \bigwedge U\, \alpha^*$, $(\bigvee_r U\, \alpha)^* \equiv \bigvee U\, \alpha^*$.

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 $\widetilde{(\alpha^*)} \equiv \alpha$. 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. ■

Ahora presentamos la definición que nos permitirá enunciar el resultado principal de esta sección:

Definición 2.11 Sea T un cálculo secuencial sobre un lenguaje formal $\mathcal{L}$ de segundo orden con igualador cuyas reglas de inferencia sean las de B y cuyos axiomas sean:

Axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica de $\mathcal{L}$.

Axiomas del igualador $\Rightarrow \bigwedge u\, u = u$ y $\Rightarrow I_n$, donde

$$I_n \equiv \bigwedge U^n \bigwedge \bar{u}\bar{v}(u_1 = v_1 \wedge \cdots \wedge u_n = v_n \wedge U^n(\bar{u}) \rightarrow U^n(\bar{v})).$$

Axiomas propios de la forma $\Rightarrow \delta$, donde δ es una sentencia de $\mathcal{L}$.

Sea $\tilde{T}$ el cálculo secuencial sobre el lenguaje $\tilde{\mathcal{L}}$ cuyas reglas de inferencia son las de LK y cuyos axiomas son:

Axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica α de $\tilde{\mathcal{L}}$.

Axiomas del igualador Los axiomas I1, I2, I3 de LK_i.

Axiomas estructurales

1. $\Rightarrow \bigwedge_* u_1 \cdots u_n\, R_0 t$,
   para todo término estructurado[3] $t(x_1, \ldots, x_n)$ de primer orden,
2. $\Rightarrow \bigvee_r U\, R_r U$, para todo $r \geq 0$.
3. $\Rightarrow \bigwedge_r U\, \neg R_s U$, para todo $r \neq s$.

Extensionalidad (para todo $r \geq 1$):

$$\Rightarrow \bigwedge_r UV(\bigwedge_0 \bar{u}(U(\bar{u}) \leftrightarrow V(\bar{u})) \rightarrow U = V).$$

Axiomas propios Las traducciones de los axiomas propios de T.

[3]Las variables x_i son todas las variables libres en t, y pueden ser de cualquier rango. El asterisco en $\bigwedge_*$ indica que cada una se cuantifica según su rango.

Notemos que los axiomas estructurales no constan de fórmulas estructuradas, al igual que el axioma de extensionalidad, que no es una fórmula estructurada porque $U = V$ no es una semifórmula estructurada (ni debe serlo, puesto que no es la traducción de ninguna semifórmula de segundo orden). En la práctica, para variables del mismo rango r, conviene considerar que

$$X = Y \equiv \bigwedge_0 \bar{u}(X(\bar{u}) \leftrightarrow Y(\bar{u}))$$

es una definición, de modo que el $=$ de la izquierda no es realmente el igualador de $\tilde{\mathcal{L}}$, pero hemos introducido el axioma de extensionalidad en la definición precedente (con el igualador "real") porque así demostraremos que, aunque convenga pensar en el igualador como un signo definido para términos de segundo orden, podemos suponer que el igualador "real" cumple la definición.

Nuestro propósito es demostrar que T y $\tilde{T}$ son esencialmente lo mismo. Antes necesitamos un resultado técnico:

Teorema 2.12 *En las condiciones anteriores, si una fórmula cuasiestructurada es demostrable en $\tilde{T}$, entonces admite una demostración formada únicamente por fórmulas cuasiestructuradas.*

Demostración: Sea una demostración en $\tilde{T}$ de un secuente $S \equiv \Gamma \Rightarrow \Delta$ formado por fórmulas cuasiestructuradas. Todos sus secuentes iniciales, excepto los de LK_i, son de la forma $\Rightarrow \delta$, donde δ es una sentencia estructurada. Llamemos Θ al conjunto formado por todas las sentencias δ que aparecen en los secuentes iniciales de este tipo en la demostración. Como son sentencias, podemos anteponer Θ en todos los secuentes de la demostración sin invalidar las variables propias. En particular, cada secuente inicial $\Rightarrow \delta$ se convierte en $\Theta \Rightarrow \delta$, que se deduce de $\delta \Rightarrow \delta$ por debilitación. Así obtenemos una demostración en LK_i del secuente $\Theta, \Gamma \Rightarrow \Delta$.

Por la observación tras el teorema de eliminación de cortes 3.5, existe una demostración en la que las únicas fórmulas de corte son igualdades $t_1 = t_2$. 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 las fórmulas de corte son cuasiestructuradas, todas las fórmulas de la demostración tienen que ser cuasiestructuradas, ya que si hubiera alguna que no lo fuera tendría que haber otra en el secuente final.

Mediante cortes con secuentes $\Rightarrow \delta$ podemos pasar de $\Theta, \Gamma \Rightarrow \Delta$ hasta $\Gamma \Rightarrow \Delta$, y tenemos así una demostración en $\tilde{T}$ formada por fórmulas cuasiestructuradas. ■

Teorema 2.13 *En las condiciones de la definición* 2.11*, una sentencia α de $\mathcal{L}$ es un teorema de T si y sólo si su traducción $\tilde{\alpha}$ es un teorema de $\tilde{T}$.*

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

$$\bigwedge u(R_0u \rightarrow u = u),$$

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

$$\bigwedge_n U \bigwedge_0 \bar{u}\bar{v}(u_1 = v_1 \wedge \cdots \wedge u_n = v_n \wedge U(\bar{u}) \rightarrow U(\bar{v})),$$

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:

$$\cfrac{\cfrac{\Theta_{S_1}, \tilde{\alpha}(t), \tilde{\Gamma} \Rightarrow \tilde{\Delta} \qquad R_0t \Rightarrow R_0t}{\Theta_{S_1}, R_0t, R_0t \rightarrow \tilde{\alpha}(t), \tilde{\Gamma} \Rightarrow \tilde{\Delta}}}{\Theta_{S_1}, R_0t, \bigwedge_0 u\, \tilde{\alpha}(u), \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

Ahora usamos que $\Theta_{S_1} \Rightarrow R_0t$ (por primer axioma estructural de $\tilde{T}$), por lo que la regla de corte nos permite eliminar R_0t 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_0x que está en Θ_{S_1} en $\bigvee u\, R_0u$, que es un teorema de $\tilde{T}$ (se deduce del primer axioma estructural), 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:

$$\dfrac{\dfrac{\Theta_{S_1},\, \tilde{\Gamma} \Rightarrow \tilde{\Delta},\, \tilde{\alpha}(Y)}{\Theta_{S_2},\, \tilde{\Gamma} \Rightarrow \tilde{\Delta},\, R_r Y \rightarrow \tilde{\alpha}(Y)}}{\Theta_{S_2},\, \tilde{\Gamma} \Rightarrow \tilde{\Delta},\, \bigwedge_r U\, \tilde{\alpha}(U)}$$

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:

$$\dfrac{\dfrac{\Theta_{S_1},\, \tilde{\alpha}(Y),\, \tilde{\Gamma} \Rightarrow \tilde{\Delta}}{\Theta_{S_2},\, R_r Y \wedge \tilde{\alpha}(Y),\, \tilde{\Gamma} \Rightarrow \tilde{\Delta}}}{\Theta_{S_2},\, \bigvee_r U\, \tilde{\alpha}(U),\, \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

Particularizador derecha Para la regla de primer orden, por los mismos argumentos empleados en la prueba de la regla izquierda del generalizador, tenemos:

$$\dfrac{\dfrac{\Theta_{S_1},\, \tilde{\Gamma} \Rightarrow \tilde{\Delta},\, \tilde{\alpha}(t) \qquad \Theta_{S_1} \Rightarrow R_0 t}{\Theta_{S_1},\, \tilde{\Gamma} \Rightarrow \tilde{\Delta},\, R_0 t \wedge \tilde{\alpha}(t)}}{\Theta_{S_1},\, \tilde{\Gamma} \Rightarrow \tilde{\Delta},\, \bigvee_0 u\, \tilde{\alpha}(u)}$$

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

$$\bigwedge\bar{u}(X(\bar{u}) \leftrightarrow Y(\bar{u})),\ s_1 = t_1, \ldots, s_r = t_r,\ X(\bar{s}) \Rightarrow Y(\bar{t})$$

y es fácil ver que se trata de un teorema de B.

3. Nos ocupamos ahora de los axiomas estructurales. En ellos hay que entender como parte de la definición de los axiomas que las variables tienen los rangos que les corresponde por el contexto.

   (a) La traducción de $\Rightarrow \bigwedge_* \bar{u}\, R_0 t(\bar{u})$ es $\Rightarrow \bigwedge\bar{u} \bigwedge u\, u = u$, que claramente es un teorema de B. no es cuasiestructurada.

   (b) La traducción de $\Rightarrow \bigvee_r U\, R_r U$ es $\Rightarrow \bigvee U \bigwedge u\, u = u$, y también es un teorema de B.

   (c) La traducción de $\Rightarrow \bigwedge_r U\, \neg R_s U$ (con $r \neq s$) es $\Rightarrow \bigwedge U\, \neg \bigvee u\, u \neq u$, y también es un teorema de B.

4. Consideremos el axioma de extensionalidad para rango r:

$$\bigwedge_r UV(\bigwedge_0 \bar{u}(U(\bar{u}) \leftrightarrow V(\bar{u})) \rightarrow U = V).$$

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.

5. Los últimos axiomas de $\tilde{T}$ son los de la forma $\Rightarrow \tilde{\alpha}$, donde α es un axioma propio de T. Su traducción es $\tilde{\alpha}^* \equiv \alpha$, luego la traducción del axioma es un teorema de T.

Ahora demostramos que las traducciones de las reglas de inferencia de la demostración siguen siendo válidas en B. Las únicas reglas para las que esto no es inmediato son las de los cuantificadores. Antes de entrar a analizarlas conviene hacer una observación general: en cada uso de una regla derecha del generalizador o izquierda del particularizador cuya fórmula principal sea $\bigwedge_r U\,\alpha(U)$ o $\bigvee_r U\,\alpha(U)$ podemos cambiar la variable propia Y para que tenga precisamente rango r.

En efecto, sólo tenemos que elegir una variable nueva Y' de rango r que no aparezca en la demostración, y si cambiamos Y por Y' en todos los secuentes que están por encima del secuente superior de la regla, todos los axiomas siguen siendo axiomas (pues esto es claramente cierto para los axiomas lógicos y los del igualador y trivialmente para los restantes, porque no tienen variables libres) y ninguna regla de inferencia deja de ser válida porque en ella cambiemos una variable libre por otra nueva (que no aparezca en los demás secuentes). Más precisamente, si hacemos este cambio en una variable propia que no tenga por encima ninguna otra, y vamos descendiendo, cada cambio no afectará a las variables propias que haya por encima, luego podemos conseguir que todas ellas tengan el rango requerido.

Pasamos ya a analizar las reglas:

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. ■

Así pues, es equivalente demostrar un teorema $\Rightarrow \alpha$ en T que demostrar $\Rightarrow \tilde{\alpha}$ en $\tilde{T}$, con la diferencia de que $\tilde{T}$ es una teoría de primer orden, por lo que en lugar del cálculo secuencial podemos usar el cálculo deductivo "a la Hilbert". Esto nos lleva a la definición siguiente con la que enunciaremos de forma definitiva el resultado que hemos obtenido:

Definición 2.14 Sea T un cálculo secuencial sobre un lenguaje formal $\mathcal{L}$ de segundo orden con igualador cuyas reglas de inferencia sean las de B y cuyos axiomas sean:

Axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica de $\mathcal{L}$.

Axiomas del igualador $\Rightarrow \bigwedge u\, u = u$ y $\Rightarrow I_n$, donde

$$I_n \equiv \bigwedge U^n \bigwedge \bar{u}\bar{v}(u_1 = v_1 \wedge \cdots \wedge u_n = v_n \wedge U^n(\bar{u}) \rightarrow U^n(\bar{v})).$$

Axiomas propios de la forma $\Rightarrow \delta$, donde δ es una sentencia de $\mathcal{L}$.

Llamaremos *traducción de primer orden* de T a la teoría axiomática de primer orden (es decir, una extensión de $K_{\tilde{\mathcal{L}}}$) cuyos axiomas propios son los siguientes:

Axiomas estructurales

1. $\bigwedge_* u_1 \cdots u_n\, R_0 t$,
   para todo término estructurado[4] $t(x_1, \ldots, x_n)$ de primer orden,
2. $\bigvee_r U\, R_r U$, para todo $r \geq 0$,
3. $\bigwedge_r U\, \neg R_s U$.

Extensionalidad (para todo $r \geq 1$):

$$\bigwedge_r UV(\bigwedge_0 \bar{u}(U(\bar{u}) \leftrightarrow V(\bar{u})) \rightarrow U = V).$$

Axiomas propios Las traducciones de los axiomas propios de T.

El teorema anterior, junto con la observación posterior al teorema 1.11, hacen inmediato el teorema siguiente:

[4]Las variables x_i son todas las variables libres en t, y pueden ser de cualquier rango. El asterisco en $\bigwedge_*$ indica que cada una se cuantifica según su rango.

Teorema 2.15 *Una sentencia α cumple que $\Rightarrow \alpha$ es un teorema de un cálculo secuencial de segundo orden en las condiciones de la definición* 2.14 *si y sólo si su traducción $\tilde{\alpha}$ es un teorema de la traducción de primer orden de T.*

Notemos que el requisito de que los axiomas propios de T sean sentencias sólo es relevante a la hora de calcular sus traducciones, pues, por lo demás, cualquier secuente es equivalente en B a uno de la forma $\Rightarrow \delta$, donde δ es una sentencia. En otras palabras, el teorema anterior es válido para cualquier cálculo secuencial T de segundo orden que cuente con los axiomas del igualador con tal de que, en su reducción de primer orden, tomemos como axiomas propios las traducciones de los axiomas propios de T expresados en la forma requerida $\Rightarrow \delta$, donde δ es una sentencia.

2.4 La aritmética de segundo orden

Definición 2.16 La *Aritmética de Peano de segundo orden* AP^2 se define como el cálculo secuencial sobre el lenguaje $\mathcal{L}_a^2$ de la aritmética de segundo orden cuyas reglas de inferencia son las de B y cuyos axiomas son:

1. Los axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica α de $\mathcal{L}_a^2$,
2. Los axiomas propios de AP distintos de los de inducción (enunciados en la definición 1.13),
3. $\Rightarrow x = x$,
4. $x = y, X(x) \Rightarrow X(y)$.
5. Comprensión: $\Rightarrow \bigvee X \bigwedge u(X(u) \leftrightarrow \alpha(u))$,
   para toda fórmula $\alpha(x)$ de $\mathcal{L}_a^2$ (que puede tener más variables libres).
6. Inducción: $X(0),\ \bigwedge u(X(u) \rightarrow X(u')) \Rightarrow X(x)$.

Si restringimos el axioma de comprensión a fórmulas aritméticas (es decir, sin variables ligadas de segundo orden) tenemos la teoría conocida como ACA_0 (por “axioma de comprensión aritmética”).

Más en general, si Ψ es un conjunto de fórmulas de $\mathcal{L}_a^2$ que contiene a las fórmulas atómicas, llamamos $\mathrm{AP}^2(\Psi)$ a la teoría que resulta de restringir el axioma de comprensión a fórmulas de Ψ.

Según el teorema 2.7, $\mathrm{AP}^2(\Psi)$ equivale a la teoría que resulta de eliminar el esquema de comprensión y considerar las reglas de inferencia de $B(\Psi)$. En particular, en AP^2 y en ACA_0 podemos eliminar el esquema de comprensión y considerar las reglas de B^2 o B_0, respectivamente.

El esquema 4. puede sustituirse obviamente por $\Rightarrow I_1$, donde

$$I_1 \equiv \bigwedge U \bigwedge uv(u = v \wedge U(u) \rightarrow U(v)),$$

y el teorema teorema 2.9 nos da que $\Rightarrow I_1$, junto con $\Rightarrow x = x$, implica en $B(\Psi)$ los axiomas del igualador de primer orden.

Observemos que el axioma de inducción es claramente equivalente en B al secuente $\Rightarrow I_0$, donde

$$I_0 \equiv \bigwedge U(U(0) \land \bigwedge u(U(u) \to U(u')) \to \bigwedge u\, U(u)),$$

el cual es a su vez equivalente en $B(\Psi)$ al esquema formado por los secuentes $\Rightarrow \mathrm{Ind}(\alpha)$, donde

$$\mathrm{Ind}(\alpha) \equiv \alpha(0) \land \bigwedge u(\alpha(u) \to \alpha(u')) \to \bigwedge u \alpha(u),$$

para toda fórmula de Ψ.

En efecto, aplicando a $\Rightarrow I_0$ la regla inversa del generalizador con $T \equiv \alpha$ obtenemos $\mathrm{Ind}(\alpha)$, mientras que considerando la fórmula atómica $\alpha \equiv X(x)$ obtenemos $\mathrm{Ind}(\alpha) \equiv I_0$.

En particular esto implica que tanto ACA_0 como AP^2 extienden a AP, pues en ambas teorías se pueden demostrar todos los casos del esquema de inducción para fórmulas sin variables de segundo orden. Sin embargo, en AP^2 contamos con la inducción para fórmulas arbitrarias, y en ACA_0 para fórmulas aritméticas (que pueden incluir variables libres de segundo orden).

Más en general, si Φ es cualquier conjunto de fórmulas de $\mathcal{L}_a^2$, podemos considerar la teoría $\mathrm{AP}^2(\Phi, \Psi)$ que resulta de restringir el esquema de comprensión de AP^2 a fórmulas de Ψ y el axioma de inducción se sustituye por el esquema $\Rightarrow \mathrm{Ind}(\alpha)$ con α en Φ.

La prueba del teorema 1.12 se adapta trivialmente para probar que en la teoría $\mathrm{AP}^2(\Phi, \Psi)$ podemos sustituir el esquema de inducción por la regla Φ-IND:

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

en la que t es un término arbitrario, $\alpha(y)$ es una fórmula de Φ y la variable propia y no aparece libre en ninguna otra fórmula distinta de las dos en las que aparece explícitamente.

Teorema 2.17 *Si Φ y Ψ son conjuntos de fórmulas de modo que Ψ contiene al menos las fórmulas atómicas, un cálculo secuencial equivalente a* $\mathrm{AP}^2(\Phi, \Psi)$ *(en el sentido de que tiene los mismos teoremas) es el que consta de las reglas de inferencia de $B(\Psi)$ más la regla Φ-IND y de los axiomas siguientes:*

1. *Los axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica α de $\mathcal{L}_a^2$,*
2. *Los axiomas propios de* AP *(enunciados en la definición 1.13),*
3. $\Rightarrow x = x$,
4. $x = y, X(x) \Rightarrow X(y)$.

Veremos (teorema 2.23) que ACA_0 es una extensión conservativa de AP. En cambio, si queremos obtener una extensión conservativa de $\mathrm{I}\Sigma_1$, sucede que, o bien tenemos que restringir el principio de inducción a fórmulas de $\mathcal{L}_a$ (es decir, que ni siquiera admitan variables libres de segundo orden), lo cual es muy débil, o bien tenemos que restringir el esquema de comprensión a fórmulas Δ_1^0. La segunda opción es preferible y nos lleva a la teoría siguiente:

Definición 2.18 La teoría[5] ACR_0 es el cálculo secuencial sobre el lenguaje $\mathcal{L}_a^2$ cuyas reglas de inferencia son las de B y cuyos axiomas son:

1. Los axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica α de $\mathcal{L}_a^2$,
2. Los axiomas propios de AP distintos de los de inducción (enunciados en la definición 1.13),
3. $\Rightarrow x = x$,
4. $x = y, X(x) \Rightarrow X(y)$.
5. Δ_1^0-COMPRENSIÓN: $\alpha \leftrightarrow \beta \Rightarrow \bigvee U \bigwedge u(U(u) \leftrightarrow \alpha(u))$,
   para toda fórmula $\alpha(x)$ de tipo Σ_1^0 y toda fórmula $\beta(x)$ de tipo Π_1^0,
6. Σ_1^0-INDUCCIÓN: $\Rightarrow \alpha(0) \land \bigwedge u(\alpha(u) \rightarrow \alpha(u')) \rightarrow \bigwedge u\alpha(u)$,
   para toda fórmula α de tipo Σ_1^0.

Como en el caso de $\mathrm{AP}^2(\Phi, \Psi)$, en ACR_0 se demuestran los axiomas del igualador de primer orden, y el principio de inducción incluye como casos particulares los correspondientes a fórmulas Σ_1, por lo que ACR_0 extiende a $\mathrm{I}\Sigma_1$.

A la hora de estudiar ACR_0, el esquema de Δ_1^0-comprensión es complicado de tratar, pues no sabemos cómo sustituirlo por reglas de inferencia (es posible hacerlo, pero el proceso es mucho más laborioso). Veremos que podemos evitar esto usando la teoría siguiente, cuya definición concreta está pensada para que se le pueda aplicar el teorema de eliminación de cortes libres que probaremos en el próximo capítulo:

Definición 2.19 La teoría ARP_0^2 es el cálculo se cuencial sobre el lenguaje $\mathcal{L}_{\mathrm{arp}}^2$ cuyas reglas de inferencia son[6] las de $B(\Delta_0^0)$ más Σ_1^0-IND, y cuyos axiomas son:

1. Los axiomas lógicos $\alpha \Rightarrow \alpha$, para toda fórmula atómica α,
2. Los secuentes $\Rightarrow \alpha$, donde α recorre las definiciones de los funtores de $\mathcal{L}_{\mathrm{arp}}$ (definición [LF 1.8]), pero con las variables sustituidas por términos arbitrarios.

[5]Las siglas corresponden a "axioma de comprensión recursiva", y el subíndice indica que el principio de inducción está restringido a fórmulas de tipo Σ_1^0, de modo que ACR es la teoría que resulta de tomar como axiomas todas las fórmulas $\mathrm{Ind}(\alpha)$, para toda fórmula α de $\mathcal{L}_a^2$.

[6]Tomamos como fórmulas Δ_0^0 de $\mathcal{L}_{\mathrm{arp}}^2$ las dadas por la definición 2.3, pero para el lenguaje formal $\mathcal{L}_{\mathrm{arp}}^2$, es decir, las fórmulas con cuantificadores acotados por términos de $\mathcal{L}_{\mathrm{arp}}^2$, que son los mismos términos de $\mathcal{L}_{\mathrm{arp}}$.

3. $St = 0 \Rightarrow$,

4. $St_1 = St_2 \Rightarrow t_1 = t_2$,

5. $\Rightarrow t = t$,

6. $t_1 = t_2,\ \alpha(t_1) \Rightarrow \alpha(t_2)$,
   para toda fórmula $\alpha(x)$ de tipo Δ_0^0 (que puede tener más variables libres).

Observemos que los esquemas 5. y 6. incluyen como casos particulares

$$\Rightarrow x = x, \qquad x = y,\ X(x) \Rightarrow X(y),$$

de los cuales se deducen los axiomas

$$\Rightarrow \bigwedge u\, u = u, \qquad \Rightarrow I_1 \equiv \ \Rightarrow \bigwedge Uuv(u = v \wedge U(u) \to U(v))$$

considerados en 2.14, y de éstos se deducen a su vez todos los casos de 5. y 6., usando las reglas inversas del generalizador. Hemos elegido estos axiomas para que sean cerrados para sustitución, es decir, que al sustituir una variable de primer orden por un término en un axioma obtengamos otro axioma y al sustituir una variable de segundo orden por una fórmula Δ_0^0 en un axioma (y el único que posee variables de segundo orden es 6.) obtengamos otro axioma.

El teorema 2.9 nos da que en ARP_0^2 se demuestran todos los axiomas del igualador de primer orden, por lo que ARP_0^2 extiende a ARP (a la teoría ARP^+ definida en 1.15) y, de hecho, a la teoría que resulta de añadirle esquema de Σ_1-inducción, que coincide con la extensión de $\mathrm{I}\Sigma_1$ con los funtores de $\mathcal{L}_{\mathrm{arp}}$ considerada en [LF 4.48].

Como en el caso de $\mathcal{L}_a^2$, la regla Σ_1^0-IND puede sustituirse por el esquema de Σ_1^0-inducción de ACR_0, y el teorema 2.7 nos dice que podemos restringir las reglas lógicas a las de B si añadimos el esquema de Δ_0^0-comprensión, de donde se sigue inmediatamente que la traducción de primer orden de ARP_0^2 en el sentido de 2.14 es precisamente la teoría axiomática a la que hemos dado el mismo nombre en [LF 7.13], luego, según [LF 7.14], sabemos que ARP_0^2 es una extensión intrascendente de ACR_0^-, donde ACR_0^- es la teoría que resulta de restringir el esquema de Δ_1^0-comprensión de ACR_0 al esquema de Δ_0^0-comprensión.

2.5 Eliminación de cortes

En este punto el lector debería releer la sección 3.1 prestando ahora atención a la los casos correspondientes a la lógica de segundo orden hasta entender el enunciado del teorema de eliminación de cortes libres para la lógica de segundo orden:

Teorema 3.4 *En un cálculo secuencial de segundo orden que conste de los axiomas y reglas de inferencia de $B(\Psi)$ más un conjunto $\mathfrak{S}$ de axiomas propios cerrados para sustitución (y, en el caso de que el lenguaje formal sea $\mathcal{L}_a^2$ o $\mathcal{L}_{\mathrm{arp}}^2$, admitimos también la regla* Φ-IND, *para un conjunto de fórmulas Φ cerrado para sustitución), todo teorema admite una demostración sin cortes libres.*

En particular tenemos el teorema de eliminación de cortes 3.6, que afirma simplemente que todo teorema de B_0 puede demostrarse sin usar la regla de corte. Como consecuencia:

Teorema 2.20 *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 en LK. ■

Para probar los resultados anunciados en las secciones precedentes necesitamos una aplicación más sofisticada del teorema de eliminación de cortes.

Teorema 2.21 *Sea $\mathcal{L}$ un lenguaje formal de segundo orden, sea Ψ un conjunto de fórmulas de $\mathcal{L}$ que contenga al menos a las fórmulas atómicas, sea $\Gamma \Rightarrow \Delta$ un secuente en $\mathcal{L}$ formado por fórmulas de primer orden y consideremos unas fórmulas de primer orden $\gamma_1(X_{1,1}^{r_{1,1}}, \ldots, X_{1,n_1}^{r_{1,n_1}}), \ldots, \gamma_m(X_{m,1}^{r_{m,1}}, \ldots, X_{m,n_m}^{r_{m,n_m}})$ cada una de las cuales tenga únicamente las variables libres indicadas (todas de segundo orden). Entonces, el secuente*

$$\bigwedge \bar{U} \gamma_1(U_{1,1}^{r_{1,1}}, \ldots, U_{1,n_1}^{r_{1,n_1}}), \ldots, \bigwedge \bar{U} \gamma_m(U_{m,1}^{r_{m,1}}, \ldots, U_{m,n_m}^{r_{m,n_m}}),\ \Gamma \Rightarrow \Delta$$

(donde $\bar{U}$ recorre todas las variables de segundo orden mostradas a continuación) es demostrable en $B(\Psi)$ si y sólo si existen fórmulas $T_{ijk} \equiv \alpha_{ijk}(x_{ij1}, \ldots, x_{ijr_{i,j}})$ en Ψ, para $i = 1, \ldots, m$, $j = 1, \ldots, n_i$, $k = 1, \ldots, s_{i,j}$, tales que el secuente

$$\{\gamma_i(T_{i1k}, \ldots, T_{in_ik})\},\ \Gamma \Rightarrow \Delta$$

(donde las llaves indican que en el antecedente están todas las fórmulas correspondientes a todos los índices i, j, k) es demostrable en B sin hacer uso de las reglas de inferencia de segundo orden.

Demostración: Observemos que en $B(\Psi)$ se demuestra

$$\bigwedge U_{i,1}^{r_{i,1}}, \ldots, U_{i,n_i}^{r_{i,n_i}} \gamma_i(U_{i,1}^{r_{i,1}}, \ldots, U_{i,n_i}^{r_{i,n_i}}) \Rightarrow \gamma_i(T_{ijk}).$$

Basta partir del teorema $\gamma_i(T_{ijk}) \Rightarrow \gamma_i(T_{ijk})$ y aplicar la regla izquierda del generalizador de segundo orden. Por lo tanto, prolongando una demostración de $\{\gamma_i(T_{ijk})\}, \Gamma \Rightarrow \Delta$ mediante cortes con los secuentes anteriores, obtenemos una demostración del primer secuente del enunciado.

Recíprocamente, supongamos que el secuente del enunciado es demostrable en $B(\Psi)$. 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 (que no puede ser la de corte).

Si se trata de una regla de segundo orden, necesariamente será la regla izquierda del generalizador, luego la demostración acaba así:

$$\frac{\bigwedge\bar{U}\gamma_1, \ldots, \bigwedge\bar{U}\gamma_{i_0}(T, U_{i_0,2}^{r_{i_0,2}} \ldots, U_{i_0,n_{i_0}}^{r_{i_0,n_{i_0}}}), \ldots, \bigwedge\bar{U}\gamma_m, \Gamma \Rightarrow \Delta}{\bigwedge\bar{U}\gamma_1(U_{1,1}^{r_{1,1}}, \ldots, U_{1,n_1}^{r_{1,n_1}}), \ldots, \bigwedge\bar{U}\gamma_m(U_{m,1}^{r_{m,1}}, \ldots, U_{m,n_m}^{r_{m,n_m}}), \Gamma \Rightarrow \Delta},$$

para cierta fórmula T de Ψ. Podemos aplicar la hipótesis de inducción a dicho secuente superior, lo que nos da una demostración (sin reglas de segundo orden) de

$$\{\gamma_i(T_{i1k}, \ldots, T_{in_ik})\}, \gamma_{i_0}(T, T_{i_0,2,k}, \ldots, T_{i_0,n_{i_0},k}), \Gamma \Rightarrow \Delta,$$

para $i \neq i_0$, y basta definir $T_{i_0,1,k} \equiv T$.

Los demás casos son triviales. Consideremos, por ejemplo, el de la regla izquierda del disyuntor:

$$\frac{\bigwedge\bar{U}\gamma_1, \ldots, \bigwedge\bar{U}\gamma_m, \alpha, \Gamma' \Rightarrow \Delta \qquad \bigwedge\bar{U}\gamma_1, \ldots, \bigwedge\bar{U}\gamma_m, \beta, \Gamma' \Rightarrow \Delta}{\bigwedge\bar{U}\gamma_1, \ldots, \bigwedge\bar{U}\gamma_m, \alpha, \alpha \vee \beta, \Gamma' \Rightarrow \Delta}$$

donde Γ' resulta de eliminar $\alpha \vee \beta$ en Γ. La hipótesis de inducción nos da demostraciones (sin reglas de segundo orden) de los secuentes

$$\{\gamma_i(T_{i1k}, \ldots, T_{in_ik})\}, \alpha, \Gamma' \Rightarrow \Delta, \qquad \{\gamma_i(T'_{i1k}, \ldots, T_{in_ik})\}, \beta, \Gamma' \Rightarrow \Delta$$

en las condiciones del enunciado, y basta aplicar la regla izquierda del disyuntor (renumerando las fórmulas T_{ijk} y T'_{ijk} para formar una única sucesión). Es este caso el que hace que no podamos considerar una única fórmula T_{ij} para variable $X_{ij}^{r_{i,j}}$. ■

Finalmente:

Teorema 2.22 *Si K es un cálculo secuencial de primer orden (con igualador), su extensión predicativa K_0 es una extensión conservativa de K, es decir, que todo secuente sin variables de segundo orden demostrable en K_0 es, de hecho, demostrable en K.*

DEMOSTRACIÓN: Sea $\Gamma \Rightarrow \Delta$ un secuente demostrable en K_0 que no contenga variables de segundo orden y sea D una demostración en K_0. De acuerdo con las observaciones tras la definición 2.8, podemos considerar que las reglas de inferencia de K_0 son las de B_0, y que sus axiomas son:

1. Axiomas lógicos $\alpha \Rightarrow \alpha$, donde α es una fórmula atómica, que puede tener variables de segundo orden.

2. Secuentes $\Rightarrow I_r$, donde
$$I_r \equiv \bigwedge U \bigwedge \bar{u}\bar{v}(u_1 = v_1 \wedge \cdots \wedge u_r = v_r \wedge U(u_1 \ldots, u_r) \to U(v_1, \ldots, v_r)).$$

3. El secuente $\Rightarrow \bigwedge u(u = u)$ y los axiomas propios de K, que no tienen variables de segundo orden (y que podemos suponer que no tienen variables libres, sin más que cuantificar universalmente todas las que tengan).

En la prueba aparecerá un número finito de secuentes iniciales de tipo $\Rightarrow I_r$, digamos que n es el máximo r que aparece. Por otra parte, si en la prueba aparecen los axiomas propios $S_1, \ldots, S_m$ y llamamos $\bar{S}_i$ a la fórmula asociada a S_i (la disyunción de las negaciones de las fórmulas de su antecedente y de las fórmulas de su consecuente), tenemos que a partir de $\Rightarrow \bar{S}_i$ se puede deducir S_i, luego podemos añadir estas deducciones a D para tener una nueva demostración con axiomas
$$\Rightarrow I_1, \quad \ldots, \quad \Rightarrow I_n, \quad \Rightarrow \bar{S}_0, \quad \ldots, \quad \Rightarrow \bar{S}_r,$$
donde $\bar{S}_0 \equiv \bigvee u\, u = u$. Si añadimos estas fórmulas a todos los antecedentes de todos los secuentes de la demostración[7] y demostramos los secuentes
$$I_1, \ldots, I_n, \bar{S}_0, \ldots, \bar{S}_r \Rightarrow \bar{S}_i$$
deduciendo $\bar{S}_i \Rightarrow \bar{S}_i$ y luego aplicando la regla de debilitación, obtenemos una demostración en B_0 del secuente
$$I_1, \ldots, I_n, \Gamma^* \Rightarrow \Delta,$$
donde Γ^* resulta de añadir a Γ las fórmulas $\bar{S}_0, \ldots, \bar{S}_n$, con lo que sólo contiene variables de primer orden, al igual que Δ.

Tenemos que $I_r \equiv \bigwedge U^r \gamma_r(U^r)$, luego estamos en las condiciones del teorema anterior, según el cual existen fórmulas de primer orden T_{ik} de modo que en B podemos demostrar el secuente
$$\{\gamma_i(T_{ik})\}, \Gamma^* \Rightarrow \Delta$$
sin usar reglas de inferencia de segundo orden. Como en los axiomas de B sólo hay fórmulas atómicas (por lo tanto, sin variables ligadas de segundo orden) en toda la demostración no puede haber variables ligadas de segundo orden.

[7] Aquí es fundamental que sean sentencias, pues si tuvieran variables libres podrían invalidar las reglas en las que alguna de ellas fuera la variable propia.

En dicha demostración, podemos sustituir cada variable libre de segundo orden X^r por la fórmula $\delta(x_1,\ldots,x_r) \equiv x_1 = x_1$, y el resultado es también una demostración en B, ya que cada axioma se transforma en un axioma y ninguna regla de inferencia deja de ser válida por la sustitución (notemos que no se introduce ninguna variable nueva, luego las variable propias de cada regla siguen siéndolo). El secuente final será de la forma

$$\{\gamma_i(T'_{ik})\}, \Gamma^* \Rightarrow \Delta,$$

pues sólo habremos modificado las fórmulas de primer orden T_{ik}. En esta demostración ya no aparecen variables de segundo orden, luego es en realidad una demostración en LK. Los secuentes $\Rightarrow \bar{S}_i$ son teoremas de K, luego, cortando con ellos, obtenemos una demostración en K del secuente

$$\{\gamma_i(T'_{ik})\}, \Gamma \Rightarrow \Delta.$$

Finalmente, si $T'_{ik} \equiv \alpha_{ik}(x_1,\ldots,x_i)$, donde α_{ik} no tiene variables de segundo orden, tenemos que

$$\gamma_i(T'_{ij}) \equiv \bigwedge \bar{u}\bar{v}(u_1 = v_1 \land \cdots \land u_i = v_i \land \alpha_{ik}(u_1\ \ldots,u_i) \to \alpha_{ik}(v_1,\ldots,v_i)),$$

luego $\Rightarrow \gamma_i(T'_{ik})$ es un teorema de LK_i, luego de K. Cortando con estos teoremas obtenemos una demostración en K de $\Gamma \Rightarrow \Delta$. ■

En el caso aritmético podemos afinar un poco más:

Teorema 2.23 ACA_0 *es una extensión conservativa de* AP.

DEMOSTRACIÓN: La prueba es esencialmente la misma que la del teorema anterior, con la diferencia de que, en lugar de los axiomas $I_1,\ldots,I_n$, ahora tenemos únicamente I_1, pero por otra parte tenemos el axioma de inducción, que es equivalente a

$$I_0 \equiv \bigwedge U(U(0) \land \bigwedge u(U(u) \to U(u')) \to \bigwedge u\, U(u)).$$

El mismo argumento empleado en el teorema anterior nos da que, si $\Gamma \Rightarrow \Delta$ es un secuente demostrable en ACA_0 que no contiene variables de segundo orden, entonces en AP podemos demostrar un secuente de la forma

$$\{\gamma_i(T'_{ik})\}, \Gamma \Rightarrow \Delta,$$

para $i = 0, 1$, donde

$$\gamma_0(T'_{0,k}) \equiv \alpha_{0k}(0) \land \bigwedge u(\alpha_{0k}(u) \to \alpha_{0k}(u')) \to \bigwedge u\, \alpha_{0k}(u),$$

donde a su vez α_{0k} es una fórmula de $\mathcal{L}_a$ (sin variables de segundo orden), luego $\gamma_0(T'_{0,k})$ es un teorema de AP, luego en AP podemos demostrar $\Gamma \Rightarrow \Delta$. ■

Tenemos pendiente demostrar que ACR_0 es una extensión conservativa de $\mathrm{I}\Sigma_1$, pero la estructura lógica del esquema de Δ^0_1-comprensión complica sustancialmente cualquier intento de prueba directa. De momento vamos a probar lo siguiente:

Teorema 2.24 *La teoría* ACR_0^- *que resulta de sustituir el esquema de* Δ_1^0*-comprensión de* ACR_0 *por el de* Δ_0^0*-comprensión es una extensión conservativa de* $\mathrm{I}\Sigma_1$.

DEMOSTRACIÓN: Explícitamente, ACR_0^- es el cálculo secuencial cuyas reglas de inferencia son las de $B(\Delta_0^0)$ y cuyos axiomas son:

1. Axiomas lógicos $\alpha \Rightarrow \alpha$, donde α es una fórmula atómica, que puede tener variables de segundo orden.

2. El secuente $\Rightarrow I_1$, donde
$$I_1 \equiv \bigwedge U \bigwedge uv(u = v \wedge U(u) \to U(v)).$$

3. El secuente $\Rightarrow \bigwedge u(u = u)$ y los axiomas propios de AP distintos de los de inducción (enunciados en la definición 1.13), que no tienen variables de segundo orden (y que podemos suponer que no tienen variables libres, sin más que cuantificar universalmente todas las que tengan).

4. Axiomas de inducción para fórmulas γ de tipo Σ_1^0, que podemos clausurar en la forma $\Rightarrow \bigwedge \bar{U}\,\mathrm{Ind}(\gamma)$, donde
$$\mathrm{Ind}(\gamma) \equiv \bigwedge \bar{v}((\gamma(0) \wedge \bigwedge u(\gamma(u) \to \gamma(u'))) \to \bigwedge u\,\gamma(u)).$$

Si un secuente $\Gamma \Rightarrow \Delta$ sin variables de segundo orden es demostrable en esta teoría, la demostración usará un número finito de axiomas de inducción, digamos los correspondientes a $\gamma_1, \ldots, \gamma_m$. Además, llamamos
$$\gamma_0(U) \equiv \bigwedge uv(u = v \wedge U(u) \to U(v)).$$

El mismo razonamiento empleado en la prueba de 2.22 nos permite transformar la demostración en una demostración en $B(\Delta_0^0)$ de un secuente de la forma
$$I_1, \bigwedge \bar{U}\,\mathrm{Ind}(\gamma_1), \ldots \bigwedge \bar{U}\,\mathrm{Ind}(\gamma_m), \Gamma^* \Rightarrow \Delta,$$
donde Γ^* resulta de añadirle a Γ sentencias correspondientes a axiomas de tipo 3. Por el teorema 2.21, en B se puede demostrar un secuente de la forma
$$\{\gamma_0(T_{0,1,k})\}, \{\mathrm{Ind}(\gamma_i(T_{i1k}, \ldots, T_{in_ik}))\}, \Gamma^* \Rightarrow \Delta$$
sin usar reglas de inferencia de segundo orden, donde $T_{ijk} \equiv \alpha_{ijk}(x)$ es una fórmula de tipo Δ_0^0. Como no se usan reglas de segundo orden y en los axiomas no hay variables ligadas de segundo orden, en toda la demostración no hay variables ligadas de segundo orden. Como en la prueba de 2.22, en la demostración podemos sustituir cada variable libre de segundo orden por la fórmula $\delta(x) \equiv x = x$, y así obtenemos otra demostración sin variables de segundo orden cuyo secuente final será de la forma
$$\{\gamma_0(T'_{0,1,k})\}, \{\mathrm{Ind}(\gamma'_{i,k})\}, \Gamma^* \Rightarrow \Delta,$$

donde ahora todas las fórmulas γ_i' son de tipo Σ_1. Como en esta demostración ya no hay variables de segundo orden, se trata de una demostración en LK. Al igual que en 2.22, tenemos que $\Rightarrow \gamma_0(T_{0,1,k})$ es un teorema de LK_i, mientras que los secuentes $\Rightarrow \mathrm{Ind}(\gamma_{i,k}')$ son parte del esquema de Σ_1-inducción, es decir, son axiomas de $\mathrm{I}\Sigma_1$. Igualmente, los secuentes que hay en Γ^* que no están en Γ son de la forma $\Rightarrow S$, donde S es un axioma de $\mathrm{I}\Sigma_1$. Cortando con todos estos secuentes obtenemos una demostración en $\mathrm{I}\Sigma_1$ del secuente $\Gamma \Rightarrow \Delta$. ■

2.6 El lema de König débil

En [LF 7.33] hemos definido la teoría axiomática LKD_0 como la que resulta de añadirle a ACR_0 el Lema de König Débil (LKD). Aunque LKD no puede demostrarse en ACR_0, en esta sección vamos a demostrar que ACR_0 y LKD_0 tienen los mismos teoremas de primer orden:

Teorema 2.25 *Una fórmula de primer orden es demostrable en* LKD_0 *si y sólo si es demostrable en* ACR_0.

Más aún, demostraremos que LKD_0 es una extensión conservativa de $\mathrm{I}\Sigma_1$:

Teorema 2.26 *Una fórmula sin variables de segundo orden es demostrable en* LKD_0 *si y sólo si es demostrable en* $\mathrm{I}\Sigma_1$.

En particular, esto implica que ACR_0 también es una extensión conservativa de $\mathrm{I}\Sigma_1$:

Teorema 2.27 *Una fórmula sin variables de segundo orden es demostrable en* ACR_0 *si y sólo si es demostrable en* $\mathrm{I}\Sigma_1$.

Para probar estos teoremas vamos a considerar varios cálculos secuenciales. En primer lugar consideramos la teoría ARP_0^2 definida en 2.19, que ha sido definida de modo que satisface las hipótesis del teorema de eliminación de cortes libres. En virtud de [LF 7.14], sabemos que ARP_0^2 es una extensión intrascendente de la teoría ACR_0^- que resulta de sustituir el esquema de Δ_1^0-comprensión de ACR_0 por el esquema de Δ_0^0-comprensión y, a su vez, 2.24 nos da que ACR_0^- es una extensión conservativa de $\mathrm{I}\Sigma_1$.

	Δ_0^0-comprensión	Δ_1^0-comprensión	LKD
$\mathcal{L}_{\mathrm{arp}}^2$	ARP_0^2	ACR_0^+	LKD_0^+
$\mathcal{L}_a^2$	ACR_0^-	ACR_0	LKD_0

Llamamos ACR_0^+ al cálculo secuencial que resulta de añadir a ARP_0^2 el esquema de Δ_1^0-comprensión, que extiende a ACR_0, y LKD_0^+ al cálculo secuencial que resulta de añadirle a ACR_0^+ el lema de König débil LKD, que extiende a LKD_0.

Basta demostrar el teorema siguiente:

Teorema 2.28 *Toda fórmula de primer orden de* $\mathcal{L}_a^2$ *demostrable en* LKD_0^+ *es demostrable, de hecho, en* ARP_0^2.

En efecto, admitiendo este teorema, si una fórmula de primer orden de $\mathcal{L}_a^2$ es demostrable en LKD_0, en particular lo es en LKD_0^+, luego, por 2.28, es demostrable en ARP_0^2, luego por [LF 7.14] lo es en ACR_0^-, luego en particular en ACR_0, y tenemos probado el teorema 2.25. Si además la fórmula no tiene variables de segundo orden, el teorema 2.24 nos da que es demostrable en $\mathrm{I}\Sigma_1$, y tenemos probado 2.26. El teorema 2.27 es consecuencia inmediata de éste.

Para probar 2.28, empezamos probando el teorema siguiente, que viene a decir que para comprobar si se cumple una fórmula de tipo Δ_0^0 en la que aparecen unos parámetros $X_1, \ldots, X_m$, en realidad basta conocer si los primeros números naturales pertenecen o no a ellos, donde "los primeros" significa los que no superen una cota que depende únicamente de los parámetros de primer orden:

Teorema 2.29 *Para cada fórmula* $\alpha(X_1, \ldots, X_m, x_1, \ldots, x_n)$ *de tipo* Δ_0^0 *cuyas variables libres de primer orden estén entre las indicadas (aunque puede tener variables de segundo orden cualesquiera) existe un término* $t_\alpha(x_1, \ldots, x_n)$ *(con las variables de primer orden entre las indicadas y sin variables de segundo orden) tal que, si llamamos* $\alpha^*(s_1, \ldots, s_m, x_1, \ldots, x_n)$ *a la fórmula que resulta de sustituir cada subfórmula* $X_i(t)$ *en* α *por* $(s_i)_t = 1$*, en* ACR_0^- *se demuestra:*

$$\bigwedge \bar{U} \bigwedge \bar{u} \bigwedge \bar{s}(s_1 \in 2^{<\omega} \land \ell(s_1) \geq t_\alpha(\bar{u}) \land \cdots \land s_m \in 2^{<\omega} \land \ell(s_m) \geq t_\alpha(\bar{u}) \land$$

$$\bigwedge i < \ell(s_1)(U_i(i) \leftrightarrow (s_1)_i = 1) \land \cdots \land \bigwedge i < \ell(s_m)(U_m(i) \leftrightarrow (s_m)_i = 1) \rightarrow$$

$$\alpha(\bar{U}, \bar{u}) \leftrightarrow \alpha^*(\bar{s}, \bar{u})),$$

así como

$$\bigwedge \bar{u}\bar{v}(u_1 \leq v_1 \land \cdots \land u_n \leq v_n \rightarrow t_\alpha(\bar{u}) \leq t_\alpha(\bar{v})).$$

Notemos que las hipótesis de la primera fórmula del enunciado dicen que $s_i \subset \chi_{U_i}$, luego lo que se afirma es que $\alpha(\bar{U}, \bar{u})$ es equivalente a la fórmula que resulta de sustituir cada U_i por una sección inicial suficientemente larga de χ_{Ui}, donde "suficientemente larga" viene determinado por el término $t_\alpha(\bar{u})$.

Demostración: Construimos t_α por recurrencia sobre α y demostramos que en ACR_0^- se puede probar lo requerido por inducción sobre α (la fórmula es de tipo Σ_1, pues afirma la existencia de una demostración).

Si α es de la forma $t_1 = t_2$, $t_1 \leq t_2$ o $Y(t)$, para una variable $Y \not\equiv X_j$, basta tomar $t_\alpha \equiv 0$, pues en este caso $\alpha^* \equiv \alpha$ y las fórmulas del enunciado se prueban trivialmente en ACR_0^-.

Si $\alpha \equiv X_j(t(\bar{x}))$, entonces $\alpha^* \equiv (s_j)_t = 1$ y basta tomar

$$t_\alpha(\bar{x}) \equiv \max\{w \mid \bigvee u_1 \leq x_1 \cdots \bigvee u_n \leq x_n \, w = t(\bar{u})\} + 1.$$

Esta definición garantiza la segunda propiedad del enunciado (la monotonía), y la primera se cumple también, pues si en ACR_0^- suponemos que $s_j \in 2^{<\omega}$, $\ell(s_j) \geq t_\alpha(\bar{x}) \geq t(\bar{x}) + 1$ y

$$\bigwedge i < \ell(s)(X_j(i) \leftrightarrow (s_j)_i = 1),$$

en particular tenemos que $X_j(t(\bar{x})) \leftrightarrow (s_j)_{t(\bar{x})} = 1$, que es lo que hay que probar.

Si $\alpha \equiv \neg\beta$, basta tomar $t_\alpha \equiv t_\beta$, pues si suponemos (para $j = 1, \ldots, m$) $s_j \in 2^{<\omega}$, $\ell(s_j) \geq t_\alpha(\bar{x})$ y que $\bigwedge i < t_\alpha(\bar{x})(X_j(i) \leftrightarrow (s_j)_i = 1)$, por hipótesis de inducción tenemos que

$$\beta(\bar{X}, \bar{x}) \leftrightarrow \beta^*(\bar{s}, \bar{x}),$$

pero, teniendo en cuenta que $\alpha^* \equiv \neg\beta^*$, esto implica que $\alpha(\bar{X}, \bar{x}) \leftrightarrow \alpha^*(\bar{s}, \bar{x})$.

Si $\alpha \equiv \beta \vee \gamma$, definimos $t_\alpha \equiv \text{máx}\{t_\beta, t_\gamma\}$. Así, si suponemos (para todo $j = 1, \ldots, m$) que $s_j \in 2^{<\omega}$, $\ell(s_j) \geq t_\alpha(\bar{x})$ y que $\bigwedge i < t_\alpha(\bar{x})(X_j(i) \leftrightarrow (s_j)_i = 1)$, en particular $\ell(s_j) \geq t_\beta(\bar{x}), t_\gamma(\bar{x})$, luego

$$\bigwedge i < t_\beta(\bar{x})(X_j(i) \leftrightarrow (s_j)_i = 1), \qquad \bigwedge i < t_\gamma(\bar{x})(X_j(i) \leftrightarrow)s_j)_i = 1),$$

luego por hipótesis de inducción

$$\beta(\bar{X}, \bar{x}) \leftrightarrow \beta^*(\bar{s}, \bar{x}), \qquad \gamma(\bar{X}, \bar{x}) \leftrightarrow \gamma^*(s, \bar{x}),$$

y como $\alpha^* \equiv \beta^* \vee \gamma^*$, de aquí se sigue que $\alpha(\bar{X}, \bar{x}) \leftrightarrow \alpha^*(\bar{s}, \bar{x})$.

Si $\alpha \equiv \bigwedge u \leq t(\bar{x})\, \beta(\bar{X}, u, \bar{x})$, definimos

$$t_\alpha(\bar{x}) \equiv \text{máx}\{w \mid \bigvee u_1 \leq x_1 \cdots \bigvee u_n \leq x_n \bigvee u \leq t(\bar{u})\, w = t_\beta(u, \bar{u})\}.$$

Claramente esta definición garantiza la condición de monotonía, y además, si suponemos que $s_j \in 2^{<\omega}$, $\ell(s_j) \geq t_\alpha(\bar{x})$ y que $\bigwedge i < t_\alpha(\bar{x})(X_j(i) \leftrightarrow (s_j)_i = 1)$, si $y \leq t(\bar{x})$ se cumple que $t_\beta(y, \bar{x}) \leq t_\alpha(\bar{x})$, por lo que

$$\bigwedge i < t_\beta(y, \bar{x})(X_j(i) \leftrightarrow (s_j)_i = 1),$$

luego, por hipótesis de inducción, $\beta(\bar{X}, y, \bar{x}) \leftrightarrow \beta^*(\bar{s}, y, \bar{x})$, luego

$$\bigwedge u \leq t(\bar{x})\, \beta(\bar{X}, u, \bar{x}) \leftrightarrow \bigwedge u \leq t(\bar{x})\, \beta^*(\bar{s}, u, \bar{x}),$$

y la última fórmula es $\alpha^*(\bar{s}, \bar{x})$.

En el caso en que $\alpha \equiv \bigvee u \leq t(\bar{x})\, \beta(\bar{X}, u, \bar{x})$ definimos t_α igualmente y la comprobación es análoga a la del caso anterior. ■

Conviene trabajar con una forma equivalente de LKD:

Teorema 2.30 *En* ACR_0^+*, el lema de König débil* LKD *es equivalente al esquema:*

$$(\mathrm{LKD}^*) \qquad \bigwedge U \bigvee u\, \alpha(U, u, x_1, \ldots, x_n) \rightarrow \bigvee w \bigwedge U \bigvee u \leq w\, \alpha(U, u, x_1, \ldots, x_n),$$

donde $\alpha(X, x, x_1, \ldots, x_n)$ *es cualquier fórmula de tipo* Δ_0^0 *cuyas variables libres de primer orden están entre las indicadas, pero puede tener más variables de segundo orden.*

Demostración: Veamos en primer lugar cómo demostrar LKD a partir de LKD*. Para ello tomamos un árbol $A \subset 2^{<\omega}$, suponemos que no tiene caminos, y vamos a demostrar que es finito.

Si X es un conjunto cualquiera, podemos considerar su función característica $\chi_X : \mathbb{N} \longrightarrow \{0,1\}$, dada por $\chi_X(n) = 1 \leftrightarrow X(n)$. Notemos que

$$\chi_X = (X \times \{1\}) \cup ((\mathbb{N} \setminus X) \times \{0\})$$

está bien definido en ACR$_0$. Por hipótesis, χ_X no es un camino en A, luego existe un $s \in 2^{<\omega}$ tal que $\bigwedge i < \ell(s)\, s_i = \chi_X(i)$ y $\neg A(s)$. Explícitamente, llamamos

$$\alpha(X, A, s) \equiv \bigwedge i < \ell(s)\, s_i \leq 1 \wedge \bigwedge i < \ell(s)(s_i = 1 \leftrightarrow X(i)) \wedge \neg A(s),$$

que es una fórmula de tipo Δ_0^0 en $\mathcal{L}^2_{\mathrm{arp}}$, y tenemos que $\bigwedge U \bigvee u\, \alpha(U, A, u)$. Por el caso particular del esquema del enunciado correspondiente a esta fórmula α, tenemos que existe un z tal que $\bigwedge U \bigvee u \leq z\, \alpha(U, A, u)$. Explícitamente:

$$\bigwedge U \bigvee u \leq z (\bigwedge i < u\, u_i = \chi_U(i) \wedge \neg A(u)).$$

Veamos que $A \subset 2^{<z}$, lo que implica que A es finito. En efecto, si $t \in 2^{<\omega}$ cumple $\ell(t) \geq z$, definimos $X = \{i \mid t_i = 1\}$, de modo que $t \subset \chi_X$. Tenemos que existe un $s \leq z$ tal que $s \subset \chi_X \wedge \neg A(s)$. Como $\ell(s) \leq s \leq z \leq \ell(t)$, de hecho $s \subset t$ y, como A es un árbol, esto implica $\neg A(t)$.

Recíprocamente, supongamos LKD, así como que $\bigwedge U \bigvee u\, \alpha(U, u, \bar{x})$, y consideremos el término $t_\alpha(x, \bar{x})$ dado por el teorema 2.29. Consideramos el conjunto

$$A = \{s \mid \bigwedge i < \ell(s)(s_i = 0 \vee s_i = 1) \wedge$$

$$\bigwedge u \leq \ell(s)(t_\alpha(u, \bar{x}) \leq \ell(s) \rightarrow \neg\alpha^*(s|_{t_\alpha(u,\bar{x})}, u, \bar{x}))\}.$$

Claramente, la definición es Δ_1^0 y A es un árbol. Veamos que es finito. En caso contrario, por LKD, tiene un camino F. Sea $X = \{i \mid F(i) = 1\}$. Por hipótesis existe un x tal que $\alpha(X, x, \bar{x})$. Sea $n = \text{máx}\{x, t_\alpha(x, \bar{x})\}$. Como F es un camino, tenemos que $s = F^n \in A$. Observemos que esto implica que

$$\bigwedge i < \ell(s)(X(i) \leftrightarrow s_i = 1).$$

Como $x \leq \ell(s)$ y $t_\alpha(x, \bar{x}) \leq \ell(s)$, la definición de A nos da entonces que $\neg\alpha^*(s|_{t_\alpha(x,\bar{x})}, x, \bar{x})$, y el teorema 2.29 nos da $\neg\alpha(X, x, \bar{x})$, en contra de la elección de x.

Por lo tanto, A es finito, luego existe un w tal que $A \subset 2^{<w}$. Vamos a probar que $\bigwedge U \bigvee u \leq w\, \alpha(U, w, \bar{x})$. Para ello tomamos un conjunto X arbitrario, consideramos su función característica χ_X y la sucesión $s = \chi_X^w$. Tenemos que $s \notin A$, luego existe un $x \leq \ell(s) = w$ tal que $t_\alpha(x, \bar{x}) \leq w$ y $\alpha^*(s|_{t_\alpha(x,\bar{x})}, x, \bar{x})$, pero esto implica $\alpha(X, x, \bar{x})$. ■

Nota Esta forma equivalente del lema de König débil tiene una interpretación topológica que aquí no vamos a necesitar, pero que tiene interés. Consideremos una fórmula $\alpha(X, x)$ de tipo Δ_0^0, que puede tener más variables libres, y vamos a usar la notación

$$X \in B_x \equiv \alpha(X, x).$$

Cada conjunto X determina y está determinado por su función característica χ_X, por lo que podemos pensar en él como en una sucesión de ceros y unos, es decir, un elemento del cubo de Cantor 2^ω. A su vez, podemos pensar que α define un conjunto $B_x \subset \{0,1\}^\omega$. El teorema 2.29 afirma que B_x es abierto para la topología producto (considerando en $\{0,1\}$ la topología discreta), pues lo que dice es que la condición $X \in B_x$ depende únicamente de $\chi_X|_{t_\alpha(x)}$, es decir, de los valores que toma X en un número finito de coordenadas.

Por lo tanto, el antecedente de LKD* afirma que los conjuntos B_x son un cubrimiento abierto de $B_x \subset \{0,1\}^\omega$, mientras que el consecuente afirma que basta un número finito de ellos para cubrir todo el espacio. En suma, el lema de König débil es una consecuencia de la compacidad del cubo de Cantor. Existen versiones alternativas que son, de hecho, equivalentes a dicha compacidad. ■

Ahora podemos desprendernos del "técnicamente molesto" principio de Δ_1^0-comprensión:

Teorema 2.31 *La teoría* LKD_0^+ *es equivalente a* ARP_0^2 *más el esquema*

$$(\mathrm{LKD}^*) \quad \bigwedge U \bigvee u\, \alpha(U, u, x_1, \ldots, x_n) \to \bigvee w \bigwedge U \bigvee u \leq w\, \alpha(U, u, x_1, \ldots, x_n),$$

donde $\alpha(X, x, x_1, \ldots, x_n)$ *es cualquier fórmula de tipo* Δ_0^0 *cuyas variables libres de primer orden están entre las indicadas, pero puede tener más variables de segundo orden.*

DEMOSTRACIÓN: Por el teorema anterior, LKD_0^+ es equivalente a ACR_0^+ más el esquema del enunciado, es decir, a ARP_0^2 más el esquema de Δ_1^0-comprensión más LKD*. Por lo tanto, basta probar que en ARP_0^2 más el LKD* se puede demostrar el esquema de Δ_1^0-comprensión. Por lo tanto, suponemos que α y β son fórmulas de tipo Δ_0^0 tales que

$$\bigvee v \alpha(x, v) \leftrightarrow \bigwedge v\, \beta(x, v),$$

y tenemos que probar que cualquiera de estas dos fórmulas define un conjunto. Para ello observamos que

$$\bigwedge w \bigvee U \bigwedge u \leq w \bigwedge xv \leq u((\alpha(x, v) \to U(x)) \land (U(x) \to \beta(x, v))).$$

En efecto, dado w, basta definir (por Δ_0^0-comprensión)

$$U = \{x \mid \bigvee v \leq w\, \alpha(x, v)\}.$$

Así, si $u \leq w$, $x, v \leq u$ y $\alpha(x, v)$, tenemos que $\bigvee v \leq w\, \alpha(x, v)$, luego $U(x)$. Por otra parte, si $U(x)$, entonces $\bigvee v\, \alpha(x, v)$, y esto equivale a $\bigwedge v\, \beta(x, v)$, luego $\beta(x, v)$.

La fórmula tras $\bigwedge u \leq w$ es de tipo Δ_0^0, luego por LKD* podemos concluir que

$$\bigvee U \bigwedge u \bigwedge xv \leq u((\alpha(x,v) \to U(x)) \land (U(x) \to \beta(x,v))).$$

Pero la acotación por u es redundante, por lo que en realidad tenemos

$$\bigvee U \bigwedge xv((\alpha(x,v) \to U(x)) \land (U(x) \to \beta(x,v))).$$

De aquí se sigue que

$$\bigwedge x(U(x) \leftrightarrow \bigvee v\, \alpha(x,v)),$$

pues si se cumple $U(x)$, entonces $\bigwedge v\, \beta(x,v)$, y esto implica $\bigvee v\, \alpha(x,v)$. ■

En otras palabras, hemos demostrado que LKD implica el esquema de Δ_1^0-comprensión en ARP_0^2, por lo que para pasar de ARP_0^2 a LKD_0^+ basta añadir LKD. Seguidamente transformamos el esquema del teorema anterior en una regla de inferencia:

Teorema 2.32 *La teoría* LKD_0^+ *es equivalente a* ARP_0^2 *más la regla de inferencia:*

$$(\mathrm{LKD}^*) \qquad \frac{\Gamma \Rightarrow \bigvee u\, \alpha(Y,u,\bar{x})}{\Gamma \Rightarrow \bigvee w \bigwedge s \in \{0,1\}^{t_\alpha(w,\bar{x})} \bigvee u \leq w\, \alpha^*(s,u,\bar{x}),}$$

donde α *es de tipo* Δ_0^0*, la fórmula* α^* *y el término* t_α *son los descritos en el teorema* 2.29 *y la variable* Y *es propia (es decir, que no puede aparecer en ninguna otra fórmula de la regla).*

Demostración: Sólo tenemos que probar que la regla del enunciado es equivalente en ARP_0^2 al esquema LKD* considerado en el teorema anterior o, equivalentemente, a los secuentes

$$\bigwedge U \bigvee u\, \alpha(U,u,\bar{x}) \Rightarrow \bigvee w \bigwedge U \bigvee u \leq w\, \alpha(U,u,\bar{x}),$$

para toda fórmula α de tipo Δ_0^0.

Para ello demostramos en primer lugar que en ARP_0^2 se demuestra que

$$\bigvee w \bigwedge U \bigvee u \leq w\, \alpha(U,u,\bar{x}) \leftrightarrow \bigvee w \bigwedge s \in \{0,1\}^{t_\alpha(w,\bar{x})} \bigvee u \leq w\, \alpha^*(s,u,\bar{x}).$$

Basta probar que

$$\bigwedge U \bigvee u \leq w\, \alpha(U,u,\bar{x}) \leftrightarrow \bigwedge s \in \{0,1\}^{t_\alpha(w,\bar{x})} \bigvee u \leq w\, \alpha^*(s,u,\bar{x}).$$

En efecto, si suponemos $\bigwedge U \bigvee u \leq w\, \alpha(U,u,\bar{x})$ y tomamos $s \in \{0,1\}^{t_\alpha(w,\bar{x})}$, consideramos el conjunto $X = \{n \mid \bigvee i < t_\alpha(w,\bar{x})\, s_i = 1\}$, de modo que se cumple $\bigwedge i < \ell(s)(X(i) \leftrightarrow s_i = 1)$. Por hipótesis existe un $x \leq w$ tal que $\alpha(X,x,\bar{x})$. Por la monotonía de t_α tenemos que $t_\alpha(x,\bar{x}) \leq t_\alpha(w,\bar{x}) = \ell(s)$, luego el teorema 2.29 nos da que $\alpha(X,x,\bar{x}) \leftrightarrow \alpha^*(s,x,\bar{x})$ y se cumple que $\bigvee u \leq w\, \alpha^*(s,u,\bar{x})$.

Recíprocamente, si suponemos $\bigwedge s \in \{0,1\}^{t_\alpha(w,\bar{x})} \bigvee u \leq w\, \alpha^*(s,u,\bar{x})$ y tomamos un conjunto X arbitrario, tomamos $s = \chi_X^{t_\alpha(w,\bar{x})}$, de modo que se cumple $\bigwedge i < \ell(s)(X(i) \leftrightarrow s_i = 1)$. Por hipótesis existe $x \leq w$ tal que $\alpha^*(s,x,\bar{x})$. La monotonía de t_α nos da que $t_\alpha(u,\bar{x}) \leq t_\alpha(w,\bar{x}) = \ell(s)$, luego el teorema 2.29 nos da que $\alpha(X,x,\bar{x}) \leftrightarrow \alpha^*(s,x,\bar{x})$, luego concluimos que $\bigvee u \leq w\, \alpha(X,u,\bar{x})$.

Por consiguiente, basta probar que añadir la regla LKD* del enunciado es equivalente tomar como axiomas los secuentes

$$\bigwedge U \bigvee u\, \alpha(U,u,\bar{x}) \Rightarrow \bigvee w \bigwedge s \in \{0,1\}^{t_\alpha(w,\bar{x})} \bigvee u \leq w\, \alpha^*(s,u,\bar{x}).$$

Si suponemos estos axiomas, es fácil demostrar la regla: partiendo del secuente $\Gamma \Rightarrow \bigvee u\, \alpha(Y,u,\bar{x})$, pasamos a $\Gamma \Rightarrow \bigwedge U \bigvee u\, \alpha(U,u,\bar{x})$ y cortamos con el axioma. Recíprocamente, si suponemos la regla, podemos demostrar el secuente

$$\bigvee u\, \alpha(Y,u,\bar{x}) \Rightarrow \bigvee u\, \alpha(Y,u,\bar{x}),$$

de ahí pasamos a

$$\bigwedge U \bigvee u\, \alpha(U,u,\bar{x}) \Rightarrow \bigvee u\, \alpha(Y,u,\bar{x}),$$

con lo que la variable Y sólo está libre en el consecuente, y aplicando la regla obtenemos el axioma. ■

En este punto interviene el resultado clave:

Teorema 2.33 *Consideremos un secuente de la forma*

$$\Gamma,\ \bigvee u_1 \alpha_1(u_1,\bar{X}), \ldots, \bigvee u_n \alpha_n(u_n,\bar{X}) \Rightarrow$$

$$\Delta,\ \bigvee v_1 \beta_1(v_1,\bar{X}), \ldots, \bigvee v_m \beta_m(v_m,\bar{X}),$$

donde:

1. *Las fórmulas α_i, β_i son de tipo Δ_0^0, con lo que las fórmulas completas son de tipo Σ_1^0 (pero admitimos que algunas puedan ser simplemente $\alpha_i(\bar{X})$ o $\beta_i(\bar{X})$, es decir, de tipo Δ_0^0),*

2. *Γ y Δ no contienen fórmulas de tipo Σ_1^0 ni en ellas aparecen las variables $X_1,\ldots,X_r$ que hemos abreviado por $\bar{X}$ (y nos referiremos a ellas como* parámetros especiales *del secuente),*

3. *En las fórmulas Σ_1^0 puede haber otras variables libres de segundo orden que sí que aparezcan en fórmulas de Γ o Δ y también variables libres de primer orden.*

Supongamos que S tiene una demostración en ARP_0^2 *en la que toda fórmula de corte es de tipo Σ_1^0 y en la que no aparecen variables ligadas de segundo orden. Entonces, en en* ARP_0^2 *podemos demostrar también el secuente*

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 \cdots u_n \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \cdots \vee \neg\alpha_n(u_n,\bar{U}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U}) \vee \cdots \vee \bigvee v_m \leq w\, \beta_m(v_m,\bar{U})).$$

DEMOSTRACIÓN: Llamemos *transformado* del secuente descrito al principio del enunciado al descrito al final, de modo que se trata de probar que si el secuente dado es demostrable en ARP_0^2 en las condiciones indicadas, también es demostrable su transformado. Para ello basta probar inductivamente que en ARP_0^2 se puede probar el transformado de cada uno de los secuentes que aparecen en la demostración dada. Notemos que todos ellos se pueden expresar en la forma que indica el enunciado sin más que separar las fórmulas de tipo Σ_1^0 que contienen. Los secuentes iniciales no tienen cuantificadores, por lo que, con la notación del enunciado, son de la forma $\Gamma \Rightarrow \Delta$, y obviamente permiten deducir su transformado $\Gamma \wedge \neg\Delta \Rightarrow$ sin más que aplicar las reglas del negador y el conjuntor.

Por lo tanto, sólo tenemos que probar que el transformado del secuente inferior de cualquier regla de inferencia puede deducirse en ARP_0^2 a partir del secuente o los secuentes superiores de la regla. Como en la demostración de partida no hay variables ligadas de segundo orden, no tenemos que comprobar las reglas para los cuantificadores de segundo orden.

Debilitación Si la fórmula principal no es de tipo Σ_1^0, el transformado del secuente inferior se deduce del transformado del secuente superior por la misma regla de debilitación. En caso contrario, el transformado del secuente inferior se obtiene del transformado del secuente superior añadiendo una fórmula en la conjunción del antecedente o en la disyunción del consecuente de la implicación, luego claramente es una consecuencia lógica de éste.

¬ izquierda Si la fórmula auxiliar α no es de tipo Σ_1^0, la conclusión es trivial (pues α está en Δ en el secuente superior y $\neg\alpha$ está en Γ en el secuente inferior, por lo que sus transformados son claramente equivalentes). En caso contrario, y considerando únicamente tres fórmulas Σ_1^0 por simplificar la notación, la regla es

$$\frac{\Gamma,\ \bigvee u_1\,\alpha_1(u_1,\bar{X},\bar{Y}) \Rightarrow \Delta,\ \bigvee v_1\,\beta_1(v_1,\bar{X},\bar{Y}),\ \bigvee v_2\,\beta_2(v_2,\bar{Y})}{\Gamma',\ \bigvee u_1\,\alpha_1(u_1,\bar{X}),\Rightarrow \Delta,\ \bigvee v_1\,\beta_1(v_1,\bar{X})},$$

donde Γ' resulta de añadir a Γ la fórmula principal: $\neg\bigvee v_2\,\beta_2(v_2,\bar{Y})$. Notemos que hemos distinguido los parámetros especiales $\bar{Y}$ que aparecen en la fórmula auxiliar (y que ya no son especiales en el secuente inferior) de los parámetros especiales $\bar{X}$ que están en otras fórmulas de tipo Σ_1^0 del secuente.

Por hipótesis de inducción, en ARP_0^2 se puede demostrar el secuente

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \vee$$
$$\bigvee v_1 \leq w\,\beta_1(v_1,\bar{U},\bar{V}) \vee \bigvee v_2 \leq w\,\beta_2(v_2,\bar{U})),$$

y tenemos que probar

$$\neg\bigvee v_2\,\beta_2(v_2,\bar{Y}),\ \Gamma \wedge \neg\Delta \Rightarrow$$
$$\bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U},\bar{Y}) \vee \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U},\bar{Y})).$$

Para ello suponemos[8] $\neg\bigvee v_2\,\beta_2(v_2,\bar Y)$, $\Gamma\wedge\neg\Delta$, tenemos que

$$\bigwedge u_1\bigvee w\bigwedge\bar U\bar V(\neg\alpha_1(u_1,\bar U,\bar V)\vee$$
$$\bigvee v_1\leq w\,\beta_1(v_1,\bar U,\bar V)\vee\bigvee v_2\leq w\,\beta_2(v_2,\bar U)).$$

Fijado un x_1 arbitrario, de aquí se sigue que existe un z tal que

$$\bigwedge\bar U\bar V(\neg\alpha_1(x_1,\bar U,\bar V)\vee\bigvee v_1\leq w\,\beta_1(v_1,\bar U,\bar V)\vee\bigvee v_2\leq z\,\beta_2(v_2,\bar U)).$$

Fijados unos parámetros $\bar X$ arbitrarios, tenemos que

$$\neg\alpha_1(x_1,\bar X,\bar Y)\vee\bigvee v_1\leq w\,\beta_1(v_1,\bar X,\bar Y)\vee\bigvee v_2\leq z\,\beta_2(v_2,\bar Y),$$

pero la hipótesis $\neg\bigvee v_2\,\beta_2(v_2,\bar Y)$ nos permite pasar a

$$\neg\alpha_1(x_1,\bar X)\vee\bigvee v_1\leq w\,\beta_1(v_1,\bar X),$$

con lo que hemos probado el transformado del secuente inferior de la regla.

¬ derecha Nuevamente, la conclusión es trivial si la fórmula auxiliar no es de tipo Σ^0_1. En otro caso la regla es

$$\frac{\Gamma,\ \bigvee u_1\,\alpha_1(u_1,\bar X,\bar Y),\bigvee u_2\alpha_2(u_2,\bar Y)\Rightarrow\Delta,\ \bigvee v_1\beta_1(v_1,\bar X,\bar Y)}{\Gamma\bigvee u_1\,\alpha_1(u_1,\bar X)\Rightarrow\Delta',\ \bigvee v_1\,\beta_1(v_1,\bar X),}$$

donde Δ' resulta de añadirle a Δ la fórmula principal $\neg\bigvee u_2\,\alpha_2(u_2,\bar Y)$.

Por hipótesis de inducción, tenemos

$$\Gamma\wedge\neg\Delta\Rightarrow\bigwedge u_1u_2\bigvee w\bigwedge\bar U\bar V(\neg\alpha_1(u_1,\bar U,\bar V)\vee\neg\alpha_2(u_2,\bar V)\vee$$
$$\bigvee v_1\leq w\,\beta_1(v_1,\bar U,\bar V))$$

y tenemos que demostrar

$$\Gamma\wedge\neg\Delta\wedge\neg\neg\bigvee u_2\,\alpha_2(u_2,\bar Y)\Rightarrow$$
$$\bigwedge u_1\bigvee w\bigwedge\bar U(\neg\alpha_1(u_1,\bar U,\bar Y)\vee\bigvee v_1\leq w\,\beta_1(v_1,\bar U,\bar Y)).$$

Para ello suponemos el antecedente, lo que nos da

$$\bigwedge u_1u_2\bigvee w\bigwedge\bar U\bar V(\neg\alpha_1(u_1,\bar U,\bar V)\vee\neg\alpha_2(u_2,\bar V)\vee\bigvee v_1\leq w\,\beta_1(v_1,\bar U,\bar V)).$$

Tomamos un x_1 arbitrario y un x_2 que cumpla $\alpha_2(x_2,\bar Y)$. Entonces tenemos que existe un z tal que

$$\bigwedge\bar U\bar V(\neg\alpha_1(x_1,\bar U,\bar V)\vee\neg\alpha_2(x_2,\bar V)\vee\bigvee v_1\leq z\,\beta_1(v_1,\bar U,\bar V)),$$

Tomamos unos parámetros $\bar X$ arbitrarios, de modo que

$$\neg\alpha_1(x_1,\bar X,\bar Y)\vee\neg\alpha_2(x_2,\bar Y)\vee\bigvee v_1\leq z\,\beta_1(v_1,\bar X,\bar Y),$$

y, como $\alpha_2(x_2,\bar Y)$, de aquí se sigue

$$\neg\alpha_1(x_1,\bar X,\bar Y)\vee\bigvee v_1\leq z\,\beta_1(v_1,\bar X,\bar Y),$$

lo que prueba el transformado del secuente inferior de la regla.

[8] Por simplicidad vamos a demostrar el consecuente a partir del antecedente considerando a ARP^2_0 como teoría de primer orden.

$\vee$ **izquierda** Si ninguna de las fórmulas auxiliares es de tipo Σ_1^0, la conclusión es inmediata. Supongamos ahora que ambas lo son, con lo que los secuentes superiores de la regla son:

$$\Gamma,\ \bigvee u_1\, \alpha_1(u_1, \bar{X}, \bar{Y}, \bar{Y}'),\ \bigvee u_2\, \alpha_2(u_2, \bar{Y}) \Rightarrow \Delta,\ \bigvee v_1 \beta_1(v_1, \bar{X}, \bar{Y}, \bar{Y}')$$

$$\Gamma,\ \bigvee u_1\, \alpha_1(u_1, \bar{X}, \bar{Y}, \bar{Y}'),\ \bigvee u_2'\, \alpha_2'(u_2', \bar{Y}') \Rightarrow \Delta,\ \bigvee v_1 \beta_1(v_1, \bar{X}, \bar{Y}, \bar{Y}')$$

y el secuente inferior es:

$$\Gamma',\ \bigvee u_1\, \alpha_1(u_1, \bar{X}) \Rightarrow \Delta,\ \bigvee v_1 \beta_1(v_1, \bar{X}),$$

donde Γ' resulta de añadir a Γ la fórmula principal:

$$\bigvee u_2\, \alpha_2(u_2, \bar{Y}) \vee \bigvee u_2'\, \alpha_2'(u_2', \bar{Y}').$$

Por hipótesis de inducción tenemos los transformados

$$\begin{gathered}\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}\bar{V}'(\neg\alpha_1(u_1, \bar{U}, \bar{V}, \bar{V}') \vee \alpha_2(u_2, \bar{V}) \vee \\ \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U}, \bar{V}, \bar{V}')), \\ \Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 u_2' \bigvee w \bigwedge \bar{U}\bar{V}\bar{V}'(\neg\alpha_1(u_1, \bar{U}, \bar{V}, \bar{V}') \vee \alpha_2'(u_2', \bar{V}') \vee \\ \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U}, \bar{V}, \bar{V}')),\end{gathered}$$

y tenemos que probar

$$\begin{gathered}(\bigvee u_2\, \alpha_2(u_2', \bar{Y}) \vee \bigvee u_2'\, \alpha_2'(u_2', \bar{Y}')) \wedge \Gamma \wedge \neg\Delta \Rightarrow \\ \bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1, \bar{U}) \vee \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U})).\end{gathered}$$

Suponiendo el antecedente, tenemos

$$\begin{gathered}\bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}\bar{V}'(\neg\alpha_1(u_1, \bar{U}, \bar{V}, \bar{V}') \vee \neg\alpha_2(u_2, \bar{V}) \vee \\ \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U}, \bar{V}, \bar{V}')), \\ \bigwedge u_1 u_2' \bigvee w \bigwedge \bar{U}\bar{V}\bar{V}'(\neg\alpha_1(u_1, \bar{U}, \bar{V}, \bar{V}') \vee \neg\alpha_2'(u_2', \bar{V}') \vee \\ \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U}, \bar{V}, \bar{V}')).\end{gathered}$$

Supongamos que $\bigvee u_2\, \alpha_2(u_2, \bar{Y})$, pues el caso en que $\bigvee u_2'\, \alpha_2'(u_2', \bar{Y}')$ es análogo. Tomamos entonces un x_1 arbitrario y un x_2 que cumpla $\alpha_2(x_2, \bar{Y})$. Tenemos entonces que existe un z tal que

$$\bigwedge \bar{U}\bar{V}\bar{V}'(\neg\alpha_1(x_1, \bar{U}, \bar{V}, \bar{V}') \vee \neg\alpha_2(x_2, \bar{V}) \vee \bigvee v_1 \leq z\, \beta_1(v_1, \bar{U}, \bar{V}, \bar{V}')).$$

Para unos parámetros arbitrarios $\bar{X}$, tenemos que

$$\neg\alpha_1(x_1, \bar{X}, \bar{Y}, \bar{Y}') \vee \neg\alpha_2(x_2, \bar{Y}) \vee \bigvee v_1 \leq z\, \beta_1(v_1, \bar{X}, \bar{Y}, \bar{Y}'),$$

pero, como $\alpha_2(x_2, \bar{Y})$, esto implica que

$$\neg\alpha_1(x_1, \bar{X}) \vee \bigvee v_1 \leq z\, \beta_1(v_1, \bar{X}),$$

lo que prueba el transformado del secuente inferior de la regla.

Falta considerar el caso en el que sólo una de las fórmulas auxiliares es de tipo Σ^0_1. En tal caso los secuentes superiores de la regla son

$$\Gamma,\ \bigvee u_1\, \alpha_1(u_1,\bar{X},\bar{Y}),\ \bigvee u_2\, \alpha_2(u_2,\bar{Y}) \Rightarrow \Delta,\ \bigvee v_1 \beta_1(v_1,\bar{X},\bar{Y})$$

$$\Gamma,\ \bigvee u_1\, \alpha_1(u_1,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1 \beta_1(v_1,\bar{X})$$

y el secuente inferior es:

$$\Gamma',\ \bigvee u_1\, \alpha_1(u_1,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1 \beta_1(v_1,\bar{X}),$$

donde Γ' resulta de eliminar α' en Γ y añadirle la fórmula principal: $\bigvee u_2\, \alpha_2(u_2,\bar{Y}) \vee \alpha'$. Los transformados son:

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \vee \alpha_2(u_2,\bar{V}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V})),$$

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U})),$$

y tenemos que probar:

$$(\bigvee u_2\, \alpha_2(u_2,\bar{Y}) \vee \alpha') \wedge \Gamma_0 \wedge \neg\Delta \Rightarrow$$

$$\bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \to \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U})).$$

donde Γ_0 resulta de eliminar α' en Γ. Suponiendo el antecedente, el caso en que $\bigvee u_2\, \alpha_2(u_2,\bar{Y})$ es análogo al del caso anterior, mientras que si se cumple α', entonces tenemos $\Gamma \wedge \neg\Delta$, y el transformado del segundo secuente superior nos da la conclusión.

$\vee$ **derecha** Por simplicidad podemos considerar la variante de la regla con una única fórmula auxiliar. Si no es de tipo Σ^0_1 la conclusión es trivial. En otro caso, la regla es

$$\frac{\Gamma,\ \bigvee u_1, \alpha_1(u_1,\bar{X},\bar{Y}) \Rightarrow \Delta,\ \bigvee v_1 \beta_1(v_1,\bar{X},\bar{Y}), \bigvee v_2 \beta_2(v_2,\bar{Y})}{\Gamma,\ \bigvee u_1, \alpha_1(u_1,\bar{X}) \Rightarrow \Delta',\ \bigvee v_1 \beta_1(v_1,\bar{X})},$$

donde Δ' resulta de añadirle a Δ la fórmula principal: $\bigvee v_2\, \beta_2(v_2,\bar{Y}) \vee \beta'$.

El transformado del secuente superior es

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V}) \vee \bigvee v_2 \leq w\, \beta_2(v_2,\bar{V})),$$

y el del secuente inferior es

$$\Gamma \wedge \neg\Delta \wedge \neg(\bigvee v_2\, \beta_2(v_2,\bar{Y}) \vee \beta) \Rightarrow$$

$$\bigwedge u_1 \bigvee w \bigwedge \bar{U}(\alpha_1(u_1,\bar{U}) \to \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U})).$$

Para probarlo suponemos el antecedente, con lo que tenemos

$$\bigwedge u_1 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \lor$$
$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V}) \lor \bigvee v_2 \leq w\, \beta_2(v_2,\bar{V})).$$

Fijamos un x_1 arbitrario, que nos da un z tal que

$$\bigwedge \bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U},\bar{V}) \lor \bigvee v_1 \leq z\, \beta_1(v_1,\bar{U},\bar{V}) \lor \bigvee v_2 \leq z\, \beta_2(v_2,\bar{V})).$$

Fijamos unos parámetros $\bar{X}$ arbitrarios, con lo que

$$\neg\alpha_1(x_1,\bar{X},\bar{Y}) \lor \bigvee v_1 \leq z\, \beta_1(v_1,\bar{X},\bar{Y}) \lor \bigvee v_2 \leq z\, \beta_2(v_2,\bar{Y}),$$

pero la hipótesis nos da que $\neg\bigvee v_2\, \beta_2(v_2,\bar{Y})$, luego podemos pasar a

$$\neg\alpha_1(x_1,\bar{X},\bar{Y}) \lor \bigvee v_1 \leq z\, \beta_1(v_1,\bar{X},\bar{Y}),$$

lo que prueba el transformado del secuente inferior.

$\bigwedge$ **izquierda** Como siempre, si la fórmula auxiliar no es de tipo Σ_1^0 la conclusión es trivial. En caso contrario, la regla es

$$\frac{\Gamma,\ \bigvee u_1\, \alpha_1\, (u_1,\bar{X},\bar{Y}), \bigvee u_2\, \alpha_2(u_2,t,\bar{Y}) \Rightarrow \Delta,\ \bigvee v_1\, \beta_1(v_1,\bar{X},\bar{Y})}{\Gamma',\ \bigvee u_1\, \alpha_1\, (u_1,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\, \beta_1(v_1,\bar{X})},$$

donde Γ' resulta de añadirle a Γ la fórmula principal: $\bigwedge u \bigvee u_2\, \alpha_2(u_2,u,\bar{Y})$. Por hipótesis de inducción tenemos el secuente

$$\Gamma \land \neg\Delta \Rightarrow \bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \lor \neg\alpha_2(u_2,t,\bar{V}) \lor$$
$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V}))$$

y tenemos que demostrar

$$\bigwedge u \bigvee u_2\, \alpha_2(u_2,u,\bar{Y}) \land \Gamma \land \neg\Delta \Rightarrow$$
$$\bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \lor \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U})).$$

Suponiendo el antecedente, tenemos, por una parte, $\bigvee u_2\, \alpha_2(u_2,t,\bar{Y})$ y, por otra,

$$\bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \lor \neg\alpha_2(u_2,t,\bar{V}) \lor \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V})).$$

Fijamos un x_1 arbitrario y tomamos un x_2 que cumpla $\alpha_2(x_2,t,\bar{Y})$. Entonces existe un z tal que

$$\bigwedge \bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U},\bar{V}) \lor \neg\alpha_2(x_2,t,\bar{V}) \lor \bigvee v_1 \leq z\, \beta_1(v_1,\bar{U},\bar{V})).$$

Fijamos parámetros $\bar{X}$ arbitrarios, de modo que

$$\neg\alpha_1(x_1,\bar{X},\bar{Y}) \lor \neg\alpha_2(x_2,t,\bar{Y}) \lor \bigvee v_1 \leq z\, \beta_1(v_1,\bar{X},\bar{Y}),$$

pero de aquí podemos pasar a

$$\neg\alpha_1(x_1,\bar{X}) \lor \bigvee v_1 \leq z\, \beta_1(v_1,\bar{X}),$$

lo que prueba el transformado del secuente inferior.

$\bigvee$ **izquierda** Como siempre, si la fórmula auxiliar no es de tipo Σ_1^0, el transformado del secuente inferior se deduce del transformado del secuente superior mediante la misma regla. En otro caso, si la fórmula auxiliar es de tipo Δ_0^0, la regla es:

$$\frac{\Gamma,\ \bigvee u_1\, \alpha_1(u_1,\bar{X}),\ \alpha_2(y,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\, \beta_1(v_1,\bar{X})}{\Gamma,\ \bigvee u_1\, \alpha_1(u_1,\bar{X}), \bigvee u_2\, \alpha_2(u_2,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\, \beta_1(v_1,\bar{X})},$$

donde la variable propia y no aparece en ninguna otra fórmula de los secuentes. El transformado del secuente superior es:

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \neg\alpha_2(y,\bar{U}) \vee \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U})),$$

y le podemos aplicar la regla derecha del generalizador para concluir

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_2 u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \neg\alpha_2(u_2,\bar{U}) \vee \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U})),$$

y esto (salvo el orden de las variables en $\bigwedge u_2 u_2$) es el transformado del secuente inferior.

Si la fórmula auxiliar es estrictamente Σ_1^0, tenemos

$$\frac{\Gamma,\ \bigvee u_1\, \alpha_1(u_1,\bar{X},\bar{Y}),\ \bigvee u_2\, \alpha_2(u_2,y,\bar{Y}) \Rightarrow \Delta,\ \bigvee v_1\, \beta_1(v_1,\bar{X},\bar{Y})}{\Gamma',\ \bigvee u_1\, \alpha_1(u_1,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\, \beta_1(v_1,\bar{X})},$$

donde Γ' resulta de añadirle a Γ la fórmula principal: $\bigvee u u_2\, \alpha_2(u_2,u,\bar{Y})$. Ahora el transformado del secuente superior es:

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{V}) \vee \neg\alpha_2(u_2,y,\bar{U},\bar{V}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V})),$$

del que podemos deducir, por la regla derecha del generalizador,

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{V}) \vee \neg\alpha_2(u_2,u,\bar{U},\bar{V}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V})).$$

Tenemos que probar:

$$\bigvee u u_2, \alpha_2(u_2,u,\bar{Y}) \wedge \Gamma \wedge \neg\Delta \Rightarrow$$

$$\bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U})).$$

Suponiendo el antecedente $\bigvee u u_2, \alpha_2(u_2,u,\bar{Y}) \wedge \Gamma \wedge \neg\Delta$, podemos fijar y, x_2 que cumplan $\alpha_2(x_2,y,\bar{Y})$ y, por otra parte, tenemos

$$\bigwedge u u_1 u_2 \bigvee w \bigwedge \bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \vee \neg\alpha_2(u_2,u,\bar{V}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U},\bar{V})).$$

Fijado un x_1 arbitrario, tenemos que existe un z tal que

$$\bigwedge \bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U},\bar{V}) \lor \neg\alpha_2(x_2,y,\bar{V}) \lor \bigvee v_1 \leq z\,\beta_1(v_1,\bar{U},\bar{V})).$$

Fijamos unos parámetros $\bar{X}$ arbitrarios, y entonces

$$\neg\alpha_1(x_1,\bar{X},\bar{Y}) \lor \neg\alpha_2(x_2,y,\bar{Y}) \lor \bigvee v_1 \leq z\,\beta_1(v_1,\bar{X},\bar{Y}),$$

pero tenemos $\alpha_2(x_2,y,\bar{Y})$, luego de aquí se sigue que

$$\neg\alpha_1(x_1,\bar{X}) \lor \bigvee v_1 \leq z\,\beta_1(v_1,\bar{X}),$$

y esto prueba el transformado del secuente inferior.

$\bigwedge$ **derecha** Si la fórmula auxiliar $\beta(y)$ no es de tipo Σ_1^0, forma parte de Δ, y en el antecedente del transformado del secuente superior tendremos $\neg\beta(y)$, mientras que en el antecedente del transformado del secuente inferior tendremos $\neg\bigwedge u\,\beta(u)$. Claramente se puede pasar del primero al segundo mediante la regla izquierda del particularizador, que nos da $\bigvee u\,\neg\beta(u)$ y luego cortando con $\neg\bigwedge u\,\beta(u) \Rightarrow \bigvee u\neg\beta(u)$.

Supongamos ahora que la fórmula auxiliar es Σ_1^0, con lo que la regla es:

$$\frac{\Gamma,\ \bigvee u_1\alpha_1(u_1,\bar{X},\bar{Y}) \Rightarrow \Delta,\ \bigvee v_1\,\beta_1(v_1,\bar{X},\bar{Y}),\ \bigvee v_2\,\beta_2(v_2,y,\bar{Y})}{\Gamma,\ \bigvee u_1\alpha_1(u_1,\bar{X}) \Rightarrow \Delta',\ \bigvee v_1\,\beta_1(v_1,\bar{X}),}$$

donde Δ' contiene la fórmula principal: $\bigwedge v\bigvee v_2\,\beta_2(v_2,v,\bar{Y})$. El transformado del secuente superior es

$$\Gamma \land \neg\Delta \Rightarrow \bigwedge u_1\bigvee w\bigwedge\bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \lor$$
$$\bigvee v_1 \leq w\,\beta_1(v_1,\bar{U},\bar{V}) \lor \bigvee v_2 \leq w\,\beta_2(v_2,y,\bar{V})),$$

de donde se sigue

$$\Gamma \land \neg\Delta \Rightarrow \bigwedge vu_1\bigvee w\bigwedge\bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U},\bar{V}) \lor$$
$$\bigvee v_1 \leq w\,\beta_1(v_1,\bar{U},\bar{V}) \lor \bigvee v_2 \leq w\,\beta_2(v_2,v,\bar{V})),$$

Tenemos que probar:

$$\Gamma \land \neg\Delta \land \neg\bigwedge v\bigvee v_2\,\beta_2(v_2,v,\bar{Y}) \Rightarrow$$
$$\bigwedge u_1\bigvee w\bigwedge\bar{U}(\neg\alpha_1(u_1,\bar{U}) \lor \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U})).$$

Suponemos el antecedente y fijamos un y tal que $\bigwedge v_2\,\neg\beta_2(v_2,y,\bar{Y})$. Ahora fijamos un u_1 arbitrario y concluimos que existe un z tal que

$$\bigwedge\bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U},\bar{V}) \lor \bigvee v_1 \leq z\,\beta_1(v_1,\bar{U},\bar{V}) \lor \bigvee v_2 \leq z\,\beta_2(v_2,y,\bar{V})).$$

Ahora fijamos parámetros $\bar{X}$ arbitrarios y entonces

$$\neg\alpha_1(x_1,\bar{X},\bar{Y}) \lor \bigvee v_1 \leq z\,\beta_1(v_1,\bar{X},\bar{Y}) \lor \bigvee v_2 \leq z\,\beta_2(v_2,y,\bar{Y}),$$

pero la hipótesis $\bigwedge v_2\neg\beta_2(v_2,y,\bar{Y})$ descarta la última alternativa y queda:

$$\neg\alpha_1(x_1,\bar{X}) \lor \bigvee v_1 \leq z\,\beta_1(v_1,\bar{X}),$$

y esto prueba el transformado del secuente inferior.

$\bigvee$ **derecha** Si la fórmula auxiliar $\beta(t)$ no es de tipo Σ_1^0, forma parte de Δ, luego en el antecedente del transformado del secuente superior aparece $\neg\beta(t)$, y la regla izquierda del generalizador nos permite sustituirlo por $\bigwedge v \neg\beta(v)$, que a su vez se transforma en $\neg\bigvee v\,\beta(v)$ cortando con $\neg\bigvee v\,\beta(v) \Rightarrow \bigwedge v \neg\beta(v)$, y así obtenemos el transformado del secuente inferior.

Supongamos ahora que la fórmula auxiliar es de tipo Δ_0^0, con lo que la regla es

$$\frac{\Gamma,\ \bigvee u_1\,\alpha_1(u_1,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\,\beta_1(v_1,\bar{X}),\ \beta_2(t,\bar{X})}{\Gamma,\ \bigvee u_1\,\alpha_1(u_1,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\,\beta_1(v_1,\bar{X}),\ \bigvee v_2\,\beta_2(v_2,\bar{X})}.$$

El transformado del secuente superior es

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U}) \vee \beta_2(t,\bar{U})),$$

de donde, por la regla derecha del particularizador, podemos deducir

$$\Gamma \wedge \neg\Delta \Rightarrow \bigvee v_2 \bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U}) \vee \beta_2(v_2,\bar{U})).$$

Tenemos que probar:

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee$$
$$\bigvee v_1 \leq w\,\beta_1(v_1,\bar{U}) \vee \bigvee v_2 \leq w\,\beta_2(v_2,\bar{U})).$$

Supuesto el antecedente, tomamos un y_2 tal que

$$\bigwedge u_1 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U}) \vee \beta_2(y_2,\bar{U})).$$

Fijamos un x_1 arbitrario, con lo que existe un z tal que

$$\bigwedge \bar{U}(\neg\alpha_1(x_1,\bar{U}) \vee \bigvee v_1 \leq z\,\beta_1(v_1,\bar{U}) \vee \beta_2(y_2,\bar{U})).$$

Llamamos $z' = \text{máx}\{z, y_2\}$, con lo que, claramente, podemos deducir

$$\bigwedge \bar{U}(\neg\alpha_1(x_1,\bar{U}) \vee \bigvee v_1 \leq z'\,\beta_1(v_1,\bar{U}) \vee \bigvee v_2 \leq z'\beta_2(v_2,\bar{U})),$$

y esto prueba el transformado del secuente inferior.

$\boldsymbol{\Sigma_1^0}$**-inducción** La regla de inducción es de la forma[9]

$$\frac{\Gamma,\ \bigvee u_1\,\alpha_1(u_1,\bar{X}),\ \bigvee u_2\,\alpha_2(u_2,y,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\,\beta_1(v_1,\bar{X}),\ \bigvee v_1\,\alpha_2(v_1,y',\bar{X})}{\Gamma,\ \bigvee u_1\,\alpha_1(u_1,\bar{X}),\ \bigvee u_2\,\alpha_2(u_2,0,\bar{X}) \Rightarrow \Delta,\ \bigvee v_1\,\beta_1(v_1,\bar{X}),\ \bigvee v_2\,\alpha_2(v_2,t,\bar{X})}$$

El transformado del secuente superior es

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \neg\alpha_2(u_2,y,\bar{U}) \vee$$
$$\bigvee v_1 \leq w\,\beta_1(v_1,\bar{U}) \vee \bigvee v_2 \leq w\,\alpha_2(v_2,y',\bar{U})).$$

[9] No es necesario distinguir el caso en que la fórmula auxiliar es de tipo Δ_0^0, pues es totalmente análogo.

Como la variable y es propia, la regla derecha del generalizador nos da

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u u_1 u_2 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \neg\alpha_2(u_2,u,\bar{U}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U}) \vee \bigvee v_2 \leq w\, \alpha_2(v_2,u',\bar{U})).$$

Tenemos que probar

$$\Gamma \wedge \neg\Delta \Rightarrow \bigwedge u_1 u_2 \bigvee w \bigwedge \bar{U}(\neg\alpha_1(u_1,\bar{U}) \vee \neg\alpha_2(u_2,0,\bar{U}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U}) \vee \bigvee v_2 \leq w\, \alpha_2(v_2,t,\bar{U})).$$

Suponemos el antecedente y fijamos x_1, x_2 arbitrarios. Vamos a probar que

$$\bigwedge u \bigvee w \bigwedge \bar{U}(\neg\alpha_1(x_1,\bar{U}) \vee \neg\alpha_2(x_2,0,\bar{U}) \vee$$

$$\bigvee v_1 \leq w\, \beta_1(v_1,\bar{U}) \vee \bigvee v_2 \leq w\, \alpha_2(v_2,u,\bar{U})).$$

Admitiendo esto, haciendo $u = t$ tenemos probado el transformado del secuente inferior.

Equivalentemente, tenemos que probar que

$$\bigwedge u \bigvee w \bigwedge \bar{U}(\neg \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U}) \wedge \alpha_1(x_1,\bar{U}) \wedge \alpha_2(x_2,0,\bar{U}) \rightarrow$$

$$\bigvee v_2 \leq w\, \alpha_2(v_2,u,\bar{U})).$$

Llamemos

$$\alpha(X_1,\ldots,X_m,z,y,x_1,\ldots,x_n) \equiv \neg \bigvee v_1 \leq z\, \beta_1(v_1,\bar{U}) \wedge$$

$$\alpha_1(x_1,\bar{U}) \wedge \alpha_2(x_2,0,\bar{U}) \rightarrow \bigvee v_2 \leq z\, \alpha_2(v_2,y,\bar{U}),$$

que es una fórmula de tipo Δ_0^0, por lo que podemos considerar el término $t_\alpha(z,y,x_1,\ldots,x_n)$ dado por el teorema 2.29. Así, para todas las sucesiones $s_1,\ldots,s_m \in \{0,1\}^{t_\alpha(z,y,\bar{x})}$, se cumple que

$$\alpha(\bar{X},z,y,\bar{x}) \leftrightarrow \alpha^*(\bar{s},z,y,\bar{x}).$$

Por lo tanto, la fórmula $\bigvee w \bigwedge \bar{U}\, \alpha(\bar{U},w,y,\bar{x})$ es equivalente a

$$\bigvee w \bigvee c(c = \{0,1\}^{t_\alpha(w,y,\bar{x})} \wedge \bigwedge s_1 \cdots s_m \in c\ \alpha^*(\bar{s},w,y,\bar{x})),$$

que es de tipo Σ_1^0, luego podemos probar $\bigwedge u \bigvee w \bigwedge \bar{U}\, \alpha(\bar{U},w,y,\bar{x})$ por Σ_1^0-inducción.

Para $u = 0$ tenemos que probar

$$\bigvee w \bigwedge \bar{U}(\neg \bigvee v_1 \leq w\, \beta_1(v_1,\bar{U}) \wedge \alpha_1(x_1,\bar{U}) \wedge \alpha_2(x_2,0,\bar{U}) \rightarrow$$

$$\bigvee v_2 \leq w\, \alpha_2(v_2,0,\bar{U})),$$

lo cual se cumple trivialmente, tomando $v_2 = x_2$. Suponemos que existe un z tal que

$$\bigwedge \bar{U}(\neg \bigvee v_1 \leq z\, \beta_1(v_1, \bar{U}) \land \alpha_1(x_1, \bar{U}) \land \alpha_2(x_2, 0, \bar{U}) \rightarrow \bigvee v_2 \leq z\, \alpha_2(v_2, n, \bar{U})).$$

Como estamos suponiendo el transformado del secuente superior de la regla de inducción (y su antecedente), tenemos que

$$\bigwedge u_2 \bigvee w \bigwedge \bar{U}(\neg \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U}) \land \alpha_1(x_1, \bar{U}) \land \alpha_2(u_2, n, \bar{U}) \rightarrow \bigvee v_2 \leq w\, \alpha_2(v_2, n', \bar{U})),$$

y en particular

$$\bigwedge u_2 \leq z \bigvee w \bigwedge \bar{U}(\neg \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U}) \land \alpha_1(x_1, \bar{U}) \land \alpha_2(u_2, n, \bar{U}) \rightarrow \bigvee v_2 \leq w\, \alpha_2(v_2, n', \bar{U})).$$

Usando como antes el teorema 2.29 podemos ver que la fórmula tras el cuantificador $\bigwedge u_2 \leq z$ es equivalente a una fórmula de tipo Σ^0_1.

En este punto usamos que en ACR_0^-, luego en ARP_0^2, se puede probar el principio de recolección para fórmulas Σ^0_1, es decir:

$$\bigwedge u \leq x \bigvee v\, \phi(u, v) \rightarrow \bigvee w \bigwedge u \leq x \bigvee v \leq w\, \phi(u, v),$$

donde ϕ es una fórmula de tipo Σ^0_1. La prueba es literalmente la misma que hemos dado en [LF 6.25], sin más que observar que la inducción se realiza sobre una fórmula de tipo Σ^0_1.

Por lo tanto, podemos concluir que existe un z' (y podemos suponer $z \leq z'$) tal que

$$\bigwedge u_2 \leq z \bigvee w \leq z' \bigwedge \bar{U}(\neg \bigvee v_1 \leq w\, \beta_1(v_1, \bar{U}) \land \alpha_1(x_1, \bar{U}) \land \alpha_2(u_2, n, \bar{U}) \rightarrow \bigvee v_2 \leq w\, \alpha_2(v_2, n', \bar{U})),$$

pero esto implica que

$$\bigwedge u_2 \leq z \bigwedge \bar{U}(\neg \bigvee v_1 \leq z'\, \beta_1(v_1, \bar{U}) \land \alpha_1(x_1, \bar{U}) \land \alpha_2(u_2, n, \bar{U}) \rightarrow \bigvee v_2 \leq z'\, \alpha_2(v_2, n', \bar{U})).$$

Ahora es fácil probar que, fijados unos valores $\bar{X}$ para los parámetros de segundo orden, se cumple

$$\neg \bigvee v_1 \leq z'\, \beta_1(v_1, \bar{X}) \land \alpha_1(x_1, \bar{X}) \land \alpha_2(x_2, 0, \bar{X}) \rightarrow \bigvee v_2 \leq z'\, \alpha_2(v_2, n', \bar{X}).$$

En efecto, por la hipótesis de inducción tenemos

$$\neg \bigvee v_1 \leq z\, \beta_1(v_1, \bar{X}) \land \alpha_1(x_1, \bar{X}) \land \alpha_2(x_2, 0, \bar{X}) \rightarrow \bigvee v_2 \leq z\, \alpha_2(v_2, n, \bar{X}),$$

y la hipótesis $\neg\bigvee v_1 \leq z'\,\beta_1(v_1,\bar{X}) \land \alpha_1(x_1,\bar{X}) \land \alpha_2(x_2,0,\bar{X})$ implica $\neg\bigvee v_1 \leq z\,\beta_1(v_1,\bar{X}) \land \alpha_1(x_1,\bar{X}) \land \alpha_2(x_2,0,\bar{X})$, que a su vez implica $\bigvee v_2 \leq z\,\alpha_2(v_2,n,\bar{X})$. Tomando un $y_2 \leq z$ que cumpla $\alpha_2(y_2,n,\bar{X})$, tenemos

$$\neg\bigvee v_1 \leq z'\,\beta_1(v_1,\bar{X}) \land \alpha_1(x_1,\bar{U}) \land \alpha_2(y_2,n,\bar{X}) \rightarrow \bigvee v_2 \leq z'\,\alpha_2(v_2,n',\bar{X}),$$

luego se cumple $\bigvee v_2 \leq z'\,\alpha_2(v_2,n',\bar{X})$. Esto termina la prueba por inducción.

Corte Finalmente estudiamos la regla de corte, sabiendo que la fórmula de corte es necesariamente de tipo Σ_1^0, luego los secuentes superiores son de la forma

$$\Gamma, \bigvee u_1\alpha_1(u_1,\bar{X}) \Rightarrow \Delta, \bigvee v_1\,\beta_1(v_1,\bar{X}), \bigvee v_2\,\beta_2(v_2,\bar{X},\bar{Y}),$$

$$\Gamma, \bigvee u_1\alpha_1(u_1,\bar{X}), \bigvee u_2\,\beta_2(u_2,\bar{X},\bar{Y}) \Rightarrow \Delta, \bigvee v_1\,\beta_1(v_1,\bar{X}),$$

y el secuente inferior es

$$\Gamma, \bigvee u_1\alpha_1(u_1,\bar{X}) \Rightarrow \Delta, \bigvee v_1\,\beta_1(v_1,\bar{X}).$$

Tenemos entonces:

$$\Gamma \land \neg\Delta \Rightarrow \bigwedge u_1\bigvee w\bigwedge\bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U}) \lor$$
$$\bigvee v_1 \leq w\,\beta_1(v_1,\bar{U}) \lor \bigvee v_2 \leq w\,\beta_2(v_2,\bar{U},\bar{V})),$$
$$\Gamma \land \neg\Delta \Rightarrow \bigwedge u_1u_2\bigvee w\bigwedge\bar{U}\bar{V}(\neg\alpha_1(u_1,\bar{U}) \lor \neg\beta_2(u_2,\bar{U},\bar{V}) \lor$$
$$\bigvee v_1 \leq w\,\beta_1(v_1,\bar{U})),$$

y tenemos que probar

$$\Gamma \land \neg\Delta \Rightarrow \bigwedge u_1\bigvee w\bigwedge\bar{U}(\neg\alpha_1(u_1,\bar{U}) \lor \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U})).$$

Suponemos el antecedente y fijamos x_1, con lo que tenemos que existe z_1 tal que

$$\bigwedge\bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U}) \lor \bigvee v_1 \leq z_1\,\beta_1(v_1,\bar{U}) \lor \bigvee v_2 \leq z_1\,\beta_2(v_2,\bar{U},\bar{V})),$$

$$\bigwedge u_2 \leq z_1\bigvee w\bigwedge\bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U}) \lor \neg\beta_2(u_2,\bar{U},\bar{V}) \lor \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U})).$$

Como en el caso precedente, el teorema 2.29 permite probar que la fórmula tras $\bigvee w$ es equivalente a una fórmula de tipo Σ_1^0, por lo que podemos aplicar el principio de recolección para fórmulas Σ_1^0 y concluir que existe un z_2 (y podemos suponer $z_1 \leq z_2$) tal que

$$\bigwedge u_2 \leq z_1\bigvee w \leq z_2\bigwedge\bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U}) \lor \neg\beta_2(u_2,\bar{U},\bar{V}) \lor \bigvee v_1 \leq w\,\beta_1(v_1,\bar{U})),$$

pero esto implica

$$\bigwedge u_2 \leq z_1\bigwedge\bar{U}\bar{V}(\neg\alpha_1(x_1,\bar{U}) \lor \neg\beta_2(u_2,\bar{U},\bar{V}) \lor \bigvee v_1 \leq z_2\,\beta_1(v_1,\bar{U})).$$

Ahora ya podemos probar que

$$\bigwedge \bar{U}(\neg\alpha_1(x_1,\bar{U}) \vee \bigvee v_1 \leq z_2\, \beta_1(v_1,\bar{U})).$$

Para ello fijamos parámetros $\bar{X}$ y $\bar{Y}$, con lo que tenemos

$$\neg\alpha_1(x_1,\bar{X}) \vee \bigvee v_1 \leq z_1\, \beta_1(v_1,\bar{X}) \vee \bigvee v_2 \leq z_1\, \beta_2(v_2,\bar{X},\bar{Y}).$$

Si se da uno de los dos primeros casos, ya tenemos lo requerido. En caso contrario tomamos $y_2 \leq z_1$ tal que $\beta_2(y_2,\bar{X},\bar{Y})$, con lo que

$$\neg\alpha_1(x_1,\bar{X}) \vee \neg\beta_2(y_2,\bar{X},\bar{Y}) \vee \bigvee v_1 \leq z_2\, \beta_1(v_1,\bar{X}),$$

pero esto implica $\neg\alpha_1(x_1,\bar{X}) \vee \bigvee v_1 \leq z_2\, \beta_1(v_1,\bar{X})$ y de nuevo tenemos la conclusión. ■

Ahora ya podemos demostrar el teorema 2.28:

Supongamos que una fórmula de primer orden ϕ es demostrable en LKD. En particular lo es en LKD$^+$, luego, por 2.32 es demostrable en el cálculo secuencial ARP_0^2 extendido con la regla de inferencia LKD*. Pero este cálculo secuencial cumple las hipótesis del teorema de eliminación de cortes libres 3.4 que probaremos en el capítulo siguiente, luego existe una demostración del secuente $\Rightarrow \phi$ en ARP_0^2+ LKD* sin cortes libres. En ella todas las fórmulas de corte vienen de secuentes iniciales, o de fórmulas principales de la regla de inducción o de la regla LKD*, luego todas las fórmulas de corte son de tipo Σ_1^0. En particular, ninguna fórmula en la prueba puede tener variables ligadas de segundo orden, ya que no pueden eliminarse por cortes y no llegan al secuente final.

Consideremos una aplicación de la regla de König que no tenga ninguna otra por encima. Entonces, la demostración hasta ese punto está en las condiciones del teorema anterior, y concluye con un secuente de la forma

$$\Gamma,\ \bigvee u_1\, \alpha_1(u_1,\bar{X},\bar{y}),\ldots,\bigvee u_n\, \alpha_n(u_n,\bar{X},\bar{y}) \Rightarrow \bigvee v\, \beta(v,Y,\bar{X},\bar{y}),$$

donde la variable Y es propia (no aparece en más fórmulas del secuente). Por el teorema anterior, en ARP_0^2 se demuestra también

$$\Gamma \Rightarrow \bigwedge \bar{u} \bigvee w \bigwedge V \bar{U}(\neg\alpha_1(u_1,\bar{U},\bar{y}) \vee \cdots \vee \neg\alpha_n(u_n,\bar{U},\bar{y}) \vee \bigvee v \leq w\, \beta(v,V,\bar{U},\bar{y})),$$

que equivale a

$$\begin{gathered}\Gamma \Rightarrow \bigwedge \bar{U} \bigwedge \bar{u} \bigvee w(\neg\alpha_1(u_1,\bar{U},\bar{y}) \vee \cdots \vee \neg\alpha_n(u_n,\bar{U},\ \bar{y}) \vee \\ \bigwedge V \bigvee v \leq w\, \beta(v,V,\bar{U},\bar{y})),\end{gathered}$$

o también a

$$\begin{gathered}\Gamma \Rightarrow \bigwedge u_1 \neg\alpha_1(u_1,\bar{X},\bar{y}) \vee \cdots \vee \bigwedge u_n \neg\alpha_n(u_n,\bar{X},\bar{y}) \vee \\ \bigvee w \bigwedge V \bigvee v \leq w\, \beta(v,V,\bar{X},\bar{y}),\end{gathered}$$

o a

$$\Gamma,\ \bigvee u_1\, \alpha_1(u_1,\bar{X},\bar{y}),\ldots,\bigvee u_n\, \alpha_n(u_n,\bar{X},\bar{y}) \Rightarrow \bigvee w \bigwedge V \bigvee v \leq w\, \beta(v,V,\bar{X},\bar{y}).$$

Pero en la prueba de 2.32 hemos visto que en ARP_0^2 se demuestra que

$$\bigvee w \bigwedge V \bigvee v \leq w\, \beta(V, u, \bar{y}) \leftrightarrow \bigvee w \bigwedge s \in \{0,1\}^{t_\beta(w,\bar{y})} \bigvee u \leq w\, \beta^*(s, u, \bar{y}),$$

por lo que también podemos probar el secuente:

$$\Gamma,\ \bigvee u_1\, \alpha_1(u_1, \bar{X}, \bar{y}), \ldots, \bigvee u_n\, \alpha_n(u_n, \bar{X}, \bar{y}) \Rightarrow$$

$$\bigvee w \bigwedge s \in \{0,1\}^{t_\beta(w,\bar{y})} \bigvee u \leq w\, \beta^*(s, u, \bar{y}),$$

que es justamente el secuente inferior de la regla de König. Por lo tanto, pasando esta demostración a otra sin cortes libres y poniéndola en lugar de la prueba del secuente superior, obtenemos una demostración del mismo secuente final, pero con una aplicación menos de la regla de König. Repitiendo el proceso tantas veces como aplicaciones tiene la demostración dada, llegamos a una prueba del secuente $\Rightarrow \phi$ en ARP_0^2. ■

Podemos generalizar los resultados obtenidos si tenemos en cuenta que el teorema 2.21 es válido también para $B(\Delta_0^0)$ más la regla TKD*, es decir, si en esta teoría se puede demostrar un secuente

$$\bigwedge \bar{U} \gamma_1(U_{1,1}^{r_{1,1}}, \ldots, U_{1,n_1}^{r_{1,n_1}}), \ldots, \bigwedge \bar{U} \gamma_m(U_{m,1}^{r_{m,1}}, \ldots, U_{m,n_m}^{r_{m,n_m}}),\ \Gamma \Rightarrow \Delta,$$

donde Γ y Δ constan de fórmulas de primer orden, entonces en B más la regla TKD* se puede demostrar un secuente de la forma

$$\{\gamma_i(T_{i1k}, \ldots, T_{in_ik})\},\ \Gamma \Rightarrow \Delta$$

sin usar las reglas de segundo orden. En efecto, en la prueba de 2.21 usamos que el secuente dado se puede demostrar sin cortes, mientras que ahora sólo podemos asegurar que admite una demostración sin cortes libres. Esto implica que las fórmulas de corte tienen que ser fórmulas principales de la regla TKD*, y esto nos asegura que son fórmulas de primer orden, por lo que si la última regla usada es la de corte, podemos aplicar la hipótesis de inducción a los dos secuentes superiores y concluir igualmente que el secuente inferior admite una demostración en las condiciones requeridas. Teniendo esto en cuenta, podemos probar:

Teorema 2.34 *Una fórmula de primer orden es demostrable en* $\mathrm{LKD}_0 + \Sigma_n^0$*-inducción si y sólo si es demostrable en* $\mathrm{ACR}_0 + \Sigma_n^0$*-inducción. Si además no tiene variables de segundo orden, esto sucede si y sólo si es demostrable en* $\mathrm{I}\Sigma_n$.

DEMOSTRACIÓN: Supongamos que un secuente $\Gamma \Rightarrow \Delta$ que conste únicamente de fórmulas de primer orden es demostrable en $\mathrm{LKD}_0 + \Sigma_n^0$-inducción. Entonces es demostrable en $\mathrm{LKD}_0^+ + \Sigma_n^0$-inducción (es decir, considerando que el lenguaje formal no es $\mathcal{L}_a^2$, sino $\mathcal{L}_{\mathrm{arp}}^2$), y esto equivale a que pueda demostrarse en el cálculo secuencial ARP_0^2 descrito en 2.19 más la regla LKD* más un número finito de axiomas $\Rightarrow \bigwedge \bar{U}\, \mathrm{Ind}(\gamma_i)$, para $i = 1, \ldots, n$, donde cada γ_i es una fórmula de tipo Σ_n^0.

Los axiomas de ARP_0^2 estaban elegidos para que cumplieran las hipótesis del teorema de eliminación de cortes libres, pero ahora nos interesa reformularlos de modo que sean sentencias de primer orden. Concretamente, podemos considerar que la demostración de $\Gamma \Rightarrow \Delta$ es una deducción en $B(\Delta_0^0)$ más la regla LKD* a partir de premisas de la forma:

1. Los secuentes $\Rightarrow \alpha$, donde α recorre las definiciones de los funtores de $\mathcal{L}_{\mathrm{arp}}$ (definición [LF 1.8]), con todas variables cuantificadas universalmente.
2. $\Rightarrow \bigwedge u\, \neg Su = 0$,
3. $\Rightarrow \bigwedge uv(Su = Sv \rightarrow u = v)$,
4. $\Rightarrow \bigwedge u\, u = u$,
5. $\Rightarrow I_1$, donde
$$I_1 \equiv \bigwedge U \bigwedge uv(u = v \wedge U(u) \rightarrow U(v)).$$
6. $\Rightarrow \bigwedge \bar{U}\ \mathrm{Ind}(\gamma)$, donde γ es una fórmula de tipo Σ_n^0 y
$$\mathrm{Ind}(\gamma) \equiv \bigwedge \bar{v}((\gamma(0) \wedge \bigwedge u(\gamma(u) \rightarrow \gamma(u'))) \rightarrow \bigwedge u\, \gamma(u)).$$

Es claro que estos axiomas permiten demostrar en $B(\Delta_0^0)$ los axiomas considerados en 2.19. Si llamamos Γ^* al conjunto que resulta de añadir a Γ las sentencias de las premisas de tipo 1, 2, 3, 4 que aparezcan en la demostración, tenemos que en $B(\Delta_0^0)$ más la regla LKD* se puede demostrar (sin premisas) un secuente de la forma

$$I_1, \bigwedge \bar{U}\, \mathrm{Ind}(\gamma_1), \ldots \bigwedge \bar{U}\, \mathrm{Ind}(\gamma_m), \Gamma^* \Rightarrow \Delta,$$

y ahora, según hemos observado antes del enunciado, podemos aplicar 2.21, que nos da una demostración en B más la regla LKD* de un secuente

$$\{\gamma_0(T_{0,1,k})\}, \{\mathrm{Ind}(\gamma_i(T_{i1k}, \ldots, T_{in_ik}))\}, \Gamma^* \Rightarrow \Delta$$

sin usar reglas de inferencia de segundo orden, donde $T_{ijk} \equiv \alpha_{ijk}(x)$ es una fórmula de tipo Δ_0^0 y

$$\gamma_0(X) \equiv \bigwedge uv(u = v \wedge X(u) \rightarrow X(v)).$$

En particular, este secuente se demuestra en LKD_0^+, y todas sus fórmulas son de primer orden. Aplicando el teorema 2.28 a la fórmula asociada a este secuente, obtenemos que también puede probarse en ARP_0^2.

Ahora bien, las fórmulas $\gamma_0(T_{0,1,k})$ son teoremas de ARP_0^2, al igual que todas las que hemos añadido a Γ para formar Γ^*, luego podemos cortarlas para obtener una demostración en ARP_0^2 del secuente

$$\{\mathrm{Ind}(\gamma_i(T_{i1k}, \ldots, T_{in_ik}))\}, \Gamma \Rightarrow \Delta.$$

Ahora usamos que ARP_0^2 es una extensión intrascendente de ACR_0^-, lo que, por una parte, significa que toda fórmula de $\mathcal{L}_{\mathrm{arp}}^2$ es equivalente en ARP_0^2 a otra de $\mathcal{L}_a^2$ y, sustituyendo cada fórmula $\gamma_i(T_{i1k},\ldots,T_{in_ik}))$ por otra equivalente en $\mathcal{L}_a^2$ (que podemos tomar también de tipo Σ_n^0), podemos suponer que todas las fórmulas del secuente están en $\mathcal{L}_a^2$ (notemos que esto no afecta a las de Γ y Δ, pues son ya fórmulas de $\mathcal{L}_a^2$), y usando de nuevo que ARP_0^2 es una extensión intrascendente de ACR_0^-, concluimos que este secuente es demostrable en ACR_0^-, luego también en ACR_0. Por último, las fórmulas $\gamma_i(T_{i1k},\ldots,T_{in_ik})$ son casos particulares del esquema de Σ_n^0-inducción, luego podemos cortarlas para obtener una demostración de $\Gamma \Rightarrow \Delta$ en $\mathrm{ACR}_0+\Sigma_n^0$-inducción del secuente $\Gamma \Rightarrow \Delta$.

Si suponemos además que las fórmulas del secuente $\Gamma \Rightarrow \Delta$ no tienen variables de segundo orden, cuando llegamos a que el secuente

$$\{\gamma_0(T_{0,1,k})\}, \{\mathrm{Ind}(\gamma_i(T_{i1k},\ldots,T_{in_ik}))\}, \Gamma^* \Rightarrow \Delta$$

es demostrable en B más la regla LKD^* sin usar reglas de segundo orden, tenemos que en toda la demostración no aparecen variables ligadas de segundo orden, pues no las hay en los axiomas y no pueden aparecer sin usar las reglas de segundo orden, pero razonando como en la prueba del teorema 2.24, es decir, sustituyendo en la demostración cualquier variable libre de segundo orden por la fórmula $\delta(x) \equiv x = x$, obtenemos una demostración de un secuente análogo (en el que Γ y Δ no se alteran, pues no contienen variables de segundo orden) de modo que en la prueba no aparecen variables de segundo orden, ni libres ni ligadas. En particular, las fórmulas $\gamma_i(T_{i1k},\ldots,T_{in_ik})$ son ahora de tipo Σ_n (sin variables de segundo orden). La conclusión es ahora que en ACR_0 se demuestra el secuente

$$\{\mathrm{Ind}(\gamma_i(T_{i1k},\ldots,T_{in_ik}))\}, \Gamma \Rightarrow \Delta,$$

cuyas fórmulas no tienen variables de segundo orden. El teorema 2.27 aplicado a la fórmula asociada al secuente nos da que éste es demostrable en $\mathrm{I}\Sigma_1$, pero las premisas son casos particulares del esquema de Σ_n-inducción, luego concluimos que el secuente es demostrable en $\mathrm{I}\Sigma_n$. ■

Capítulo III

Eliminación de cortes

Nos ocupamos ahora del teorema fundamental que justifica el esfuerzo que hemos hecho por reformular la lógica matemática en términos del cálculo secuencial. Por desgracia, no existe un teorema general de eliminación de cortes del cual se puedan deducir varios casos particulares de interés, sino que existen muchos teoremas similares que admiten demostraciones más o menos similares. En este capítulo vamos a formular cuatro contextos en los que se puede demostrar un teorema de eliminación de cortes con esencialmente el mismo argumento, dos correspondientes a la lógica de primer orden y dos a la de segundo orden.

3.1 Formulación del teorema

Empezamos formulando con precisión los cuatro casos que consideraremos:

1a Tenemos un cálculo secuencial sobre un lenguaje de primer orden arbitrario $\mathcal{L}$, cuyas reglas de inferencia son las de LK y los axiomas son los *axiomas lógicos* $\alpha \Rightarrow \alpha$, donde α es una fórmula atómica, más un conjunto $\mathfrak{S}$ de *axiomas propios* (que puede incluir los axiomas de LK_i).

Suponemos además que $\mathfrak{S}$ es *cerrado para sustitución*, en el sentido de que si S es un secuente de $\mathfrak{S}$, el secuente que resulta de sustituir en todas las fórmulas de S una variable x por un término t está en $\mathfrak{S}$. Esto se cumple también para los axiomas lógicos, luego se cumple para todos los axiomas. Si $\mathfrak{S}$ incluye los axiomas de LK_i, éstos cumplen también esta condición de sustitución.

1b La misma situación anterior salvo que el lenguaje $\mathcal{L}$ es concretamente $\mathcal{L}_a$ o $\mathcal{L}_{\mathrm{arp}}$ y las reglas de inferencia incluyen además la regla Φ-IND:

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

donde y es una variable propia y la fórmula α pertenece a una clase de fórmulas Φ.

Además de la hipótesis sobre $\mathfrak{S}$ enunciada en el caso anterior, suponemos también que Φ es cerrado para sustitución, en el sentido de que al sustituir una variable x por un término t en una fórmula de Φ obtenemos una fórmula de Φ.

2a Tenemos un cálculo secuencial sobre un lenguaje de segundo orden $\mathcal{L}$ (pleno o reducido), cuyas reglas de inferencia son las de $B(\Psi)$, donde el conjunto de fórmulas Ψ que contiene al menos las fórmulas atómicas, y cuyos axiomas son los *axiomas lógicos* $\alpha \Rightarrow \alpha$, donde α es una fórmula atómica, más un conjunto $\mathfrak{S}$ de *axiomas propios*.

Suponemos que $\mathfrak{S}$ y Ψ son *cerrados para sustitución* en el sentido siguiente:

1. Si S es un secuente de $\mathfrak{S}$, el secuente que resulta de sustituir en todas las fórmulas de S una variable x por un término t está en $\mathfrak{S}$.
2. Si $\alpha(x)$ está en Ψ y t es un término, entonces $\alpha(t)$ está en Ψ.
3. Si X es una variable de rango $r \geq 1$ y $T \equiv \beta(x_1, \ldots, x_r, \bar{y}, \bar{Y})$ es una fórmula de Ψ, entonces:
   (a) Si $\alpha(X)$ está en Ψ y X puede sustituirse por T en $\alpha(X)$, entonces $\alpha(T)$ está en Ψ.
   (b) Si S es un secuente de $\mathfrak{S}$ y X puede sustituirse por T en todas las fórmulas de S, entonces el secuente que resulta de hacer las sustituciones está en $\mathfrak{S}$.

Notemos que la propiedad 2. hace que la propiedad 1. valga también para los axiomas lógicos, luego vale para todos los axiomas.

2b La misma situación anterior salvo que el lenguaje $\mathcal{L}$ es concretamente $\mathcal{L}_a^2$ o $\mathcal{L}_{\mathrm{arp}}^2$ y las reglas de inferencia incluyen además la regla de inducción Φ-IND, para cierto conjunto de fórmulas Φ.

Además de las hipótesis del caso anterior, suponemos que si $\alpha(X)$ está en Φ (donde ahora, necesariamente, $r = 1$) y X puede sustituirse por T en $\alpha(X)$, entonces $\alpha(T)$ está en Φ.

Las reglas de inferencia se clasifican en *estructurales* (debilitación y corte), *lógicas* (las de B_0) y en los casos aritméticos tenemos además una *regla de inferencia propia* (la de inducción).

En realidad vamos a considerar un quinto caso, que podríamos llamar **2c**, pero que a efectos prácticos es una mínima variante de **2b**. Se trata del cálculo secuencial ARP_0^2+LKD* descrito en el teorema 2.32 (véase 2.19 para la definición de ARP_0^2), que satisface todos los requisitos de **2b** tomando como Ψ el conjunto de las fórmulas Δ_0^0 de $\mathcal{L}_{\mathrm{arp}}^2$ y como Φ el conjunto de las fórmulas Σ_1^0, pero que incluye la regla de inferencia propia adicional LKD*, que en toda la demostración del teorema de eliminación de cortes se trata exactamente igual que la regla de inducción.

A continuación introducimos los conceptos necesarios para enunciar el teorema:

Definición 3.1 Un *hilo* en una demostración 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.

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 inmediato 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 el ejemplo de la página 30, cada descendente 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[1] 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.

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]Notemos que estos conceptos no dependen únicamente de las fórmulas, sino de su posición en la demostración.

1. Si α está en un axioma de $\mathfrak{S}$ o es una fórmula principal de una regla de inducción (o LKD*), 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[2] del secuente inferior de una regla de inferencia, $p(\alpha)$ es el máximo de las profundidades de sus ascendientes inmediatos.

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 es una fórmula principal de una regla de inducción (o LKD*), 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 30 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.

[2]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.

La demostración del ejemplo de la página 30 no tiene cortes libres. Ahora ya podemos enunciar el resultado central:

Teorema 3.2 (De eliminación de cortes libres) *Todo secuente demostrable en cualquiera de los cuatro casos considerados admite una demostración sin cortes libres.*

O, más explícitamente:

Teorema 3.3 *En un cálculo secuencial que conste de los axiomas y reglas de inferencia de* LK *más un conjunto $\mathfrak{S}$ de axiomas propios cerrado para sustitución (y, en el caso de que el lenguaje formal sea $\mathcal{L}_a$ o $\mathcal{L}_{\mathrm{arp}}$, admitimos también la regla* Φ-IND*, para un conjunto de fórmulas Φ cerrado para sustitución), todo teorema admite una demostración sin cortes libres.*

Teorema 3.4 *En un cálculo secuencial de segundo orden*[3] *que conste de los axiomas y reglas de inferencia de $B(\Psi)$ más un conjunto $\mathfrak{S}$ de axiomas propios cerrados para sustitución (y, en el caso de que el lenguaje formal sea $\mathcal{L}_a^2$ o $\mathcal{L}_{\mathrm{arp}}^2$, admitimos también la regla* Φ-IND*, para un conjunto de fórmulas Φ cerrado para sustitución), todo teorema admite una demostración sin cortes libres.*

En el caso de LK, en el que no hay regla de inducción y $\mathfrak{S}$ es el conjunto vacío, no hay fórmulas de profundidad 0, luego no hay cortes fijos, luego tenemos el siguiente caso particular:

Teorema 3.5 (de eliminación de cortes) *Si un secuente puede demostrarse en* LK*, entonces puede demostrarse sin usar la regla de corte.*

Esto no significa que la regla de corte sea redundante, pues no podemos prescindir de ella a la hora de deducir consecuencias de unas premisas dadas (el teorema precedente sólo se aplica a demostraciones, es decir, a deducciones sin premisas adicionales).

Si tomamos como $\mathfrak{S}$ el conjunto de los axiomas del igualador, las fórmulas de profundidad 0 son necesariamente de la forma $t_1 = t_2$, por lo que el teorema de eliminación de cortes implica que todo teorema de LK_i admite una demostración en la que las únicas fórmulas de corte son de la forma $t_1 = t_2$.

Similarmente, la versión de segundo orden se aplica a la lógica predicativa B_0, es decir, al cálculo secuencial que resulta de tomar como Ψ el conjunto de todas las fórmulas de primer orden y con el conjunto $\mathfrak{S}$ de axiomas propios vacío. Claramente se cumplen las hipótesis del teorema de eliminación de cortes libres, pero en una demostración no puede haber cortes fijos, luego la conclusión es:

Teorema 3.6 (de eliminación de cortes) *Si un secuente puede demostrarse en B_0, entonces puede demostrarse sin usar la regla de corte.*

[3]El cálculo ARP_0^2+ LKD* también cumple este teorema.

Ejemplo Ahora podemos entender la importancia en el cálculo secuencial de la distinción entre variables libres y ligadas. Imaginemos que no hubiéramos establecido dicha distinción y que una misma variable pudiera aparecer libre en una fórmula y ligada en otra. Entonces esto sería una demostración en LK:

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

Sin embargo, el secuente final, a pesar de que debería ser demostrable (porque es verdadero en cualquier modelo) no puede demostrarse sin cortes. En efecto, una demostración sin cortes tendría que ser necesariamente de esta forma:

$$\dfrac{\dfrac{Rxy \Rightarrow Rst}{Rxy \Rightarrow \bigvee x\, Rsx}}{Rxy \Rightarrow \bigvee yx\, Ryx}$$

para ciertos términos s, t, pero, para que el secuente inicial fuera un axioma, tendrían que ser $s \equiv x$, $t \equiv y$, pero eso es imposible, porque la “demostración” sería:

$$\dfrac{\dfrac{Rxy \Rightarrow Rxy}{Rxy \Rightarrow \bigvee x\, Rxx}}{Rxy \Rightarrow \bigvee yx\, Ryx}$$

pero el secuente intermedio no es un teorema lógico en virtud del teorema de corrección 1.4, pues es fácil definir un modelo en el que es falso. Vemos que para que la regla derecha del particularizador siguiera siendo válida habría que introducir la restricción de que la variable que se introduce al particularizar no esté libre en la fórmula, pero eso sólo haría más patente la imposibilidad de demostrar sin cortes el secuente final. ■

3.2 Prueba del teorema de eliminación de cortes

Las condiciones sobre sustitución que hemos impuesto sirven principalmente para que se cumplan los teoremas siguientes:

Teorema 3.7 *En las condiciones anteriores, sea D una demostración, 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: 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, la derecha del generalizador (de primer o segundo orden) o la de inducción (o LKD*), pero en éstas tenemos en cuenta que 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 (y al realizar la sustitución las fórmulas que estaban en Ψ o Φ se convierten en fórmulas de la misma clase), luego la regla sigue siendo válida. ■

Necesitamos una versión de segundo orden de este teorema, y para ello necesitamos modificar provisionalmente los supuestos de los casos de segundo orden 2a y 2b. En principio hemos supuesto que consideramos cálculos secuenciales cuyos axiomas lógicos sean los secuentes $\alpha \Rightarrow \alpha$ donde α es una fórmula atómica, pero a partir de aquí imponemos una condición adicional:

> *En los casos* 2a *y* 2b *suponemos que el cálculo secuencial considerado tiene como axiomas todos los secuentes de la forma $\alpha \Rightarrow \alpha$ con la fórmula α en el conjunto Ψ, aunque no sea atómica.*

Demostraremos el teorema de eliminación de cortes con este supuesto, pero luego podemos eliminarlo, pues, dada una demostración de un secuente que parta de los axiomas lógicos usuales (para fórmulas atómicas) el teorema nos dará una demostración sin cortes en la que se admiten como axiomas los secuentes $\alpha \Rightarrow \alpha$ con α en Ψ, pero dichos secuentes se pueden demostrar sin cortes en B (como se ve en la prueba del teorema 1.5, que se adapta trivialmente a la lógica de segundo orden), luego la demostración se puede completar hasta una demostración sin cortes libres a partir de los axiomas lógicos usuales.

Con este artificio, el teorema siguiente se prueba igual que el anterior:

Teorema 3.8 *Sea D una demostración, sea X una variable que no se use como variable propia en ninguna regla de inferencia de D y sea $T \equiv \alpha(\bar{x})$ una fórmula de Ψ que no contenga ninguna variable propia de ninguna regla de inferencia de D y tal que X pueda sustituirse por T en todos los secuentes de 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.*

Sólo hay que observar que, con la hipótesis adicional que acabamos de añadir, al sustituir X por T en un axioma de tipo $\alpha(X) \Rightarrow \alpha(X)$, seguimos teniendo un axioma de este tipo (pero la fórmula $\alpha(T)$ ya no tiene por qué ser atómica).

Definición 3.9 Una demostración 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 (o LKD*), 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 3.10 *Toda demostración puede transformarse en una demostración regular del mismo secuente sin más que cambiar unas variables propias por otras.*

Demostración: Observemos que si en una demostración D cambiamos todas las apariciones de una variable libre de primer orden x (o de segundo orden X) por otra y (resp. Y) que no aparezca en D, el resultado es una nueva demostración. Esto se sigue de los dos teoremas precedentes, aplicados al término y o a la fórmula atómica $T \equiv Y(x_1, \ldots, x_r)$ (de modo que sustituir X por T es lo mismo que sustituir X por Y).

Así pues, dada una demostración D, para cada secuente S que resulte de aplicar una regla derecha del generalizador, o de una regla izquierda del particularizador o de inducción (o LKD*), consideramos la subdemostración D' formada por los secuentes de D situados sobre S, que es en sí misma una demostración de S. Al cambiar la variable propia por otra que no aparezca en D obtenemos otra 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. ■

Pasamos ya a la prueba del teorema de eliminación de cortes. Un hecho que usaremos a menudo será el siguiente:

Observación 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 en primer lugar un caso sencillo de eliminación de cortes:

Teorema 3.11 *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[4] 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 que es:

$$\begin{array}{c} D_0 \\ \vdots \\ \Gamma \Rightarrow \Delta \\ \hline \Gamma \Rightarrow \Delta,\, \alpha \end{array}$$

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

[4]Para formalizar esta inducción en ARP tenemos en cuenta que, según el lector observará, la nueva demostración D' se construye siempre quitando partes de la demostración D (quitando fórmulas en secuentes, o secuentes enteros, o subárboles), sin añadir nunca nada nuevo. Por lo tanto, dada D, podemos considerar el conjunto $F(D)$ de todas las fórmulas que aparecen en D y el número $N(D)$ de reglas de inferencia que se usan en D y formar el conjunto $X(D)$ de todas las demostraciones formadas con fórmulas de $F(D)$ con a lo sumo $N(D)$ reglas de inferencia, y a su vez los conjuntos $X_n(D)$ de demostraciones en $X(D)$ con exactamente n reglas de inferencia. Basta construir un funtor que a cada n le asigne una aplicación

$$H(D, n) : X_n(D) \times \mathcal{P}F(D) \longrightarrow X(D),$$

de modo que si $D^* \in X_n(D)$ y $a \in \mathcal{P}F(D)$ es un conjunto de fórmulas con profundidad $-\infty$ en el último secuente de D^*, entonces $H(D, n)(D^*, a)$ es una demostración en las condiciones del teorema del secuente que resulta de eliminar las fórmulas de a del último secuente de D^*. El argumento que vamos a dar muestra cómo definir $H(D, n)$ supuesto definido $H(D, m)$ para todo $m < n$.

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 antecesores.)

b) Si $\alpha \vee \beta$ 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. (La regla LKD* se trata análogamente.) ■

El núcleo de la prueba del teorema de eliminación de cortes libres es el resultado siguiente:

Teorema 3.12 *Sea D una demostración 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 3.10, 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. En primer lugar consideramos el caso en que 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 (o LKD*). Transformamos D_1 como sigue:

Cada axioma lógico $\epsilon \Rightarrow \epsilon$ lo reemplazamos por

$$\dfrac{\begin{array}{c} D_2 \\ \vdots \\ \epsilon,\, \Gamma \Rightarrow \Delta \end{array}}{\epsilon,\, \Gamma \Rightarrow \Delta,\, \epsilon}$$

de modo que la profundidad de ϵ en el consecuente final es $-\infty$. Añadiendo Γ y Δ en los secuentes posteriores (y aquí tenemos en cuenta que, como la demostración es regular, en Γ y Δ no puede haber variables libres que sean propias en alguna regla de inferencia anterior) 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 ϵ, $\Gamma \Rightarrow \Delta$ 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.

Si ϵ no es atómica, no puede ser $p = 0$ (o el corte sería fijo), luego $p \geq 1$.

El mismo argumento empleado en el caso precedente nos permite sustituir cada axioma lógico que contenga un ascendiente de ϵ en D_1 o D_2 por una demostración en la que el ascendiente pase a tener profundidad $-\infty$. Así obtenemos nuevas demostraciones D_1 y D_2 que siguen teniendo cortes libres de profundidad $< p$ y la profundidad de las dos fórmulas de corte es menor o igual que la original. Si alguna de ellas es $-\infty$, basta aplicar el teorema anterior para eliminar ϵ y obtener una demostración de $\Gamma \Rightarrow \Delta$ en las condiciones requeridas. Si alguna de ellas es 0, el corte pasa a ser fijo y ya tenemos la prueba deseada. Por lo tanto, no sólo tenemos que $p \geq 1$, sino que podemos suponer que las fórmulas de corte ϵ no tienen ascendientes directos en axiomas lógicos.

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 (o LKD*), que tienen profundidad 0.

3. Fórmulas principales de reglas derechas del negador, que pueden tener cualquier profundidad no nula.

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,[5] mientras que las que tengan dos secuentes superiores, si a uno

[5]Notemos que no se puede añadir α como fórmula colateral en una regla si α contiene una variable propia de dicha regla, pero como todas las reglas que consideramos tienen $\neg\alpha$ en el consecuente, es seguro que ninguna variable de α será propia para dicha regla.

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 (o LKD*).

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:

$$\frac{\begin{array}{c} D_1' \\ \vdots \\ \alpha,\,\Gamma \Rightarrow \Delta,\,\neg\alpha \end{array} \qquad \begin{array}{c} D_2 \\ \vdots \\ \dfrac{\neg\alpha,\,\Gamma \Rightarrow \Delta}{\neg\alpha,\,\alpha,\,\Gamma \Rightarrow \Delta} \end{array}}{\alpha,\,\Gamma \Rightarrow \Delta}$$

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

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

lo que la transforma en una regla de debilitación. En las fórmulas posteriores mantenemos los α y 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:

$$\frac{\begin{array}{c} D_1' \\ \vdots \\ \Gamma \Rightarrow \Delta, \alpha, \beta, \alpha \vee \beta \end{array} \qquad \dfrac{\begin{array}{c} D_2 \\ \vdots \\ \alpha \vee \beta, \Gamma \to \Delta \end{array}}{\alpha \vee \beta, \Gamma \Rightarrow \Delta, \alpha, \beta}}{\Gamma \Rightarrow \Delta, \alpha, \beta}$$

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 D_2 también podemos eliminar los asdendientes directos de $\alpha \vee \beta$ que procedan de axiomas lógicos, pero en este punto se rompe la simetría del caso anterior. Ahora 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:

$$
\dfrac{\dfrac{\begin{matrix} D_1'' \\ \vdots \\ \Gamma \Rightarrow \Delta,\, \alpha,\, \beta \end{matrix} \qquad \dfrac{\begin{matrix} D_2'^\beta \\ \vdots \\ \beta,\, \Gamma \Rightarrow \Delta \end{matrix}}{\beta,\, \Gamma \Rightarrow \Delta,\, \alpha}}{\Gamma \Rightarrow \Delta,\, \alpha} \qquad \begin{matrix} D_2'^\alpha \\ \vdots \\ \alpha,\, \Gamma \Rightarrow \Delta \end{matrix}}{\Gamma \Rightarrow \Delta}
$$

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 3.7. 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:

$$\dfrac{\dfrac{\begin{matrix} D_1 \\ \vdots \\ \Gamma \Rightarrow \Delta, \bigvee u\, \alpha(u)\end{matrix}}{\alpha(y), \Gamma \Rightarrow \Delta, \bigvee u\, \alpha(u)} \qquad \begin{matrix} D_2' \\ \vdots \\ \bigvee u\, \alpha(u), \alpha(y), \Gamma \Rightarrow \Delta\end{matrix}}{\alpha(y), \Gamma \Rightarrow \Delta}$$

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_2, 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 3.7 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

$$\frac{\Gamma' \Rightarrow \Delta',\, \alpha(t_i)}{\Gamma' \Rightarrow \Delta',\, \bigvee u\, \alpha(u)}$$

por

$$\dfrac{\dfrac{\dfrac{\begin{matrix} \vdots \\ \Gamma' \Rightarrow \Delta',\, \alpha(t_i)\end{matrix}}{\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta,\, \alpha(t_i)} \qquad \dfrac{\begin{matrix} D_2''(t_i) \\ \vdots \\ \alpha(t_i),\, \Gamma \Rightarrow \Delta\end{matrix}}{\alpha(t_i),\, \Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta}}{\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta}}{\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta,\, \bigvee u\, \alpha(u)}$$

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 $\epsilon \equiv \bigwedge u\, \alpha(u)$ es completamente análogo al precedente.

También es análogo el caso en que $\epsilon \equiv \bigvee U\, \alpha(U)$, pero vamos a detallarlo. Cada aplicación en D_2 de la regla izquierda del particularizador que genera un ascendiente directo de ϵ será de la forma

$$\frac{\alpha(Y),\, \Gamma' \Rightarrow \Delta'}{\bigvee U \alpha(U),\, \Gamma' \Rightarrow \Delta'}$$

y la transformamos en

$$\frac{\alpha(Y),\, \Gamma' \Rightarrow \Delta'}{\bigvee U \alpha(U),\, \alpha(Y),\, \Gamma' \Rightarrow \Delta'},$$

donde Y es una variable que no aparezca en D, y usamos la misma en todos los casos. Al sustituir Y_i por Y en todos los secuentes que están por encima del secuente superior, obtenemos una demostración de $\alpha(Y), \Gamma' \Rightarrow \Delta'$, esta vez en virtud del teorema 3.8, tomando $T \equiv Y(x_1, \ldots, x_r)$, de modo que sustituir Y_i por T es simplemente sustituir Y_i por Y. Añadiendo $\alpha(Y)$ en los secuentes inferiores (usando la regla de debilitación cuando haga falta para enlazar con otras ramas) obtenemos una demostración D_2' de $\bigvee U \alpha(U), \alpha(Y), \Gamma \Rightarrow \Delta$, de la que obtenemos, exactamente igual que en el caso de primer orden, una demostración D_2'' de $\alpha(Y), \Gamma \Rightarrow \Delta$.

Ahora el teorema 3.8 nos da que si $T \equiv \alpha(\bar{x})$ es una fórmula de Ψ que no contenga ninguna variable propia de ninguna regla de inferencia de D_2'' y tal que Y pueda sustituirse por T en todos los secuentes de D_2'', entonces al realizar la sustitución obtenemos una demostración $D_2''(T)$ del secuente $\alpha(T), \Gamma \Rightarrow \Delta$ en la que las fórmulas y cortes tienen la misma profundidad que sus correspondientes en D_2''.

Pasamos entonces a D_1 y cambiamos cada regla

$$\frac{\Gamma' \Rightarrow \Delta',\, \alpha(T_i)}{\Gamma' \Rightarrow \Delta',\, \bigvee U\, \alpha(U)}$$

por

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\vdots\\ \Gamma' \Rightarrow \Delta',\, \alpha(T_i)\end{matrix}}{\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta,\, \alpha(T_i)} \qquad \dfrac{\begin{matrix}D_2''(T_i)\\ \vdots\\ \alpha(T_i),\, \Gamma \Rightarrow \Delta\end{matrix}}{\alpha(T_i),\, \Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta}}{\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta}}{\Gamma',\, \Gamma \Rightarrow \Delta',\, \Delta,\, \bigvee U \alpha(U)}$$

El mismo razonamiento del caso de primer orden nos permite llegar a una demostración D_1' del secuente $\Gamma \Rightarrow \Delta, \bigvee U \alpha(U)$ en las mismas condiciones, de ahí se llega a su vez a la conclusión requerida.

El caso $\epsilon \equiv \bigwedge U \alpha(U)$ es análogo. ■

Aplicando sucesivamente el teorema anterior podemos reducir la profundidad máxima de los cortes libres en una demostración:

Teorema 3.13 *Si D es una demostración cuyos cortes libres tengan todos profundidad $\leq p$, con $p \geq 0$, existe otra 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[6] sobre el número de cortes libres de profundidad p 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:

Demostración (de 3.2): Por el teorema anterior podemos conseguir una demostración cuyos cortes libres (en caso de tenerlos) tengan todos profundidad $-\infty$. Si los hay, aplicamos 3.11, que nos da una prueba sin cortes libres. ■

[6]En ARP podemos construir un funtor que transforme cada demostración D en las condiciones del enunciado en otra con menos cortes libres de profundidad p (o que la deje invariante si no tiene ninguno). Iterando el funtor tantas veces como cortes libres de profundidad p tiene una demostración dada, obtenemos otra sin cortes libres de profundidad p.

Capítulo IV

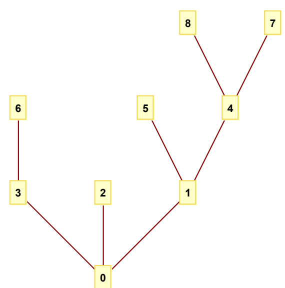
Ordinales

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

$$\omega < \omega^\omega < \omega^{\omega^\omega} < \omega^{\omega^{\omega^\omega}} < \quad \cdots$$

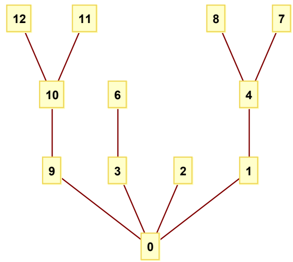
el supremo de todos estos ordinales se llama ϵ_0, y es el menor ordinal que no puede expresarse en términos de números naturales y ω mediante sumas, productos o potencias. En este capítulo veremos que los ordinales menores que ϵ_0 pueden definirse en la Aritmética Recursiva Primitiva, de modo que es 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.

4.1 Hércules y la Hidra I

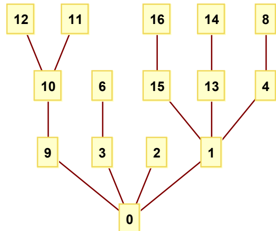


La figura muestra una *hidra*. Es simplemente un árbol con una raíz (en la figura marcada con un 0), de la que sale un número finito de ramas, de cada una de las cuales sale a su vez un número finito de ramas, y así sucesivamente, hasta alcanzar una cierta altura finita. Los nodos terminales de los que 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.

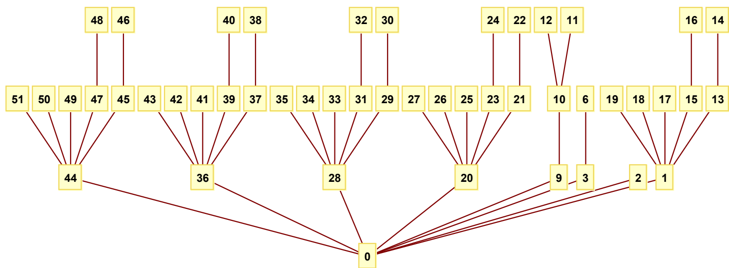
Hay que entender que hemos numerado los nodos simplemente para facilitar las referencias, pero la numeración no forma parte de la hidra. Si renumeramos los nodos seguiremos teniendo la misma hidra.



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:



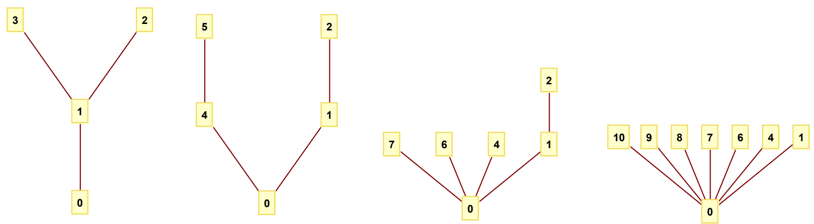
En el tercer asalto, la arista $1-4$ generó los cuellos de las cabezas 17, 18 y 19, mientras que en el cuarto asalto la arista $0-1$ ha generado las cuatro aristas $0-20$, $0-28$, $0-36$ y $0-44$. Ahora la Hidra tiene 29 cabezas.

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.



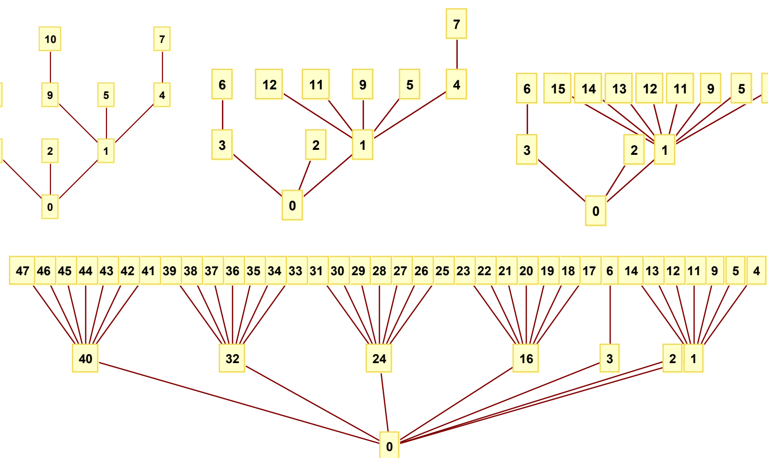
Vemos que al tercer asalto ha quedado reducida a una hidra-bebé, que tras el décimo asalto estará muerta.

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

$$\begin{array}{c}989\,053\,388\,168\,938\,379\,565\,429\,552\,367\,644\,648\,402\,300\,582\\379\,429\,351\,736\,318\,357\,588\,790\,729\,278\,822\,309\,452\,445\,327\end{array}$$

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.

4.2 Ordinales en la aritmética

Trabajamos en la aritmética recursiva primitiva ARP, donde consideramos el funtor definido como sigue:

$$\begin{aligned} F_{\preceq}(0) &= 0, \\ F_{\preceq}(n+1) &= \{x \leq \langle n, n\rangle \mid \bigvee \alpha\beta \leq n(x = \langle \alpha, \beta\rangle \wedge \cdots)\}, \end{aligned}$$

donde los puntos suspensivos son la conjunción de las fórmulas siguientes:

1. $\bigwedge ij < \ell(\alpha)(i \leq j \rightarrow \langle \alpha_j, \alpha_i\rangle \in F_{\preceq}(n))$,
2. $\bigwedge ij < \ell(\beta)(i \leq j \rightarrow \langle \beta_j, \beta_i\rangle \in F_{\preceq}(n))$,
3. $\alpha \sqsubseteq \beta \vee \bigvee i < \ell(\alpha)(i < \ell(\beta) \wedge \alpha|_i = \beta|_i \wedge \alpha_i \neq \beta_i \wedge \langle \alpha_i, \beta_i\rangle \in F_{\preceq}(n))$.

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

$$\alpha < n \wedge \beta < n \rightarrow (\langle \alpha, \beta\rangle \in F_{\preceq}(n) \leftrightarrow \langle \alpha, \beta\rangle \in F_{\preceq}(n+1)).$$

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

$$\alpha < n \wedge \beta < n \wedge n \leq m \rightarrow (\langle \alpha, \beta\rangle \in F_{\preceq}(n) \leftrightarrow \langle \alpha, \beta\rangle \in F_{\preceq}(m)).$$

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 $\preceq$:

$$\alpha \preceq \beta \leftrightarrow \bigwedge ij < \ell(\alpha)(i \leq j \rightarrow \alpha_j \preceq \alpha_i) \wedge \bigwedge ij < \ell(\beta)(i \leq j \rightarrow \beta_j \preceq \beta_i) \wedge$$

$$\alpha \sqsubseteq \beta \vee \bigvee i < \ell(\alpha)(i < \ell(\beta) \wedge \alpha|_i = \beta|_i \wedge \alpha_i \prec \beta_i),$$

donde hemos usado la notación $x \prec y \equiv (x \preceq y \wedge x \neq y)$.

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

$$\alpha \preceq \beta \to \alpha \in E \land \beta \in E,$$

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 4.1 *La relación $\preceq$ es una relación de orden total en E, es decir:*

1. $\bigwedge \alpha \in E\, \alpha \preceq \alpha,$
2. $\bigwedge \alpha\beta \in E(\alpha \preceq \beta \land \beta \preceq \alpha \to \alpha = \beta),$
3. $\bigwedge \alpha\beta\gamma \in E(\alpha \preceq \beta \land \beta \preceq \gamma \to \alpha \preceq \gamma),$
4. $\bigwedge \alpha\beta \in E(\alpha \preceq \beta \lor \beta \preceq \alpha).$

Demostración: 1) La reflexividad es inmediata.

2) Supongamos que existe un par (α, β) que incumple la propiedad 2, de modo que $\alpha \preceq \beta \land \beta \preceq \alpha$, 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 $\alpha \preceq \alpha \land \beta \preceq \beta$. Si se cumple $\alpha \sqsubseteq \beta$ o $\beta \sqsubseteq \alpha$ es inmediato que se cumple $\alpha \preceq \beta \lor \beta \preceq \alpha$. 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 $\alpha_i \preceq \beta_i \lor \beta_i \preceq \alpha_i$, luego de hecho $\alpha_i \prec \beta_i \lor \beta_i \prec \alpha_i$, y esto implica $\alpha \preceq \beta \lor \beta \preceq \alpha$, 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 4.2 *Se cumple:*

1. $0 \in E \land \bigwedge \alpha \in E\, 0 \preceq \alpha.$
2. $\bigwedge \alpha \in E(\alpha' \in E \land \alpha \prec \alpha').$
3. $\bigwedge \alpha\beta \in E(\alpha \prec \beta \to \alpha' \preceq \beta).$

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 del ejemplo tras [LF 2.6]):

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 4.3 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 4.4 *Se cumple:*

1. $\omega \in E$,
2. $\bigwedge n\, \hat{n} \prec \omega$,
3. $\bigwedge \alpha \in E (\bigvee n\, \alpha = \hat{n} \lor \omega \preceq \alpha)$.

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 $\hat{n} \prec \omega$.

[1] Incidentalmente, es $\omega = \langle \hat{1} \rangle = \langle 1 \rangle = 2$.

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 4.5 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 4.6 *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 del ejemplo tras [LF 2.6] 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 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,

$$2 \cdot 3 = 2 \cdot (1 + 1 + 1) = 2 + 2 + 2 = 6.$$

Más en general, si k es un ordinal finito, se cumple que $\alpha \cdot k = \alpha + \cdots + \alpha$ con k sumandos.

[2] El hecho de que podamos definirla en ARP prueba que es recursiva primitiva o, más precisamente, que (en ACR_0) podemos definir una función recursiva primitiva $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ que se restringe a la suma en $E \times E$.

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 4.7 *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 en ACR_0 podemos probar que el producto de ordinales se extiende a una aplicación recursiva primitiva $f : \mathbb{N}^2 \longrightarrow \mathbb{N}$.

[4] Por ello la prueba es formalizable en ARP y la aplicación $(\alpha, \beta) \mapsto \delta$ es recursiva primitiva.

Teorema 4.8 *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:

$$\omega_{k+1}(\alpha\#\beta) = \omega^{\omega_k(\alpha\#\beta)} \geq \omega^{\omega_k(\alpha)\#\omega_k(\beta)} \geq \omega^{\omega_k(\alpha)}\#\omega^{\omega_k(\beta)} = \omega_{k+1}(\alpha)\#\omega_{k+1}(\beta).$$

■

4.3 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 4.9 *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 4.10 *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 4.11 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 4.12 *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 4.12 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 $\{\lambda[n]\}_{n=0}^{\infty}$.

4.4 Inducción transfinita

Uno de los teoremas básicos sobre ordinales que se demuestran en la teoría de conjuntos es que están bien ordenados, es decir, que todo conjunto no vacío de ordinales tiene un mínimo elemento. Podemos plantearnos —y va a ser crucial— si podemos probar este hecho en el contexto aritmético en el que hemos definido los ordinales (menores que ϵ_0).

Observemos en primer lugar que las fórmulas $\alpha \in E$ y $\alpha \preceq \beta$ son fórmulas Δ_0 de $\mathcal{L}_{\rm arp}$, que tienen una interpretación natural, es decir, tenemos definido lo que significa que un número natural sea o no un ordinal y lo que significa que un (número natural que sea un) ordinal sea mayor o menor que otro. Más aún, se trata de relaciones recursivas primitivas. Podemos programar a un ordenador para que nos diga si un número natural dado es o no un ordinal y, dados dos ordinales, cuál es el menor de ellos (respecto de la relación $\preceq$).

Si ahora nos preguntamos si es verdad o no que todo conjunto no vacío de ordinales tiene un mínimo elemento (respecto de la relación $\preceq$), la única precaución es que no tenemos ninguna determinación de lo que hay que entender por "todo conjunto de ordinales". Formalizar esta afirmación en estos términos nos obligaría a considerar la aritmética de segundo orden, pero de momento podemos restringirnos a considerar conjuntos definibles mediante fórmulas de un determinado lenguaje formal, y así, podemos plantearnos si, para una fórmula $\phi(\alpha)$ de $\mathcal{L}_{\rm arp}$, o de $\mathcal{L}_a$ (tal vez con más variables libres), es verdadera la fórmula

$$\phi-\mathrm{MIN} \equiv \bigvee \alpha \in E\, \phi(\alpha) \rightarrow \bigvee \alpha \in E(\phi(\alpha) \wedge \bigwedge \delta \prec \alpha \neg\phi(\delta)).$$

Esto puede reformularse en términos de una generalización del principio de inducción:

$$\phi-\mathrm{IND}(\epsilon_0) \equiv \bigwedge \alpha \in E(\bigwedge \delta \prec \alpha\, \phi(\delta) \rightarrow \phi(\alpha)) \rightarrow \bigwedge \alpha \in E\, \phi(\alpha).$$

Este principio de inducción afirma que si, suponiendo que todos los ordinales $\delta \prec \alpha$ cumplen $\phi(\delta)$, podemos asegurar que se cumplen $\phi(\alpha)$, entonces podemos concluir que todos los ordinales cumplen $\phi(\alpha)$.

La relación entre ambos principios es que en ARP podemos probar que

$$\phi - \mathrm{IND}(\epsilon_0) \leftrightarrow \neg\phi - \mathrm{MIN}.$$

En efecto, si suponemos $\neg\phi-$MIN, así como que

$$\bigwedge \alpha \in E(\bigwedge \delta \prec \alpha\, \phi(\delta) \rightarrow \phi(\alpha)),$$

podemos probar $\bigwedge \alpha \in E\, \phi(\alpha)$ por reducción al absurdo. Si $\bigvee \alpha \in E\, \neg\phi(\alpha)$, por $\neg\phi-$MIN, tenemos que

$$\bigvee \alpha \in E(\neg\phi(\alpha) \wedge \bigwedge \delta \prec \alpha\, \phi(\delta)),$$

que contradice a lo supuesto, luego tenemos $\phi - \mathrm{IND}(\epsilon_0)$. Recíprocamente, si suponemos el principio de inducción y negamos $\neg\phi-$MIN, tenemos que

$$\bigvee \alpha \in E \neg\phi(\alpha) \wedge \bigwedge \alpha \in E(\bigwedge \delta \prec \alpha \neg\phi(\delta) \rightarrow \neg\phi(\alpha)),$$

pero entonces el principio de inducción nos da $\bigwedge \alpha \in E\, \neg\phi(\alpha)$ y tenemos una contradicción.

Así pues, podemos plantearnos si es cierto el principio de inducción para todas las fórmulas ϕ de $\mathcal{L}_{\mathrm{arp}}$ o de $\mathcal{L}_a$ o, mejor aún, si podemos demostrarlo en ARP, o en AP, o en alguna otra teoría aritmética. Y sucede que la razón fundamental por la que nos hemos interesado por la formalización aritmética de los ordinales es que, como veremos en el capítulo siguiente, existe una fórmula $\phi(\alpha)$ de tipo Π_1 en $\mathcal{L}_{\mathrm{arp}}$ (con α como única variable libre) tal que en ARP se puede demostrar que

$$\phi - \mathrm{IND}(\epsilon_0) \rightarrow \mathrm{Consis}\ulcorner \mathrm{AP} \urcorner.$$

Por lo tanto, el segundo teorema de incompletitud de Gödel [LF 9.8] nos asegura que en AP no es posible demostrar el principio de inducción transfinita hasta ϵ_0 ni siquiera para fórmulas de tipo Π_1. No obstante, vamos a ver que en AP "casi" se puede demostrar $\phi - \mathrm{IND}(\epsilon_0)$ para cualquier fórmula (aritmética) ϕ.

Para ello definimos un principio más débil:

$$\phi - \mathrm{IND}(\theta) \equiv \bigwedge \alpha \in E(\bigwedge \delta \prec \alpha\, \phi(\delta) \rightarrow \phi(\alpha)) \rightarrow \bigwedge \alpha \prec \theta\, \phi(\alpha).$$

Así, la hipótesis es la misma que la de $\phi-\mathrm{IND}(\epsilon_0)$, pero la conclusión se restringe a ordinales menores que θ. Vamos a probar que en AP se puede demostrar

$$\phi - \mathrm{IND}(\omega^{(1)}), \quad \phi - \mathrm{IND}(\omega^{(2)}), \quad \phi - \mathrm{IND}(\omega^{(3)}), \quad \ldots$$

para toda fórmula ϕ, lo cual nos asegura que si la sentencia

$$\bigwedge \alpha \in E(\bigwedge \delta \prec \alpha\, \phi(\delta) \rightarrow \phi(\alpha))$$

es verdadera (o, en caso de que ϕ tenga otras variables libres, si la fórmula es satisfecha respecto a cierta valoración), entonces también se cumple

$$\bigwedge \alpha \prec \omega^{(1)}\, \phi(\alpha), \quad \bigwedge \alpha \prec \omega^{(2)}\, \phi(\alpha), \quad \bigwedge \alpha \prec \omega^{(3)}\, \phi(\alpha), \quad \ldots$$

y esto implica que la fórmula $\bigwedge \alpha \in E\, \phi(\alpha)$ también es verdadera, aunque esto no es demostrable en AP, pues tenemos una demostración distinta para cada ordinal $\omega^{(n)}$, es decir, para cada numeral n, no una única demostración en la que n sea una variable.

Dada una fórmula $\phi(\alpha)$ de $\mathcal{L}_a$ (tal vez con más variables libres), definimos

$$\phi^*(\alpha) \equiv \bigwedge \beta \preceq \alpha\, \phi(\beta),$$

$$\phi'(\eta) \equiv \bigwedge \alpha(\phi^*(\alpha) \to \phi^*(\alpha + \omega^\eta)).$$

Notemos que si ϕ es de tipo Π_n, entonces ϕ^* también es de tipo Π_n, mientras que $\phi'(\eta)$ es de tipo Π_{n+1}. El interés de estas definiciones se debe al teorema siguiente (que se demuestra en ARP, como todos los teoremas que hemos probado hasta ahora):

Teorema 4.13 *Si ϕ es una fórmula de $\mathcal{L}_a$ (o de $\mathcal{L}_{\mathrm{arp}}$), se cumple*

$$\bigwedge n(\phi(0) \land \bigwedge \alpha \preceq \omega^{(n)} \phi'(\alpha) \to \bigwedge \alpha \preceq \omega^{(n+1)} \phi(\alpha)).$$

DEMOSTRACIÓN: Si suponemos $\phi(0) \land \bigwedge \alpha \preceq \omega^{(n)} \phi'(\alpha)$, en particular $\phi'(\omega^{(n)})$, que, por definición, es

$$\bigwedge \alpha(\phi^*(\alpha) \to \phi^*(\alpha + \omega^{(n+1)})).$$

En particular, para $\alpha = 0$, tenemos que $\phi^*(0) \to \phi^*(\omega^{(n+1)})$, pero $\phi^*(0)$ equivale a $\phi(0)$, luego tenemos $\phi^*(\omega^{(n+1)})$, que es lo que hay que probar. ■

Así pues, si queremos probar que todos los ordinales hasta $\omega^{(n+1)}$ cumplen $\phi(\alpha)$, basta probar que todos los ordinales hasta $\omega^{(n)}$ cumplen $\phi'(\alpha)$. Esto nos lleva al teorema siguiente:

Teorema 4.14 *Si $\phi(\alpha)$ es una fórmula de $\mathcal{L}_a$ de tipo Π_n, en $\mathrm{I}\Sigma_n$ se demuestra*

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi(\beta) \to \phi(\alpha)) \to \bigwedge \eta \in E(\bigwedge \delta \prec \eta\, \phi'(\delta) \to \phi'(\eta)).$$

DEMOSTRACIÓN: Suponemos

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi(\beta) \to \phi(\alpha)) \tag{4.1}$$

y observamos que esto implica

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi^*(\beta) \to \phi^*(\alpha)). \tag{4.2}$$

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 (4.1), podemos concluir $\phi(\alpha)$, luego concluimos $\bigwedge \beta \preceq \alpha\, \phi(\beta)$, que es $\phi^*(\alpha)$.

Fijamos ahora $\eta \in E$ y suponemos

$$\bigwedge \delta \prec \eta\, \phi'(\delta). \tag{4.3}$$

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 (4.1) 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

$$\bigwedge k\, \phi^*(\alpha + \omega^\delta \cdot k). \tag{4.4}$$

Notemos que la fórmula es de tipo Π_n, por lo que podemos razonar en $\mathrm{I}\Sigma_n$. Para $k = 0$ esto se reduce a $\phi^*(\alpha)$, y estamos suponiendo que se cumple. Ahora suponemos $\phi^*(\alpha + \omega^\delta \cdot k)$. Por (4.3) 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 (4.4), 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 (4.4) se cumple $\phi^*(\alpha + \omega^\delta \cdot k)$, luego también $\phi^*(\beta)$. Por (4.2) 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 (4.3) 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 (4.2) tenemos $\phi^*(\alpha + \omega^\eta)$. ■

Así ya es fácil probar:

Teorema 4.15 *Si $\phi(\alpha)$ es una fórmula de $\mathcal{L}_a$ de tipo Π_m, en $\mathrm{I}\Sigma_{n+m-1}$ se puede probar $\phi - \mathrm{IND}(\omega^{(n)})$.*

DEMOSTRACIÓN: Por simplicidad vamos a tomar $n = 4$, pero el argumento es general. Suponemos

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi(\beta) \to \phi(\alpha)),$$

de donde, aplicando repetidamente el teorema anterior,

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi'(\beta) \to \phi'(\alpha)),$$

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi''(\beta) \to \phi''(\alpha)),$$

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi'''(\beta) \to \phi'''(\alpha)). \tag{4.5}$$

Notemos que la primera aplicación es válida en $\mathrm{I}\Sigma_m$, la segunda en $\mathrm{I}\Sigma_{m+1}$ y la tercera en $\mathrm{I}\Sigma_{m+2}$, es decir, en $\mathrm{I}\Sigma_{n+m-2}$.

Observemos que de aquí se deduce en particular $\phi'(0)$, $\phi''(0)$, $\phi'''(0)$, mientras que $\phi(0)$ se deduce de la hipótesis inicial.

En particular (4.5) vale para todo ordinal finito α, es decir, que para cada número natural k, tenemos que

$$\bigwedge l < k\, \phi'''(\bar{l}) \rightarrow \phi'''(\bar{k}),$$

donde $\bar{l}$, $\bar{k}$ representan los ordinales finitos correspondientes a l y k. La fórmula $\phi'''(\bar{k})$ es Π_{m+3}, es decir, Π_{n+m-1}, luego en $\mathrm{I}\Sigma_{n+m-1}$ podemos concluir por inducción que $\bigwedge k\, \phi'''(\bar{k})$ o, equivalentemente, que $\bigwedge \alpha \prec \omega^{(1)}\, \phi'''(\alpha)$.

Aplicando (4.5) a $\alpha = \omega$ tenemos $\bigwedge \alpha \preceq \omega^{(1)}\, \phi'''(\alpha)$. Ahora aplicamos repetidamente 4.13 (usando, sucesivamente, $\phi''(0), \phi'(0), \phi(0)$) 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 $n \equiv 0, 1, 2, 3, 4 \ldots$ ■

En particular:

Teorema 4.16 (Gentzen) *Si $\phi(\alpha)$ es una fórmula de $\mathcal{L}_a$ y θ es un numeral que nombra un ordinal, entonces* $\underset{\mathrm{AP}}{\vdash} \phi - \mathrm{IND}(\theta)$.

Demostración: A partir de θ podemos determinar explícitamente un número natural n tal que en AP se demuestra que $\theta \prec \omega^{(n)}$. Por el teorema anterior en AP se demuestra $\phi - \mathrm{IND}(\omega^{(n)})$, y esto implica $\phi - \mathrm{IND}(\theta)$. ■

Más precisamente, si $\phi(\alpha)$ es una fórmula de tipo Π_1, hemos demostrado que, para cada número natural n,

$$\underset{\mathrm{I}\Sigma_n}{\vdash} \phi - \mathrm{IND}(\omega^{(n)}).$$

Observaciones El argumento del teorema 4.15 no nos da que

$$\underset{\mathrm{AP}}{\vdash} \bigwedge n\ \phi - \mathrm{IND}(\omega^{(n)}),$$

lo cual sería equivalente a

$$\underset{\mathrm{AP}}{\vdash} \phi - \mathrm{IND}(\epsilon_0),$$

pues, dado n, necesitamos aplicar el teorema 4.14 un total de $n-1$ veces para pasar de ϕ a ϕ con $n-1$ comitas, y eso no tiene ningún sentido si n es una variable y no un numeral concreto. Tal y como señalábamos, esto no es casual y no hay posibilidad de mejorarlo, pues, como veremos en el capítulo siguiente, si pudiéramos probar $\phi - \mathrm{IND}(\epsilon_0)$ en AP, para cierta fórmula Π_1, podríamos probar también Consis AP.

De este modo, en AP, si suponemos

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\, \phi(\beta) \rightarrow \phi(\alpha)),$$

podemos demostrar que todos los ordinales menores que uno cualquiera θ en particular cumplen $\phi(\alpha)$, es decir, podemos probar que todo ordinal $\alpha \prec \omega^{(1)}$ cumple $\phi(\alpha)$, y que todo ordinal $\alpha \prec \omega^{(2)}$ cumple $\phi(\alpha)$, y que todo ordinal $\alpha \prec \omega^{(3)}$ cumple $\phi(\alpha)$, y esto nos asegura que la fórmula $\bigwedge\alpha \in E\,\phi(\alpha)$ es verdadera en su interpretación natural, pues todo ordinal es menor que $\omega^{(1)}$ o que $\omega^{(2)}$, o que $\omega^{(3)}$, etc., pero basta para probar $\bigwedge\alpha \in E\,\phi(\alpha)$.

En otros términos, tenemos un argumento que prueba que el principio de inducción transfinita $\phi - \mathrm{IND}(\epsilon_0)$ es verdadero y que es formalizable en AP excepto por el último paso, el que requiere pasar de que todos los ordinales menores que cualquier $\omega^{(n)}$ (para $n = 1, 2, 3, \ldots$) cumplen $\phi(\alpha)$ a que todos los ordinales cumplen $\phi(\alpha)$. Esto es cierto, pero no es demostrable en AP porque ni siquiera puede expresarse mediante una fórmula de $\mathcal{L}_a$.

Notemos que si si $\phi(\alpha)$ es una fórmula tal que $\underset{\mathrm{AP}}{\vdash} \bigwedge\alpha \in E\,\phi(\alpha)$, entonces, trivialmente, $\underset{\mathrm{AP}}{\vdash} \phi - \mathrm{IND}(\epsilon_0)$. Cuando decimos que no podemos probar $\phi - \mathrm{IND}(\epsilon_0)$ en AP queremos decir únicamente que no tenemos un argumento general que pruebe esto para cualquier fórmula ϕ, porque no podemos probarlo para ciertas fórmulas concretas ϕ. Si $\phi(\alpha)$ es una de estas fórmulas (y veremos que podemos tomar por ejemplo una fórmula Π_1 con α como única variable libre), la sentencia $\phi - \mathrm{IND}(\epsilon_0)$ es un ejemplo de sentencia aritmética verdadera (en su interpretación natural) no demostrable en AP. Por supuesto, Consis AP es otro ejemplo.

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). ■

Para terminar vamos a dar otra "casi" demostración de $\phi - \mathrm{IND}(\epsilon_0)$ en AP que es conceptualmente más simple. Para ello observamos que

$$\neg\phi - \mathrm{IND}(\epsilon_0) \leftrightarrow \bigvee\alpha \in E\neg\phi(\alpha) \wedge \bigwedge\alpha \in E(\neg\phi(\alpha) \rightarrow \bigvee\delta \prec \alpha\neg\phi(\delta)).$$

Bajo este supuesto, podemos definir una fórmula de $\mathcal{L}_a$, que podemos representar por $y = \alpha_m$, para la que podemos demostrar $\bigwedge m(\alpha_m \in E \wedge \alpha_{m+1} \prec \alpha_m)$, es decir, que α_m es una sucesión estrictamente decreciente de ordinales.

En efecto, basta considerar la fórmula que afirma que existe un número natural s tal que $\ell(s) = m+1$, $y = s_m$, s_0 es el menor número natural (respecto de $\leq$) tal que $s_0 \in E \wedge \neg\phi(s_0)$ y, para cada $i < m$, s_{i+1} es el menor número natural tal que $s_{i+1} \prec s_i \wedge \neg\phi(s_{i+1})$.

Por lo tanto, para probar $\phi - \mathrm{IND}(\epsilon_0)$ basta demostrar que no existen sucesiones decrecientes de ordinales. El problema es que esto ni siquiera puede expresarse en $\mathcal{L}_a$, pero vamos a demostrar lo siguiente:

Teorema 4.17 *Dada una fórmula aritmética $y = \alpha_m$, podemos construir otra $y = \beta_m$ tal que en* AP *podemos probar que, para todo n, si*

$$\bigwedge m(\alpha_m \in E \land \alpha_{m+1} \prec \alpha_m) \land \alpha_0 < \omega^{(n+1)},$$

entonces

$$\bigwedge m(\beta_m \in E \land \beta_{m+1} \prec \beta_m) \land \beta_0 < \omega^{(n)}.$$

En otras palabras, a partir de una sucesión decreciente de ordinales menores que $\omega^{(n+1)}$ podemos construir otra sucesión decreciente de ordinales menores que $\omega^{(m)}$. Conviene destacar que aquí no suponemos que n sea un numeral, sino que se trata simplemente de una variable de $\mathcal{L}_a$.

DEMOSTRACIÓN: Pongamos que $\alpha_m = \omega^{\delta_0^m} + \cdots + \omega^{\delta_{r_m}^m}$, donde $r_m \geq 1$ y $\delta_0^m \succeq \cdots \succeq \delta_{r_m}^m$. Entonces $\beta_0 = \delta_0^0 \prec \omega^{(n)}$. En efecto, si fuera $\omega^{(n)} \preceq \delta_0^0$, entonces

$$\omega^{(n+1)} = \omega^{\omega^{(n)}} \preceq \omega^{\delta_0^0} \preceq \alpha_0,$$

en contra de lo supuesto.

Observemos ahora que, si todos los δ_0^m fueran iguales a β_0, para que la sucesión dada sea decreciente tendría que ser $\bigwedge m\; r_m \geq 1$. Si a su vez todos los δ_1^m fueran iguales a β_0, tendría que ser $\bigwedge m\, r_m \geq 2$, etc., luego tiene que haber un k_0 tal que

$$\bigwedge i < k_0 \bigwedge m\, \delta_i^m = \beta_0 \land \bigvee m\, \delta_{k_0}^m \prec \beta_0.$$

Tomamos el mínimo m_1 tal que $\beta_1 = \delta_{k_0}^{m_1} \prec \beta_0$. En estos términos, la sucesión dada es dela forma

$$\begin{array}{rcl}
\alpha_0 & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_0} + \cdots \\
\alpha_1 & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_0} + \cdots \\
\vdots & & \vdots \\
\alpha_{m_1} & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_1} + \cdots \\
\alpha_{m_1+1} & = & \omega^{\beta_0} \cdot k_0 + \cdots
\end{array}$$

Ahora podemos repetir el proceso con β_1, es decir, tiene que existir un mínimo número natural k_1 tal que, si $k_0 \leq i < k_0 + k_1$ y $m \geq m_1$, se cumple que $\delta_i^m = \beta_1$, pero existe un mínimo $m_2 \geq m_1$ tal que $\beta_2 = \delta_{k_0+k_1}^{m_2} \prec \beta_1$. Así:

$$\begin{array}{rcl}
\alpha_0 & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_0} + \cdots \\
\alpha_1 & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_0} + \cdots \\
\vdots & & \vdots \\
\alpha_{m_1} & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_1} \cdot k_1 + \omega^{\beta_1} + \cdots \\
\alpha_{m_1+1} & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_1} \cdot k_1 + \omega^{\beta_1} + \cdots \\
\vdots & & \vdots \\
\alpha_{m_2} & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_1} \cdot k_1 + \omega^{\beta_2} + \cdots \\
\alpha_{m_2+1} & = & \omega^{\beta_0} \cdot k_0 + \omega^{\beta_1} \cdot k_1 + \cdots
\end{array}$$

Es fácil ver que este proceso permite definir una fórmula aritmética $y = \beta_m$ que cumple lo requerido. ■

Con esto obtenemos una demostración alternativa del teorema 4.16: si suponemos $\neg\phi - \mathrm{IND}(\theta)$, donde θ es un numeral, podemos encontrar un numeral n tal que $\theta \prec \omega^{(n)}$, y podemos construir una fórmula aritmética $y = \alpha_m$ que determine una sucesión decreciente de ordinales con $\alpha_0 \prec \omega^{(n)}$, y aplicando $n-1$ veces el teorema 4.17, obtendríamos otra sucesión decreciente tal que $\alpha_0 \prec \omega$, lo cual es imposible.

Inducción transfinita en $\mathbf{ACA_0}$ En la aritmética de segundo orden ACA_0 podemos llevar un poco más lejos la "casi demostración" del principio de inducción transfinita que acabamos de ver.

Para empezar, en ACR_0 podemos enunciar un principio general de inducción transfinita:

$$\mathrm{IND}(\epsilon_0) \equiv \bigwedge X(X \subset E \land \bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\ \beta \in X \to \alpha \in X) \to X = E).$$

Dada una fórmula aritmética $\phi(\alpha)$, al aplicar esta sentencia al conjunto

$$X = \{\alpha \mid \alpha \in E \land \phi(\alpha)\}$$

obtenemos $\phi - \mathrm{IND}(\epsilon_0)$. El argumento que hemos dado justo antes del teorema 4.17 nos permite probar una implicación del teorema siguiente:

Teorema 4.18 ($\mathbf{ACA}_0$) $\mathrm{IND}(\epsilon_0) \leftrightarrow \neg\bigvee F(F : \mathbb{N} \longrightarrow E$ *decreciente*$)$.

Demostración: Hay que entender que "decreciente" significa que F cumple $\bigwedge m\, F(m+1) \prec F(m)$, lo que a su vez implica $\bigwedge mn(m < n \to F(n) \prec F(m))$.

Si $\neg\mathrm{IND}(\epsilon_0)$, existe un conjunto $X \subset E$ tal que

$$\bigwedge \alpha \in E(\bigwedge \beta \prec \alpha\ \beta \in X) \to \alpha \in X),$$

pero existe $\alpha_0 \in E \setminus X$. Equivalentemente, $\bigwedge \alpha \in E(\alpha \notin X \to \bigvee \beta \prec \alpha\, \beta \notin X)$, y esto permite definir recurrentemente una función $F : \mathbb{N} \longrightarrow E$ decreciente.

Recíprocamente, si $F : \mathbb{N} \longrightarrow E$ es decreciente, llamamos X al complementario de su rango, que tiene la propiedad de que si $\alpha \in E$ y $\bigwedge \beta \prec \alpha\, \beta \in X$, también $\alpha \in X$, pues si $\alpha \notin X$, entonces $\alpha = F(n)$, para cierto n, con lo que $\beta = F(n+1) \prec \alpha$ cumple $\beta \notin X$, en contra de lo supuesto. Según $\mathrm{IND}(\epsilon_0)$ podríamos concluir que $X = E$, pero esto significa que el rango de F es vacío, lo cual es absurdo. ■

En segundo lugar, como todo ordinal es menor que un $\omega^{(n)}$, llamando

$$\Psi(n) \equiv \bigvee F(F : \mathbb{N} \longrightarrow E \text{ decreciente} \land F(0) < \omega^{(n)}),$$

en ACA_0 se prueba trivialmente que la existencia de una sucesión decreciente de ordinales equivale a $\bigvee n\, \Psi(n)$, luego

$$\mathrm{IND}(\epsilon_0) \leftrightarrow \bigwedge n\, \neg\Psi(n).$$

Finalmente, el argumento con el que hemos probado 4.17 se adapta trivialmente para probar que

$$\neg\Psi(0) \wedge \bigwedge n(\neg\Psi(n) \rightarrow \neg\Psi(n+1)).$$

En efecto, $\neg\Psi(0)$ es trivial, y si existe una sucesión $F : \mathbb{N} \longrightarrow E$ decreciente con $F(0) \prec \omega^{(n+1)}$, en la prueba de 4.17 hemos visto cómo construir otra sucesión $G : \mathbb{N} \longrightarrow E$ decreciente con $G(0) \prec \omega^{(n)}$. Sólo hay que cambiar la fórmula $y = \alpha_n$ por $y = F(x)$, de modo que G se define por una fórmula aritmética con F como única variable de segundo orden.

Por lo tanto, lo único que nos falta para demostrar $\mathrm{IND}(\epsilon_0)$ en ACA_0 es

$$\neg\Psi(0) \wedge \bigwedge n(\neg\Psi(n) \rightarrow \neg\Psi(n+1)) \rightarrow \bigwedge n \neg\Psi(n),$$

es decir, extender el principio de inducción a la fórmula $\neg\Psi(n)$, que no es aritmética, sino que es lo que se conoce como una fórmula Π^1_1 (una fórmula equivalente a una fórmula aritmética precedida de un cuantificador universal de segundo orden).

El teorema de incompletitud nos asegura que este principio de inducción no es demostrable en ACA_0, pues, si lo fuera, podríamos demostrar $\mathrm{IND}(\epsilon_0)$, luego $\phi - \mathrm{IND}(\epsilon_0)$, para cualquier fórmula aritmética ϕ, luego —según veremos en el capítulo siguiente— podríamos probar Consis AP, pero ACA_0 es una extensión conservativa de AP (teorema 2.23), luego también podríamos probar Consis AP en AP, lo cual es imposible.

Desde un punto de vista informal, la situación es la siguiente: en principio, se podría cuestionar que la afirmación “no existen sucesiones decrecientes de ordinales” tiene un significado bien definido, pues no podemos concebir la totalidad de las sucesiones de ordinales para determinar lo que significa que ninguna de ellas sea decreciente, pero el argumento del teorema 4.17 nos proporciona un argumento totalmente convincente de que si, de algún modo, tenemos determinada una sucesión decreciente de ordinales menores que $\omega^{(n+1)}$, a partir de ella podemos construir otra por debajo de $\omega^{(n)}$, y el hecho de que podamos demostrar esto da sentido a la afirmación: aunque no podamos concebir la totalidad de las sucesiones de ordinales, sabemos razonar que si existiera una por debajo de $\omega^{(n+1)}$ existiría otra por debajo de $\omega^{(n)}$, luego considerando el mínimo número natural n tal que existe una sucesión decreciente de ordinales por debajo de $\omega^{(n)}$ (que obviamente no puede ser 0), tenemos una contradicción. Esto es una prueba informal de que, en efecto, no existen sucesiones decrecientes de ordinales, que no es formalizable en ACA_0 porque la contradicción final equivale al principio de inducción respecto de una fórmula que no es aritmética, pero acabamos de razonar que dicha fórmula (la que afirma que no existen sucesiones decrecientes de ordinales por debajo de $\omega^{(n)}$) tiene un significado informal preciso desde el momento en que sabemos cómo razonar que es cierta.

Más precisamente, en el capítulo siguiente veremos que es posible programar un ordenador para que, a partir de la demostración de una contradicción en AP, genere una sucesión decreciente de ordinales, de la que podríamos determinar su primer término y, por consiguiente, encontrar un n concreto de modo que la sucesión generada estaría por debajo de $\omega^{(n)}$, y acabamos de dar un razonamiento informal por el que esto nos lleva a una contradicción.

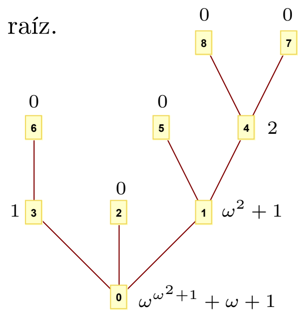
4.5 Hércules y la Hidra II

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 4.1 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 4.1 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. ■

4.6 Inducción transfinita aritmética

Observemos que la prueba del teorema 4.15 es válida en cualquier teoría T que represente a AP aunque la fórmula ϕ no sea aritmética, con tal de que en T no haya restricciones a las fórmulas a las que podemos aplicar el principio de inducción, y esto a su vez se traduce en que el teorema 4.16 es válido también en T, es decir, que si T es una teoría que represente a AP en la que el principio de inducción sea válido para cualquier fórmula, entonces en T se puede probar $\phi - \mathrm{IND}(\theta)$ para todo numeral θ que nombre un ordinal (menor que ϵ_0) y para toda fórmula ϕ, no necesariamente aritmética.

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 4.19 *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

$$\bigwedge t(\bigwedge s \triangleleft t\, \alpha(s) \rightarrow \alpha(t)) \rightarrow \bigwedge s \in A\, \alpha(s)$$

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*

$$\sigma_n \in A \wedge \sigma_{n+1} \triangleleft \sigma_n.$$

Para probar formalmente este teorema necesitamos considerar como metateoría la teoría RA_0 descrita en [LF 7.44].

Demostración: Consideremos 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 [LF 9.11] 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 considerar el lenguaje $\mathcal{L}_a^F$ que resulta de añadir un funtor F a $\mathcal{L}_{\mathrm{arp}}$ y considerar el modelo $\mathbb{N}_{\mathcal{F}}$ de $\mathcal{L}_a^F$ que extiende al modelo natural de $\mathcal{L}_a$ interpretando F como la función $\mathcal{F}$. Es claro que $\mathbb{N}_{\mathcal{F}} \vDash \Phi$, donde

$$\Phi \equiv \bigwedge u((F(u) = 0 \vee F(u) = 1) \wedge$$

$$(F(u) = 1 \rightarrow (u \in \mathrm{Sent}(\ulcorner \mathcal{L}_a \urcorner) \wedge \cdots)) \wedge (F(u) = 0 \wedge u \in \mathrm{Sent}(\ulcorner \mathcal{L}_a \urcorner) \rightarrow \cdots)),$$

donde $u \in \mathrm{Sent}(\ulcorner \mathcal{L}_a \urcorner)$ significa que u es una sentencia de $\mathcal{L}_a$, los primeros puntos suspensivos son la conjunción de las fórmulas siguientes:

1. $\bigwedge t_1 t_2 < u(u = t_1 \ulcorner{=}\urcorner t_2 \rightarrow \mathrm{Dn}(t_1) = \mathrm{Dn}(t_2))$,
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. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge u = \ulcorner\bigwedge\urcorner v\alpha \rightarrow \bigwedge m\, F(\mathtt{S}_v^{0^{(m)}}\alpha) = 1)$,
5. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge u = \ulcorner\bigvee\urcorner v\alpha \rightarrow \bigvee n\, F(\mathtt{S}_v^{0^{(n)}}\alpha) = 1)$.

y los segundos puntos suspensivos son la conjunción de:

1. $\bigwedge t_1 t_2 < u(u = t_1 \ulcorner{=}\urcorner t_2 \rightarrow \mathrm{Dn}(t_1) \neq \mathrm{Dn}(t_2))$,
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. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge u = \ulcorner\bigwedge\urcorner v\alpha \rightarrow \bigvee n\, F(\mathtt{S}_v^{0^{(n)}}\alpha) = 0)$,
5. $\bigwedge \alpha v(v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge u = \ulcorner\bigvee\urcorner v\alpha \rightarrow \bigwedge m\, F(\mathtt{S}_v^{0^{(m)}}\alpha) = 0)$.

Más aún, la sentencia Φ determina completamente a F, en el sentido de que si M es un modelo de $\mathcal{L}_a^F$ que extiende al modelo natural de $\mathcal{L}_a$ 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

$$\underset{\mathrm{AP}}{\vdash}(\Phi \rightarrow (F(\ulcorner\alpha\urcorner) = 1 \leftrightarrow \alpha)),$$

donde AP es la teoría sobre $\mathcal{L}_a^F$ con los axiomas de AP.

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:

$$\Phi' \equiv \bigwedge u_0 v_0 u_1 v_1 u_2 v_2 u_3 v_3 v m \bigvee n u_4 v_4 (v_0 = F(u_0) \wedge \cdots \wedge v_4 = F(u_4) \wedge$$
$$u_3 = \mathtt{S}_v^{0^{(m)}} u_1 \wedge u_4 = \mathtt{S}_v^{0^{(n)}} u_1 \rightarrow ((v_0 = 0 \vee v_0 = 1) \wedge$$
$$(v_0 = 1 \rightarrow u_0 \in \mathrm{Sent}(\ulcorner\mathcal{L}_a\urcorner) \wedge \cdots) \wedge (v_0 = 0 \wedge u_0 \in \mathrm{Sent}(\ulcorner\mathcal{L}_a\urcorner) \rightarrow \cdots)))$$

donde los primeros puntos suspensivos son la conjunción de las fórmulas:

1. $\bigwedge t_1 t_2 < u_0(u_0 = t_1 \ulcorner{=}\urcorner t_2 \rightarrow \mathrm{Dn}(t_1) = \mathrm{Dn}(t_2))$,
2. $u_0 = \ulcorner\neg\urcorner u_1 \rightarrow v_1 = 0$,
3. $u_0 = u_1\ulcorner\vee\urcorner u_2 \rightarrow v_1 = 1 \vee v_2 = 1)$,
4. $v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge u_0 = \ulcorner\bigwedge\urcorner v u_1 \rightarrow v_3 = 1$,
5. $v \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \wedge u_0 = \ulcorner\bigvee\urcorner v u_1 \rightarrow v_4 = 1$.

y los segundos son la conjunción de las fórmulas:

1. $\bigvee t_1 t_2 < u_0 (u_0 = t_1 \ulcorner\!=\!\urcorner t_2 \land \mathrm{Dn}(t_1) \neq \mathrm{Dn}(t_2))$,
2. $u_0 = \ulcorner\neg\urcorner u_1 \rightarrow v_1 = 1$,
3. $u_0 = u_1 \ulcorner\lor\urcorner u_2 \rightarrow v_1 = 0 \land v_2 = 0)$,
4. $u_0 \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \land u_0 = \ulcorner\bigwedge\urcorner v u_1 \rightarrow v_4 = 0$,
5. $u_0 \in \mathrm{VarLig}(\ulcorner\mathcal{L}_a\urcorner) \land u_0 = \ulcorner\bigvee\urcorner v u_1 \rightarrow v_3 = 0$.

A su vez, podemos contraer los cuantificadores, de modo que Φ' es equivalente a $\bigwedge u \bigvee v\, \Psi(u, v)$, donde

$$\Psi(u, v) \equiv \ell(u) = 10 \land \ell(v) = 3 \land u_0 = F(u_4) \land u_1 = F(u_5) \land u_2 = F(u_6) \land$$

$$u_3 = F(u_7) \land v_0 = F(v_1) \rightarrow \phi(u, v),$$

y $\phi(u, v)$ es una fórmula de $\mathcal{L}_a$ que podemos tomar de tipo Σ_1 y, más aún, de tipo Δ_1 en $\mathrm{I}\Sigma_1$. 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 llamamos $\mathcal{L}_a^{F,G}$ al lenguaje que resulta de añadir a $\mathcal{L}_a^F$ un segundo funtor G 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

$$\Psi'(u, v) \equiv \ell(u) = 10 \land \ell(v) = 3 \land v = G(u) \land$$

$$u_0 = F(u_4) \land u_1 = F(u_5) \land u_2 = F(u_6) \land u_3 = F(u_7) \land v_0 = F(v_1) \rightarrow \phi(u, v)$$

y, más aún, si un modelo M extiende al modelo natural de $\mathcal{L}_a$ y cumple

$$M \vDash \bigwedge uv\, \Psi'(u, v),$$

necesariamente $M(F)$ es $\mathcal{F}$. Igualmente, para toda sentencia α de $\mathcal{L}_a$,

$$\underset{\mathrm{AP}}{\vdash} (\bigwedge uv\, \Psi'(u, v) \rightarrow (F(\ulcorner\alpha\urcorner) \leftrightarrow \alpha)).$$

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 $\mathcal{L}_a^H$ que resulta de añadir a $\mathcal{L}_a$ 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

$$\Psi''(u, v) \equiv \ell(u) = 10 \land \ell(v) = 3 \land v = H(2u + 1) \land u_0 = H(2u_4) \land$$

$$u_1 = H(2u_5) \land u_2 = H(2u_6) \land u_3 = H(2u_7) \land v_0 = H(2v_1) \rightarrow \phi(u, v).$$

Así, 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

$$\underset{\mathrm{AP}}{\vdash} (\bigwedge uv\, \Psi''(u,v) \rightarrow (H(2^{\ulcorner\alpha\urcorner}) \leftrightarrow \alpha)).$$

Nuevamente podemos contraer los cuantificadores definiendo

$$\Psi'''(u) \equiv \ell(u) = 16 \land \ell(u_{10}) = 3 \land u_{10} = 2\cdot u|_{10} + 1 \land u_{11} = 2u_4 \land$$

$$u_{12} = 2u_5 \land u_{13} = 2u_6 \land u_{14} = 2u_7 \land u_{15} = 2(u_{10})_1 \land u_0 = H(u_{11}) \land$$

$$u_1 = H(u_{12}) \land u_2 = H(u_{13}) \land u_3 = H(u_{14}) \land (u_{10})_0 = H(u_{15}) \rightarrow \phi'(u),$$

donde $\phi'(u) \equiv \phi(u|_{10}, u_{10})$ es una fórmula Σ_1 de $\mathcal{L}_a$ (de tipo Δ_1 en $\mathrm{I}\Sigma_1$). 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

$$s \in A \equiv \bigwedge u \leq \ell(s)(\ell(u) = 16 \land \ell(u_{10}) = 3 \land u_{10} = 2\cdot u|_{10} + 1 \land$$

$$u_{11} = 2u_4 \land u_{12} = 2u_5 \land u_{13} = 2u_6 \land u_{14} = 2u_7 \land u_{15} = 2(u_{10})_1 \land$$

$$u_0 = s(u_{11}) \land u_1 = s(u_{12}) \land u_2 = s(u_{13}) \land u_3 = s(u_{14}) \land$$

$$(u_{10})_0 = s(u_{15}) \rightarrow \phi'(u)),$$

de modo que $s \in A$ es una fórmula de $\mathcal{L}_a$ (sin funtores añadidos) de tipo Δ_1 en $\mathrm{I}\Sigma_1$ que obviamente cumple

$$\bigwedge st(s \sqsubseteq t \land t \in A \rightarrow s \in A).$$

Ahora $\bigwedge u\, \Psi'''(u)$ es equivalente a

$$\bigwedge s(\bigwedge i < \ell(s)\, s_i = H(i) \rightarrow s \in A).$$

En particular, si llamamos σ_n al numeral correspondiente a la sucesión

$$\langle \mathcal{H}(0), \ldots, \mathcal{H}(n-1)\rangle,$$

tenemos que[6]

$$\underset{\mathrm{I}\Sigma_1}{\vdash} (\sigma_n \in A \land \sigma_n \sqsubset \sigma_{n+1}).$$

Definimos[7]

$$s \trianglelefteq t \equiv s \in A \land t \in A \land (t \sqsubseteq s \lor \bigvee i < \ell(s)(i < \ell(t) \land s|_i = t_i \land s(i) < t(i))).$$

[6]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 Σ_1, luego es demostrable por el teorema [LF 6.17].

[7]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].

Tanto $s \in A$ como $s \trianglelefteq t$ son fórmulas Δ_1 en $\mathrm{I}\Sigma_1$.

Es fácil probar en $\mathrm{I}\Sigma_1$ que $\trianglelefteq$ es una relación de orden total, es decir, que cumple las cuatro sentencias enumeradas en el enunciado de 4.19. Esto no depende de la definición de A. Como obviamente $t \sqsubset s \rightarrow s \triangleleft t$, los numerales σ_n que tenemos definidos cumplen

$$\underset{\mathrm{I}\Sigma_1}{\vdash} (\sigma_n \in A \wedge \sigma_{n+1} \triangleleft \sigma_n).$$

Finalmente vamos a probar en AP el principio de inducción transfinita.

Para ello suponemos que $\bigwedge t \in A(\bigwedge s \triangleleft t\, \alpha(s) \rightarrow \alpha(t))$, pero que existe un $s \in A$ tal que $\neg\alpha(s)$. Notemos que entonces,

$$\bigwedge t \in A(\neg\alpha(t) \rightarrow \bigvee s \in A(s \triangleleft t \wedge \neg\alpha(s))).$$

Recordemos que en AP podemos demostrar que si $\bigvee u, \phi(u)$ existe un (único) mínimo número natural que cumple $\phi(u)$, y lo podemos representar por $\mu u\, \phi(u)$. En particular podemos definir

$$s_0 \equiv \mu s\, (s \in A \wedge \neg\alpha(s)), \quad s_{n+1} \equiv \mu s(s \in A \wedge \neg\alpha(s) \wedge s \triangleleft s_n),$$

y una simple inducción prueba que

$$\bigwedge n(s_n \in A \wedge \neg\alpha(s_n) \wedge s_{n+1} \triangleleft s_n).$$

Ahora distinguimos dos casos:

1) $\bigwedge m \bigvee n \geq m\, s_n \not\sqsubseteq s_{n+1}$. Entonces llamamos

$$n_0 = \mu n\, s_n \not\sqsubseteq s_{n+1}, \qquad n_{k+1} = \mu n(n \geq n_k + 1 \wedge s_n \not\sqsubseteq s_{n+1}).$$

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

$$\bigwedge n(s'_n \in A \wedge s'_{n+1} \triangleleft s'_n \wedge s'_n \not\sqsubseteq s'_{n+1}).$$

Por lo tanto, para cada n existe un único i_n tal que

$$i_n < \ell(s'_n) \wedge i_n < \ell(s'_{n+1}) \wedge s'_n|_{i_n} = s'_{n+1}|_{i_n} \wedge s'_{n+1}(i_n) < s'_n(i_n).$$

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

$$n_0 = \mu n(n \geq r \wedge i_n = k), \quad n_{j+1} = \mu n(n \geq n_j + 1 \wedge i_n = k),$$

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.

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

$$\bigwedge n(t_n \in A \land t_n \sqsubset t_{n+1}).$$

En ambos casos tenemos que

$$\bigwedge n \overset{1}{\bigvee} k \bigvee m(n < \ell(t_m) \land t_m(n) = k),$$

por lo que podemos definir

$$H(n) = k \equiv \bigvee m(n < \ell(t_m) \land t_m(n) = k),$$

Así, trivialmente se cumple

$$\bigwedge s(\bigwedge i < \ell(s)\, s_i = H(i) \to s \in A),$$

Es claro entonces que se cumple $\bigwedge u\, \Psi'''(u)$, pero interpretando ahora $\Psi'''(u)$ como una fórmula de $\mathcal{L}_a$, 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

$$V(\alpha \ulcorner\lor\urcorner \beta) \leftrightarrow V(\alpha) \lor V(\beta).$$

4. Si $\ulcorner\bigwedge\urcorner v\, \alpha$ es una sentencia de $\ulcorner\mathcal{L}_a\urcorner$, entonces

$$V(\ulcorner\bigwedge\urcorner v\, \alpha) \leftrightarrow \bigwedge n\, V(\mathtt{S}_v^{N(n)}\alpha)).$$

5. Si $\ulcorner\bigvee\urcorner v\, \alpha$ es una sentencia de $\ulcorner\mathcal{L}_a\urcorner$, entonces

$$V(\ulcorner\bigvee\urcorner v\, \alpha) \leftrightarrow \bigvee m\, V(\mathtt{S}_v^{N(m)}\alpha)).$$

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 [LF 9.11] 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 $\mathrm{I}\Sigma_1$ 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 V

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 o, más explícitamente, vamos a dar un prodecimiento explícito que, a partir de una demostración de una contradicción en AP, nos daría una sucesión decreciente de ordinales menores que ϵ_0. Nos ocuparemos de ello en la segunda sección, mientras que en la tercera 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 cuarta sección combinaremos las ideas de ambas pruebas para obtener otros resultados relacionados. En la primera sección probaremos algunos resultados previos que vamos a necesitar. Todos los resultados de este capítulo pueden formalizarse y probarse en $\mathrm{I}\Sigma_1$, o incluso en ARP.

5.1 Sentencias Δ_0 en AP($\varnothing$)

En esta sección estudiamos un poco más a fondo el cálculo secuencial AP($\varnothing$) introducido en 1.13, teniendo en cuenta la nota tras el teorema 1.14. Más aún, vamos a considerar también como axiomas de AP($\varnothing$) los secuentes

$$\Rightarrow 0 \leq s, \qquad s \leq t' \Rightarrow s \leq t, s = t',$$

para términos cualesquiera s y t.

Como todos ellos son teoremas de $\mathrm{I}\Sigma_1$, es claro que, aunque esta versión de AP($\varnothing$) es más fuerte que la definida en 1.13, la teoría AP(Φ) que resulta de añadir la regla de inducción para fórmulas de tipo Σ_n, o bien para todas las fórmulas aritméticas, es la misma teoría AP(Φ) que se obtiene a partir de la versión original de AP($\varnothing$). En particular, todos los teoremas de AP($\varnothing$) son teoremas de AP(Σ_1).

Vamos a probar un refinamiento de un caso particular del teorema de Σ_1-completitud [LF 6.17]. Empezamos probando una variante de [LF 6.2]. Recordemos que, según la definición 1.13, la teoría $\mathrm{AP}(\varnothing)$ es la aritmética de Peano sin la regla de inducción.

Teorema 5.1 *Para todo par de números naturales m y n,*

1. *Si $m = n$, en $\mathrm{AP}(\varnothing)$ se puede probar $\Rightarrow 0^{(m)} = 0^{(n)}$.*
2. *Si $m \neq n$, en $\mathrm{AP}(\varnothing)$ se puede probar $0^{(m)} = 0^{(n)} \Rightarrow$.*
3. *Si $m \leq n$, en $\mathrm{AP}(\varnothing)$ se puede probar $\Rightarrow 0^{(m)} \leq 0^{(n)}$.*
4. *Si $m > n$, en $\mathrm{AP}(\varnothing)$ se puede probar $0^{(m)} \leq 0^{(n)} \Rightarrow$.*
5. *En $\mathrm{AP}(\varnothing)$ se puede probar*

$$\Rightarrow 0^{(m)} + 0^{(n)} = 0^{(m+n)}, \qquad \Rightarrow 0^{(m)}0^{(n)} = 0^{(mn)}$$

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 $0^{(m)} \equiv 0^{(n)}$, por lo que el secuente $\Rightarrow 0^{(m)} = 0^{(n)}$ es un axioma del igualador.

2) Supongamos que $m < n$ (el caso $m > n$ se trata de forma similar). Tenemos que

$$0^{(n-m)} = 0^{(0)} \Rightarrow$$

es un axioma de Peano. La prueba dada en 1.8 del secuente

$$0^{(0)} = 0^{(n-m)} \Rightarrow 0^{(n-m)} = 0^{(0)}$$

no usa cortes esenciales. Cortando estos dos secuentes obtenemos una prueba de

$$0^{(0)} = 0^{(n-m)} \Rightarrow .$$

Vamos a ver que, para todo k, podemos demostrar el secuente

$$0^{(k)} = 0^{(n-m+k)} \Rightarrow .$$

Lo tenemos probado para $k = 0$ y, si vale para k, basta cortar con el axioma de Peano

$$0^{(k+1)} = 0^{(n-m+k+1)} \Rightarrow 0^{(k)} = 0^{(n-m-k)}.$$

El caso particular $k = m$ nos da una demostración de $0^{(m)} = 0^{(n)} \Rightarrow$.

3) Lo probamos por inducción sobre n. Si $n = 0$ necesariamente $m = n = 0$, y $\Rightarrow 0^{(0)} \leq 0^{(0)}$ es un axioma.

Si vale para n y se cumple $m \leq n + 1$, o bien $m = n + 1$, en cuyo caso $0^{(m)} \equiv 0^{(n+1)}$ y $\Rightarrow 0^{(m)} \leq 0^{(n+1)}$ es un axioma, o bien $m \leq n$, en cuyo caso, por hipótesis de inducción, podemos probar $\Rightarrow 0^{(m)} \leq 0^{(n)}$ y cortando este secuente y el axioma $\Rightarrow 0^{(n)} \leq 0^{(n+1)}$, con el axioma

$$0^{(m)} \leq 0^{(n)},\ 0^{(n)} \leq 0^{(n+1)} \Rightarrow 0^{(m)} \leq 0^{(n+1)},$$

obtenemos como teorema $\Rightarrow 0^{(m)} \leq 0^{(n+1)}$.

4) Si $m > n$, entonces $n \leq m$ y $n \neq m$, luego, por los casos ya probados, en AP($\varnothing$) podemos demostrar $\Rightarrow 0^{(n)} \leq 0^{(m)}$ y $0^{(m)} = 0^{(n)} \Rightarrow$. Cortando con el axioma

$$0^{(m)} \leq 0^{(n)},\ 0^{(n)} \leq 0^{(m)} \Rightarrow 0^{(m)} = 0^{(n)}$$

obtenemos $0^{(m)} \leq 0^{(n)} \Rightarrow$.

5) Probamos el caso de la suma por inducción sobre n. Para $n = 0$ el secuente $\Rightarrow 0^{(m)} + 0^{(0)} = 0^{(m)}$ es un axioma.

Supongamos que tenemos una demostración de $\Rightarrow 0^{(m)} + 0^{(n)} = 0^{(m+n)}$. Cortando con el axioma del igualador

$$0^{(m)} + 0^{(n)} = 0^{(m+n)} \Rightarrow (0^{(m)} + 0^{(n)})' = 0^{(m+n+1)}$$

obtenemos $\Rightarrow (0^{(m)} + 0^{(n)})' = 0^{(m+n+1)}$. A su vez, cortando con el axioma del igualador

$$(0^{(m)} + 0^{(n)})' = 0^{(m)} + 0^{(n+1)},\ (0^{(m)} + 0^{(n)})' = 0^{(m+n+1)}$$
$$\Rightarrow 0^{(m)} + 0^{(n+1)} = 0^{(m+n+1)}$$

obtenemos $(0^{(m)} + 0^{(n)})' = 0^{(m+n+1)} \Rightarrow 0^{(m)} + 0^{(n+1)} = 0^{(m+n+1)}$, pero a su vez $\Rightarrow (0^{(m)} + 0^{(n)})' = 0^{(m)} + 0^{(n+1)}$ es un axioma de Peano, y cortando con él llegamos a $\Rightarrow 0^{(m)} + 0^{(n+1)} = 0^{(m+n+1)}$.

En el caso del producto, de nuevo $\Rightarrow 0^{(m)} \cdot 0^{(0)} = 0^{(0)}$ es un axioma. Supongamos que podemos probar $\Rightarrow 0^{(m)} \cdot 0^{(n)} = 0^{(mn)}$. Consideramos entonces el axioma del igualador

$$0^{(m)} \cdot 0^{(n+1)} = 0^{(m)} \cdot 0^{(n)} + 0^{(m)},\ 0^{(m)} \cdot 0^{(n)} = 0^{(mn)} \Rightarrow 0^{(m)} \cdot 0^{(n+1)} = 0^{(mn)} + 0^{(m)}$$

y lo cortamos con $\Rightarrow 0^{(m)} \cdot 0^{(n)} = 0^{(mn)}$ y con el axioma

$$\Rightarrow 0^{(m)} \cdot 0^{(n+1)} = 0^{(m)} \cdot 0^{(n)} + 0^{(m)},$$

lo que nos da una demostración de $\Rightarrow 0^{(m)} \cdot 0^{(n+1)} = 0^{(mn)} + 0^{(m)}$. Por el caso de la suma, ya probado, podemos demostrar

$$\Rightarrow 0^{(mn)} + 0^{(m)} = 0^{(m(n+1))},$$

y mediante cortes entre los dos últimos secuentes y el axioma del igualador

$$0^{(m)} \cdot 0^{(n+1)} = 0^{(mn)} + 0^{(m)},\ 0^{(mn)} + 0^{(m)} = 0^{(m(n+1))} \Rightarrow 0^{(m)} \cdot 0^{(n+1)} = 0^{(m(n+1))},$$

obtenemos una demostración de $\Rightarrow 0^{(m)} \cdot 0^{(n+1)} = 0^{(m(n+1))}$. ■

La definición siguiente es un caso particular de [LF 6.10]:

Definición 5.2 A cada designador t de $\mathcal{L}_a$ le asignamos un número natural $d(t)$ mediante el criterio siguiente:

1. $d(0) = 0$,
2. $d(t') = d(t) + 1$,
3. $d(s + t) = d(s) + d(t)$,
4. $d(s \cdot t) = d(s)d(t)$.

Técnicamente, d es un funtor definible en ARP mediante [LF 2.23]. Notemos que $d(t)$ no es sino el número $\mathrm{Dn}(t, v)$ definido en [LF 6.10], que a su vez es el número natural denotado por t en el modelo natural de $\mathcal{L}_a$, pero lo hemos definido sin hacer referencia alguna a modelos.

Teorema 5.3 *Sean s y t designadores de $\mathcal{L}_a$.*

1. *Si $n = d(s)$, en* $\mathrm{AP}(\varnothing)$ *se demuestra $\Rightarrow 0^{(n)} = s$. Además la prueba no requiere cortes esenciales.*
2. *Si $\Rightarrow s = t$ es demostrable en* $\mathrm{AP}(\varnothing)$ *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* $\mathrm{AP}(\varnothing)$ *sin cortes esenciales.*

Demostración: 1) Razonamos por inducción sobre la longitud de s. Si tiene longitud 1, necesariamente $s \equiv 0^{(0)}$, y $n = d(0^{(0)}) = 0$. Ciertamente $\Rightarrow 0^{(0)} = 0^{(0)}$ es demostrable, porque es un axioma.

Si $s = t'$ y $n = d(t)$, por hipótesis de inducción podemos probar $\Rightarrow 0^{(n)} = t$ sin cortes esenciales. Pero entonces $d(s) = n + 1$ y tenemos

$$\frac{\Rightarrow 0^{(n)} = t \qquad 0^{(n)} = t \Rightarrow 0^{(n+1)} = s}{\Rightarrow 0^{(n+1)} = s}$$

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:

$$\frac{\Rightarrow 0^{(m)} = t_1 \qquad 0^{(m)} = t_1,\, 0^{(n)} = t_2 \Rightarrow 0^{(m)} + 0^{(n)} = s}{0^{(n)} = t_2 \Rightarrow 0^{(m)} + 0^{(n)} = s}$$

donde el secuente superior izquierdo es demostrable por hipótesis de inducción y el superior derecho es un axioma del igualador. Cortando con $\Rightarrow 0^{(n)} = t_2$ (que también es demostrable por hipótesis de inducción) obtenemos una demostración del secuente $\Rightarrow 0^{(m)} + 0^{(n)} = s$. Por el teorema anterior tenemos también que $\Rightarrow 0^{(m)} + 0^{(n)} = 0^{(m+n)}$. Mediante cortes con los secuentes que expresan la simetría y la transitividad de la igualdad (que se demuestran sin cortes esenciales) obtenemos $\Rightarrow 0^{(m+n)} = s$.

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 1.9 (que se demuestran sin cortes esenciales y, obviamente, sin la regla de inducción). ■

Ahora consideramos un caso particular de la definición [LF 6.11]:

Definición 5.4 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. $\vDash_0 s = t$ si y sólo si $d(s) = d(t)$,
2. $\vDash_0 s \leq t$ si y sólo si $d(s) \leq d(t)$,
3. $\vDash_0 \neg\alpha$ si y sólo si no $\vDash_0 \alpha$,
4. $\vDash_0 \alpha \vee \beta$ si y sólo si $\vDash_0 \alpha$ o $\vDash_0 \beta$,
5. $\vDash_0 \bigwedge u \leq t\, \alpha(u)$ si y sólo si para todo $m \leq d(t)$ se cumple $\vDash_0 \alpha(0^{(m)})$.
6. $\vDash_0 \bigvee u \leq t\, \alpha(u)$ si y sólo si existe un $m \leq d(t)$ tal que $\vDash_0 \alpha(0^{(m)})$.

El mismo argumento empleado en la demostración de [LF 6.11] justifica que esta definición es formalizable en $\mathrm{I}\Sigma_1$, o incluso en ARP. Más detalladamente, dada una sentencia α de tipo Δ_0, podemos considerar sus variables ligadas $u_0, \ldots, u_n$ en el orden en que aparecen en ella (de izquierda a derecha). Cada una aparecerá en la forma $\bigwedge u_i \leq t_i$ o $\bigvee u_i \leq t_i$, para cierto semitérmino t_i, de modo que t_0 no tiene variables libres, $t_1(u_0)$ tiene a lo sumo la variable libre u_0, $t_2(u_0, u_1)$ tiene a lo sumo u_0, u_1, etc. Podemos definir entonces

$$c_0 = c(\alpha, 0) = d(t_0), \quad c_{i+1} = c(\alpha, i+1) = d(t_{i+1}(0^{(c_0)}, \ldots, 0^{(c_i)})),$$

y a su vez podemos definir el conjunto finito $C(\alpha)$ de todas las sentencias de la forma $\beta(0^{(m_0)}, \ldots, 0^{(m_n)})$, donde $\beta(u_0, \ldots, u_n)$ es una subsemifórmula de α y $m_i \leq c(\alpha, i)$.

Podemos partir $C(\alpha)$ en los conjuntos $C_j(\alpha)$ formados por las sentencias de $C(\alpha)$ que tienen a lo sumo j signos lógicos (entre conectores y cuantificadores). Finalmente, en ARP podemos definir un funtor diádico tal que $F(\alpha, j) : C_j(\alpha) \longrightarrow \{0, 1\}$, a partir del cual definimos $\vDash_0 \alpha \equiv F(\alpha, s_\alpha) = 1$, donde s_α es el número de signos lógicos de α.

El funtor F se define por recursión sobre j. La definición precedente determina la definición de F. En efecto, $F(\alpha, 0)(\beta)$ se define mediante los apartados 1) y 2) y, supuesto definido $F(\alpha, j)$, podemos definir $F(\alpha, j+1)(\beta)$ trivialmente en todos los casos posibles para β salvo cuando β empieza por un cuantificador. Pongamos que

$$\beta \equiv \bigwedge u_k \leq t_k(0^{(m_0)}, \ldots, 0^{(m_{k-1})})\gamma(0^{(m_0)}, \ldots, 0^{(m_{k-1})}, u_k),$$

donde $m_i \leq c(\alpha, i)$. Entonces

$$d(t_k(0^{(m_0)}, \ldots, 0^{(m_{k-1})})) \leq d(t_k(0^{(c_0)}, \ldots, 0^{(c_{k-1})})) = c(\alpha, k),$$

luego podemos definir $F(\alpha, j)(\beta) = 1$ si y sólo si, para todo

$$m_k \leq t_k(0^{(m_0)}, \ldots, 0^{(m_{k-1})}),$$

se cumple $F(\alpha, j)(\gamma(0^{(m_0)}, \ldots, 0^{(m_k)})) = 1$, lo cual es correcto porque, ciertamente,

$$\gamma(0^{(m_0)}, \ldots, 0^{(m_k)}) \in C_j(\alpha).$$

El caso en que β empieza por un cuantificador existencial es análogo. ■

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. Esto es consecuencia de que la definición anterior puede formalizarse en ARP, pero también es inmediato a partir de la definición que podemos programar un ordenador que determine si se cumple o no en cualquier caso.

Con esto podemos probar el teorema siguiente, cuyo interés radica en que la demostración es estrictamente finitista. En particular, no hace referencia alguna a modelos:

Teorema 5.5 *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.

Si S es un secuente en $\mathcal{L}_a$ formado únicamente por sentencias Δ_0, podemos definir $\vDash_0 S$ como $\vDash_0 \bar{S}$, donde $\bar{S}$ es la fórmula formada por la disyunción de las negaciones de las sentencias de su antecedente y las fórmulas de su consecuente (entendiendo que $\vDash_0 S$ es falso para el secuente vacío).

Todos los axiomas de AP (entendiendo por AP el cálculo secuencial AP(Φ), donde Φ es la clase de todas las fórmulas de $\mathcal{L}_a$), 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.[1]

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. ■

[1]Esto supone formalizar la prueba del teorema de corrección 1.4.

Finalmente probamos el resultado de completitud que vamos a necesitar:

Teorema 5.6 *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[2] (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 5.3 podemos probar $\Rightarrow 0^{(m)} = s$, $\Rightarrow 0^{(n)} = t$. Según 5.1 podemos probar $\Rightarrow 0^{(m)} = 0^{(n)}$ (resp. $\Rightarrow 0^{(m)} \leq 0^{(n)}$) o bien $0^{(m)} = 0^{(n)} \Rightarrow$ (resp. $0^{(m)} \leq 0^{(n)} \Rightarrow$) 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 $\Rightarrow 0^{(m)} \leq 0^{(n)}$ basta considerar el axioma

$$0^{(m)} = s,\, 0^{(n)} = t,\, 0^{(m)} \leq 0^{(n)} \Rightarrow s \leq t.$$

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 $\alpha \equiv \beta \vee \gamma$ 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 $\beta(0^{(m)})$ es verdadera, luego por hipótesis de inducción[3] podemos demostrar $\Rightarrow \beta(0^{(m)})$.

Veamos que, para todo $m \leq n$, podemos probar $y \leq 0^{(m)} \Rightarrow \beta(y)$.

Cortando los axiomas

$$y \leq 0^{(0)},\, 0^{(0)} \leq y \Rightarrow y = 0^{(0)}, \qquad \Rightarrow 0^{(0)} \leq y$$

obtenemos $y \leq 0^{(0)} \Rightarrow y = 0^{(0)}$. Por otra parte, 5.3 nos da

$$0^{(0)} = y,\, \beta(0^{(0)}) \Rightarrow \beta(y).$$

Cortando estos secuentes con $y = 0^{(0)} \Rightarrow 0 = 0^{(y)}$, obtenemos $y \leq 0^{(0)} \Rightarrow \beta(y)$.

[2]Técnicamente, con la notación con la que hemos justificado que la definición de $\vDash_0$ es formalizable en ARP, para que la prueba de este teorema sea también formalizable en ARP, lo que hacemos es definir un funtor que a cada sentencia de $C_j(\alpha)$ le hace corresponder una demostración del secuente correspondiente $\Rightarrow \beta$ o $\beta \Rightarrow$, y este funtor se define por recursión sobre j.

[3]Notemos que $\beta(0^{(m)})$ puede tener mayor longitud que α, pero tiene menos signos lógicos.

Si podemos probar $y \leq 0^{(m)} \Rightarrow \beta(y)$ y $m+1 \leq n$ consideramos el axioma

$$y \leq (0^{(m)})' \Rightarrow y \leq 0^{(m)},\ y = (0^{(m)})'.$$

También tenemos

$$\Rightarrow \beta((0^{(m)})'), \qquad (0^{(m)})' = y,\ \beta((0^{(m)})') \Rightarrow \beta(y), \qquad y = (0^{(m)})' \Rightarrow (0^{(m)})' = y.$$

Mediante cortes inesenciales llegamos a $y \leq (0^{(m)})' \Rightarrow \beta(y)$.

En particular, para $m = n$ tenemos una demostración de $y \leq 0^{(n)} \Rightarrow \beta(y)$. Cortando con $\Rightarrow 0^{(n)} = t$ y con axiomas del igualador llegamos a $y \leq t \Rightarrow \beta(y)$, desde donde ya podemos concluir:

$$\dfrac{\dfrac{y \leq t \Rightarrow \beta(y)}{\Rightarrow y \leq t \rightarrow \beta(y)}}{\bigwedge u \leq t\, \beta(u)}$$

Si α es falsa, entonces existe un $m \leq n$ tal que $\beta(0^{(m)})$ es falsa, luego por hipótesis de inducción podemos demostrar $\beta(0^{(m)}) \Rightarrow$. Como $0^{(m)} \leq t$ es verdadera, por la parte ya probada podemos demostrar $\Rightarrow 0^{(m)} \leq t$. La regla izquierda del implicador nos da

$$0^{(m)} \leq t \rightarrow \beta(0^{(m)}) \Rightarrow$$

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 $\beta(0^{(m)})$ es verdadera, luego por hipótesis de inducción podemos demostrar $\Rightarrow \beta(0^{(m)})$.

Como en el caso anterior, también podemos probar $\Rightarrow 0^{(m)} \leq t$, y por la regla derecha del conjuntor llegamos a $\Rightarrow 0^{(m)} \leq t \wedge \beta(0^{(m)})$. 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 $\beta(0^{(m)})$ es falsa, luego por hipótesis de inducción podemos demostrar $\beta(0^{(m)}) \Rightarrow$. Ahora probamos por inducción sobre m que podemos demostrar $y \leq 0^{(m)},\ \beta(y) \Rightarrow$.

Para $m = 0$ usamos como antes que $y \leq 0^{(0)} \Rightarrow y = 0^{(0)}$, lo cual, combinado con

$$\beta(0^{(0)}) \Rightarrow, \qquad 0^{(0)} = y,\ \beta(0^{(0)}) \Rightarrow \beta(y), \qquad y = 0^{(0)} \Rightarrow 0^{(0)} = y,$$

nos da $y \leq 0^{(0)},\ \beta(y) \Rightarrow$.

Si podemos probar $y \leq 0^{(m)},\ \beta(y) \Rightarrow$ y $m+1 \leq n$, cortamos con el axioma

$$y \leq 0^{(m+1)} \Rightarrow y \leq 0^{(m)},\ y = 0^{(m+1)}$$

y con

$$\beta(0^{(m+1)}) \Rightarrow, \qquad y = 0^{(m+1)},\ \beta(y) \Rightarrow \beta(0^{(m+1)})$$

obtenemos $y \leq 0^{(m+1)},\ \beta(y) \Rightarrow$.

En particular podemos probar $y \leq 0^{(n)},\ \beta(y) \Rightarrow$, y usando $\Rightarrow 0^{(n)} = t$ podemos llegar a $y \leq t,\ \beta(y) \Rightarrow$. Aplicando las reglas izquierdas del conjuntor y del particularizador llegamos finalmente a $\bigvee u \leq t\, \beta(u) \Rightarrow$. ■

5.2 La consistencia de AP

Tal y como hemos explicado en el capítulo anterior, la prueba de Gentzen de la consistencia de AP 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 5.7 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[4] S. Si no hay ninguno, la altura es 0. En particular, el secuente final de una demostración siempre tiene altura 0.

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.

[4] 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.

Ejemplo La demostración del ejemplo de la página 30 tiene ordinal $\omega^{\omega^{\omega^2+5}}$. La figura muestra los ordinales de los últimos secuentes:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{1 \qquad 2}{3}}{3}}{4}}{5} \qquad \dfrac{\dfrac{\dfrac{\dfrac{6}{7} \qquad \dfrac{10}{11}}{17}}{18}}{\omega^2}}{\omega^{\omega^{\omega^2+5}}}$$

■

Teorema 5.8 *Sea S un secuente en una demostración D y sea D' una demostración que prolongue a D. Entonces $o(S; D') \leq o(S; D)$.*

DEMOSTRACIÓN: Razonamos inductivamente que si la desigualdad se cumple para todos los secuentes que están por encima de S, también se cumple para S. Distinguimos los mismos casos que en la definición del ordinal de una demostración:

1. Si S es un secuente inicial, trivialmente $o(S; D') = 1 = o(S; D)$.

2. Si S se sigue de S_1 por debilitación, entonces

$$o(S; D') = o(S_1; D') \leq o(S_1; D) = o(S_1; D').$$

3. Si S se sigue de S_1 y S_2 por la regla izquierda del disyuntor, entonces

$$o(S; D') = o(S_1; D')\#o(S_2; D') \leq o(S_1; D)\#o(S_2; D) = o(S; D).$$

El caso 4. es inmediato y, en los casos 5. y 6., sólo hay que tener en cuenta lo siguiente: la diferencia de alturas $h_1 - h_0$ es positiva si todas las inducciones y cortes posteriores tienen grado estrictamente menor que la fórmula de corte o inducción de la regla de la que se obtiene S, y es 0 en caso contrario. En D' puede haber más cortes o inducciones por debajo de S, por lo que un valor positivo de $h_1 - h_0$ en D puede volverse nulo en D', pero no al revés, luego en cualquier caso $h'_1 - h'_0 \leq h_1 - h_0$, de donde se sigue que $o(S; D') \leq o(S; D)$. ■

El teorema siguiente lo usaremos a menudo:

Teorema 5.9 *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 $o(S_1; D'_1) < o(S_1; D)$. 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 $S = S_1$, pues, usando el teorema anterior,

$$o(S_1; D') \leq o(S_1; D'_1) < o(S_1; D).$$

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 5.10 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 30 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 5.11 *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 esencial 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. ■

Ahora ya podemos probar el resultado principal:

Teorema 5.12 *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 3.10 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 3.7 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 5.3 nos da una demostración de $\Rightarrow 0^{(m)} = t$ y a su vez de otra demostración E del secuente $\alpha(0^{(m)}) \overset{q}{\Rightarrow} \alpha(t)$ 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 3.7 nos da que, para todo número natural n, al sustituir y por $0^{(n)}$ en D_0 obtenemos una demostración $D_0(0^{(n)})$ del secuente

$$\alpha(0^{(n)}), \Gamma \Rightarrow \Delta,\, \alpha(0^{(n+1)})$$

(notemos que y no puede aparecer en Γ o en Δ). Ahora encadenamos así las demostraciones $D_0(0^{(n)})$:

$$\dfrac{\dfrac{\begin{matrix} D_0(0^{(0)}) \\ \vdots \\ \alpha(0^{(0)}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(0^{(1)}) \end{matrix} \quad \begin{matrix} D_0(0^{(1)}) \\ \vdots \\ \alpha(0^{(1)}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(0^{(2)}) \end{matrix}}{\alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(2)})} \quad \begin{matrix} D_0(0^{(2)}) \\ \vdots \\ \alpha(0^{(2)}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(0^{(3)}) \end{matrix}}{\alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(3)})}$$

hasta llegar a una demostración del secuente

$$\alpha(0), \Gamma \Rightarrow \Delta,\, \alpha(0^{(m)})$$

y, a su vez, combinando la prueba con E, obtenemos:

$$\dfrac{\begin{matrix} \vdots \\ \alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(m)}) \end{matrix} \qquad \begin{matrix} E \\ \vdots \\ \alpha(0^{(m)}) \Rightarrow \alpha(t) \end{matrix}}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t)}$$

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 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 $\alpha(0^{(n)})$ tienen el mismo grado que $\alpha(y)$, luego todos los cortes situados en D' entre un secuente

$$\alpha(0^{(n)}), \Gamma \Rightarrow \Delta,\, \alpha(0^{(n+1)})$$

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 $D_0(0^{(n)})$ 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

$$\alpha(0^{(n)}), \Gamma \Rightarrow \Delta,\, \alpha(0^{(n+1)})$$

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:

$$o(\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(2)}); D') = \mu \# \mu,$$
$$o(\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(3)}); D') = \mu \# \mu \# \mu$$

y así:

$$o(\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(m)}); D') = \mu * m,$$

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 5.9 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:

$$\dfrac{\begin{array}{c} D_0 \\ \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha \end{array} \qquad \begin{array}{c} \alpha \Rightarrow \alpha \\ \vdots \\ \alpha,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta' \end{array}}{\begin{array}{c} \Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \end{array}}$$
$$\begin{array}{c} \vdots \\ \Rightarrow \end{array}$$

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

$$\dfrac{\begin{array}{c} D_0 \\ \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha \end{array}}{\Gamma,\, \Gamma' \overset{\mu}{\Rightarrow} \Delta,\, \Delta'}$$
$$\begin{array}{c} \vdots \\ \Rightarrow \end{array}$$

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 5.9 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:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha\end{array} \qquad \begin{array}{c}\vdots\\ \dfrac{\Gamma'' \Rightarrow \Delta''}{\alpha,\, \Gamma'' \Rightarrow \Delta''}\\ \vdots\\ \alpha,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta'\end{array}}{\begin{array}{c}\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'\\ \vdots\\ \Rightarrow\end{array}}$$

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':

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

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

$$\omega_{h-h'}(o(S; D)) \geq o(S'; D'). \tag{5.1}$$

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 5.9 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 (5.1) 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 4.8,

$$\omega_{h-h'}(o(S_0; D) = \omega_{h-h'}(o(S; D)\#o(\bar{S}; D)) \geq$$

$$\omega_{h-h'}(o(S; D))\#\omega_{h-h'}(o(\bar{S}; D)) \geq o(S'; D')\#o(\bar{S}'; D') = o(S'_0; D').$$

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 5.5.

• Por el teorema 5.11 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

$$
\begin{array}{c}
\begin{array}{cc}
\begin{array}{c}
\vdots \\
\dfrac{\alpha,\, \Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1}{\Gamma_1 \Rightarrow \Delta_1,\, \neg\alpha} \\
\vdots
\end{array}
&
\begin{array}{c}
\vdots \\
\dfrac{\Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1',\, \alpha}{\neg\alpha,\, \Gamma_1' \Rightarrow \Delta_1'} \\
\vdots
\end{array}
\end{array} \\
\dfrac{\Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \neg\alpha \quad (h_1) \quad \neg\alpha,\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'} \\
\vdots \\
\Gamma'' \overset{\nu}{\Rightarrow} \Delta'' \quad (h_0) \\
\vdots \\
\Rightarrow
\end{array}
$$

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:

$$
\begin{array}{c}
\begin{array}{cc}
\begin{array}{c}
\begin{array}{cc}
\begin{array}{c} \vdots \end{array}
&
\begin{array}{c}
\vdots \\
\dfrac{\Gamma_1' \overset{\nu_1}{\Rightarrow} \Delta_1',\, \alpha}{\neg\alpha,\, \Gamma_1' \Rightarrow \Delta_1',\, \alpha} \\
\vdots
\end{array}
\end{array} \\
\dfrac{\Gamma \overset{\xi_1}{\Rightarrow} \Delta,\, \neg\alpha \quad (h_1) \quad \neg\alpha,\, \Gamma' \overset{\xi_2}{\Rightarrow} \Delta',\, \alpha}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha} \\
\vdots \\
\Gamma'' \Rightarrow \Delta'',\, \alpha \quad (h)
\end{array}
&
\begin{array}{c}
\begin{array}{cc}
\begin{array}{c}
\vdots \\
\dfrac{\alpha,\, \Gamma_1 \overset{\nu_2}{\Rightarrow} \Delta_1}{\alpha,\, \Gamma_1 \Rightarrow \Delta_1,\, \neg\alpha} \\
\vdots
\end{array}
&
\begin{array}{c} \vdots \end{array}
\end{array} \\
\dfrac{\alpha,\, \Gamma \overset{\xi_3}{\Rightarrow} \Delta,\, \neg\alpha \quad (h_1) \quad \neg\alpha,\, \Gamma' \overset{\xi_4}{\Rightarrow} \Delta'}{\alpha,\, \Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'} \\
\vdots \\
(h) \quad \alpha,\, \Gamma'' \Rightarrow \Delta''
\end{array}
\end{array} \\
\hline
\Gamma'' \overset{\nu'}{\Rightarrow} \Delta'' \quad (h_0) \\
\vdots \\
\Rightarrow
\end{array}
$$

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[5]

$$\omega_{m-k}(\omega_{l-m}(\epsilon_1'\#\epsilon_2')\#\omega_{l-m}(\epsilon_1''\#\epsilon_2'')) < \omega_{m-k}(\omega_{l-m}(\epsilon_1\#\epsilon_2)) = \omega_{l-m}(\epsilon_1\#\epsilon_2),$$

o, lo que es lo mismo,

$$\nu = o(\Gamma'' \Rightarrow \Delta'', D') < o(\Gamma'' \Rightarrow \Delta'', D) = \nu'.$$

El teorema 5.9 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

$$\begin{array}{c}
\dfrac{\begin{array}{c}\vdots \\ \dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha}{\Gamma_1 \Rightarrow \Delta_1,\, \alpha \vee \beta} \\ \vdots \\ \Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \alpha \vee \beta \quad (h_1)\end{array} \qquad \begin{array}{c}\vdots \qquad\qquad \vdots \\ \dfrac{\alpha,\, \Gamma_1' \Rightarrow \Delta_1' \qquad \beta,\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}{\alpha \vee \beta,\, \Gamma_1' \Rightarrow \Delta_1'} \\ \vdots \\ \alpha \vee \beta,\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'} \\
\vdots \\
\Gamma'' \overset{\nu}{\Rightarrow} \Delta'' \quad (h_0) \\
\vdots \\
\Rightarrow
\end{array}$$

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:

$$\begin{array}{c}
\dfrac{\begin{array}{c}\dfrac{\begin{array}{c}\vdots \\ \dfrac{\Gamma_1 \Rightarrow \Delta_1,\, \alpha}{\Gamma_1 \Rightarrow \Delta_1,\, \alpha,\, \alpha \vee \beta} \\ \vdots \\ \Gamma \overset{\xi_1}{\Rightarrow} \Delta,\, \alpha, \alpha \vee \beta \quad (h_1)\end{array} \quad \begin{array}{c}\vdots \\ \alpha \vee \beta,\, \Gamma' \overset{\xi_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha} \\ \vdots \\ \Gamma'' \overset{\nu_1}{\Rightarrow} \Delta'',\, \alpha \quad (h)\end{array} \qquad \begin{array}{c}\dfrac{\begin{array}{c}\vdots \\ \Gamma \overset{\xi_3}{\Rightarrow} \Delta,\, \alpha \vee \beta \quad (h_1)\end{array} \quad \begin{array}{c}\vdots \\ \dfrac{\alpha,\, \Gamma_1' \Rightarrow \Delta_1'}{\alpha \vee \beta,\, \alpha,\, \Gamma_1' \Rightarrow \Delta_1'} \\ \vdots \\ \alpha \vee \beta,\, \alpha,\, \Gamma' \overset{\xi_4}{\Rightarrow} \Delta'\end{array}}{\alpha,\, \Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'} \\ \vdots \\ (h) \quad \alpha,\, \Gamma'' \overset{\nu_2}{\Rightarrow} \Delta''\end{array}}{\Gamma'' \overset{\nu'}{\Rightarrow} \Delta'' \quad (h_0)} \\
\vdots \\
\Rightarrow
\end{array}$$

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 $h_0 \leq h < h_1$.

[5] 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

$$\begin{array}{c}
\begin{array}{ccc}
\vdots & & \vdots \\
\dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \Rightarrow \Delta_1,\, \bigvee u\, \alpha(u)} & & \dfrac{\alpha(y),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}{\bigvee u\, \alpha(u),\, \Gamma_1' \Rightarrow \Delta_1'} \\
\vdots & & \vdots
\end{array} \\
\dfrac{\Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\, \alpha(u) \quad (h_1) \quad \bigvee u\, \alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'} \\
\vdots \\
\Gamma'' \overset{\nu}{\Rightarrow} \Delta'' \quad (h_0) \\
\vdots \\
\Rightarrow
\end{array}$$

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:

$$\begin{array}{c}
\begin{array}{ccc}
\vdots & & \\
\dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \Rightarrow \Delta_1,\, \alpha(t),\, \bigvee u\, \alpha(u)} & & \\
\vdots & & \vdots
\end{array} \\
\dfrac{\Gamma \overset{\xi_1}{\Rightarrow} \Delta,\, \alpha(t), \bigvee u\, \alpha(u) \quad (h_1) \quad \bigvee u\, \alpha(u),\, \Gamma' \overset{\xi_2}{\Rightarrow} \Delta'}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha(t)} \\
\vdots \\
\Gamma'' \Rightarrow \Delta'',\, \alpha(t) \quad (h)
\end{array}$$

$$\dfrac{\dfrac{\vdots}{\Gamma \overset{\xi_3}{\Rightarrow} \Delta, \bigvee u\, \alpha(u)} \quad (h_1) \quad \dfrac{\dfrac{\dfrac{\vdots}{\alpha(t), \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\, \alpha(u), \alpha(t), \Gamma_1' \Rightarrow \Delta_1'}}{\bigvee u\, \alpha(u), \alpha(t), \Gamma' \overset{\xi_4}{\Rightarrow} \Delta'}}{\dfrac{\alpha(t), \Gamma, \Gamma' \Rightarrow \Delta, \Delta'}{\dfrac{\vdots}{(h) \quad \alpha(t), \Gamma'' \Rightarrow \Delta''}}}$$

Estos dos bloques se combinan mediante un corte:

$$\dfrac{\dfrac{\vdots}{\Gamma'' \Rightarrow \Delta'', \alpha(t)} \quad (h) \quad \dfrac{\vdots}{\alpha(t), \Gamma'' \Rightarrow \Delta''}}{\dfrac{\Gamma'' \overset{\nu'}{\Rightarrow} \Delta'' \quad (h_0)}{\dfrac{\vdots}{\Rightarrow}}}$$

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. ■

La prueba de este teorema es formalizable en ARP. Más explícitamente, podemos definir un funtor $F(D)$ de modo que

$$\underset{\text{ARP}}{\vdash}(\overset{D}{\underset{\ulcorner\text{AP}\urcorner}{\vdash}}(\varnothing\Rightarrow\varnothing)\rightarrow\overset{F(D)}{\underset{\ulcorner\text{AP}\urcorner}{\vdash}}(\varnothing\Rightarrow\varnothing)\wedge o(F(D))<o(D)).$$

De aquí se deduce este teorema informal:

Teorema 5.13 (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.

Para formalizar este teorema en ARP basta expresarlo en términos de inducción transfinita: considerando la fórmula Π_1

$$\phi(\alpha)\equiv\neg\bigvee D(\overset{D}{\underset{\text{AP}}{\vdash}}(\varnothing\Rightarrow\varnothing)\wedge o(D)=\alpha),$$

obtenemos que

$$\underset{\text{ARP}}{\vdash}\bigwedge\alpha\in E(\neg\phi(\alpha)\rightarrow\bigvee\beta\prec\alpha\,\neg\phi(\beta))),$$

y esto equivale a

$$\underset{\text{ARP}}{\vdash}(\bigwedge\alpha\in E(\bigwedge\beta\prec\alpha\,\phi(\beta))\rightarrow\phi(\alpha)),$$

Por consiguiente,

$$\underset{\text{ARP}}{\vdash}(\phi-\text{IND}(\epsilon_0)\rightarrow\bigwedge\alpha\in E\,\phi(\alpha)\,),$$

pero $\bigwedge\alpha\in E\,\phi(\alpha)$ afirma que hay una fórmula que no puede ser demostrada en AP, luego implica Consis$\ulcorner\text{AP}\urcorner$ y así concluimos que

$$\underset{\text{ARP}}{\vdash}(\phi-\text{IND}(\epsilon_0)\rightarrow\text{Consis}\ulcorner\text{AP}\urcorner),$$

tal y como ya avanzábamos en el capítulo anterior. Así tenemos que la inducción transfinita hasta ϵ_0 (al menos para cierta fórmula ϕ de tipo Π_1) no es demostrable en AP.

¿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.*

Gentzen consideraba incuestionable la inducción hasta ϵ_0, pero 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 una propiedad de ϵ_0, que a su vez puede ser justificada satisfactoriamente. El lector tendrá que juzgar por sí mismo si le parece convincente la demostración que hemos presentado en el capítulo anterior, aunque es difícil juzgar si un argumento es convincente cuando uno ya está convencido *a priori* de su conclusión. ■

5.3 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 1.18 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 30 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 5.6:

Teorema 5.14 *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 5.6 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 5.9. De hecho necesitamos una versión ligeramente más general:

Teorema 5.15 *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 5.9, 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 $\mathrm{I}\Sigma_1$, vamos a dar aquí unas definiciones más generales:

Definición 5.16 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 5.11:

Teorema 5.17 *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 5.18 *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 3.10 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 3.7 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:

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, y \leq t \to \alpha(y)\end{array}}{\begin{array}{c}\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u)\\ \vdots\\ \Rightarrow\end{array}}$$

(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 $\alpha(0^{(k)})$ es falsa, pero entonces $0^{(k)} \leq t \to \alpha(0^{(k)})$ es falsa, y por 5.14 podemos demostrar el secuente $0^{(k)} \leq t \to \alpha(0^{(k)}) \overset{0}{\Rightarrow}$ 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 3.7 nos da una demostración del secuente

$$\Gamma \overset{\mu}{\Rightarrow} \Delta,\, 0^{(k)} \leq t \to \alpha(0^{(k)}).$$

Consideramos la demostración alternativa:

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, 0^{(k)} \leq t \to \alpha(0^{(k)})\end{array} \qquad \begin{array}{c}\vdots\\ 0^{(k)} \leq t \to \alpha(0^{(k)}) \overset{0}{\Rightarrow}\end{array}}{\Gamma \overset{\mu}{\Rightarrow} \Delta}}{\begin{array}{c}\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u)\\ \vdots\\ \Rightarrow\end{array}}$$

Si la fórmula principal en verdadera, entonces por 5.14 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

$$\dfrac{\begin{array}{c}\vdots\\ \overset{0}{\Rightarrow} \bigwedge u \leq t\, \alpha(u)\end{array}}{\begin{array}{c}\Gamma \overset{0}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u)\\ \vdots\\ \Rightarrow\end{array}}$$

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 5.15 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

$$\frac{\begin{array}{c}\vdots\\ y \leq t \wedge \alpha(y),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\end{array}}{\begin{array}{c}\bigvee u \leq t\, \alpha(u),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\\ \vdots\\ \Rightarrow\end{array}}$$

Si la fórmula principal es verdadera, entonces existe un $k \leq d(t)$ tal que $\alpha(0^{(k)})$ es verdadera, luego podemos construir la demostración alternativa:

$$\frac{\dfrac{\begin{array}{c}\vdots\\ \overset{0}{\Rightarrow} 0^{(k)} \leq t \wedge \alpha(0^{(k)})\end{array} \qquad \begin{array}{c}\vdots\\ 0^{(k)} \leq t \wedge \alpha(0^{(k)}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\end{array}}{\Gamma \overset{\mu}{\Rightarrow} \Delta}}{\begin{array}{c}\bigvee u \leq t\, \alpha(u),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\\ \vdots\\ \Rightarrow\end{array}}$$

mientras que si la fórmula principal es falsa, tenemos simplemente

$$\frac{\begin{array}{c}\vdots\\ \bigvee u \leq t\, \alpha(u) \overset{0}{\Rightarrow}\end{array}}{\begin{array}{c}\bigvee u \leq t\, \alpha(u),\, \Gamma \overset{0}{\Rightarrow} \Delta\\ \vdots\\ \Rightarrow\end{array}}$$

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 5.3 nos da una demostración de $\overset{0}{\Rightarrow} 0^{(m)} = t$ y a su vez de otra demostración E del secuente $\alpha(0^{(m)}) \overset{q}{\Rightarrow} \alpha(t)$ 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 1.17, 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 3.7 nos da que, para todo número natural n, al sustituir y por $0^{(n)}$ en D_0 obtenemos una demostración $D_0(0^{(n)})$ del secuente

$$\alpha(0^{(n)}), \Gamma \overset{\mu}{\Rightarrow} \Delta,\ \alpha(0^{(n+1)})$$

(notemos que y no puede aparecer en Γ o en Δ). Ahora encadenamos así las demostraciones $D_0(0^{(n)})$:

$$\dfrac{\dfrac{\begin{array}{c} D_0(0^{(0)}) \\ \vdots \\ \alpha(0^{(0)}),\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\ \alpha(0^{(1)}) \end{array} \quad \begin{array}{c} D_0(0^{(1)}) \\ \vdots \\ \alpha(0^{(1)}),\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\ \alpha(0^{(2)}) \end{array}}{\alpha(0^{(0)}),\ \Gamma \Rightarrow \Delta,\ \alpha(0^{(2)})} \quad \begin{array}{c} D_0(0^{(2)}) \\ \vdots \\ \alpha(0^{(2)}),\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\ \alpha(0^{(3)}) \end{array}}{\alpha(0^{(0)}),\ \Gamma \Rightarrow \Delta,\ \alpha(0^{(3)})}$$

hasta llegar a una demostración del secuente

$$\alpha(0^{(0)}), \Gamma \Rightarrow \Delta,\ \alpha(0^{(m)})$$

y, a su vez, combinando la prueba con E obtenemos:

$$\dfrac{\begin{array}{c} \vdots \\ \alpha(0^{(0)}),\ \Gamma \Rightarrow \Delta,\ \alpha(0^{(m)}) \end{array} \qquad \begin{array}{c} E \\ \vdots \\ \alpha(0^{(m)}) \Rightarrow \alpha(t) \end{array}}{\alpha(0),\ \Gamma \Rightarrow \Delta,\ \alpha(t)}$$

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 el ordinal en D' de los secuentes

$$\alpha(0^{(n)}), \Gamma \Rightarrow \Delta,\ \alpha(0^{(n+1)})$$

sigue siendo μ (pues ahora el ordinal de un secuente sólo depende de los secuentes que tiene por encima). A su vez:

$$o(\alpha(0^{(0)}),\ \Gamma \Rightarrow \Delta,\ \alpha(0^{(2)}); D') = \mu\#\mu,$$

$$o(\alpha(0^{(0)}),\ \Gamma \Rightarrow \Delta,\ \alpha(0^{(3)}); D') = \mu\#\mu\#\mu$$

y así:

$$o(\alpha(0^{(0)}),\ \Gamma \Rightarrow \Delta,\ \alpha(0^{(m)}); D') = \mu * m,$$

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 5.15 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

$$\cfrac{\begin{array}{c} D_0 \\ \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha \end{array}}{\begin{array}{c} \Gamma,\, \Gamma' \overset{\mu}{\Rightarrow} \Delta,\, \Delta' \\ \vdots \\ \Rightarrow \end{array}}$$

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 5.15 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:

$$\cfrac{\begin{array}{c} \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha \end{array} \qquad \begin{array}{c} \cfrac{\begin{array}{c}\vdots \\ \Gamma'' \Rightarrow \Delta''\end{array}}{\alpha,\, \Gamma'' \Rightarrow \Delta''} \\ \vdots \\ \alpha,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta' \end{array}}{\begin{array}{c} \Gamma,\, \Gamma' \overset{\xi}{\Rightarrow} \Delta,\, \Delta' \\ \vdots \\ \Rightarrow \end{array}}$$

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 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':

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

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 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':

$$\dfrac{\begin{array}{c}\vdots\\ \Gamma'' \Rightarrow \Delta''\\ \vdots\\ \Gamma' \overset{\nu}{\Rightarrow} \Delta'\end{array}}{\Gamma,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta,\, \Delta'}$$
$$\begin{array}{c}\vdots\\ \Rightarrow\end{array}$$

Es claro que $\nu = o(\alpha,\, \Gamma' \Rightarrow \Delta'; D) = o(\Gamma' \Rightarrow \Delta'; D')$, luego $\xi = \mu \# \nu \geq \nu$ y el teorema 5.15 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 5.5.

Por consiguiente, podemos aplicar el teorema 5.17, 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:

$$
\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \stackrel{\nu_1}{\Rightarrow} \Delta_1,\ \alpha(t)}{\Gamma_1 \stackrel{\nu_1+1}{\Rightarrow} \Delta_1,\ \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma \stackrel{\mu_1}{\Rightarrow} \Delta,\ \bigvee u\,\alpha(u)\end{array} \qquad \begin{array}{c}\vdots\\ \dfrac{\alpha(y),\ \Gamma_1' \stackrel{\nu_2}{\Rightarrow} \Delta_1'}{\bigvee u\,\alpha(u),\ \Gamma_1' \stackrel{\nu_2+1}{\Rightarrow} \Delta_1'}\\ \vdots\\ \bigvee u\,\alpha(u),\ \Gamma' \stackrel{\mu_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\ \Gamma' \Rightarrow \Delta,\ \Delta'}\\
\vdots\\
\Rightarrow
\end{array}
$$

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 3.7, 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 5.14 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:

$$
\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \stackrel{\nu_1}{\Rightarrow} \Delta_1,\ \alpha(t)}{\Gamma_1 \stackrel{\nu_1+1}{\Rightarrow} \Delta_1,\ \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma \stackrel{\mu_1}{\Rightarrow} \Delta,\ \bigvee u\,\alpha(u)\end{array} \quad (h_1) \quad \begin{array}{c}\dfrac{\dfrac{\begin{array}{c}\vdots\\ \stackrel{0}{\Rightarrow} \alpha(t)\end{array} \qquad \begin{array}{c}\vdots\\ \alpha(t),\ \Gamma_1' \stackrel{\nu_2}{\Rightarrow} \Delta_1'\end{array}}{\Gamma_1' \stackrel{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\,\alpha(u),\ \Gamma_1' \stackrel{\nu_2}{\Rightarrow} \Delta_1'}\\ \vdots\\ \bigvee u\,\alpha(u),\ \Gamma' \stackrel{\mu_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\ \Gamma' \Rightarrow \Delta,\ \Delta'}\\
\vdots\\
\Rightarrow
\end{array}
$$

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 5.15 nos da que $o(D') < o(D)$. ■

Por consiguiente, tenemos el siguiente teorema informal:

Teorema 5.19 *Si* $\mathrm{I}\Sigma_1$ *es contradictoria, existe una sucesión infinita estrictamente decreciente de ordinales menores que* ω^ω.

Este teorema se formaliza en ARP en términos de la inducción transfinita hasta ω^ω. Concretamente, si $\phi(\alpha)$ es la fórmula Π_1 que expresa que no existen demostraciones del secuente vacío en $\mathrm{I}\Sigma_1$ de ordinal menor que α, en ARP se puede probar

$$\phi - \mathrm{Ind}(\omega^\omega) \rightarrow \mathrm{Consis}\ulcorner \mathrm{I}\Sigma_1 \urcorner.$$

Esto encaja con que, según la observación tras el teorema 4.16,

$$\underset{\mathrm{I}\Sigma_2}{\vdash} \phi - \mathrm{IND}(\omega^\omega),$$

lo que nos da que

$$\underset{\mathrm{I}\Sigma_2}{\vdash} \mathrm{Consis}\ulcorner \mathrm{I}\Sigma_1 \urcorner,$$

como ya habíamos probado en [LF 6.22].

5.4 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 5.20 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 30 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 5.21 *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 5.14 sigue siendo válido para esta nueva asignación de ordinales. También podemos probar una versión de los teoremas 5.9 o 5.15 modificando ligeramente los cálculos de la demostración:

Teorema 5.22 *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.

Como en 5.9, 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 5.23 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 5.17 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 $I\Sigma_n$ 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 1.18 nos asegura que S^* admite una demostración en $I\Sigma_n$ 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 5.24 *Sea D una demostración en $I\Sigma_n$ 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 3.10 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 3.7 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:

$$\begin{array}{c} \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, y \leq t \rightarrow \alpha(y) \\ \hline \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u) \\ \vdots \\ S^* \end{array}$$

(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 $\alpha(0^{(k)})$ es falsa, pero entonces $0^{(k)} \leq t \rightarrow \alpha(0^{(k)})$ es falsa, y por 5.14 podemos demostrar el secuente $0^{(k)} \leq t \rightarrow \alpha(0^{(k)}) \overset{0}{\Rightarrow}$ 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 3.7 nos da una demostración del secuente

$$\Gamma \overset{\mu}{\Rightarrow} \Delta,\, 0^{(k)} \leq t \rightarrow \alpha(0^{(k)}).$$

Consideramos la demostración alternativa:

$$\dfrac{\dfrac{\begin{matrix}\vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\, 0^{(k)} \leq t \rightarrow \alpha(0^{(k)})\end{matrix} \qquad \begin{matrix}\vdots \\ 0^{(k)} \leq t \rightarrow \alpha(0^{(k)}) \overset{0}{\Rightarrow}\end{matrix}}{\Gamma \overset{\mu}{\Rightarrow} \Delta}}{\begin{matrix}\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u) \\ \vdots \\ S^*\end{matrix}}$$

Si la fórmula principal en verdadera, entonces por 5.14 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

$$\dfrac{\begin{matrix}\vdots \\ \overset{0}{\Rightarrow} \bigwedge u \leq t\, \alpha(u)\end{matrix}}{\begin{matrix}\Gamma \Rightarrow \Delta,\, \bigwedge u \leq t\, \alpha(u) \\ \vdots \\ S^*\end{matrix}}$$

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 $\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \bigwedge u \leq t\, \alpha(u)$ no hay inducciones (no hay reglas propias, en general), podemos aplicar el teorema 5.22 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

$$\dfrac{\begin{matrix}\vdots \\ y \leq t \wedge \alpha(y),\, \Gamma \overset{\mu}{\Rightarrow} \Delta\end{matrix}}{\begin{matrix}\bigvee u \leq t\, \alpha(u),\, \Gamma \overset{\mu}{\Rightarrow} \Delta \\ \vdots \\ S^*\end{matrix}}$$

Si la fórmula principal es verdadera, entonces existe un $k \leq d(t)$ tal que $\alpha(0^{(k)})$ es verdadera, luego podemos construir la demostración alternativa:

$$\dfrac{\dfrac{\begin{array}{cc}\vdots & \vdots \\ \stackrel{0}{\Rightarrow} 0^{(k)} \leq t \wedge \alpha(0^{(k)}) & 0^{(k)} \leq t \wedge \alpha(0^{(k)}),\, \Gamma \stackrel{\mu}{\Rightarrow} \Delta\end{array}}{\Gamma \stackrel{\mu}{\Rightarrow} \Delta}}{\bigvee u \leq t\, \alpha(u),\, \Gamma \stackrel{\mu}{\Rightarrow} \Delta}$$

$$\begin{array}{c}\vdots \\ S^*\end{array}$$

mientras que si la fórmula principal es falsa, tenemos simplemente

$$\dfrac{\begin{array}{c}\vdots \\ \bigvee u \leq t\, \alpha(u) \stackrel{0}{\Rightarrow}\end{array}}{\bigvee u \leq t\, \alpha(u),\, \Gamma \Rightarrow \Delta}$$

$$\begin{array}{c}\vdots \\ S^*\end{array}$$

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

$$\frac{\alpha(y),\, \Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha(y') \quad (h_1)}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t) \quad (h_0)},$$

donde las fórmulas principales son sentencias.

Sea $m = d(t)$, de modo que el teorema 5.3 nos da una demostración de $\stackrel{0}{\Rightarrow} 0^{(m)} = t$ y a su vez de otra demostración E del secuente $\alpha(0^{(m)}) \stackrel{q}{\Rightarrow} \alpha(t)$ 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 1.17, 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 3.7 nos da que, para todo número natural n, al sustituir y por $0^{(n)}$ en D_0 obtenemos una demostración $D_0(0^{(n)})$ del secuente

$$\alpha(0^{(n)}), \Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha(0^{(n+1)})$$

(notemos que y no puede aparecer en Γ o en Δ). Ahora encadenamos así las demostraciones $D_0(0^{(n)})$:

$$\dfrac{\dfrac{\begin{matrix} D_0(0^{(0)}) \\ \vdots \\ \alpha(0^{(0)}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(0^{(1)}) \end{matrix} \qquad \begin{matrix} D_0(0^{(1)}) \\ \vdots \\ \alpha(0^{(1)}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(0^{(2)}) \end{matrix}}{\alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(2)})} \qquad \begin{matrix} D_0(0^{(2)}) \\ \vdots \\ \alpha(0^{(2)}),\, \Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(0^{(3)}) \end{matrix}}{\alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(3)})}$$

hasta llegar a una demostración del secuente

$$\alpha(0^{(0)}), \Gamma \Rightarrow \Delta,\, \alpha(0^{(m)})$$

y, a su vez, combinando la prueba con E obtenemos:

$$\dfrac{\begin{matrix} \\ \vdots \\ \alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(m)}) \end{matrix} \qquad \begin{matrix} E \\ \vdots \\ \alpha(0^{(m)}) \Rightarrow \alpha(t) \end{matrix}}{\alpha(0),\, \Gamma \Rightarrow \Delta,\, \alpha(t)}$$

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 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 $\alpha(0^{(n)})$ tienen el mismo grado que $\alpha(y)$, luego todos los cortes situados en D' entre un secuente

$$\alpha(0^{(n)}), \Gamma \Rightarrow \Delta,\, \alpha(0^{(n+1)})$$

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 $D_0(0^{(n)})$ 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

$$\alpha(0^{(n)}), \Gamma \Rightarrow \Delta,\, \alpha(0^{(n+1)})$$

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:

$$o(\alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(2)}); D') = \mu\#\mu,$$
$$o(\alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(3)}); D') = \mu\#\mu\#\mu$$

y así:

$$o(\alpha(0^{(0)}),\, \Gamma \Rightarrow \Delta,\, \alpha(0^{(m)}); D') = \mu * m,$$

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 5.22 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:

$$\begin{array}{c} \vdots \\ \dfrac{\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha(t)}{\Gamma \overset{\mu+2}{\Rightarrow} \Delta,\, \bigvee u\, \alpha(u)} \\ \vdots \\ \Gamma' \overset{\nu}{\Rightarrow} \Delta',\, \bigvee u\, \alpha(u) \end{array}$$

Como la regla es explícita, $\alpha(t)$ es una sentencia Δ_0, luego, según el teorema 5.14, 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

$$\dfrac{\dfrac{\begin{array}{c}\vdots\\ \stackrel{0}{\Rightarrow} \alpha(t)\end{array}}{\stackrel{2}{\Rightarrow} \bigvee u\,\alpha(u)}}{\Gamma' \Rightarrow \Delta', \bigvee u\,\alpha(u)}$$

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

$$\begin{array}{c}\dfrac{\dfrac{\Gamma \stackrel{\mu}{\Rightarrow} \Delta, \alpha(t) \qquad \alpha(t) \stackrel{0}{\Rightarrow}}{\Gamma \stackrel{\mu}{\Rightarrow} \Delta}}{\Gamma \stackrel{\mu}{\Rightarrow} \Delta, \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma' \stackrel{\nu'}{\Rightarrow} \Delta', \bigvee u\,\alpha(u)\end{array}$$

Como hemos probado el secuente $\Gamma \Rightarrow \Delta, \bigvee u\,\alpha(u)$ con ordinal $\mu < \mu + 2$, el teorema 5.22 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

$$\begin{array}{c} \begin{array}{cc} D_0 & \alpha \Rightarrow \alpha \\ \vdots & \vdots \\ \Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha & \alpha,\, \Gamma' \stackrel{\nu}{\Rightarrow} \Delta' \end{array} \\ \hline \Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\ \vdots \\ S^* \end{array}$$

donde Δ' contiene un descendiente del α situado en el consecuente del axioma. Entonces podemos simplificar D hasta una demostración D' de la forma

$$\begin{array}{c} D_0 \\ \vdots \\ \Gamma \stackrel{\mu}{\Rightarrow} \Delta,\, \alpha \\ \hline \Gamma,\, \Gamma' \stackrel{\mu'}{\Rightarrow} \Delta,\, \Delta' \\ \vdots \\ S^* \end{array}$$

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 $\Gamma \Rightarrow \Delta,\, \alpha$ 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 5.22 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:

$$
\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\mu}{\Rightarrow} \Delta,\ \alpha \quad (h_1)\end{array} \qquad \begin{array}{c}\vdots \\ \dfrac{\Gamma''\Rightarrow\Delta''}{\alpha,\ \Gamma''\Rightarrow\Delta''}\\ \vdots\\ \alpha,\ \Gamma'\overset{\nu}{\Rightarrow}\Delta'\end{array}}{\Gamma,\ \Gamma'\overset{\xi}{\Rightarrow}\Delta,\ \Delta' \quad (h_0)}\\
\vdots\\
S^*
\end{array}
$$

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 $\alpha,\ \Gamma''\Rightarrow\Delta''$, entonces α "aparece" aunque no usemos la regla de debilitación que la introduce en D, con lo que podemos considerar demostración alternativa D':

$$
\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \Gamma \Rightarrow \Delta,\ \alpha\end{array} \qquad \begin{array}{c}\vdots \\ \Gamma''\Rightarrow\Delta''\\ \vdots\\ \alpha,\ \Gamma'\Rightarrow\Delta'\end{array}}{\Gamma,\ \Gamma'\Rightarrow\Delta,\ \Delta'}\\
\vdots\\
S^*
\end{array}
$$

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 $\alpha,\ \Gamma''\Rightarrow\Delta''$, 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':

$$\begin{array}{c} \vdots \\ \Gamma'' \Rightarrow \Delta'' \\ \vdots \\ \Gamma' \overset{\nu'}{\Rightarrow} \Delta' \ (h_0) \\ \hline \Gamma,\, \Gamma' \overset{\nu''}{\Rightarrow} \Delta,\, \Delta' \ (h_0) \\ \vdots \\ S^* \end{array}$$

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 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

$$\omega_{h-h'}(o(S; D)) \geq o(S'; D'). \tag{5.2}$$

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 4.8,

$$\xi = \omega_{h_1-h_0}(\mu\#\nu) \geq \omega_{h_1-h_0}(\mu)\#\omega_{h_1-h_0}(\nu) \geq \mu\#\omega_{h_1-h_0}(\nu) \geq \mu\#\nu' \geq \nu''.$$

El teorema 5.22 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 (5.2). 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,

$$\begin{aligned}\omega_{h-h'}(o(S;D)\#o(\bar{S};D)) &\geq \omega_{h-h'}(o(S;D))\#\omega_{h-h'}(o(\bar{S};D))\\ &\geq o(S';D')\#o(\bar{S}';D')\end{aligned}$$

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

$$\begin{aligned}\omega_{h-h'}(o(S;D)\#o(\bar{S};D)) &= \omega_{h-h'}(o(S;D))\\ &\geq o(S';D') = o(S';D')\#o(\bar{S}';D').\end{aligned}$$

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 5.17, 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:

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}}{\Gamma_1 \overset{\nu_1+2}{\Rightarrow} \Delta_1,\, \bigvee u\,\alpha(u)} \atop {\vdots \atop \Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\,\alpha(u)} \quad (h_1) \quad \dfrac{\dfrac{\vdots}{\alpha(y),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\,\alpha(u),\, \Gamma_1' \overset{\nu_2+2}{\Rightarrow} \Delta_1'} \atop {\vdots \atop \bigvee u\,\alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \atop \vdots}$$

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 3.7, 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 5.14, 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:

$$\dfrac{\dfrac{\dfrac{\vdots}{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}}{\Gamma_1 \overset{\nu_1+1}{\Rightarrow} \Delta_1,\, \bigvee u\,\alpha(u)} \atop {\vdots \atop \Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\,\alpha(u)} \quad (h_1) \quad \dfrac{\dfrac{\dfrac{\vdots \atop \overset{0}{\Rightarrow} \alpha(t) \qquad \vdots \atop \alpha(t),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}{\Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}}{\bigvee u\,\alpha(u),\, \Gamma_1' \overset{\nu_2+1}{\Rightarrow} \Delta_1'} \atop {\vdots \atop \bigvee u\,\alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \atop \vdots}$$

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 5.22 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:

$$\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \overset{\nu_1+2}{\Rightarrow} \Delta_1,\, \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma \overset{\mu_1}{\Rightarrow} \Delta,\, \bigvee u\,\alpha(u)\end{array} \quad (h_1) \quad \begin{array}{c}\vdots\\ \dfrac{\alpha(y),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}{\bigvee u\,\alpha(u),\, \Gamma_1' \overset{\nu_1+2}{\Rightarrow} \Delta_1'}\\ \vdots\\ \bigvee u\,\alpha(u),\, \Gamma' \overset{\mu_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}\\
\vdots\\
\Gamma'' \overset{\nu}{\Rightarrow} \Delta'' \quad (h_0)\\
\vdots
\end{array}$$

Ahora consideramos la demostración alternativa D' siguiente, que por razones tipográficas descomponemos en dos bloques:

$$\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \dfrac{\Gamma_1 \overset{\nu_1}{\Rightarrow} \Delta_1,\, \alpha(t)}{\Gamma_1 \overset{\nu_1+1}{\Rightarrow} \Delta_1,\, \alpha(t),\, \bigvee u\,\alpha(u)}\\ \vdots\\ \Gamma \overset{\xi_1}{\Rightarrow} \Delta,\, \alpha(t), \bigvee u\,\alpha(u)\end{array} \quad (h_1) \quad \begin{array}{c}\vdots\\ \bigvee u\,\alpha(u),\, \Gamma' \overset{\xi_2}{\Rightarrow} \Delta'\end{array}}{\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta',\, \alpha(t)}\\
\vdots\\
\Gamma'' \Rightarrow \Delta'',\, \alpha(t) \quad (h)
\end{array}$$

$$\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \Gamma \overset{\xi_3}{\Rightarrow} \Delta,\, \bigvee u\,\alpha(u)\end{array} \quad (h_1) \quad \begin{array}{c}\vdots\\ \dfrac{\alpha(t),\, \Gamma_1' \overset{\nu_2}{\Rightarrow} \Delta_1'}{\bigvee u\,\alpha(u),\, \alpha(t),\, \Gamma_1' \overset{\nu_2+1}{\Rightarrow} \Delta_1'}\\ \vdots\\ \bigvee u\,\alpha(u),\, \alpha(t),\, \Gamma' \overset{\xi_4}{\Rightarrow} \Delta'\end{array}}{\alpha(t),\, \Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'}\\
\vdots\\
(h) \quad \alpha(t), \Gamma'' \Rightarrow \Delta''
\end{array}$$

Estos dos bloques se combinan en un corte:

$$\begin{array}{c}
\dfrac{\begin{array}{c}\vdots\\ \Gamma'' \Rightarrow \Delta'',\, \alpha(t) \quad (h)\end{array} \qquad \begin{array}{c}\vdots\\ (h) \quad \alpha(t), \Gamma'' \Rightarrow \Delta''\end{array}}{\Gamma'' \overset{\nu'}{\Rightarrow} \Delta'' \quad (h_0)}\\
\vdots
\end{array}$$

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 $\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta'$ 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'. 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

$$\frac{\dfrac{S_1' \qquad\qquad S_2'}{\Gamma'' \Rightarrow \Delta'',\, \alpha(t)} \qquad \dfrac{S_1'' \qquad\qquad S_2''}{\alpha(t),\, \Gamma'' \Rightarrow \Delta''}}{\Gamma'' \Rightarrow \Delta''}$$

y los ordinales son:

$$\dfrac{\dfrac{\epsilon_1' \qquad \epsilon_2'}{\omega_{h_1-h}(\epsilon_1'\#\epsilon_2')} \qquad \dfrac{\epsilon_1'' \qquad \epsilon_2''}{\omega_{h_1-h}(\epsilon_1''\#\epsilon_2'')}}{\omega_{h_1-h_0}\big(\omega_{h_1-h}(\epsilon_1'\#\epsilon_2')\#\omega_{h_1-h}(\epsilon_1''\#\epsilon_2'')\big)}$$

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[6]

$$\omega_{h-h_0}\big(\omega_{h_1-h}(\epsilon_1'\#\epsilon_2')\#\omega_{h_1-h}(\epsilon_1''\#\epsilon_2'')\big)$$
$$< \omega_{h-h_0}(\omega_{h_1-h}(\epsilon_1\#\epsilon_2)) = \omega_{h_1-h}(\epsilon_1\#\epsilon_2),$$

o, lo que es lo mismo,

$$\nu = o(\Gamma'' \Rightarrow \Delta'', D') < o(\Gamma'' \Rightarrow \Delta'', D) = \nu'.$$

El teorema 5.22 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 1.18 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 5.25 *Si D es una demostración del secuente vacío en $\mathrm{I}\Sigma_n$, existe otra D' tal que $o(D') < o(D)$.*

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 3.7, podríamos convertirla en una demostración formada sólo por sentencias Δ_0, en contra del teorema 5.5.

Así pues, el teorema anterior nos proporciona concretamente una demostración que cumple $o(D') < o(D)$. ■

Como en las dos secciones precedentes, de aquí obtenemos:

Teorema 5.26 *Si $\mathrm{I}\Sigma_n$ es contradictoria, existe una sucesión infinita estrictamente decreciente de ordinales menores que $\omega^{(n+1)}$.*

Esto se formaliza en ARP considerando la fórmula ϕ_n de tipo Π_1 que afirma que no existen demostraciones del secuente vacío en $\mathrm{I}\Sigma_n$. En ARP se prueba que

$$\phi_n - \mathrm{IND}(\omega^{(n+1)}) \rightarrow \mathrm{Consis}\ulcorner \mathrm{I\Sigma_n} \urcorner,$$

[6]Aquí usamos que si $\eta' \leq \eta'' < \eta$, entonces $\omega^{\eta'}\#\omega^{\eta''} = \omega^{\eta''} + \omega^{\eta'} < \omega^\eta$.

lo que, unido a que, según la observación tras el teorema 4.16,

$$\underset{\mathrm{I}\Sigma_{\mathrm{n+1}}}{\vdash} \phi - \mathrm{IND}(\omega^{(n+1)}),$$

lo que nos da que

$$\underset{\mathrm{I}\Sigma_{\mathrm{n+1}}}{\vdash} \mathrm{Consis}\ulcorner \mathrm{I}\Sigma_{\mathrm{n}} \urcorner,$$

como ya habíamos probado en [LF 6.22].

Capítulo VI

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

$$\bigwedge v \in E(\bigwedge v \prec u\, \phi(v) \rightarrow \phi(u)) \rightarrow \bigwedge u \in E\, \phi(u)$$

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.

6.1 Buenos órdenes demostrables

En el capítulo IV 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.

En esta sección trabajamos en la aritmética de segundo orden RA_0 [LF 7.44], en la que podemos definir el modelo natural de $\mathcal{L}_a$.

Definición 6.1 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. $n \in D$ si y sólo si $\mathbb{N} \vDash 0^{(n)} \trianglelefteq 0^{(n)}$,
2. $\mathbb{N} \vDash (x \trianglelefteq y \rightarrow x \trianglelefteq x \land y \trianglelefteq y)$,
3. $\mathbb{N} \vDash (x \trianglelefteq y \land y \trianglelefteq x \rightarrow x = y)$,
4. $\mathbb{N} \vDash (x \trianglelefteq y \land y \trianglelefteq z \rightarrow x \trianglelefteq z)$,
5. $\mathbb{N} \vDash (x \trianglelefteq y \lor y \trianglelefteq x)$.

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 IV 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

$$m \trianglelefteq n \quad \text{si y sólo si} \quad \mathbb{N} \vDash 0^{(m)} \trianglelefteq 0^{(n)}.$$

Tenemos así que $\trianglelefteq$ es una relación de orden total sobre el conjunto D. Definimos

$$x \vartriangleleft y \equiv x \trianglelefteq y \land x \neq y,$$

que es también una fórmula Σ_1 y claramente

$$m \trianglelefteq n \quad \text{si y sólo si} \quad \text{no } n \vartriangleleft m \quad \text{si y sólo si} \quad \mathbb{N} \vDash \neg 0^{(n)} \vartriangleleft 0^{(m)},$$

con lo que la relación $\trianglelefteq$ es en realidad Δ_1, luego recursiva [LF 8.20], 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. Informalmente, 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:*

$$n_0 \vartriangleright n_1 \vartriangleright n_2 \vartriangleright \cdots$$

3. *Para toda propiedad $P(n)$, si para todo $n \in D$, el hecho de que todo $m \vartriangleleft n$ 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 4.4 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 4.6 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 4.19 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 6.2 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) si[2] 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 $x \in A \land y \in A \land x \trianglelefteq y$.

[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

$$\bigwedge u \in D(\bigwedge v \lhd u\, \phi(v) \rightarrow \phi(u)) \rightarrow \bigwedge u \in D\, \phi(u).$$

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 4.19 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 ($Rn \leftrightarrow n$ 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 4.19 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

$$x \unlhd_n y \equiv x \unlhd y \unlhd \omega^{(0^{(n)})}$$

sí que representa un buen orden demostrable sobre el conjunto de los ordinales menores o iguales que $\omega^{(n)}$, pues, tal y como hemos señalado al principio de la sección 4.6, la prueba del teorema 4.15 (luego la de 4.16) 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,

$$x \unlhd y \equiv (x \leq y \wedge \bigwedge u \leq x\, \phi(u)) \vee (y \leq x \wedge \bigvee u \leq x\, \neg\phi(u)).$$

Así, si llamamos F a la relación dada por Fn si y sólo si $\mathbb{N} \vDash \phi(0^{(n)})$, tenemos que si todo n cumple Fn, entonces la relación $\trianglelefteq$ 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 $x \trianglelefteq y$ 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 $\underset{\mathrm{AP}}{\vdash} \bigwedge u\, u \trianglelefteq u$, 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

$$\bigwedge uv(u \trianglelefteq v \leftrightarrow u \leq v),$$

y es fácil ver entonces que $x \trianglelefteq y$ representa un buen orden demostrable. Recíprocamente, si $x \trianglelefteq y$ 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:

$$\bigwedge u(\bigwedge v \lhd u \bigwedge w \leq v\, \phi(w) \rightarrow \bigwedge w \leq u\, \phi(w)) \rightarrow \bigwedge u \bigwedge w \leq u\, \phi(w).$$

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

$$x \leq x + 1 \land \bigvee w \leq x\, \neg\phi(w),$$

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

$$\phi(x) \equiv \neg \underset{\ulcorner \mathrm{AP} \urcorner}{\overset{x}{\vdash}} \ulcorner 0 \neq 0 \urcorner,$$

de modo que $\bigwedge u\, \phi(u)$ es $\mathrm{Consis}\ulcorner \mathrm{AP} \urcorner$. Concluimos que la fórmula $x \trianglelefteq y$ 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

$$m \precsim n \quad \text{si y sólo si} \quad G(m) \trianglelefteq G(n).$$

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

$$\phi(x,y) \equiv (x \neq 0 \land x \neq 0^{(n_0)} \land y = x) \lor$$
$$(x = 0 \land y = 0^{(n_0)}) \lor (x = 0^{(n_0)} \land y = 0)$$

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 6.3 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*

$$\mathrm{IT}(\trianglelefteq) \equiv \bigwedge u(\bigwedge v \lhd u\, Rv \to Ru) \to \bigwedge u\, Ru.$$

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 $m \lhd n$, 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 $n \lhd m$.

6.2 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 IV 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 6.4 *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',*

$$k \lhd k' \quad \textit{si y sólo si} \quad F(k) \prec F(k').$$

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 o, al menos, las formalizables en RA_0.

Un cálculo secuencial para $\mathbf{AP}^R$ De acuerdo con la definición 6.3 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 [LF 4.1], 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 [LF 7.46], 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 [LF 4.5], 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 6.3 sea demostrable en AP^R equivale claramente a que lo sea el secuente

$$\mathrm{IT}(\trianglelefteq) \equiv \bigwedge u (\bigwedge v \lhd u\, Rv \rightarrow Ru) \Rightarrow Rx$$

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

$$\bigwedge v \lhd t\, Rv \Rightarrow Rt,$$

[4]Podríamos introducir también una regla izquierda de sustitución de forma obvia, pero no la vamos a necesitar.

donde t es un término arbitrario, y cuyo secuente final sea de la forma

$$\Rightarrow R0^{(m_1)}, \ldots, R0^{(m_n)}.$$

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 3.7 y 3.10 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 $\bigwedge v \lhd y\, Rv \Rightarrow Ry$,

$$\dfrac{\dfrac{\dfrac{\bigwedge v \lhd y\, Rv \Rightarrow Ry}{\Rightarrow \bigwedge v \lhd y\, Rv \rightarrow Ry}}{\Rightarrow \bigwedge u(\bigwedge v \lhd u\, Rv \rightarrow Ru)} \qquad \begin{matrix}\vdots \\ \bigwedge u(\bigwedge v \lhd u\, Rv \rightarrow Ru) \Rightarrow Rx\end{matrix}}{\Rightarrow Rx}$$

el teorema 3.7 nos da que, para todo número natural m, al sustituir x por $0^{(m)}$ en $D(x)$ obtenemos una demostración IT, que llamaremos $D(0^{(m)})$, del secuente $\Rightarrow R0^{(m)}$.

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 5.9 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 debilitación.

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 5.12:

Teorema 6.5 *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 3.10 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 3.7 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 5.12 nos da una demostración de ordinal menor con el mismo secuente final (en esta parte de la prueba de 5.12 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.

[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.

• Supongamos ahora que la parte final de D contiene un axioma lógico, es decir, un secuente de la forma $\alpha \Rightarrow \alpha$.

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:

$$\begin{array}{c}
\begin{array}{cc}
D_0 & \alpha \Rightarrow \alpha \\
\vdots & \vdots \\
\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha & \alpha,\, \Gamma' \overset{\nu}{\Rightarrow} \Delta'
\end{array} \\
\hline
\Gamma,\, \Gamma' \Rightarrow \Delta,\, \Delta' \\
\vdots \\
\Rightarrow R0^{(m_1)}, \ldots, R0^{(m_n)}
\end{array}$$

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

$$\begin{array}{c}
D_0 \\
\vdots \\
\Gamma \overset{\mu}{\Rightarrow} \Delta,\, \alpha \\
\hline
\Gamma,\, \Gamma' \overset{\mu}{\Rightarrow} \Delta,\, \Delta' \\
\vdots \\
\Rightarrow R0^{(m_1)}, \ldots, R0^{(m_n)}
\end{array}$$

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 5.9 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:

$$\frac{\dfrac{Rs \Rightarrow Rs}{s = t,\, Rs \Rightarrow Rs}}{s = t,\, Rs \Rightarrow Rt} \qquad \frac{s = t \Rightarrow}{s = t,\, Rs \Rightarrow Rt}$$

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 $R0^{(m_i)}$. No perdemos generalidad si suponemos que se trata de $R0^{(m_n)}$. La situación es:

$$\begin{array}{c} \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta \\ \hline \Gamma \overset{\mu}{\Rightarrow} \Delta,\, Rt \\ \vdots \\ \overset{\nu}{\Rightarrow} R0^{(m_1)}, \ldots, R0^{(m_n)}. \end{array}$$

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'

$$\begin{array}{c} \vdots \\ \Gamma \overset{\mu}{\Rightarrow} \Delta \\ \vdots \\ \overset{\nu}{\Rightarrow} R0^{(m_1)}, \ldots, R0^{(m_{n-1})},\ (R0^{(m_n)}) \end{array}$$

en cuyo secuente final no estará $R0^{(m_n)}$ 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 5.12 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 5.12, 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:

[6] La prueba de (5.1) vale igualmente sin más que contemplar un caso adicional para la regla de sustitución, que es análogo al caso de la regla de debilitación.

La demostración D contiene al menos una regla de inferencia lógica o un secuente inicial de tipo IT.

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 $R0^{(m_i)}$.

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 5.12 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 $R0^{(m_1)}$. Éste será descendiente de una sentencia inductiva Rt, de modo que el secuente $\Rightarrow t = 0^{(m_1)}$ 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

$$0^{(m)} \lhd t \equiv \bigvee u(\alpha(0^{(m)}, t, u) \land 0^{(m)} \neq t)$$

es verdadera en el modelo natural de AP, luego existe un k tal que

$$\mathbb{N} \vDash \alpha(0^{(m)}, t, 0^{(k)})$$

y, por [LF 7.46] tenemos que el secuente $\Rightarrow \alpha(0^{(m)}, t, 0^{(k)}) \land 0^{(m)} \neq t$ es demostrable en ARP, luego es un axioma de AP.

Consideremos la demostración siguiente en AP^R:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Rightarrow \alpha(0^{(m)}, t, 0^{(k)}) \land 0^{(m)} \neq t}{\Rightarrow 0^{(m)} \lhd t}}{\neg 0^{(m)} \lhd t \Rightarrow} \qquad R0^{(m)} \Rightarrow R0^{(m)}}{0^{(m)} \lhd t \rightarrow R0^{(m)} \Rightarrow R0^{(m)}}}{\bigwedge v \lhd t Rv \Rightarrow R0^{(m)}}}{\bigwedge v \lhd t Rv \Rightarrow Rt,\ R0^{(m)}}$$

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 $0^{(m)} \lhd t \rightarrow R0^{(m)} \equiv \neg 0^{(m)} \lhd t \lor R0^{(m)}$.

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 $R0^{(m_1)}$. Si intercalamos el paso

$$\frac{\bigwedge v \lhd t\, Rv \overset{6}{\Rightarrow} Rt}{\bigwedge v \lhd t\, Rv \overset{6}{\Rightarrow} Rt,\ R0^{(m)}}$$

y añadimos $R0^{(m)}$ en los consecuentes de todos los secuentes situados por debajo, obtenemos una demostración con el mismo ordinal, pero con secuente final

$$\Rightarrow R0^{(m)},\ R0^{(m_1)}, \ldots, R0^{(m_n)}.$$

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 5.9, 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 6.6 Si D es una demostración IT y k es un número natural tal que $k \lhd n(D)$, llamaremos *reducción* de D a k a la demostración IT obtenida aplicando repetidamente proceso descrito en la prueba teorema anterior hasta que se cumpla $n(D') = k$.

Ahora ya podemos demostrar el teorema 6.4:

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 $D(0^{(k)})$ del secuente $\Rightarrow R0^{(k)}$, que obviamente cumple $n(D(0^{(k)})) = k$.

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 $D(0^{(k)})$ del secuente $\Rightarrow R0^{(k)}$.

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

$$o(D(0^{(k)})) = o(D(x)) \prec o(D(x)) + 1,$$

luego $o(D_k) \prec o(D(x)) + 1$, pues $o(D_k) \preceq o(D(0^{(r)}))$, para cierto r, de donde se sigue inmediatamente que $F(k) \prec \mu$. ■

6.3 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 6.7 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 6.8 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 6.9 *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]

$$h(a_1,\ldots,a_m) = a \quad \text{si y sólo si} \quad \mathbb{N} \vDash \phi(a_1,\ldots,a_m,a)$$

$$g_i(a_1,\ldots,a_n) = a \quad \text{si y sólo si} \quad \mathbb{N} \vDash \psi_i(a_1,\ldots,a_n,a)$$

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

$$\chi(\bar{x},y) \equiv \bigvee y_1 \cdots y_m(\psi_1(\bar{x},y_1) \land \cdots \land \psi_m(\bar{x},y_m) \land \phi(y_1,\ldots,y_m,y)).$$

[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 deducimos del teorema siguiente:

Teorema 6.10 *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 5.24. 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 5.24 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 3.7, 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 5.4 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 5.6, en AP($\varnothing$) se puede demostrar $\Rightarrow \phi(\bar{a},a)$. 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 1.17 podemos suponer que consta únicamente de fórmulas de tipo Σ_k y por 3.10 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 3.7, 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 3.7 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 6.11 *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 [LF 8.31], existe una fórmula $\phi(x_1, \ldots, x_n, x, y)$ de tipo Δ_0 tal que

$$f(a_1, \ldots, a_n) = a \quad \text{si y sólo si} \quad \mathbb{N} \vDash \bigvee u\, \phi(a_1, \ldots, a_n, u, a)$$

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 6.10, 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 6.12 *Las funciones demostrablemente recursivas en* AP *son las funciones recursivas primitivas respecto de algún ordinal.*

6.4 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 sobre sucesiones fundamentales que vamos a necesitar:

Teorema 6.13 *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 6.14 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 6.7 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 6.15 *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 6.16 *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 6.13 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 4.11:

Teorema 6.17 *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 4.12 tenemos que $\beta < \alpha[n]$, luego, por hipótesis de inducción, $h_\beta(n) < h_{\alpha[n]}(n) = h_\alpha(n)$. ■

Teorema 6.18 *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 6.19 *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

$$f(x_1, \ldots, x_n, x+1) = h(x_1, \ldots, x_n, x, f(x_1, \ldots, x_n, x))$$

$$< \text{máx}\{h_{\omega^\alpha}(\text{máx}\{x_1, \ldots, x_n, x, f(x_1, \ldots, x_n, x)\}), M\}$$

$$\leq \text{máx}\{h_{\omega^\alpha}(\text{máx}\{x_1, \ldots, x_n, x, h_{\omega^\alpha}^{x+1}(\text{máx}\{x_1, \ldots, x_n, x, M\})\}), M\}$$

$$\leq h_{\omega^\alpha}(h_{\omega^\alpha}^{x+1}(\text{máx}\{x_1, \ldots, x_n, x, M\})) \leq h_{\omega^\alpha}^{x+2}(\text{máx}\{x_1, \ldots, x_n, x+1, M\}).$$

Esto termina el razonamiento inductivo. Si llamamos

$$M' = \text{máx}\{x_1, \ldots, x_{n+1}, M\} + 1,$$

tenemos que

$$f(x_1, \ldots, x_{n+1}) < h_{\omega^\alpha}^{x_{n+1}+1}(M') \leq h_{\omega^\alpha}^{M'}(M') = h_{\omega^{\alpha+1}}(M')$$

$$= h_{\omega^{\alpha+1}}(\text{máx}\{x_1, \ldots, x_{n+1}, M\} + 1) = h_{\omega^{\alpha+1}+1}(\text{máx}\{x_1, \ldots, x_{n+1}, M\})$$

$$= h_{\omega^{\alpha+1}+1}(\text{máx}\{x_1, \ldots, x_{n+1}\})$$

si $\text{máx}\{x_1, \ldots, x_{n+1}\} > M$. ■

Teorema 6.20 *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 6.17 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 6.15 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 6.21 *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 6.12 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 6.22 *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 6.23 *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 $\mathrm{I}\Sigma_{n-1}$ 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 5.24, y en caso contrario, $r(D) = D$. Teniendo en cuenta la nota tras el teorema 6.11 así como el teorema 6.19, 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 6.17, pues, por el teorema 6.22 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 6.22, tenemos que $c(\omega^{(n)}\cdot|x|) = (n+1)c(O(x)) < (n+1)x < u(x)$, luego 6.17 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 6.24 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 6.25 *Las funciones demostrablemente recursivas en* AP *son las funciones de la clase de Hardy.*

DEMOSTRACIÓN: Por la nota tras el teorema 6.11, 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 6.23, 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

$$\phi(x,y) \equiv \bigwedge i < y\, q(x,i) \neq q(x,i+1) \land q(x,y) = q(x,y+1).$$

Por el teorema 6.23 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 6.17 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 6.21 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 6.26 $\tilde{h}_\alpha(n) = \tilde{h}_{L_\alpha(n)}(n) = n + L_\alpha(n)$.

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 6.27 (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. ■

6.5 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 [LF 2.13] 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 6.28 (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 6.29 *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 6.30 $G_k(\omega^\alpha) = (k+2)^{G_k(\alpha)}$.

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 6.31 $G_k(P_k(\alpha)) = P_k(G_k(\alpha))$.

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 6.32 $n + 3 + \mu k\,(Q_{n,k}(\alpha) = 0) = h_\alpha(n + 3)$.

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 6.33 (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 $h_{\omega^{(n)}}(n) > n$. ■

Apéndice A

La teoría de conjuntos 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 [LF sección 5.5]:

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:

$$\bigwedge u\, u = u, \qquad \bigwedge W \bigwedge uv(u = v \land W(u) \to W(v)),$$

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:[1]

$$\bigwedge U(\mathrm{Un}\, U \to \bigwedge a \bigvee b \bigwedge v(v \in b \leftrightarrow \bigvee uw(u \in a \land w = (u, v) \land U(w)))),$$

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 A.1 *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 2.23, cambiando el axioma de inducción por el de reemplazo.

■

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

[1]Si admitiéramos variables de segundo orden de rango 2 el axioma de reemplazo admitiría un enunciado más simple:

$$\bigwedge U(\bigwedge uv_1v_2(U(u, v_1) \land U(u, v_2) \to v_1 = v_2) \to \bigwedge a \bigvee b \bigwedge v(v \in b \leftrightarrow \bigvee u \in a\, U(u, v))).$$

resulta de añadir a ZF^* los axiomas de infinitud, partes, regularidad y elección [LF sección 5.5], y se corresponde con la teoría NB que resulta de añadir a NB^* estos 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 $\gamma \to \delta$ 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 2.6.

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 ACA_0 establece entre conjuntos y números naturales.

Para precisar esta idea extendemos la relación de pertenencia a clases arbitrarias mediante la definición:

$$X \in Y \equiv \bigvee v(Y(v) \land \bigwedge u(X(u) \leftrightarrow u \in v)).$$

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 A.2 *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:

$$\operatorname{cto} X \equiv \bigvee U v(U(v) \wedge \bigwedge u(X(u) \leftrightarrow u \in v)).$$

Se trata de probar que $U(v)$ es redundante. Para ello razonamos como sigue:

$$\cfrac{\cfrac{\cfrac{\Rightarrow y = y}{\Rightarrow y = y,\, Y(y)} \qquad Y(y) \Rightarrow Y(y)}{y = y \to Y(y) \Rightarrow Y(y)}}{Y(y) \leftrightarrow Y(y) \Rightarrow Y(y)}$$

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

$$\bigwedge u(X(u) \leftrightarrow u \in y),\, (Y(y) \leftrightarrow y = y) \Rightarrow Y(y) \wedge \bigwedge u(X(u) \leftrightarrow u \in y)$$

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

$$\cfrac{\bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \Rightarrow \operatorname{cto} X}{\Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \to \operatorname{cto} X}$$

La implicación contraria es más sencilla:

$$\begin{array}{c}
\bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigwedge u(X(u) \leftrightarrow u \in y) \\ \hline
y \in Y, \bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigwedge u(X(u) \leftrightarrow u \in y) \\ \hline
y \in Y \wedge \bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigwedge u(X(u) \leftrightarrow u \in y) \\ \hline
y \in Y \wedge \bigwedge u(X(u) \leftrightarrow u \in y) \Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \\ \hline
\bigvee v(v \in Y \wedge \bigwedge u(X(u) \leftrightarrow u \in v)) \Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \\ \hline
\operatorname{cto} X \Rightarrow \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v) \\ \hline
\Rightarrow \operatorname{cto} X \to \bigvee v \bigwedge u(X(u) \leftrightarrow u \in v)
\end{array}$$

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 $\mathcal{L}_{\mathrm{tc}}$ 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 $\mathcal{L}_{\mathrm{tc}}$, a cada fórmula α del primero le asociamos la fórmula $\tilde{\alpha}$ de $\mathcal{L}_{\mathrm{tc}}$ 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. $\widetilde{\bigvee u\,\alpha(u)} \equiv \bigvee U(\operatorname{cto} U \wedge \tilde{\alpha}(U)) \equiv \bigvee u\,\tilde{\alpha}(u)$,

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 A.3 *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 $\mathcal{L}_{\mathrm{tc}}$, 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:

$$\dfrac{\dfrac{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \tilde{\alpha}(Y)}{\Theta_{S_2},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \mathrm{cto}\,Y \to \tilde{\alpha}(Y)}}{\Theta_{S_2},\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \bigwedge u\, \tilde{\alpha}(u)}$$

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:

$$\dfrac{\dfrac{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\alpha}(Y),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}{\Theta_{S_2},\ \mathrm{cto}\,Y \land \tilde{\alpha}(Y),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}}{\Theta_{S_2},\ \bigvee u\, \tilde{\alpha}(u),\ \tilde{\Gamma} \Rightarrow \tilde{\Delta}}$$

donde la variable Y sirve como variable propia por la misma razón que en el caso anterior.

Particularizador derecha Ahora tenemos:

$$\dfrac{\dfrac{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \tilde{\alpha}(Y) \qquad \mathrm{cto}\,Y \Rightarrow \mathrm{cto}\,Y}{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \mathrm{cto}\,Y \land \tilde{\alpha}(Y)}}{\Theta_{S_2},\ \mathrm{cto}\,Y,\ \tilde{\Gamma} \Rightarrow \tilde{\Delta},\ \bigvee u\, \tilde{\alpha}(u)}$$

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

$$X = Y \equiv \bigwedge u(X(u) \leftrightarrow Y(u)), \qquad X \in Y \equiv \bigvee v(Y(v) \land \bigwedge u(X(u) \leftrightarrow u \in v)).$$

Teorema A.4 *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 A.3 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

$$\bar{\alpha} \equiv \bigvee u(u \in Y \wedge \bigwedge v(X(v) \leftrightarrow v \in u)), \quad \tilde{\bar{\alpha}} \equiv \bigvee u(u \in Y \wedge \bigwedge v(v \in X \leftrightarrow v \in u)),$$

y, de nuevo por el axioma de extensionalidad, $\tilde{\bar{\alpha}}$ 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 A.5 *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 A.3. 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 $\alpha \leftrightarrow \bar{\bar{\alpha}}$.

Si $\alpha \equiv x_1 \in x_2$, entonces

$$\tilde{\alpha} \equiv X_1 \in X_2, \qquad \bar{\tilde{\alpha}} \equiv \bigvee v (X_2(v) \land \bigwedge u (X_1(u) \leftrightarrow u \in v)).$$

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 $\alpha \equiv \neg\beta$, $\alpha \equiv \beta \lor \gamma$, $\alpha \equiv \bigwedge U \beta(U)$ 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

$$\tilde{\alpha} \equiv \bigwedge U (\mathrm{cto}\, U \to \tilde{\beta}(U)), \qquad \bar{\tilde{\alpha}} \equiv \bigwedge U (\mathrm{cto}\, U \to \bar{\tilde{\beta}}(U)).$$

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 A.2 podemos razonar como sigue:

$$\dfrac{\dfrac{\dfrac{I(x_{n+1}, X_{n+1}) \Rightarrow \mathrm{cto}\, X_{n+1}}{I(x_{n+1}, X_{n+1}) \Rightarrow \mathrm{cto}\, X_{n+1},\ \beta(x_{n+1})} \quad \Gamma,\ I(x_{n+1}, X_{n+1}),\ \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \beta(x_{n+1})}{\Gamma,\ I(x_{n+1}, X_{n+1}),\ \mathrm{cto}\, X_{n+1} \to \bar{\tilde{\beta}}(X_{n+1}) \Rightarrow \beta(x_{n+1})}}{\Gamma,\ I(x_{n+1}, X_{n+1}),\ \bigwedge U (\mathrm{cto}\, U \to \bar{\tilde{\beta}}(U)) \Rightarrow \beta(x_{n+1})}$$

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

$$\Gamma,\ \bigwedge U (\mathrm{cto}\, U \to \bar{\tilde{\beta}}(U)) \Rightarrow \bigwedge u\, \beta(u),$$

y a su vez

$$\Gamma \Rightarrow \bigwedge U (\mathrm{cto}\, U \to \bar{\tilde{\beta}}(U)) \to \bigwedge u\, \beta(u).$$

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 A.2) 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

$$\begin{array}{c}
\Gamma,\ \bigwedge u\, \beta(u),\ \mathrm{cto}\, X_{n+1} \Rightarrow \bar{\bar{\tilde{\beta}}}(X_{n+1}) \\ \hline
\Gamma,\ \bigwedge u\, \beta(u) \Rightarrow \mathrm{cto}\, X_{n+1} \rightarrow \bar{\bar{\tilde{\beta}}}(X_{n+1}) \\ \hline
\Gamma,\ \bigwedge u\, \beta(u) \Rightarrow \bigwedge U (\mathrm{cto}\, U \rightarrow \bar{\bar{\tilde{\beta}}}(U)) \\ \hline
\Gamma \Rightarrow \bigwedge u\, \beta(u) \rightarrow \bigwedge U (\mathrm{cto}\, U \rightarrow \bar{\bar{\tilde{\beta}}}(U))
\end{array}$$

Combinando las dos implicaciones con la regla del conjuntor concluimos:

$$\Gamma \Rightarrow \bigwedge u\, \beta(u) \leftrightarrow \bigwedge U (\mathrm{cto}\, U \rightarrow \bar{\bar{\tilde{\beta}}}(U)).$$

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

$$\begin{array}{c}
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \bar{\bar{\tilde{\beta}}}(X_{n+1}) \Rightarrow \beta(x_{n+1}) \\ \hline
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \bar{\bar{\tilde{\beta}}}(X_{n+1}) \Rightarrow \bigvee u\, \beta(u) \\ \hline
\Gamma,\ \bigvee v \bigwedge u (X_{n+1}(u) \leftrightarrow u \in v),\ \bar{\bar{\tilde{\beta}}}(X_{n+1}) \Rightarrow \bigvee u\, \beta(u)
\end{array}$$

El teorema A.2 y la regla de corte nos permiten pasar a:

$$\begin{array}{c}
\Gamma,\ \mathrm{cto}\, X_{n+1},\ \bar{\bar{\tilde{\beta}}}(X_{n+1}) \Rightarrow \bigvee u\, \beta(u) \\ \hline
\Gamma,\ \mathrm{cto}\, X_{n+1} \wedge \bar{\bar{\tilde{\beta}}}(X_{n+1}) \Rightarrow \bigvee u\, \beta(u) \\ \hline
\Gamma,\ \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U)) \Rightarrow \bigvee u\, \beta(u) \\ \hline
\Gamma \Rightarrow \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U)) \rightarrow \bigvee u\, \beta(u)
\end{array}$$

Para la implicación opuesta partimos de

$$\Gamma,\ I(x_{n+1}, X_{n+1}),\ \beta(x_{n+1}) \Rightarrow \bar{\bar{\tilde{\beta}}}(X_{n+1}),$$

que, junto con $I(x_{n+1}, X_{n+1}) \Rightarrow \mathrm{cto}\, X_{n+1}$, nos da

$$\begin{array}{c}
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \beta(x_{n+1}) \Rightarrow \mathrm{cto}\, X_{n+1} \wedge \bar{\bar{\tilde{\beta}}}(X_{n+1}) \\ \hline
\Gamma,\ I(x_{n+1}, X_{n+1}),\ \beta(x_{n+1}) \Rightarrow \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U)) \\ \hline
\Gamma,\ \bigvee U \bigwedge u (U(u) \leftrightarrow u \in x_{n+1}),\ \beta(x_{n+1}) \Rightarrow \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U)) \\ \hline
\Gamma,\ \bigwedge v \bigvee U \bigwedge u (U(u) \leftrightarrow u \in v),\ \beta(x_{n+1}) \Rightarrow \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U))
\end{array}$$

La segunda fórmula del antecedente es un axioma de compresión, luego podemos cortarlo y pasar a:

$$\begin{array}{c}
\Gamma,\ \beta(x_{n+1}) \Rightarrow \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U)) \\ \hline
\Gamma,\ \bigvee u\, \beta(u) \Rightarrow \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U)) \\ \hline
\Gamma \Rightarrow \bigvee u\, \beta(u) \rightarrow \bigvee U (\mathrm{cto}\, U \wedge \bar{\bar{\tilde{\beta}}}(U))
\end{array}$$

Combinando las dos implicaciones con la regla del conjuntor obtenemos la coimplicación. ■

En particular:

Teorema A.6 *Una sentencia* α *de* $\mathcal{L}_{\rm tc}$ *es un teorema de* ZF* *si y sólo si* $\tilde{\alpha}$ *es un teorema de* NBG*.

Demostración: Por A.1 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 A.1, 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 $\mathcal{L}_{\rm tc}$ 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 A.3 y A.4 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 A.5 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). ■

Índice de Materias