Notas sobre el teorema de Goodstein*

Josep Maria Blasco

Espacio Psicoanalítico de Barcelona
Balmes, 32, 2º 1ª – 08007 Barcelona
jose.maria.blasco@epbcn.com
+34 93 454 89 78

25 de mayo de 2005

Índice general

*URL de este documento: `https://www.epbcn.com/pdf/jose-maria-blasco/2005-05-25-Notas-sobre-el-Teorema-de-Goodstein.pdf`. Estas notas informales sobre el teorema de Goodstein se distribuyeron en sus varias versiones y como texto de apoyo en el transcurso de la presentación realizada por el autor durante tres sesiones del Seminario de Teoría de Conjuntos organizado por el grupo de investigación en Teoría de Conjuntos del Departamento de Lógica, Historia y Filosofía de la Ciencia de la Universidad de Barcelona. Las diversas sesiones se realizaron durante los meses de Abril y Mayo de 2005. Ésta es la versión "final" de las notas, que no aspiran a ser completas ni exhaustivas, y probablemente contienen algunos errores.

1 Introducción

La sentencia verdadera pero demostrablemente indemostrable construida en la prueba del primer teorema de incompletitud de Gödel es muy compleja y artificial. ¿Existen sentencias aritméticas "normales", es decir, no construidas *ex profeso*, tales que ni la sentencia ni su negación sean demostrables en aritmética de Peano? De no ser así, podría muy bien ser que el teorema de Gödel, con ser verdadero, sólo se aplicase a sentencias "raras", y, por tanto, no afectase en absoluto a las matemáticas "normales".

Esta esperanza demostró no tener fundamento: en 1977, Jeff Paris y Leo Harrington publicaron un artículo [5] en el que demostraban que una variación del teorema de Ramsey finito era verdadero pero indemostrable en aritmética de Peano (la demostración es trivial acudiendo a la versión infinita de dicho teorema); aunque se trata de un problema de naturaleza combinatoria bastante abstracto, claramente no es una sentencia artificial, sino una sentencia matemática "normal". Ello despertó el interés de numerosos investigadores, y dio origen a una serie de artículos con nuevos descubrimientos matemáticos, cada vez más asequibles (es decir, más "normales"), que son también indemostrables en aritmética de Peano.

En este texto nos ocupamos del más conocido de todos ellos: el teorema de Goodstein, y la demostración de que dicho teorema no es demostrable en aritmética de Peano. En el resto de esta introducción vamos a presentar de modo informal el teorema de Goodstein.

La sección 2 estará dedicada a recordar hechos básicos sobre los números ordinales, y a presentar las *secuencias fundamentales*, un instrumento técnico que usaremos constantemente durante todo el texto.

En la sección 3 damos la demostración de Cichon [1], reconstruyendo las demostraciones, que en [1] sólo están indicadas, y añadiendo los lemas necesarios para hacer del resumen, en la medida de lo posible, un texto auto-contenido; no demostramos los teoremas 3.28 y 3.39, para los cuáles remitimos al lector a las referencias [7] y [8].

1.1 Secuencias débiles de Goodstein

Definición 1.1. *Dados dos números naturales $m > 0$ y $n > 1$, denotamos por $m_{(n}$ la* ***expresión del número** m **en base** n, es decir,*

$$m_{(n} = \sum_{1 \le i \le k} a_i \cdot n^{e_i} = a_1 \cdot n^{e_1} + ... + a_k \cdot n^{e_k},$$

donde $k > 0$, $e_1 > ... > e_k \ge 0$, $n > a_1, ..., a_{k-1} > 0$.

Ejemplos:

(1) $21_{(2} = 2^4 + 2^2 + 1$.
(2) $261_{(2} = 2^8 + 2^2 + 1$.

Definición 1.2. *Dados dos números naturales $m > 0$ y $n \ge 2$, la* ***expresión del número** m **en pura base** n se define como sigue: consideremos la expresión de m en base n:*

$$m_{(n} = \sum_{1 \le i \le k} a_i \cdot n^{e_i} = a_1 \cdot n^{e_1} + ... + a_k \cdot n^{e_k},$$

con las condiciones de la definición 1.1. Entonces la expresión de m en pura base n es:

$$\begin{cases} m_{[n} = m & \textit{si } m < n, \textit{ y} \\ m_{[n} = \sum_{1 \le i \le k} a_i \cdot n^{e_{i[n}} & \textit{en otro caso.} \end{cases}$$

Es decir: expresamos el número m en base n, cuidando después de expresar a su vez los exponentes, los exponentes de los exponentes, etc., también en base n, hasta que la representación se estabilice.

Ejemplos:

(1) $21_{[2} = 2^{4_{[2}} + 2^{2_{[2}} + 1 = 2^{2^2} + 2^2 + 1.$
(2) $261_{[2} = 2^{8_{[2}} + 2^{2_{[2}} + 1 = 2^{2^{3_{[2}}} + 2^2 + 1 = 2^{2^{2+1}} + 2^2 + 1.$

Definición 1.3 (Goodstein 1944 [2])**.** *Sea $m > 0$, $n \geq 2$, y $x \geq n$ o $x = \omega$. Definimos el* ***resultado de substituir en la expresión de** m **en (pura) base** n **la base** n **por** x, operaciones que denotamos por $m^x_{(n}$ y $m^x_{[n}$ respectivamente, del siguiente modo: calculamos el mayor exponente e de n tal que n^e no supera a m,*

$$e = \max\{k : n^k \leq m\}$$

y, una vez calculado e, calculamos el mayor coeficiente a tal que $a \cdot n^e$ no supere a m,

$$a = \max\{k : k \cdot n^e \leq m\};$$

una vez definidos e y a, definimos

$$m^x_{[n} := \begin{cases} m & \textit{si } m < n, \\ a \cdot x^{e^x_{[n}} + (m - a \cdot n^e)^x_{[n} & \textit{en otro caso,} \end{cases}$$

y

$$m^x_{(n} := \begin{cases} m & \textit{si } m < n, \\ a \cdot x^{e} + (m - a \cdot n^e)^x_{(n} & \textit{en otro caso.} \end{cases}$$

Ejemplos:
(1) $21^3_{[2} = 3^{4^3_{[2}} + 5^3_{[2} = 3^{3^3} + 3^3 + 1.$
(2) $21^\omega_{(2} = \omega^4 + 5^\omega_{(2} = \omega^4 + \omega^2 + 1.$

Observación 1.4. *Es claro que $m^n_{(n} = m^n_{[n} = m$ para cualesquiera $m \geq 0$, $n \geq 2$.*

Definición 1.5. *Para cada $k \geq 2$, definimos dos funciones $o_k : \omega \to \omega^\omega$ y $O_k : \omega \to \epsilon_0$ del siguiente modo:*

$$o_k(n) := n^\omega_{(k},$$

y

$$O_k(n) := n^\omega_{[k}.$$

Observación 1.6. *Es una consecuencia inmediata de la definición de $O_n(m)$ y $o_n(m)$ que si*

$$m_{(n} = \sum_{1 \leq i \leq n} a_i \cdot n^{e_i},$$

con $n > a_1, ..., a_n > 0$ *y* $e_1 > ... > e_n \geq 0$, *entonces*

$$o_n(m) = \sum_{1 \leq i \leq n} a_i \cdot \omega^{e_i}$$

y

$$O_n(m) = \sum_{1 \leq i \leq n} a_i \cdot \omega^{O_n(e_i)}.$$

Definición 1.7. ***Secuencias débiles de Goodstein.*** *Sea* m *un número natural; hagamos*

$$m_0 = m,$$

y construyamos m_1 *del siguiente modo: substituimos la base* 2 *por* 3 *en la expresión en base* 2 *de* m_0, *y restamos* 1 *al resultado, es decir, en nuestra notación, hacemos*

$$m_1 = (m_0)^3_{(2} - 1.$$

Los siguientes elementos m_i *de la serie se construyen aplicando el mismo procedimiento: en general,*

$$m_{i+1} = (m_i)^{i+3}_{(i+2} - 1.$$

La serie de números así obtenida se denomina la ***secuencia débil de Goodstein comenzando por*** m.

La definición se generaliza sin dificultad al caso en que comenzamos por una base $n \geq 2$ *cualquiera; en ese caso, la ecuación pasa a ser*

$$m_{i+1} = (m_i)^{i+n+1}_{(i+n} - 1.$$

Ejemplo: Tomemos $m = 21$:

$m_0 = m_{(2} = 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^0 = 21$
$m_1 = 1 \cdot 3^4 + 1 \cdot 3^2 + 1 \cdot 2^0 - 1 = 1 \cdot 3^4 + 1 \cdot 3^2 = 90$
$m_2 = 1 \cdot 4^4 + 1 \cdot 4^2 - 1 = 1 \cdot 4^4 + 3 \cdot 4^1 + 3 \cdot 4^0 = 256 + 12 + 3 = 271$
$m_3 = 1 \cdot 5^4 + 3 \cdot 5^1 + 3 \cdot 5^0 - 1 = 1 \cdot 5^4 + 3 \cdot 5^1 + 2 \cdot 5^0 = 625 + 15 + 2 = 642$
$m_4 = 1 \cdot 6^4 + 3 \cdot 6^1 + 2 \cdot 6^0 - 1 = 1 \cdot 6^4 + 3 \cdot 6^1 + 1 \cdot 6^0 = 1296 + 18 + 1 = 1315$
...

Es fácil ver que la secuencia m_i crece rápidamente, tanto más rápidamente cuanto mayor es m. Por eso puede resultar sorprendente el siguiente

Teorema 1.8 (Beckmann y McAloon, para secuencias débiles)**.** *Sea* m_i *la secuencia débil de Goodstein comenzando por* m *en base* n*; entonces,*

(a) Para cada número natural $m > 0$ *y cada base* $n \geq 2$, *hay un* k *tal que* $m_k = 0$.

(b) Este hecho no es demostrable en aritmética primitiva recursiva.

Para poder demostrar (a) necesitaremos un lema y algunas observaciones; la demostración de (b) deberá esperar al teorema 3.38.

Lema 1.9. *Para cada* $m > 0$, $n \geq 2$, $k \geq n$,

(a) $m^{\omega}_{(n} = (m^k_{(n})^{\omega}_{(k}$, *y*

(b) $m^\omega_{[n} = (m^k_{[n})^\omega_{[k}$,

es decir,

(a) $o_n(m) = o_k(m^k_{(n})$, *y*
(b) $O_n(m) = O_k(m^k_{[n})$.

Prueba. Demostramos (a); la demostración de (b) es similar.

Usamos inducción en la forma de $m_{(n}$: si $m < n$, claramente $o_n(m) = m$, $m^k_{(n} = m$, y $o_k(m) = m$; si $m \geq n$, sean a y e como en la definición 1.3; entonces

$$o_n(m) = m^\omega_{(n} = a \cdot \omega^e + (m - a \cdot n^e)^\omega_{(n};$$

por otra parte,

$$m^k_{(n} = a \cdot k^e + (m - a \cdot n^e)^k_{(n},$$

de donde

$$\begin{aligned} o_k(a \cdot k^e + (m - a \cdot n^e)^k_{(n}) &= o_k(a \cdot k^e) + o_k((m - a \cdot n^e)^k_{(n}) \\ &= a \cdot \omega^e + o_k((m - a \cdot n^e)^k_{(n}), \end{aligned}$$

y aplicamos la hipótesis inductiva. □

Observación 1.10. *Sean* $m_1 > m_2 > 0$, *y* $k \geq 2$; *entonces es inmediato a partir de las definiciones de* $o_k(n)$ *y* $O_k(n)$ *que*

(a) $o_k(m_1) > o_k(m_2)$, *y*
(b) $O_k(m_1) > O_k(m_2)$.

Observación 1.11. *Si* $n \geq 2$ *y* $0 < m < n$, *entonces* $o_n(m) = O_n(m) = m$; *y si* $m \geq n$, *entonces* $O_n(m) \geq o_n(m) > m$. *Por tanto,* $O_n(m) \geq o_n(m) \geq m$ *para cualquier* m.

Ahora es sencillo demostrar la parte (a) del teorema 1.8.

Demostración de 1.8 (a). La secuencia m_i se obtiene del siguiente modo:

$$\begin{aligned} &m_0 = m_{(n} \\ &m_1 = (m_1)^{n+1}_{(n} - 1 \\ &m_2 = (m_2)^{n+2}_{(n+1} - 1 \\ &\ldots \end{aligned}$$

Consideremos una secuencia paralela de ordinales o_i obtenidos mediante

$$o_i = o_{n+i}(m_i),$$

es decir,

$$\begin{array}{ll} m_0 = m_{(n} & o_0 = o_n(m_0) = o_n(m) \\ m_1 = (m_0)^{n+1}_{(n} - 1 & o_1 = o_{n+1}(m_1) = o_{n+1}((m_0)^{n+1}_{(n} - 1) \\ m_2 = (m_1)^{n+2}_{(n+1} - 1 & o_2 = o_{n+2}(m_2) = o_{n+2}((m_1)^{n+2}_{(n+1} - 1) \\ \ldots & \end{array}$$

es decir, para cada $k > 0$,

$$o_{k+1} = o_{n+k+1}(m_{k+1}) = o_{n+k+1}((m_k)_{(n+k}^{n+k+1} - 1),$$

por la observación 1.10,

$$o_{n+k+1}((m_k)_{(n+k}^{n+k+1} - 1) < o_{n+k+1}((m_k)_{(n+k}^{n+k+1}),$$

y por el lema 1.9,

$$o_{n+k+1}((m_k)_{(n+k}^{n+k+1}) = o_{n+k}(m_k) = o_k,$$

es decir, $o_{k+1} < o_k$ para cada k, de modo que los ordinales o_i forman una secuencia estrictamente decreciente

$$o_0 > o_1 > o_2 > ... > o_k > ...;$$

como no hay secuencias estrictamente decrecientes infinitas de ordinales, forzosamente hay algún i tal que $o_i = 0$. Pero si ahora aplicamos la observación 1.11, para cada $k > 0$ es $o_k \geq m_k$, y por tanto también $m_i = 0$. $\square$

Ejemplo: Tomemos $m = 21$; entonces,

$$\begin{array}{ll}
m_0 = 1 \cdot 2^4 + 1 \cdot 2^2 + 1 \cdot 2^0 & o_0 = 1 \cdot \omega^4 + 1 \cdot \omega^2 + 1 \cdot \omega^0 \\
m_1 = 1 \cdot 3^4 + 1 \cdot 3^2 & o_1 = 1 \cdot \omega^4 + 1 \cdot \omega^2 \\
m_2 = 1 \cdot 4^4 + 3 \cdot 4^1 + 3 \cdot 4^0 & o_2 = 1 \cdot \omega^4 + 3 \cdot \omega^1 + 3 \cdot \omega^0 \\
m_3 = 1 \cdot 5^4 + 3 \cdot 5^1 + 2 \cdot 5^0 & o_3 = 1 \cdot \omega^4 + 3 \cdot \omega^1 + 2 \cdot \omega^0 \\
m_4 = 1 \cdot 6^4 + 3 \cdot 6^1 + 1 \cdot 6^0 & o_4 = 1 \cdot \omega^4 + 3 \cdot \omega^1 + 1 \cdot \omega^0 \\
... & ...
\end{array}$$

1.2 Secuencias fuertes de Goodstein

La definición de secuencia débil de Goodstein admite una generalización inmediata:

Definición 1.12. *Sean $m \in \omega$ y $n \geq 2$. La* ***secuencia (fuerte) de Goodstein comenzando por*** *m* ***en base*** *n se define recursivamente del siguiente modo:*

$$m_0 = m,$$

y, para cada $k \geq 0$,

$$m_{k+1} = (m_k)_{[k+n}^{k+n+1} - 1.$$

Ejemplos:

(1) Tomando $m = 7$, $n = 2$, tenemos

$m_0 = 2^2 + 2^1 + 1 = 7$,
$m_1 = 3^3 + 3^1 + 1 - 1 = 27 + 3 = 30$,
$m_2 = 4^4 + 4 - 1 = 4^4 + 3 = 256 + 3 = 259$,
$m_3 = 5^5 + 3 - 1 = 3125 + 2 = 3127$,
...

(2) Tomando $m = 21 = 2^{2^2} + 2^2 + 1$, $n = 2$, obtenemos:

$m_0 = 2^{2^2} + 2^2 + 1 = 21,$
$m_1 = 3^{3^3} + 3^3 + 1 - 1 = 3^{3^3} + 3^3 = 3^{27} + 27 = 7625597485014 \cong 7,6 \cdot 10^{12},$
$m_2 = 4^{4^4} + 4^4 - 1 = 4^{4^4} + 3 \cdot 4^3 + 3 \cdot 4^2 + 3 \cdot 4 + 3 \cong 1.3 \cdot 10^{154},$
$m_3 = 5^{5^5} + 3 \cdot 5^3 + 3 \cdot 5^2 + 3 \cdot 5 + 2 \cong 10^{2184},$
...

Teorema 1.13 (Goodstein 1944 [2])**.** *Denotemos por m_i la secuencia (fuerte) de Goodstein comenzando por m en base $n \geq 2$; entonces*
(a) Para cada número natural m y cada base n, hay un k tal que $m_k = 0$.
(b) Este hecho no es demostrable en aritmética de Peano.

Demostración de (a). La demostración es idéntica a la del teorema 1.8, sin más que substituir $o_i = o_{n+i}(m)$ por $O_i = O_{n+i}(m)$ y aplicar las variantes correspondientes de los lemas y observaciones utilizados. □

Observación 1.14. *Goodstein [2] demostró que el teorema es válido para cualquier función creciente (no necesariamente de modo estricto) de cambio de bases; es decir, si*

$$f : \omega \to \omega$$

cumple $f(n+1) \geq f(n)$ para cualquier $n \in \omega$, entonces

$$m_1 = (m_0)^{f(n)}_{[n},$$

etc. En el teorema anterior tomamos $f : n \mapsto n+1$.

2 Ordinales y secuencias fundamentales

2.1 Hechos básicos sobre los ordinales

Recordamos, en la mayoría de los casos sin demostración, los hechos básicos sobre los ordinales que usaremos en el resto del texto.

Definición 2.1 (ϵ-números y ϵ_0; Cantor 1897 [**can97**], § 20)**.** *Existen ordinales α denominados **ϵ-números** tales que $\omega^\alpha = \alpha$. El menor entre los ϵ-números se denomina ϵ_0, y es el límite de la secuencia $\langle \omega, \omega^\omega, \omega^{\omega^\omega}, ...\rangle$, es decir,*

$$\epsilon_0 = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}}.$$

Definición 2.2 (Diferencia de dos ordinales; Cantor 1897 [**can97**], § 14 (10))**.** *Dados dos ordinales $\alpha > \beta$, siempre es posible encontrar un ordinal $\gamma \leq \alpha$ tal que $\beta + \gamma = \alpha$; a este ordinal se le llama la **resta** o **diferencia** de α y β, y se denota $\alpha - \beta$.*

Lo que diferencia a los ordinales de los enteros es que la resta de α y β puede ser α aunque $\beta \neq 0$: por ejemplo, $\omega - 7 = \omega$, ya que $7 + \omega = \omega$, y $\omega^\omega - \omega \cdot 2 = \omega^\omega$, ya que $\omega \cdot 2 + \omega^\omega = \omega^\omega$.

Lema 2.3. *Sea $\alpha = \omega^{\alpha_0} \cdot a$, y $\beta = \omega^{\beta_0}$, con $\beta_0 < \alpha_0$. Entonces existe un único ordinal γ tal que $\beta \cdot \gamma = \alpha$. Este ordinal es exactamente $\gamma = \omega^{\alpha_0 - \beta_0} \cdot a$, y por tanto podemos denotar, sin peligro de ambigüedad, $\gamma = \frac{\alpha}{\beta}$.*

Prueba. Claramente $\beta \cdot \gamma = \omega^{\beta_0} \cdot (\omega^{\alpha_0 - \beta_0} \cdot a) = (\omega^{\beta_0} \cdot \omega^{\alpha_0 - \beta_0}) \cdot a = \omega^{\beta_0 + (\alpha_0 - \beta_0)} \cdot a = \omega^{\alpha_0} \cdot a = \alpha$. □

Definición 2.4 (Formal normal de Cantor; Cantor, 1897 [**can97**], § 17)**.** *Todo ordinal α puede ser representado de forma única en **forma normal**:*

$$\alpha = \omega^{\alpha_0} \cdot a_0 + \omega^{\alpha_1} \cdot a_1 + ... + \omega^{\alpha_n} \cdot a_n,$$

donde $\alpha_0 > \alpha_1 > ... > \alpha_n \geq 0$, $\alpha \geq \alpha_0$, y $a_i \in \omega \setminus \{0\}$ para $1 \leq i \leq n$.

Lema 2.5. *Si $\alpha < \epsilon_0$ y $\alpha = \omega^{\alpha_0} \cdot a_0 + \omega^{\alpha_1} \cdot a_1 + ... + \omega^{\alpha_n} \cdot a_n$ es su descomposición en forma normal, entonces $\alpha > \alpha_0$.*

Prueba. Ya que ϵ_0 es el menor número β tal que $\omega^\beta = \beta$, si fuese $\alpha = \alpha_0$ tendríamos $\alpha \geq \omega^{\alpha_0} = \omega^\alpha \geq \alpha$, de donde $\alpha = \omega^\alpha$, absurdo. □

Lema 2.6. *Cualquier ordinal límite $\lambda < \epsilon_0$ puede expresarse como $\omega^\delta \cdot (\gamma + 1)$, con $\delta > 0$ y $\gamma \geq 0$.*

Prueba. Pongamos

$$\lambda = \omega^{\alpha_1} \cdot a_1 + ... + \omega^{\alpha_n} \cdot a_n,$$

con $\lambda > \alpha_1 > ... > \alpha_n > 0$ y $0 < a_1, ..., a_n < \omega$. Entonces si $\beta_i = \alpha_i - \alpha_n$, $1 \leq i < n$, se tiene que $\omega^{\alpha_n} \cdot \omega^{\beta_i} = \omega^{\alpha_n + \beta_i} = \omega^{\alpha_i}$, y por tanto

$$\lambda = \omega^{\alpha_n}(\omega^{\beta_1} \cdot a_1 + ... + \omega^{\beta_{n-1}} \cdot a_{n-1} + (a_n - 1) + 1),$$

y basta con tomar $\delta = \alpha_n$ y $\gamma = \omega^{\beta_1} \cdot a_1 + ... + \omega^{\beta_{n-1}} \cdot a_{n-1} + (a_n - 1)$. □

2.2 Secuencias fundamentales

En 1897, Cantor [**can97**] define las **secuencias fundamentales** (o **series fundamentales**) que convergen hacia un ordinal límite α. Así, por ejemplo, ω puede verse como el límite de la secuencia $\langle 0, 1, 2, ... \rangle$, $\omega \cdot 2$ como el límite de $\langle \omega + 0, \omega + 1, \omega + 2, ... \rangle$, ω^ω como el límite de $\langle \omega^0, \omega^1, \omega^2, ... \rangle$, y ϵ_0 como el límite de $\langle \omega, \omega^\omega, \omega^{\omega^\omega}, ... \rangle$.

Cambiando el punto de vista, podemos definir, dado un ordinal límite $\lambda < \epsilon_0$, una función f_λ que, aplicada a cada $n \in \omega$, nos de el término n-ésimo de la secuencia fundamental que converge hacia λ. Así, por ejemplo, $f_\omega(n) = n$, para cada $n \in \omega$, y, similarmente, $f_{\omega \cdot 2}(n) = \omega + n$, $f_{\omega^\omega}(n) = \omega^n$, etc.

Un tercer punto de vista nos permite considerar las secuencias fundamentales que convergen hacia un ordinal límite como herramientas para la diagonalización (esto quedará más claro al definir la jerarquía de Hardy en la sección 3.5; véase también 3.5.1 para una discusión más detallada del concepto de secuencia fundamental para ordinales $\alpha < \omega_1$).

Escribiremos $\{\lambda\}(n)$ en vez de $f_\lambda(n)$ (es la notación empleada en [8] para ordinales límite y en [4] para cualquier ordinal $\alpha < \epsilon_0$), y completaremos la definición para ordinales no límites poniendo $\{0\}(n) = 0$ y $\{\alpha+1\}(n) = \alpha$, para cada $\alpha < \epsilon_0$.

Más formalmente:

Definición 2.7 (Wainer, 1972 [8]; Ketonen-Soloway, 1981 [4]). *Sea $\alpha \leq \epsilon_0$. La* ***secuencia fundamental de*** *α es la función $\{\alpha\} : \omega \to \epsilon_0$ definida por:*

(α0) $\{0\}(n) = 0$;
(α1) $\{\alpha + 1\}(n) = \alpha$;
(α2) $\{\omega^{\delta+1} \cdot (\gamma + 1)\}(n) = \omega^{\delta+1} \cdot \gamma + \omega^{\delta} \cdot n$;
(α3) $\{\omega^{\delta} \cdot (\gamma + 1)\}(n) = \omega^{\delta} \cdot \gamma + \omega^{\{\delta\}(n)}$, *si δ es un ordinal límite.*
(α4) $\{\epsilon_0\}(0) = 1$, *y* $\{\epsilon_0\}(n + 1) = \omega^{\{\epsilon_0\}(n)}$.

Ejemplos:

(1) $\{\omega\}(n) = \{\omega^{0+1} \cdot (0 + 1)\}(n) = \omega^{0+1} \cdot 0 + \omega^{0} \cdot n = n$, aplicando ($\alpha$2).

(2) $\{\omega + 1\}(n) = \omega$, aplicando ($\alpha$1) (y, en general, $\{\omega + m + 1\}(n) = \omega + m$).

(3) $\{\omega \cdot 2\}(n) = \{\omega^{0+1} \cdot (1 + 1)\}(n) = \omega^{0+1} \cdot 1 + \omega^{0} \cdot n = \omega + n$, aplicando ($\alpha$2).

(4) $\{\omega \cdot (m + 1)\}(n) = \{\omega^{0+1} \cdot (m + 1)\}(n) = \omega^{0+1} \cdot m + \omega^{0} \cdot n = \omega \cdot m + n$, aplicando ($\alpha$2).

(5) $\{\omega^2\}(n) = \{\omega^{1+1} \cdot (0 + 1)\}(n) = \omega^{1+1} \cdot 0 + \omega^{1} \cdot n = \omega \cdot n$, aplicando ($\alpha$2).

(6) $\{\omega^{\omega}\}(n) = \{\omega^{\omega} \cdot (0 + 1)\}(n) = \omega^{\omega} \cdot 0 + \omega^{\{\omega\}(n)} = \omega^{n}$, aplicando ($\alpha$3) y (1).

(7) $\{\omega^{\omega^{\omega}}\}(n) = \{\omega^{\omega^{\omega}} \cdot (0 + 1)\}(n) = \omega^{\omega^{\omega}} \cdot 0 + \omega^{\{\omega^{\omega}\}(n)} = \omega^{\omega^{n}}$, aplicando ($\alpha$3) y (6).

Los siguientes lemas están destinados a demostrar que nuestra definición de las secuencias fundamentales coincide con el significado intuitivo que les hemos asignado más arriba.

Lema 2.8. *Si $\alpha > 0$, entonces $\{\alpha\}(n) < \alpha$.*

Prueba. Por inducción en (α0)$-$(α4). El único paso que requiere alguna atención es (α3). Pero (α3) es $\{\omega^{\delta} \cdot (\gamma + 1)\}(n) = \omega^{\delta} \cdot \gamma + \omega^{\{\delta\}(n)}$, y como por hipótesis inductiva $\{\delta\}(n) < \delta$, entonces $\omega^{\{\delta\}(n)} < \omega^{\delta}$, ya que $\{\delta\}(n) < \delta < \epsilon_0$. □

Observación 2.9. *Nótese que, por otra parte, $0 < \alpha < \beta$ no implica necesariamente que $\{\alpha\}(n) < \{\beta\}(n)$, ya que, por ejemplo, $\{\omega^{\omega}\}(n) = \omega^{n}$ por el ejemplo (6), pero, si $m > n$, $\{\omega^{m+1}\}(n) = \{\omega^{m+1} \cdot (0+1)\}(n) = 0 + \omega^{m} \cdot n > \omega^{n}$, aunque $\omega^{m+1} < \omega^{\omega}$.*

Lema 2.10. *Sean $n \in \omega$ y $\lambda \leq \epsilon_0$ límite. Entonces $\{\lambda\}(n + 1) > \{\lambda\}(n)$.*

Prueba.

Caso $\lambda = \omega$: $\{\omega\}(n + 1) = n + 1 > n = \{\omega\}(n)$.

Caso $\lambda = \omega^{\delta+1} \cdot (\gamma + 1)$:

$$\begin{aligned} \{\omega^{\delta+1} \cdot (\gamma + 1)\}(n + 1) \quad &= \omega^{\delta+1} \cdot \gamma + \omega^{\delta} \cdot (n + 1) \\ &> \omega^{\delta+1} \cdot \gamma + \omega^{\delta} \cdot n \\ &= \{\omega^{\delta+1} \cdot (\gamma + 1)\}(n). \end{aligned}$$

Caso $\lambda = \omega^{\delta} \cdot (\gamma + 1)$: $\{\omega^{\delta} \cdot (\gamma + 1)\}(n + 1) = \omega^{\delta} \cdot \gamma + \omega^{\{\delta\}(n+1)}$, y por hipótesis inductiva $\{\delta\}(n + 1) > \{\delta\}(n)$.

Caso $\lambda = \epsilon_0$: $\{\epsilon_0\}(n + 1) = \omega^{\{\epsilon_0\}(n)} > \{\epsilon_0\}(n)$. □

Lema 2.11. *Sea $\lambda < \epsilon_0$ un ordinal límite. Entonces* $\sup\{\{\lambda\}(n) : n \in \omega\} = \lambda$.

Prueba. Por inducción sobre la forma de λ.

Claramente

$$\sup\{\{\omega\}(0), \{\omega\}(1), ..., \{\omega\}(n), ...\} = \sup\{0, 1, ..., n, ...\} = \omega,$$

e igualmente

$$\sup\{\{\epsilon_0\}(0), \{\epsilon_0\}(1), \{\epsilon_0\}(2), ...\} = \sup\{1, \omega, \omega^\omega, \omega^{\omega^\omega}, ...\} = \epsilon_0;$$

sea ahora $\lambda = \omega^{\delta+1} \cdot (\gamma + 1)$; entonces

$$\begin{aligned}
&\sup\{\{\omega^{\delta+1} \cdot (\gamma + 1)\}(n) : n \in \omega\} = \\
&\sup\{\omega^{\delta+1} \cdot \gamma, \omega^{\delta+1} \cdot \gamma + \omega^\delta, \omega^{\delta+1} \cdot \gamma + \omega^\delta \cdot 2, ...\} = \\
&\omega^{\delta+1} \cdot \gamma + \omega^\delta \cdot \omega = \\
&\omega^{\delta+1} \cdot \gamma + \omega^{\delta+1} = \\
&\omega^{\delta+1} \cdot (\gamma + 1);
\end{aligned}$$

finalmente, si $\lambda = \omega^\delta \cdot (\gamma + 1)$ con δ límite, entonces

$$\begin{aligned}
&\sup\{\{\omega^\delta \cdot (\gamma + 1)\}(n) : n \in \omega\} = \\
&\sup\{\omega^\delta \cdot \gamma + \omega^{\{\delta\}(n)} : n \in \omega\},
\end{aligned}$$

y basta aplicar la hipótesis inductiva a $\delta < \lambda$. □

Corolario 2.12. *Sean $\alpha < \lambda \leq \epsilon_0$, con λ límite. Entonces:*

(a) hay un mínimo $k \in \omega$ tal que $\{\lambda\}(k) > \alpha$, y por tanto
(b) para cada $n \geq k$ es $\{\lambda\}(n) > \alpha$.

Prueba. (a) Usar el lema 2.11 y reducción al absurdo. (b) Aplicar el lema 2.10. □

Definición 2.13. *Sean $\alpha, \beta < \epsilon_0$, y supongamos que $\alpha = \omega^{\alpha_1} \cdot a_1 + ... + \omega^{\alpha_n} \cdot a_n$ y $\beta = \omega^{\beta_1} \cdot b_1 + ... + \omega^{\beta_m} \cdot b_m$ son sus respectivas formas normales de Cantor, con $\alpha_1 > ... > \alpha_n$ y $\beta_1 > ... > \beta_m$. Diremos que α **engrana con** β, y escribiremos $\alpha \gg \beta$, si y sólo si $\alpha_n > \beta_1$.*

Observación 2.14. *Si $\alpha \gg \beta$, entonces α es forzosamente un ordinal límite.*

Lema 2.15. *Sean $\alpha, \beta < \epsilon_0$, y supongamos que $\alpha \gg \beta > 0$. Entonces $\{\alpha + \beta\}(n) = \alpha + \{\beta\}(n)$.*

Prueba. Basta ver que en la definición de $\{\gamma\}(n)$ sólo se altera el término más a la derecha de la expresión de γ en forma normal de Cantor. Procedemos por inducción en β:

Caso $\beta = \gamma + 1$:

$$\begin{aligned}
\{\alpha + (\gamma + 1)\}(n) &= \{(\alpha + \gamma) + 1\}(n) \\
&= \alpha + \gamma \\
&= \alpha + \{\gamma + 1\}(n) \\
&= \alpha + \{\beta\}(n).
\end{aligned}$$

Caso límite:

(a) Si $\beta = \omega^{\delta+1}(\gamma+1)$, entonces $\alpha+\beta = \omega^{\delta+1}(\alpha/\omega^{\delta+1}+\gamma+1)$, y por tanto

$$\begin{aligned}\{\alpha+\beta\}(n) &= \omega^{\delta+1}(\alpha/\omega^{\delta+1}+\gamma)+\omega^{\delta}\cdot n\\ &= \alpha+\omega^{\delta+1}\cdot\gamma+\omega^{\delta}\cdot n\\ &= \alpha+\{\beta\}(n).\end{aligned}$$

(b) Si $\beta = \omega^{\delta}(\gamma+1)$, con δ límite, entonces

$$\begin{aligned}\{\alpha+\beta\}(n) &= \{\omega^{\delta}((\alpha/\omega^{\delta}+\gamma)+1)\}(n)\\ &= \alpha+\omega^{\delta}\cdot\gamma+\omega^{\{\delta\}(n)}\\ &= \alpha+\{\beta\}(n).\end{aligned}$$

□

3 La demostración de Cichon

3.1 Estructura de la demostración

La demostración de Cichon [1] es concisa, elegante y clara: partimos de un natural m; lo escribimos en pura base n, y cambiamos en la expresión de m en pura base n todas las ocurrencias de n por ω para obtener un ordinal $\alpha = O_n(m)$. Construiremos una colección de funciones G_k que cambian ω por k en un ordinal α; es claro que m_1 será $G_3(\alpha)-1$. También construiremos una serie de funciones $P_k(\alpha)$ que, aplicadas a un natural $p+1$, dan p, y aplicadas a un ordinal cualquiera, dan un anterior determinado de ese ordinal. Con esta notación, si $n=2$, $m_1 = P_3(G_3(\alpha))$.

Uno de los teoremas centrales de la demostración de Cichon será que, para cualquier k, $G_kP_k = P_kG_k$, donde la composición de funciones se expresa multiplicativamente. Así, tendremos $m_1 = G_3P_3(\alpha)$; pero ahora es claro que $P_3(\alpha)$ será el siguiente ordinal a considerar: esta vez tendremos que expresarlo en base 4 y restarle uno, esto es, $m_2 = P_4G_4P_3(\alpha)$; pero $P_4G_4P_3(\alpha) = G_4P_4P_3(\alpha)$, etc. A la larga, deberemos obtener una serie $P_kP_{k-1}...P_4P_3(\alpha) = 0$; y veremos que el mínimo k con esta propiedad es exactamente $H_\alpha(3)-1$ (en general, $H_\alpha(n+1)-1$), donde los H_α son miembros de la jerarquía de Hardy, funciones de crecimiento muy rápido.

Esto nos dará finalmente la prueba buscada: las secuencias débiles de Goodstein estan mayorizadas sólo por H_{ω^ω}, que es esencialmente una versión de la función de Ackermann, y que, como es sabido, no es primitiva recursiva; y las secuencias (fuertes) de Goodstein estan mayorizadas sólo por H_{ϵ_0}, pero para cada función $f:\omega\to\omega$ demostrablemente recursiva hay un α tal que H_α mayoriza a f, es decir,

$$PA \vdash \forall x \exists y H_\alpha(x) = y,$$

y un argumento diagonal similar al clásico sobre la función de Ackermann nos permitirá ver que H_{ϵ_0} no puede ser demostrablemente recursiva, esto es,

$$PA \nvdash \forall x \exists y H_{\epsilon_0}(x) = y.$$

Notación. *En esta sección denotaremos la composición de funciones de manera multiplicativa, es decir, si f y g son funciones, expresaremos $fg : x \mapsto f(g(x))$ en vez de $f\circ g$. Igualmente, definiremos f^0 como la identidad para cualquier función f, $f^1 = f$, y $f^{n+1} = ff^n$.*

3.2 Esquema funcional y referencia

Esta es la lista de funciones usadas en la demostración, y los enunciados de los principales teoremas, con sus referencias, para verificación y consulta.

$O_n : \omega \to \epsilon_0$: $O_n(m)$, poner m en pura base n y cambiar n por ω [1.5].
$G_n : \epsilon_0 \to \omega$: $G_n(\alpha)$, substituir ω por n en α [3.1].

$$\left.\begin{array}{l} G_n O_n(m) = m \\ O_n G_n(\alpha) = \alpha \end{array}\right\} [3.7]$$

$P_n : \epsilon_0 \to \epsilon_0$: $P_n(\alpha)$ es $\alpha - 1$, de acuerdo con $\{\alpha\}(n)$ [3.8].

$$G_n P_n = P_n G_n \text{ [3.9]}$$

$H_\alpha : \epsilon_0 \to n$: número de pasos P_i para llegar a $m_k = 0$ [3.13].

$$\mu k(P_k P_{k-1} ... P_{n+1} O_n(m)) = H_{O_n(m)}(n+1) - 1 \text{ [3.15]}$$

$A_n : \omega \to \omega$: la función de Ackermann [3.22].

$$f(n) = A_n(n) \text{ no es primitiva recursiva [3.29].}$$

$HA_n : \omega \to \omega$: la función de Ackermann-Hardy [3.30].

$$HA_n \gg A_{n+1} \text{ [3.35].}$$

3.3 De ordinales a enteros

Definición 3.1 (La jerarquía de crecimiento lento (Slow-growing hierarchy; véase [1])). *Sea $n < \omega$, y $\alpha < \epsilon_0$. Definimos*
$G_n(0) = 0$,
$G_n(\alpha + 1) = G_n(\alpha) + 1$, *y*
$G_n(\alpha) = G_n(\{\alpha\}(n))$ *si α es límite.*

Ejemplos:

(1) $G_n(1) = G_n(0 + 1) = G_n(0) + 1 = 1$, y, como es fácil ver por inducción, $G_n(m) = m$ para cada $m < \omega$.
(2) $G_n(\omega) = G_n(\{\omega\}(n)) = G_n(n) = n$, aplicando el ejemplo (1).
(3) $G_n(\omega + m) = G_n(\omega) + m = n + m$.
(4) $G_n(\omega \cdot 2) = G_n(\{\omega \cdot 2\}(n)) = G_n(\omega + n) = 2n$, y, como puede verse fácilmente por inducción, $G_n(\omega \cdot m) = mn$ para cada $m < \omega$.
(5) $G_n(\omega^2) = G_n(\{\omega^2\}(n)) = G_n(\omega \cdot n) = n^2$, aplicando el ejemplo (4).

Los ejemplos parecen sugerir que el efecto de G_n sobre un ordinal α es el de reemplazar ω por n en la expresión de α en forma normal de Cantor. Demostraremos formalmente esta propiedad de G_n mediante una serie de lemas.

Lema 3.2. *Si $n > 0$ y $\alpha < \epsilon_0$, entonces $G_n(\alpha) = 0$ si y sólo si $\alpha = 0$.*

Prueba. Por definición de G_n, si $\alpha = 0$ entonces $G_n(0) = 0$. Inversamente, si $\alpha > 0$, y por inducción en α:

Caso $\alpha = \beta + 1$*:* $G_n(\beta + 1) = G_n(\beta) + 1 > 0$.

Caso límite: $G_n(\alpha) = G_n(\{\alpha\}(n)) > 0$ aplicando el lema 2.8, y por hipótesis inductiva. □

Lema 3.3 (Cichon, 1983: [1], lema 1.(1))**.** *Si* $\alpha \gg \beta$*, entonces* $G_n(\alpha + \beta) = G_n(\alpha) + G_n(\beta)$.

Prueba. Por inducción en β:

Caso 0*:*

$$\begin{aligned} G_n(\alpha + 0) &= G_n(\alpha) \\ &= G_n(\alpha) + 0 \\ &= G_n(\alpha) + G_n(0). \end{aligned}$$

Caso $\beta + 1$*:*

$$\begin{aligned} G_n(\alpha + (\beta + 1)) &= G_n((\alpha + \beta) + 1) \\ &= G_n(\alpha + \beta) + 1 \\ &= G_n(\alpha) + G_n(\beta) + 1 \\ &= G_n(\alpha) + G_n(\beta + 1). \end{aligned}$$

Caso límite: Sea $\beta = \bigcup_{\gamma<\beta} \gamma$. Como $\alpha \gg \beta$, $\alpha + \beta$ es límite, y por tanto $G_n(\alpha+\beta) = G_n(\{\alpha+\beta\}(n))$. Pero por el lema (2.15) $\{\alpha+\beta\}(n) = \alpha+\{\beta\}(n)$, y por el lema (2.8), $\{\beta\}(n) < \beta$, y por tanto podemos aplicar la hipótesis inductiva para obtener

$$\begin{aligned} G_n(\{\alpha + \beta\}(n)) &= G_n(\alpha + \{\beta\}(n)) \\ &= G_n(\alpha) + G_n(\{\beta\}(n)) \\ &= G_n(\alpha) + G_n(\beta). \end{aligned}$$

□

Lema 3.4. *Sea* $\lambda = \omega^\delta \cdot m < \epsilon_0$*, con* $m \in \omega$*. Entonces* $G_n(\lambda) = G_n(\omega^\delta) \cdot m$*.*

Prueba. Por doble inducción sobre δ y m:

Caso $\delta = 0$*:* $G_n(\lambda) = G_n(m) = m = 1 \cdot m = G_n(1) \cdot m = G_n(\omega^0) \cdot m$.

Caso $\delta = \alpha + 1$*:*

$$G_n(\lambda) = G_n(\omega^{\alpha+1} \cdot m) = G_n(\{\omega^{\alpha+1} \cdot m\}(n)).$$

Si $m = 0$, entonces

$$G_n(\{\omega^{\alpha+1} \cdot m\}(n)) = G_n(\{0\}(n)) = G_n(0) = 0 = G_n(\omega^\delta) \cdot 0.$$

Si $m = p + 1$, entonces

$$\begin{aligned} &G_n(\{\omega^{\alpha+1} \cdot m\}(n)) = \\ &G_n(\{\omega^{\alpha+1} \cdot (p + 1)\}(n)) = \\ &G_n(\omega^{\alpha+1} \cdot p + \omega^\alpha \cdot n), \end{aligned}$$

y como $\omega^{\alpha+1} \cdot p \gg \omega^{\alpha} \cdot n$,

$$\begin{array}{l}
G_n(\omega^{\alpha+1} \cdot p + \omega^{\alpha} \cdot n) = \\
G_n(\omega^{\alpha+1} \cdot p) + G_n(\omega^{\alpha} \cdot n) = \\
G_n(\omega^{\alpha+1}) \cdot p + G_n(\{\omega^{\alpha+1}\}(n)) = \\
G_n(\omega^{\alpha+1}) \cdot p + G_n(\omega^{\alpha+1}) = \\
G_n(\omega^{\alpha+1}) \cdot m.
\end{array}$$

Caso δ límite: Si $m = 0$, trivialmente $G_n(\lambda) = G_n(0) = 0 = G_n(0) \cdot 0 = G_n(\omega^{\delta}) \cdot 0$.

Supongamos ahora que $m = p + 1$; entonces

$$\begin{array}{l}
G_n(\lambda) = \\
G_n(\omega^{\delta} \cdot m) = \\
G_n(\{\omega^{\delta} \cdot m\}(n)) = \\
G_n(\{\omega^{\delta} \cdot (p+1)\}(n)) = \\
G_n(\omega^{\delta} \cdot p + \omega^{\{\delta\}(n)}),
\end{array}$$

y como $\{\delta\}(n) < \delta$, $\omega^{\delta} \cdot p \gg \omega^{\{\delta\}(n)}$, y por tanto

$$\begin{array}{l}
G_n(\omega^{\delta} \cdot p + \omega^{\{\delta\}(n)}) = \\
G_n(\omega^{\delta} \cdot p) + G_n(\omega^{\{\delta\}(n)}) = \\
G_n(\omega^{\delta}) \cdot p + G_n(\{\omega^{\delta}\}(n)) = \\
G_n(\omega^{\delta}) \cdot p + G_n(\omega^{\delta}) = \\
G_n(\omega_{\delta}) \cdot (p+1) = \\
G_n(\omega_{\delta}) \cdot m
\end{array}.$$

□

Lema 3.5 (Cichon, 1983: [1], lema 1.(2))**.** *Sean $0 < \alpha < \epsilon_0$ y $n > 0$. Entonces $G_n(\omega^{\alpha}) = n^{G_n(\alpha)}$.*

Prueba. Por inducción en α:

Caso 0: $G_n(\omega^0) = G_n(1) = 1 = n^0 = n^{G_n(0)}$.

Caso $\alpha = \beta + 1$:

$$\begin{aligned}
G_n(\omega^{\beta+1}) &= G_n(\{\omega^{\beta+1}\}(n)) \\
&= G_n(\omega^{\beta} \cdot n) \\
&= G_n(\omega^{\beta}) \cdot n \\
&= n^{G_n(\beta)} \cdot n \\
&= n^{G_n(\beta)+1} \\
&= n^{G_n(\beta+1)}.
\end{aligned}$$

Caso $\alpha = \bigcup_{\beta<\alpha} \beta$:

$$\begin{aligned}
G_n(\omega^{\alpha}) &= G_n(\{\omega^{\alpha}\}(n)) \\
&= G_n(\omega^{\{\alpha\}(n)}),
\end{aligned}$$

y como $\{\alpha\}(n) < \alpha$,

$$\begin{aligned}
G_n(\omega^{\{\alpha\}(n)}) &= n^{G_n(\{\alpha\}(n))} \\
&= n^{G_n(\alpha)}.
\end{aligned}$$

□

Lema 3.6 (Cichon, 1983: [1], observación 1)**.** *Sea $\alpha < \epsilon_0$. $G_n(\alpha)$ se obtiene tomando la representación de α en forma normal de Cantor, y reemplazando en todas partes ω por n.*

Prueba. Por inducción sobre la forma normal de α: sea

$$\alpha = \omega^{\alpha_1} \cdot a_1 + ... + \omega^{\alpha_n} \cdot a_n, \quad \alpha > \alpha_1 > ... > \alpha_n.$$

Por el lema (3.3), $G_n(\alpha) = G_n(\omega^{\alpha_1} \cdot a_1) + ... + G_n(\omega^{\alpha_n} \cdot a_n)$, por el lema (3.4), $G_n(\alpha) = G_n(\omega^{\alpha_1}) \cdot a_1 + ... + G_n(\omega^{\alpha_n}) \cdot a_n$, y por el lema (3.5), $G_n(\alpha) = n^{G_n(\alpha_1)} \cdot a_1 + ... + n^{G_n(\alpha_n)} \cdot a_n$. □

Teorema 3.7. *Sean $m \geq 0$ y $n \geq 2$; entonces,*

$$G_n O_n(m) = m;$$

inversamente, si $n \geq 2$ y $\alpha < \epsilon_0$, entonces

$$O_n G_n(\alpha) = \alpha$$

Prueba. Aplicar la observación 1.6 y el lema 3.6. □

3.4 Traducción de las secuencias de Goodstein

El teorema 3.7 nos permite pasar de ordinales a naturales, y viceversa. En la construcción de los ordinales O_i en la demostración de los teoremas 1.13 y 1.8, es claro que $m_i = G_{i+2}(O_i)$ y que $O_i = O_{i+2}(m_i)$; por tanto, en un cierto sentido, nos da lo mismo trabajar con la serie m_i que trabajar con la serie O_i y después aplicar el correspondiente G_{i+2}. La siguiente familia de funciones P_n nos dará un correlato para los O_i de la operación de restar 1 a los m_i.

Definición 3.8 (Cichon, 1983 [1])**.** *Sea $\alpha < \epsilon_0$, y $n < \omega$. El n-**anterior** de α se define mediante:*

$P_n(0) = 0,$
$P_n(\alpha + 1) = \alpha,$ *y*
$P_n(\lambda) = P_n(\{\lambda\}(n))$ *para λ límite.*

Ejemplos:
(1) $P_n(m + 1) = m$ para cualesquiera $m, n \in \omega$.
(2) $P_{n+1}(\omega) = P_{n+1}(\{\omega\}(n + 1)) = P_{n+1}(n + 1) = n$.
(3) $P_5(\omega^3) = P_5(\{\omega^3\}(5)) = P_5(\omega^2 \cdot 5) = P_5(\{\omega^2 \cdot 5\}(5)) = P_5(\omega^2 \cdot 4 + \omega \cdot 5) = P_5(\omega^2 \cdot 4 + \omega \cdot 4 + 5) = \omega^2 \cdot 4 + \omega \cdot 4 + 4$.
(4) $P_3(\omega^4) = P_3(\omega^3 \cdot 3) = P_3(\omega^3 \cdot 2 + \omega^2 \cdot 3) = P_3(\omega^3 \cdot 2 + \omega^2 \cdot 2 + \omega \cdot 3) = P_3(\omega^3 \cdot 2 + \omega^2 \cdot 2 + \omega \cdot 2 + 3) = \omega^3 \cdot 2 + \omega^2 \cdot 2 + \omega \cdot 2 + 2$.

Los ejemplos (3) y (4) corroboran lo que decíamos más arriba: P_n se comporta como esperábamos, produciendo el ordinal "anterior" a un ordinal límite dado (una vez comprometidos a una base n). El siguiente teorema muestra que da lo mismo aplicar G_n y restar 1 que aplicar P_n y después G_n.

Teorema 3.9 (Cichon, 1983: [1], lema 2)**.** *Sean $\alpha < \epsilon_0$, y $n < \omega$. Entonces*

$$G_n P_n(\alpha) = P_n G_n(\alpha) \ \ (= G_n(\alpha) \dot{-} 1).$$

Prueba. Por inducción en α:

Caso 0*:*

$$G_nP_n(0) = G_n(0) = 0 = P_n(0) = P_nG_n(0).$$

Caso $\alpha = \beta + 1$*:*

$$G_nP_n(\beta + 1) = G_n(\beta),$$

y por otra parte,

$$P_nG_n(\beta + 1) = P_n(G_n(\beta) + 1) = G_n(\beta).$$

Caso límite:

$$\begin{aligned} G_nP_n(\alpha) &= G_nP_n(\{\alpha\}(n)) \\ &= P_nG_n(\{\alpha\}(n)) \\ &= P_nG_n(\alpha). \end{aligned}$$

□

Llegamos así al punto central de la demostración: sea $m \in \omega$, y consideremos la secuencia de Goodstein asociada a m comenzando en base n. Por definición es $m_0 = m$; hagamos $\alpha = O_n(m)$. Ahora m_1 será $P_{n+1}G_{n+1}(\alpha)$, que por el lema (3.9) será igual a $G_{n+1}P_{n+1}(\alpha)$; m_2 se formará como $P_{n+2}G_{n+2}P_{n+1}(\alpha)$, que por el lema (3.9) será igual a $G_{n+2}P_{n+2}P_{n+1}(\alpha)$; y, en general,

$$m_k = G_{k+n}P_{k+n}P_{k+n-1}...P_{n+1}(\alpha).$$

El teorema de Goodstein afirma que hay un k' tal que $m_{k'} = 0$; pero, en virtud del lema (3.2), esto equivale a decir que hay un k tal que

$$P_kP_{k-1}...P_{n+1}(\alpha) = 0. \tag{1}$$

3.5 La jerarquía de Hardy

3.5.1 Nota histórica, con una disgresión sobre las secuencias fundamentales

En 1904, Hardy [3] construye un conjunto de números reales de cardinalidad $\aleph_1$ del siguiente modo (estamos siguiendo la exposición de Wainer en [8]): asociamos a cada secuencia de números naturales un real de la manera habitual; a continuación, asignamos a cada ordinal numerable un real del siguiente modo: comenzamos con la secuencia identidad, y en cada paso suprimimos el primer elemento; en los ordinales límites, diagonalizamos. Veamos qué se obtiene para los primeros ordinales mediante este método:

0	$0, 1, 2, 3, 4, 5, ...$	$H_0(n) = n$
1	$1, 2, 3, 4, 5, 6, ...$	$H_1(n) = n + 1$
2	$2, 3, 4, 5, 6, 7, ...$	$H_2(n) = n + 2$
...		
m	$m, m + 1, m + 2, ...$	$H_m(n) = n + m$
...		
ω	$0, 2, 4, 6, 8, 10, ...$	$H_\omega(n) = 2n$
$\omega + 1$	$2, 4, 6, 8, 10, 12, ...$	$H_{\omega+1}(n) = 2n + 2$
$\omega + 2$	$4, 6, 8, 10, 12, 14, ...$	$H_{\omega+2}(n) = 2n + 4$
...		
$\omega + m$	$2m, 2m + 2, 2m + 4, ...$	$H_{\omega+m}(n) = 2n + 2m$
...		
$\omega \cdot 2$	$0, 4, 8, 12, 16, ...$	$H_{\omega \cdot 2}(n) = 4n$
...		
$\omega \cdot 3$	$0, 8, 16, 24, 32, 48, ...$	$H_{\omega \cdot 3}(n) = 8n$
...		
ω^2	$0, 2, 8, 24, 64, ...$	$H_{\omega^2}(n) = 2^n n$
...		

Si se examina el método con algún detenimiento se observará que el problema que aparece entonces es el siguiente: ¿cómo diagonalizar, en el caso general?; es decir, ¿cómo definir de un modo único una secuencia fundamental para cada ordinal contable límite λ? Para ordinales $\lambda < \epsilon_0$ las secuencias fundamentales $\{\lambda\}(n)$ definidas en 2.7 pueden ser suficientes; pero suponer que para cada ordinal límite menor que ω_1 hay una secuencia fundamental no es trivial.

Para verlo, examinemos el caso de los ϵ-números, definidos en 2.1: en [**can97**], Cantor demuestra que el segundo ϵ-número, ϵ_1, se forma del siguiente modo: hagamos $\alpha_0 = \epsilon_0 + 1$, y definamos recursivamente $\alpha_{\beta+1} = \omega^{\alpha_\beta}$; entonces, $\epsilon_1 = \bigcup_{\beta<\omega} \alpha_\beta$. Del mismo modo podemos construir ϵ_2 (a partir de $\epsilon_1 + 1$), ϵ_3, ...; ϵ_ω será $\bigcup_{\alpha<\omega} \epsilon_\alpha$; a partir de ϵ_ω, podemos construir $\epsilon_{\omega+1}$, etc. El conjunto $\{\epsilon_\alpha : \alpha < \omega_1\}$ es cerrado y cofinal en ω_1.

¿Cuáles serían las reglas más "naturales" para definir secuencias fundamentales que converjan a ϵ_α, para cualquier $\alpha < \omega$? Parecen claras las siguientes:

(ϵ0) $\{\epsilon_0\}(0) = 1$, y $\{\epsilon_0\}(n + 1) = \omega^{\{\epsilon_0\}(n)}$ (es la regla (α4) de 2.7);
(ϵ1) $\{\epsilon_{\alpha+1}\}(0) = \epsilon_\alpha + 1$, y $\{\epsilon_{\alpha+1}\}(n + 1) = \omega^{\{\epsilon_{\alpha+1}\}(n)}$;
(ϵ2) $\{\epsilon_\lambda\}(n) = \epsilon_{\{\lambda\}(n)}(n)$, para λ límite.

¿Cuál es el problema con estas reglas? Ninguno, *excepto que formularlas requiere un conocimiento detallado de la estructura de los ϵ-números.* Y, ¿cuántos casos "especiales", como los ϵ-números, podemos esperar encontrar? Si se reflexiona, la respuesta es clara: ω_1.

He aquí, por ejemplo, un nuevo tipo de número: como para cada $\alpha < \omega_1$ hay un $\epsilon_\alpha < \omega_1$, en particular existen ϵ_{ϵ_0}, $\epsilon_{\epsilon_{\epsilon_0}}$,..., y, finalmente, el primer punto fijo de la función ϵ, es decir, el primer α tal que $\alpha = \epsilon_\alpha$; es claro que

$$\alpha = \epsilon_{\epsilon_{\epsilon_{\cdot_{\cdot_{\cdot}}}}}.$$

Para estos números hará falta una nueva colección de reglas para determinar las secuencias fundamentales. Podría parecer, entonces, que no hay una manera constructiva de asignar secuencias fundamentales para segmentos iniciales grandes de $[\omega, \omega_1)$; todavía menos, si tenemos en cuenta que las secuencias fundamentales tienen que "comportarse bien" respecto de la diagonalización. Sin embargo, puede demostrarse que, para cada segmento inicial de $[\omega, \omega_1)$, hay un sistema de secuencias fundamentales que "se comporta bien"; pero, a la vez, que esto es imposible si pretendemos tener secuencias fundamentales para la totalidad de $[\omega, \omega_1)$:

Definición 3.10 (Rose 1984 [6])**.** *Sea Δ un segmento inicial de $[\omega, \omega_1)$, y consideremos una asignación A de secuencias fundamentales a los ordinales límites de Δ. Diremos que A tiene la* ***propiedad de Bachmann*** *si y sólo si para cada $\lambda \in \Delta$ y cada $n \in \omega$, si λ y μ son ordinales límites y*

$$\{\lambda\}(n) < \mu < \{\lambda\}(n+1),$$

entonces

$$\{\lambda\}(n) \leq \{\mu\}(0).$$

Teorema 3.11 (Rose 1984 [6])**.** *Hay una asignación de secuencias fundamentales con la propiedad de Bachmann para cada segmento inicial de $[\omega, \omega_1)$.*

Teorema 3.12 (Bachmann 1967, véase Rose 1984 [6])**.** *No existe ninguna asignación de secuencias fundamentales con la propiedad de Bachmann para la totalidad de $[\omega, \omega_1)$.*

Aunque nosotros no saldremos de $[\omega, \epsilon_0)$. Y para lo que nos interesa: las funciones de Hardy H_α, con $\alpha \leq \epsilon_0$, van a medir exactamente el valor de k en la expresión (1).

3.5.2 Definición de la jerarquía

Definición 3.13 (La jerarquía de Hardy; Wainer, 1972 [8])**.** *Para cada $\alpha \leq \epsilon_0$, definimos una función $H_\alpha : \omega \to \omega$ del siguiente modo:*

$H_0(n) = n$;
$H_{\alpha+1}(n) = H_\alpha(n+1)$, *y*
$H_\alpha(n) = H_{\{\alpha\}(n)}(n)$ *si α es límite.*

Ejemplos:

(1) $H_1(n) = H_0(n+1) = n+1$, y en general $H_m(n) = n+m$.
(2) $H_\omega(n) = H_{\{\omega\}(n)}(n) = H_n(n) = 2n$.
(3) $H_{\omega+1}(n) = H_\omega(n+1) = 2(n+1)$, y en general $H_{\omega+m}(n) = 2(n+m)$.
(4) $H_{\omega\cdot 2}(n) = H_{\{\omega\cdot 2\}(n)}(n) = H_{\omega+n}(n) = 2(n+n) = 2^2 n$.
(5) $H_{\omega\cdot 2+m}(n) = H_{\omega\cdot 2}(n+m) = 2^2(n+m)$.
(6) $H_{\omega\cdot 3}(n) = H_{\{\omega\cdot 3\}(n)}(n) = H_{\omega\cdot 2+n}(n) = H_{\omega\cdot 2}(2n) = 2^2 \cdot 2n = 2^3 n$.
(7) En general $H_{\omega\cdot m}(n) = 2^m n$.
(8) $H_{\omega^2}(n) = H_{\{\omega^2\}(n)}(n) = H_{\omega\cdot n}(n) = 2^n n$.
(9) $H_{\omega^2+m}(n) = H_{\omega^2}(n+m) = 2^{n+m}(n+m)$.

Antes de continuar con los ejemplos será útil demostrar el siguiente

Lema 3.14. *Si* $\epsilon_0 > \alpha \gg \beta \geq 0$, *entonces* $H_{\alpha+\beta}(n) = H_\alpha(H_\beta(n))$.

Prueba. Por inducción sobre β:
Caso 0*:* $H_{\alpha+0}(n) = H_\alpha(n) = H_\alpha(H_0(n))$.
Caso $\beta = \gamma + 1$*:*

$$\begin{aligned} H_{\alpha+\beta}(n) &= H_{\alpha+\gamma+1}(n) \\ &= H_{\alpha+\gamma}(n+1) \\ &= H_\alpha(H_\gamma(n+1)) \\ &= H_\alpha(H_{\gamma+1}(n)) \\ &= H_\alpha(H_\beta(n)). \end{aligned}$$

Caso límite: Si β es límite, como $\alpha \gg \beta$, también $\alpha + \beta$ es límite, y, por tanto,

$$H_{\alpha+\beta}(n) = H_{\{\alpha+\beta\}(n)}(n);$$

pero $\{\alpha + \beta\}(n) = \alpha + \{\beta\}(n)$ por el lema (2.15), y como $\{\beta\}(n) < \beta$ podemos aplicar la hipótesis inductiva, de modo que

$$\begin{aligned} H_{\alpha+\beta}(n) &= H_{\alpha+\{\beta\}(n)}(n) \\ &= H_\alpha(H_{\{\beta\}(n)}(n)) \\ &= H_\alpha(H_\beta(n)). \end{aligned}$$

□

Ejemplos (continuación):

(10) $H_{\omega^2+\omega\cdot m}(n) = H_{\omega^2}(H_{\omega\cdot m}(n)) = H_{\omega^2}(2^m n) = 2^{2^m n}2^m n$.
(11) $H_{\omega^2\cdot(m+1)}(n) = H_{\omega^2\cdot m+\omega\cdot n}(n) = H_{\omega^2\cdot m}(H_{\omega\cdot n}(n)) = H_{\omega\cdot m}(2^n n)$.
(12) $H_{\omega^2\cdot 2} = H_{\omega^2}(2^n n) = 2^{2^n n}2^n n = 2^{(2^n+1)n}n$.
(13) $H_{\omega^2\cdot 3} = H_{\omega^2}(2^{(2^n+1)n}n) = 2^{2^{(2^n+1)n}n}2^{(2^n+1)n}n$.

Teorema 3.15. *Sean* $0 < \alpha < \epsilon_0$ *y* $n > 0$. *Entonces*

$$\mu k[P_k P_{k-1} ... P_{n+1}(\alpha) = 0] = H_\alpha(n+1) - 1.$$

Prueba. Por inducción sobre α:
Caso 1*:* Si $\alpha = 1$, entonces $P_{n+1}(\alpha) = 0$ para cualquier n, y por tanto $k = n + 1$; por otra parte, $H_1(n+1) = n + 2$, y $H_1(n+1) - 1 = n + 1$.
Caso $\alpha = \beta + 1$*:* Supongamos que

$$P_k P_{k-1} ... P_{n+1}(\beta) = 0 \text{ y } H_\beta(n+1) - 1 = k.$$

Entonces

$$P_{n+1}(\beta + 1) = \beta,$$

hay un mínimo k' tal que

$$P_{k'} P_{k'-1} ... P_{n+2}(\beta) = 0 \text{ y } H_\beta(n+2) - 1 = k',$$

pero

$$H_\beta(n+2) = H_{\beta+1}(n+1) = H_\alpha(n+1),$$

y por tanto

$$
\begin{aligned}
&P_{k'}P_{k'-1}...P_{n+2}(\beta) = \\
&P_{k'}P_{k'-1}...P_{n+2}P_{n+1}(\beta+1) = \\
&P_{k'}P_{k'-1}...P_{n+2}P_{n+1}(\alpha) = 0
\end{aligned}
$$

y

$$H_\alpha(n+1) - 1 = k'.$$

Caso α límite: $P_kP_{k-1}...P_{n+1}(\alpha) = P_kP_{k-1}...P_{n+1}(\{\alpha\}(n+1)) = 0$, y por tanto $H_{\{\alpha\}(n+1)}(n+1) - 1 = k$, es decir, $H_\alpha(n+1) - 1 = k$. □

Por tanto, la jerarquía de Hardy nos servirá para medir exactamente cuántas iteraciones son necesarias para llegar a 0 en una secuencia de Goodstein.

Ejemplos:

(1) Caso $m = 4$, empezando en base 2, secuencia débil:

$$
\begin{aligned}
&k = H_{o_2(4)})(2+1) - 1 = \\
&H_{\omega^2}(3) - 1 = \\
&2^3 3 - 1 = \\
&23,
\end{aligned}
$$

y por tanto $m_{21} = 0$ (ya que $21 = 23 - 2$).

(2) Caso $m = 5$, empezando en base 2, secuencia débil:

$$
\begin{aligned}
&k = H_{o_2(5)})(2+1) - 1 = \\
&H_{\omega^2+1}(3) - 1 = \\
&2^4 4 - 1 = \\
&63,
\end{aligned}
$$

y por tanto $m_{61} = 0$ (ya que $61 = 63 - 2$).

(3) Caso $m = 7$, empezando en base 2, secuencia débil:

$$
\begin{aligned}
&k = H_{o_2(7)})(2+1) - 1 = \\
&H_{\omega^2+\omega+1}(3) - 1 = \\
&H_{\omega^2}H_\omega(4) - 1 \\
&H_{\omega^2}(8) - 1 = 2^8 8 - 1 = \\
&2047,
\end{aligned}
$$

y por tanto $m_{2045} = 0$ (ya que $2045 = 2047 - 2$).

(4) Caso $m = 8$, empezando en base 2, secuencia débil:

$$
\begin{aligned}
&k = H_{o_2(8)})(2+1) - 1 = \\
&H_{\omega^3}(3) - 1 = \\
&H_{\omega^2.3}(3) - 1 = \\
&H_{\omega^2\cdot 2+\omega\cdot 3}(3) - 1 = \\
&H_{\omega^2.2}(24) - 1 = \\
&H_{\omega^2+\omega\cdot 24}(24) - 1 = \\
&H_{\omega^2}(2^{24}24) - 1 = \\
&2^{2^{24}24}2^{24}24 - 1 = \\
&2^{2^{24}24+24+3}3 - 1 = \\
&2^{402653211}3 - 1 \cong 10^{1.2\cdot 10^8}
\end{aligned}
$$

(5) Caso $m = 4$, empezando en base 2, secuencia fuerte:

$$\begin{aligned}
&k = H_{O_2(4)}(2+1) - 1 = \\
&H_{\omega^\omega}(3) - 1 = \\
&H_{\omega^3}(3) - 1 = \\
&2^{402653211}3 - 1.
\end{aligned}$$

Estudiaremos algunas propiedades más de la función H que vamos a necesitar más adelante.

Lema 3.16. *Para cada $k \in \omega$, $1 \leq m \in \omega$, $H_{\omega^k \cdot m}(n) = H^m_{\omega^k}(n)$.*

Prueba. Por doble inducción sobre k y m:
Caso $k = 0$: $H_m(n) = m + n = H^m_1(n)$.
Caso $k+1$, $m = 1$: $H_{\omega^{k+1}\cdot 1}(n) = H^1_{\omega^{k+1}}(n)$.
Caso $k+1$, $m+1$:

$H_{\omega^{k+1}\cdot(m+1)}(n) =,$	Como $\omega^{k+1} \cdot (m+1)$ es límite, aplicamos
$H_{\omega^{k+1}\cdot m + \omega^k \cdot n}(n) =,$	$\{\omega^{k+1} \cdot (m+1)\}(n) = \omega^{k+1} \cdot m + \omega^k \cdot n.$
$H_{\omega^{k+1}\cdot m} H_{\omega^k \cdot n}(n) =,$	Por el lema 3.14.
$H_{\omega^{k+1}\cdot m} H_{\omega^{k+1}}(n) =,$	Por el lema 3.16.
$H^m_{\omega^k} \cdot H^1_{\omega^k}(n) =$	Por hipótesis inductiva.
$H^{m+1}_{\omega^k}(n).$	Por nuestra notación.

□

Lema 3.17. *Para cada $k \in \omega$, $H_{\omega^{k+1}}(n) = H^n_{\omega^k}(n)$.*

Prueba. $H_{\omega^{k+1}}(n) = H_{\omega^k \cdot n}(n) = H^n_{\omega^k}(n)$. □

Lema 3.18. *Sea $n \in \omega$ y $\alpha \leq \epsilon_0$. Entonces $H_\alpha(n+1) > H_\alpha(n)$.*

Prueba.
Caso 0: $H_0(n+1) = n + 1 > n = H_0(n)$.
Caso $\alpha = \beta + 1$:

$$\begin{aligned}
H_\alpha(n+1) &= H_{\beta+1}(n+1) \\
&= H_\beta(n+2) \\
&> H_\beta(n+1) \\
&= H_{\beta+1}(n) \\
&= H_\alpha(n).
\end{aligned}$$

Caso $\alpha = \lambda$ límite:

$$\begin{aligned}
H_\lambda(n+1) &= H_{\{\lambda\}(n+1)}(n+1) \\
&> H_{\{\lambda\}(n+1)}(n),
\end{aligned}$$

y como $\lambda > \{\lambda\}(n+1) > \{\lambda\}(n)$ por los lemas 2.8 y 2.10,

$$\begin{aligned}
H_{\{\lambda\}(n+1)}(n) &> H_{\{\lambda\}(n)}(n) \\
&= H_\lambda(n).
\end{aligned}$$

□

Definición 3.19. *Sean $f, g : \omega \to \omega$. Diremos que f* ***mayoriza a*** *g, y escribiremos $f \gg g$, si $f(n) > g(n)$ para casi todo $n \in \omega$, es decir, si $|\{m : f(m) \leq g(m)\}| < \omega$, o, lo que es equivalente, si hay un $k \in \omega$ tal que para todo $n > k$ se da $f(n) > g(n)$.*

Lema 3.20. *Sean $f, g, h : \omega \to \omega$. Si $f \gg g$ y $g \gg h$, entonces $f \gg h$.*

Prueba. Como $f \gg g$, hay un k_1 tal que $\forall n > k_1(f(n) > g(n))$, y como $g \gg h$, hay un k_2 tal que $\forall n > k_2(g(n) > h(n))$, y basta con tomar $k = \max(k_1, k_2)$. $\square$

Lema 3.21. *Si $\alpha < \beta \leq \epsilon_0$, entonces $H_\alpha \ll H_\beta$.*

Prueba. Fijemos α, y por inducción en β.

Caso $\beta = \alpha + 1$: $H_\alpha(n) < H_\alpha(n+1)$ por el lema 3.18, pero $H_\alpha(n+1) = H_{\alpha+1}(n) = H_\beta(n)$.

Caso $\beta = \gamma + 1 > \alpha + 1$: $H_\alpha(n) = H_{\gamma+1}(n) = H_\gamma(n+1)$, y por hipótesis inductiva $H_\gamma(n+1) > H_\alpha(n+1)$, y por el lema 3.18, $H_\alpha(n+1) > H_\alpha(n)$.

Caso $\alpha < \beta = \lambda, \lambda$ límite: Aplicando el corolario 2.12, hay un mínimo k tal que $\{\lambda\}(n) > \alpha$ para cada $n \geq k$; por tanto para cada $n > k$, $H_\lambda(n) = H_{\{\lambda\}(n)}(n)$, por hipótesis inductiva hay un mínimo k_n tal que para $m > k_n$ es $H_{\{\lambda\}(n)}(m) > H_\alpha(m)$. Nos queda por demostrar que si hacemos

$$K = \{k, k_0, k_1, k_2, ...\},$$

entonces

$$\sup K < \omega;$$

en caso contrario, consideremos $I = \{p \in K : p > k+1\}$, y elijamos una enumeración creciente $I = \{i_0, i_1, i_2 ...\}$; entonces $\sup\{\{\lambda\}(i_j - 1) : j \in \omega\} = \lambda$ por ser $\sup I = \omega$, pero por otra parte $\sup\{\lambda\}(i_j - 1) \leq \alpha$, absurdo. $\square$

3.6 $H_{\omega^k}(n)$ es ackermanniana

Los siguientes lemas están destinados a probar que $H_{\omega^n}(m)$ es una variación de la función de Ackermann. De este modo, y basándonos en el hecho conocido de que la función de Ackermann mayoriza a todas las funciones primitivas recursivas, y por tanto su diagonal no es primitiva recursiva, tendremos que $H_{\omega^n}(n)$ no puede ser primitiva recursiva; y, como las secuencias débiles de Goodstein no están acotadas por ningún $H_{\omega^k}(n)$ para ningún k, su cota es $H_{\omega^\omega}(n)$, y por tanto el teorema débil de Goodstein no es demostrable en aritmética primitiva recursiva.

3.6.1 La función de Ackermann

Definición 3.22. *La* ***función de Ackermann*** *se define recursivamente del siguiente modo:*

$A_0(n) = n + 1$

$A_{m+1}(n) = A_m^{n+1}(1)$

Lema 3.23.

(1) $A_1(n) = n + 2$

(2) $A_2(n) = 2n + 3$

(3) $A_3(n) = 2^{n+3} - 3$

Prueba.

(1) Claramente $A_0^2(n) = A_0(n+1) = n+2$, y en general $A_0^m(n) = n+m$, y por tanto $A_1(n) = A_0^{n+1}(1) = n+2$.

(2) $A_1^2(n) = A_1(n+2) = n+4$, y en general $A_1^m(n) = n+2m$, de donde $A_2(n) = A_1^{n+1}(1) = 1 + 2(n+1) = 2n+3$.

(3) $A_3(0) = A_2(1) = 2+3 = 5 = 8-3 = 2^{0+3} - 3$, y si $A_3(n) = 2^{n+3} - 3$, entonces $A_3(n+1) = A_2^{n+2}(1) = A_2 A_2^{n+1}(1) = A_2 A_3(n) = A_2(2^{n+3} - 3) = 2(2^{n+3} - 3) + 3 = 2^{(n+1)+3} + 3$. □

Lema 3.24. *La definición 3.22 es equivalente a la siguiente, más tradicional:*
$f(0, n) = n + 1$;
$f(m+1, 0) = f(m, 1)$;
$f(m+1, n+1) = f(m, f(m+1, n))$.

Prueba. Por doble inducción sobre los argumentos de f.

Casos $m = 0, 1$: Claramente $A_0(n) = n+1 = f(0, n)$, y $A_1(n) = A_0^{n+1}(1) = n+2 = f(1, n)$

Caso $m > 1, n = 0, 1$: $f(m+1, 0) = f(m, 1) = A_m(1) = A_m^{0+1}(1) = A_{m+1}(0)$, y $f(m+1, 1) = f(m, f(m+1, 0)) = A_m(f(m+1, 0)) = A_m(A_m(1)) = A_m^{1+1}(1)) = A_{m+1}(1)$.

Caso $m > 1, n > 1$:

$$\begin{aligned} f(m+1, n+1) &= f(m, f(m+1, n)) \\ &= A_m f(m+1, n) \\ &= A_m f(m, f(m+1, n-1)) \\ &= A_m^2 f(m+1, n-1) \\ &= ... \\ &= A_m^{n+1} f(m+1, 0) \\ &= A_m^{n+1} f(m, 1) \\ &= A_m n + 2(1) \\ &= A_{m+1}(n+1). \end{aligned}$$

□

Lema 3.25. *Para cada $m, n \in \omega$,*

$$A_m(n) > n.$$

Prueba. Por doble inducción en m, n.

Caso $m = 0$: $A_0(n) = n + 1 > n$.

Caso $m+1, n = 0$: $A_{m+1}(0) = A_m^1(1) > 1 > 0$.

Caso $m+1, n+1$: $A_{m+1}(n+1) = A_m^{n+2}(1) = A_m A_m^{n+1}(1) = A_m A_{m+1}(n) \geq A_m(n+1) > n+1$. □

Lema 3.26. *Para cada $m, n \in \omega$, $A_{m+1}(n) > A_m(n)$.*

Prueba. Por doble inducción sobre m, n:

Caso $m = 0, 1$: $A_1(2) = n+2 > n+1 = A_0(n)$, y $A_2(n) = 2n+3 > n+2 = A_1(n)$.

Caso $m+1, n = 0$: $A_{m+1}(0) = A_m(1) > A_{m-1}(1) = A_m(0)$.

Caso $m+1, n+1$: $A_{m+1}(n+1) = A_m^{n+2}(1) > A_{m-1}^{n+2}(1) = A_m(n+1)$. □

Lema 3.27. *Para cada $m, n, p \in \omega$,*

$$A_m(n+1) > A_m(n),$$

y, por tanto,

$$n > p \to A_m(n) > A_m(p).$$

Prueba. Por inducción en m.

Caso $m = 0, 1$: Inmediato, ya que $n + 2 = A_0(n+1) > n + 1 = A_0(n)$ y $n + 3 = A_1(n+1) > n + 2 = A_1(n)$.

Caso $m + 1$: $A_{m+1}(n) = A_m^{n+1}(1) > A_m^{n+1}(0) = A_m^n A_m(0) > A_m^n A_{m-1}(1) > A_{m-1}^{n+1}(1) = A_m(n)$. □

Teorema 3.28. *Sea $f : \omega \to \omega$ una función primitiva recursiva. Entonces existe un $k \in \omega$ tal que $A_k \gg f$.*

Prueba. Damos un esbozo de la demostración: asignemos un rango a cada función primitiva recursiva de la forma natural; el producto tiene rango superior a la suma (puesto que la necesita), la exponenciación tiene rango superior al producto, etc. Es claro que el producto mayoriza a la suma, la exponenciación al producto, etc. Pero A_2 es del orden del producto, A_3 es del orden de la exponenciación, etc. Por tanto, la suma estará mayorizada por A_2, el producto por A_3, etc.; y, en general, y por inducción sobre el rango de la función f, habrá siempre un k tal que $A_k \gg f$. Dicho de otro modo: las funciones primitivas recursivas son del orden de la identidad, la suma, el producto, la exponenciación, etc.; podemos concebir una abstracción, la n-operación, donde la 0-operación sería la identidad, la 1-operación sería la suma, la 2-operación sería el producto, etc.; pero *no podemos operar de forma primitiva recursiva con la i-operación, donde i es una variable.* □

Corolario 3.29. *La función $f(n) = A_n(n)$ no es primitiva recursiva.*

Prueba. En caso contrario, y aplicando el teorema 3.28, existiría un $k \in \omega$ tal que $A_k \gg f$. Pero esto es imposible: debería existir un $k' \in \omega$ tal que para todo $n > k'$ fuese $A_k(n) > f(n) = A_n(n)$, pero para $n > \max(k, k')$ forzosamente $f(n) = A_n(n) > A_k(n)$ en virtud del lema 3.26, una contradicción. □

3.6.2 Definición y propiedades de HA

Definición 3.30. *Para cada $k \in \omega$, definamos $HA_k : \omega \to \omega$ del siguiente modo:*

$$HA_k(n) = H_{\omega^k}(n).$$

Lema 3.31. *Para cada $k, n \in \omega$,*

(1) $HA_0(n) = n + 1$.
(2) $HA_{k+1}(n) = HA_k^n(n)$.

Prueba.

(1) $HA_0(n) = H_{\omega^0}(n) = H_1(n) = H_0(n+1) = n + 1$.
(2) $HA_{k+1}(n) = H_{\omega^{k+1}}(n) = H^n_{\omega^k}(n) = HA_k^n(n)$ aplicando el lema 3.17. □

Lema 3.32.

(1) $HA_1(n) = 2n$
(2) $HA_2(n) = 2^n n$

Prueba.

(1) $HA_1(n) = HA_0^n(n) = n + n = 2n.$
(2) $HA_2(n) = HA_1^n(n) = 2^n n.$ □

Lema 3.33. *Para cada* $m, n \in \omega$, $HA_m(n) > n$.

Prueba. Por inducción en m.
Caso 0*:* $HA_0(n) = n + 1 > n.$
Caso $m + 1$*:* $HA_{m+1}(n) = HA_m^n(n) > n.$ □

Lema 3.34. *Para cada* $m, n, p \in \omega$,

$$HA_m(n + 1) > HA_m(n),$$

y, por tanto,

$$p > n \to HA_m(p) > HA_m(n).$$

Prueba. Por inducción en m.
Caso 0*:* $HA_0(n + 1) = n + 2 > n + 1 = HA_0(n).$
Caso $m + 1$*:*

$$\begin{aligned} HA_{m+1}(n + 1) \quad &= HA_m^{n+1}(n + 1) \\ &> HA_m^{n+1}(n) \\ &> HA_m^{n}(n) \\ &= HA_{m+1}(n). \end{aligned}$$

□

Lema 3.35. *Para cada* $n > 1$, $HA_n \gg A_{n+1}$.

Prueba. Por inducción en n:
Caso 2*:* $HA_2(m) = 2^m m > 2^{m+3} - 3 = 2^m 8 - 3 = A_3(m)$ para cada $m \geq 8$.
Caso $n + 1$*:* $HA_{n+1}(m) = HA_n^m(m)$; por hipótesis inductiva, hay un k tal que

$$HA_n(m) > A_{n+1}(m) \text{ para cada } m > k;$$

si aplicamos el lema 3.34, tendremos

$$HA_n^2(m) > HA_n A_{n+1}(m) \text{ para cada } m > k,$$

pero por el lema 3.25 es $A_{n+1}(m) > m > k$, y podemos aplicar la hipótesis inductiva para obtener

$$HA_n^2(m) > A_{n+1}^2(m) \text{ para cada } m > k;$$

aplicando reiteradamente el mismo procedimiento, llegamos a

$$HA_n^m(m) > A_{n+1}^m(m) \text{ para cada } m > k. \tag{2}$$

Por otra parte, $A_{n+1}(m) > A^2_{n+1}(1)$ sin más que tomar $m > A_{n+1}(1)$, y por tanto, si

$$m > \max(2, k, A_{n+1}(1)), \tag{3}$$

será

$$\begin{array}{ll} HA_{n+1}(m) = HA^m_n(m) & \text{por definición de } HA \\ > A^m_{n+1}(m) & \text{por (2)} \\ = A^{m-1}_{n+1}A_{n+1}(m) & \text{ya que } m > 2 \\ > A^{m-1}_{n+1}A^2_{n+1}(1) & \text{por (3)} \\ = A^{m+1}_{n+1}(1) & \text{por nuestra notación} \\ = A_{n+2}(m). & \text{por definición de } A. \end{array}$$

□

Corolario 3.36. *Si $f : \omega \to \omega$ es una función primitiva recursiva, hay un $k \in \omega$ tal que $HA_k \gg f$.*

Prueba. Por el teorema 3.28, hay un j tal que $A_j \gg f$; por el lema 3.35, $HA_k \gg A_j$, con $k = j - 1$; y por el lema 3.20, $HA_k \gg f$. □

Corolario 3.37. *La función $f(n) = H_{\omega^\omega}(n) = H_{\omega^n}(n) = HA_n(n)$ no es primitiva recursiva.*

Prueba. Idéntica a la del corolario 3.29. □

3.7 El teorema débil de Goodstein no es demostrable en PRA

Teorema 3.38. *Sea $m \in \omega$, y denotemos por m_i su correspondiente secuencia débil de Goodstein en base $n \geq 2$. La función*

$$f(m) = \mu k(m_k = 0)$$

no es primitiva recursiva.

Prueba. Es una consecuencia inmediata del corolario (3.37). □

3.8 El teorema de Goodstein no es demostrable en PA

Teorema 3.39 (Wainer, 1970 [7], [8])**.** *Para cada $\alpha < \epsilon_0$, H_α es demostrablemente recursiva, y por tanto*

$$PA \vdash \forall x \exists y H_\alpha(x) = y;$$

además, dada cualquier función demostrablemente recursiva f, hay un $\alpha < \epsilon_0$ tal que H_α mayoriza a f.

Corolario 3.40. *$H_{\epsilon_0}(n)$ mayoriza a todas las funciones demostrablemente recursivas, y por tanto*

$$PA \nvdash \forall x \exists y H_{\epsilon_0}(x) = y.$$

Prueba. Por el teorema 3.39, basta ver que $H_{\epsilon_0} > H_\alpha$ para cada $\alpha < \epsilon_0$: de este modo, H_{ϵ_0} no puede ser demostrablemente recursiva, pues en caso contrario habría un $\beta < \epsilon_0$ tal que $H_\beta \gg H_{\epsilon_0}$, lo cual es imposible ya que sin más que elegir n tal que $\{\epsilon_0\}(n) > \beta$ (lo que es posible por el corolario 2.12) es con seguridad $H_{\{\epsilon_0\}(n)} \gg H_\beta$ por el lema 3.21, y basta con aplicar un argumento similar al del caso límite del lema 2.11 para obtener una cota k tal que para cada $n > k$, $H_{\epsilon_0}(n) = H_{\{\epsilon_0\}(n)}(n) > H_\beta(n)$. □

Corolario 3.41. *Sea $m \in \omega$, $n \geq 2$, y denotemos por m_i su correspondiente secuencia (fuerte) de Goodstein comenzando por m en base n; entonces*

$$PA \nvdash \forall m \exists k (m_k = 0).$$

Prueba. Por el teorema 3.15, $k = H_\alpha(n+1) - 1$, donde $\alpha = O_n(m)$. Pero, como podemos elegir m de modo que α sea tan grande como queramos, $f(m) = \mu k(m_k = 0)$ no puede estar mayorizada por ningún H_β, la única función que mayoriza a $f(m)$ es H_{ϵ_0}, y $f(m)$ no puede ser demostrablemente recursiva. □

Referencias

[1] E. A. Cichon. “A short proof of two recently discovered independence results using recursion-theoreric methods”. En: *Proceedings of the American Mathematical Society* 87 (1983), págs. 704-706.

[2] R. L. Goodstein. “On the restricted ordinal system”. En: *J. Symbolic Logic* 9 (1944), págs. 33-41.

[3] G. H. Hardy. “A theorem concerning the infinite cardinal numbers”. En: *Quarterly Journal of Mathematics* 35 (1904), págs. 87-94.

[4] J. Ketonen y R. Soloway. “Rapidly Growing Ramsey functions”. En: *Ann. of Math* 113 (1981), págs. 267-314.

[5] Jeff Paris y Leo Harrington. “A mathematical incompleteness in Peano arithmetic”. En: *Handbook of Mathematical Logic*. Ed. por J. Barwise. Amsterdam: North-Holland, 1977, págs. 1133-1142.

[6] H. E. Rose. *Subrecursion. Functions and Hierarchies*. Oxford Logic Guides. Oxford: Clarendon Press, 1978.

[7] S. S. Wainer. “A classification of the ordinal recursive functions”. En: *Arch. Math. Logik Grundlagenforsch.* 13 (1970), págs. 136-153.

[8] S. S. Wainer. “Ordinal recursion, and a refinement of the extended Grzegorczyk hierarchy”. En: *J. Symbolic Logic* 37 (1972), págs. 281-292.

Índice alfabético