Teorema de Goodstein : un Teorema no Demostrable

Jorge Armando Ortega Erazo

Universidad del Cauca

Facultad de Ciencias Naturales, Exactas y de la Educación

Departamento de Matemáticas

Programa de Matemáticas

Popayán

2013

Teorema de Goodstein : un Teorema no Demostrable

JORGE ARMANDO ORTEGA ERAZO

Trabajo de Grado
En modalidad de Seminario de Grado, presentado como requisito parcial
para optar al título de Matemático

Director
FREDDY WILLIAM BUSTOS RENGIFO

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Programa de Matemáticas
Popayán
2013

Nota de aceptación

Director: **Mat. Freddy William Bustos**

Jurado: **Mg. Diego Fernando Ruíz**

Jurado: **Esp. Diego Ramiro Correa**

Popayán, 30 de abril de 2013

Dedicado a mis padres

y mis hermanos.

AGRADECIMIENTOS

Doy infinitas gracias a:

Dios por darme salud para poder cumplir mis metas.

A mis queridos padres y hermanos por su apoyo incondicional y la confianza y paciencia puestas en mí.

A mi director el profesor Freddy Bustos por su gran colaboración en esta etapa de mi carrera.

A los miembros del comité de seguimiento por sus aportes y en general a todos los profesores que estuvieron presentes durante todo mi proceso de formación.

A mis amigos y compañeros por la ayuda y compañía en toda esta etapa de mi vida.

Jorge Armando Ortega Erazo

Universidad del Cauca

Abril de 2013

ÍNDICE GENERAL

I. INTRODUCCIÓN

Uno de los grandes resultados de los trabajos de *Gödel* fue demostrar que cualquier sistema formal lo suficientemente potente para describir la aritmética de los números naturales contiene proposiciones indecidibles. Estas son proposiciones enunciadas en el lenguaje del sistema de las cuales no se puede demostrar ni que son falsas, ni que son verdaderas por medio del lenguaje del sistema.

Gödel en su trabajo mostró como ejemplo de este tipo de proposiciones, una proposición «rebuscada», dejando a la comunidad matemática una pregunta: ¿Si las proposiciones indecidibles que existen son sentencias tan raras, que más da que existan o no, si al parecer no afectarán la matemática?

Fue hasta los trabajos de *Paris y Harrington* [1] en 1977 donde se empezó a darle importancia real a los indecidibles, pues fueron estos matemáticos los primeros en encontrar un *indecidible matemático* el cual lleva el nombre de *Teorema de Ramsey*. Después de este hallazgo matemático empezó un real interés por encontrar proposiciones indecidibles, y es en esta búsqueda donde se encontró uno de los más famosos, **el Teorema de Goodstein**, cuya indecibilidad fue demostrada en 1982 por Kirby y Paris [2].

El Teorema de Goodstein fue planteado y demostrado en 1944 por el matemático inglés Rouben Louis Goodstein pero utilizando una teoría más allá de los números naturales, la teoría de ordinales [3]. En 1983 *Cichon* publicó una demostración diferente a la presentada por *Kirby y Paris*, y es esta demostración la que se describe en este trabajo.

[1] Paris, J. and Harrington, L. A Mathematical Incompleteness in Peano Arithmetic. In Handbook for Mathematical Logic (Ed. J. Barwise). Amsterdam, Netherlands: North-Holland, 1977.

[2] L. Kirby, J. Paris, Accessible independence results for Peano Arithmetic, Bull. Lon. Math. Soc. 14 (1982) 285-293.

[3] Goodstein, R. (1944), «On the restricted ordinal theorem», Journal of Symbolic Logic 9: 33-41

II. PRELIMINARES

Las siguientes definiciones y pruebas de los teoremas se puede consultar en [6].

Definición 0.1. *Diremos que dos conjuntos A, B son equipotentes (tienen el mismo cardinal) y escribiremos $|A| = |B|$ si existe una función biyectiva $f : A \to B$. Si solo sabemos que existe una función inyectiva $f : A \to B$, escribiremos $|A| \leq |B|$.*

Definición 0.2. *Un conjunto S se dice contable si $|S| = |\mathbb{N}|$.*

Teorema 0.1. *Si A, B son conjuntos contables entonces $A \times B$ es contable.*

Teorema 0.2. *Sea I un conjunto contable de índices. Si S_i es un conjunto contable para cada i en I entonces*

$$S := \bigcup_{i \in I} S_i$$

es contable. Es decir que la unión contable de conjuntos contables es un conjunto contable.

Teorema 0.3. *Sea S un conjunto contable y notemos por seq(S) el conjunto de las sucesiones finitas de elementos de S. Entonces seq(S) es contable.*

NÚMEROS ORDINALES

Los números ordinales se definen como una extensión de los naturales y se construyen siguiendo los dos principios de generación: la operación sucesor y el paso al límite. Los ordinales finitos son los números naturales, los cuales conforman un conjunto bien ordenado por la relación de pertenencia. A su vez cada número natural es un conjunto bien ordenado por la pertenencia, es decir

$$0 = \phi, 1 = 0 \cup \{0\}, 2 = 1 \cup \{1\} = \{0, 1\}, 3 = 2 \cup \{2\} = \{0, 1, 2\}, ...$$

En general, cada natural n satisface que $n = \{m \in \mathbb{N} : m < n\} = \{0, 1, 2, ..., n-1\}$. La notación $n+1$ representa el sucesor de n el cual se define como $n \cup \{n\}$. El primer ordinal infinito es ω que representa el conjunto de los números naturales $\mathbb{N}$, es decir $\omega = \mathbb{N}$ y también tienen sentido $\omega + 1 = \omega \cup \{\omega\} = \{0, 1, 2, ..., n, ..., \omega\}$. Cada ordinal α es el conjunto de los ordinales anteriores a él y es sucesor si tiene la forma $\alpha = \beta + 1$ para algún ordinal β, y es límite si no es sucesor.

En los ordinales también tenemos un *teorema de recursión* y un *principio de inducción* los cuales llamamos transfinitos. En particular, el principio de inducción transfinita tiene las siguientes dos versiones

1. Si siempre que una propiedad P es válida para todo ordinal $\beta < \alpha$, entonces la propiedad P es válida para todo ordinal α.

2. Si tenemos una propiedad $P(x)$ tal que

    a) $P(0)$ se cumple,

    b) Para cualquier ordinal α, $P(\alpha)$ implica $P(\alpha + 1)$,

    c) Para cualquier ordinal límite $\alpha \neq 0$, si $P(\beta)$ se cumple para todo $\beta < \alpha$ entonces $P(\alpha)$ se cumple

    entonces $P(\alpha)$ se cumple para todo ordinal α.

En los ordinales se pueden definir las operaciones suma, producto y exponenciación, las cuales son compatibles con las respectivas operaciones en $\mathbb{N}$. Por lo anterior se pueden estudiar propiedades de los ordinales que permitan deducir consecuencias importantes para el conjunto de los números naturales [9].

Las operaciones entre ordinales permiten generar ordinales cada vez mayores, como se puede observar a continuación

$$0, 1, 2, 3, ..., n, ..., \omega, \omega + 1, \omega + 2, ..., \omega + n, ..., \omega + \omega = \omega \cdot 2, \omega \cdot 2 + 1, ...$$

$$\omega \cdot 3, ..., \omega \cdot 4, ..., \omega \cdot \omega = \omega^2, \omega^2 + 1, ...$$

$$\omega^2 \cdot 2, ..., \omega^3, ..., \omega^4, ..., \omega^\omega, \omega^\omega + 1, ..., \omega^\omega \cdot 2, ...$$

$$\omega^\omega \cdot \omega = \omega^{\omega+1}, ..., \omega^{\omega^2}, ..., \omega^{\omega^3}, ..., \omega^{\omega^\omega}, ..., \omega^{\omega^{\omega^\omega}}, ...$$

Dado cualquier conjunto de ordinales X, su unión es también un ordinal el cual es llamado el *supremo* de X, pues de hecho él cumple la definición usual de supremo. En notación tenemos $\sup X = \bigcup X$. Por ejemplo

- $\sup \{1, 3, 7, 10\} = 10$
- $\sup \{n : n \in \omega\} = \omega$
- $\sup \{\omega + n : n \in \omega\} = \omega \cdot 2$
- $\sup \{\omega^n : n \in \omega\} = \omega^\omega$.

Un ordinal especial es $\epsilon_0 = sup \left\{\omega, \omega^\omega, \omega^{\omega^\omega}, ...\right\}$ el cual tiene la particularidad de ser el menor ordinal α tal que $\omega^\alpha = \alpha$. El ordinal ϵ_0 será muy importante pues el álgebra que manejaremos en este trabajo será con ordinales mas pequeños que ϵ_0.

Así como es posible representar cualquier número natural en una base fija, en los ordinales tenemos una situación similar usando como base ω. Concretamente tenemos el siguiente resultado.

Forma normal Cantor. Todo ordinal $\alpha > 0$ puede ser representado de forma única como

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

donde $\alpha_0 > \alpha_1 > \cdots > \alpha_n \geq 0$ y $a_i \in \mathbb{N} - \{0\}$ para $1 \leq i \leq n$.

A continuación presentamos algunas proposiciones relacionadas con la forma normal de Cantor. En la primera de ellas omitiremos la demostración, la cual puede ser consultada en [9].

Lema 0.1. *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 resta o diferencia de α y β, y se denota $\alpha - \beta$.*

Lema 0.2. *Sea $\alpha = \omega^{\alpha_0} \cdot a$,y $\beta = \omega^{\beta_0}$, con $\beta_0 < \alpha_0$. 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, $\gamma = \frac{\alpha}{\beta}$.*

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

□

Proposición 0.1. *Si $\alpha < \epsilon_0$ y $\alpha = \omega^{\alpha_0} \cdot a_0 + \cdots + \omega^{\alpha_n} \cdot a_n$ es su descomposición en forma normal, entonces $\alpha > \alpha_0$*

Demostración. Si $\alpha \leq \alpha_0$ tendríamos $\omega^\alpha \leq \omega^{\alpha_0} \leq \alpha$ y como siempre tenemos $\alpha \leq \omega^\alpha$, obtendríamos $\alpha = \omega^\alpha$ contradiciendo el hecho de que ϵ_0 es el menor ordinal tal que $\epsilon_0 = \omega^{\epsilon_0}$. □

Proposición 0.2. *Cualquier ordinal límite $\lambda < \epsilon_0$ puede expresarse como $\omega^\delta \cdot (\gamma + 1)$, con $\delta > 0$ y $\gamma \geq 0$.*

Demostración. Escribamos λ en forma normal

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

con $\lambda > \alpha_1 > \cdots > \alpha_n > 0$ 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

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

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

Como consecuencia de esta proposición, al considerar ordinales límites tendremos en cuenta que estos tienen la forma $\omega^\delta \cdot (\gamma + 1)$ en donde δ puede a su vez ser sucesor o ser límite.

Definición 0.3. *Sean $\alpha, \beta < \epsilon_0$, y supongamos que $\alpha = \omega^{\alpha_1} \cdot a_1 + \omega^{\alpha_2} \cdot a_2 + \cdots + \omega^{\alpha_n} \cdot a_n$ y $\beta = \omega^{\beta_1} \cdot b_1 + \omega^{\beta_2} \cdot b_2 + \cdots + \omega^{\beta_m} \cdot b_m$ son sus respectivas formas normales de Cantor con $\alpha_1 > \cdots > \alpha_n$ y $\beta_1 > \cdots > \beta_m$. Diremos que α* ***engrana con*** *β y escribiremos $\alpha >> \beta$, si y sólo si $\alpha_n > \beta_1$.*

CAPÍTULO 1

FUNCIONES PRIMITIVAS RECURSIVAS Y FUNCIONES RECURSIVAS

Diremos que una función f de $\mathbb{N}^k$ en $\mathbb{N}$ es calculable si existe un algoritmo que la calcula [2]. Esta definición no es rigurosa en el sentido en que deja pendiente la definición de «algoritmo que la calcula». Tenemos entonces la noción de función recursiva que busca formalizar la idea de calculabilidad. De hecho existe la Tesis de Church la cual afirma que una función es calculable si y solo si es recursiva.
Empezaremos definiendo una subclase de la clase de todas las funciones recursivas, las cuales son llamadas primitivas recursivas.

1.1. Funciones Primitivas Recursivas

Definición 1.1. *Dado $k \in \mathbb{N}$, una función de $\mathbb{N}^k$ en $\mathbb{N}$ se dice* primitiva recursiva ***(pr)*** *si es una de las siguientes funciones que llamaremos básicas*

- función constante 0: $Z(x) = 0$
- función sucesor: $S(x) = x + 1$
- k-ésima proyección: $P_k^n(x_1, ..., x_n) = x_k$

o puede obtenerse a partir de cualquiera de ellas usando alguna de las siguientes reglas:

1. *Composición*

   - Si $f(y_1, ..., y_n)$ y $g_1(x_1, ..., x_k), ..., g_n(x_1, ..., x_k)$ son **pr** entonces $h(x_1, ..., x_k) = f(g_1(x_1, ..., x_k), ..., g_n(x_1, ..., x_k))$ es **pr**.

2. *Recurrencia primitiva*

   - Si $f(x_1, ..., x_k)$ y $g(x_1, ..., x_k, y, z)$ son **pr** también es **pr** la función $h(x_1, ..., x_k, y)$ definida de la siguiente manera:

$$\begin{cases} h(x_1, ..., x_k, 0) = f(x_1, ..., x_k) \\ h(x_1, ..., x_k, S(y)) = g(x_1, ..., x_k, y, h(x_1, ..., x_k, y)) \end{cases}$$

1.2. Ejemplos

Ejemplo 1.1. *La función identidad $I(x) = x$, es **pr**, ya que $I(x) = P_1^1(x) = x$ que es **pr** por definición.*

Ejemplo 1.2. *La función constante $C_n(x) = n$ para todo x es **pr**, pues $C_0(x) = Z(x)$ y $C_n(x) = S(S(...S(Z(x))))$ n-veces para $n \geq 1$ (regla 1).*

Ejemplo 1.3. *La función suma $h(x, y) = x + y$ es **pr**. En efecto sean $f(x) = I(x)$ y $g(x, y, z) = S(P_3^3(x, y, z))$, entonces:*

$$\begin{cases} h(x, 0) = x + 0 = f(x) \\ h(x, S(y)) = x + S(y) = S(x + y) = g(x, y, h(x, y)). \end{cases}$$

Ejemplo 1.4. *La función producto* $h(x,y) = x \cdot y$ *es* ***pr****. Sean* $f(x) = Z(x)$ *y* $g(x,y,z) = x + z$ *entonces:*

$$\begin{cases} h(x,0) = x \cdot 0 = 0 = Z(x) \\ h(x,S(y)) = x \cdot S(y) = x + x \cdot y = g(x,y,h(x.y)). \end{cases}$$

Ejemplo 1.5. *La función exponenciación* $h(x,y) = x^y$ *es* ***pr****. Sean* $f(x) = S(Z(x))$ *y* $g(x,y,z) = x \cdot z$*, entonces:*

$$\begin{cases} h(x,0) = x^0 = 1 = S(Z(x)) = f(x) \\ h(x,S(y)) = x^{S(y)} = x \cdot x^y = g(x,y,h(x,y)). \end{cases}$$

Ejemplo 1.6. *La función* $h(x) = x - 1$ *es* ***pr*** *definida mediante* $h(0) = 0 = Z(0)$ *y* $h(S(x)) = x$*. Entonces la resta truncada*

$$x - y = \begin{cases} x - y & si\ x \geq y \\ 0 & si\ x < y \end{cases}$$

es ***pr*** *pues corresponde a* $x - 0 = x$ *y* $x - S(y) = h(x - y)$*.*

1.3. Propiedades de las funciones pr

Definición 1.2. *Una función* $f : A \subseteq \mathbb{N}^k \rightarrow \mathbb{N}$ *se dice que es total, si el dominio de* f *es todo* $\mathbb{N}^k$*.*

Proposición 1.1. *Si* f *es una función* ***pr****, entonces es total.*

Demostración. Las funciones básicas son totales, pues el dominio de las funciones Z y S es todo $\mathbb{N}$, y el de P es $\mathbb{N}^k$. Veamos ahora que la composición preserva la totalidad. En efecto, sean $f(y_1,...,y_n)$, $g_1(x_1,...,x_k)$, $g_2(x_1,...,x_k)$,...,$g_n(x_1,...,x_k)$ funciones totales, queremos ver que $h(x_1,...,x_k) := f(g_1(x_1,...,x_k),...,g_n(x_1,...,x_k))$ es total. Sea $X \in \mathbb{N}^k$ podemos calcular $x_i = g_i(X)$ para $i = 1,...,n$ pues cada g_i es total. Entonces existe y tal que $y = f(x_1, x_2, ..., x_n)$ pues f es total. Por lo tanto existe $y \in \mathbb{N}$ tal que $y = h(X)$.

Para la recursión sean $f(x_1, ..., x_k)$ y $g(x_1, ..., x_k, y, z)$ funciones totales. Veamos que $h(x_1, ..., x_k, y)$ definida como

$$\begin{cases} h(x_1, ..., x_k, 0) = f(x_1, ..., x_k) \\ h(x_1, ..., x_k, S(y)) = g(x_1, ..., x_k, y, h(x_1, ..., x_k, y)) \end{cases}$$

es total. En efecto sea $X = (x_1, ..., x_k, x_{k+1})$ y $X' = (x_1, ..., x_k)$; Si $x_{k+1} = 0$ entonces existe y tal que $y = f(X')$ pues f es total, por tanto existe y tal que $y = h(X)$. Por otro lado, si $x_{k+1} > 0$ entonces $x_{k+1} = S(z)$ para algún natural z, y existe un y tal que $y = g(X', z, h(X', y))$ por ser g total. En ambos casos obtenemos que existe y con $y = h(X)$.

Así, toda función **pr** es total. $\square$

Proposición 1.2. *Si f y g son funciones primitivas recursivas (**pr**), entonces $f+g$ es **pr**. Donde $(f+g)(x) := f(x) + g(x)$.*

Demostración. Definamos la suma de las funciones f y g como $h(x) := f(x)+g(x)$ y dado que $h(x) = \text{sum}(f(x), g(x))$ donde *sum* no es más que la función suma y f y g son **pr** entonces concluimos que h así definida es una función **pr** por ser composición de funciones **pr**. $\square$

Prácticamente todas las funciones elementales de la teoría de números son primitivas recursivas [2], pero existen funciones de $\mathbb{N}^k$ en $\mathbb{N}$ que no son primitivas recursivas como lo muestra el siguiente lema.

Lema 1.1. *El conjunto de las funciones primitivas recursivas es contable, por lo tanto existen funciones de $\mathbb{N}^k$ en $\mathbb{N}$ que no son recursivas primitivas para cada $k \in \mathbb{N}^k$.*

Demostración. Definamos

$\Omega_0 = \{f : f\text{es una función básica}\}$ y $\Omega_{n+1} = \Omega_n \cup C(\Omega_n) \cup RP(\Omega_n)$, donde

$C(\Omega_n) = \{f(g_1(x_1, ..., x_k), ..., g_m(x_1, ..., x_k)) : f, g_i \in \Omega_n, m \in \mathbb{N}^+\}$
$RP(\Omega_n) = \{h :\ h \text{ es definida por recurrencia primitiva a partir de } f, g \in \Omega_n\}$.

Vemos que Ω_0 es contable, pues es un conjunto contable. Además, si Ω_n es contable, el conjunto de sucesiones finitas de funciones en Ω_n es contable; por lo tanto $C(\Omega_n)$ es contable. Similarmente, el conjunto de pares de funciones en Ω_n es contable, y $RP(\Omega_n)$ es contable. De esta manera queda demostrado que Ω_{n+1} es contable, y por inducción todo Ω_n es contable. Evidentemente, la clase de las funciones **pr** coincide con

$$\Omega = \bigcup_{n=0}^{\infty} \Omega_n$$

y por lo tanto debe ser contable. Ahora, sabemos que el conjunto $\left\{f | f : \mathbb{N}^k \to \mathbb{N}\right\}$ no es contable [6], por lo tanto $\left\{f | f : \mathbb{N}^k \to \mathbb{N}\right\} - \Omega$ sigue siendo no contable. $\square$

El lema anterior no es constructivo, en el sentido de que no nos da ejemplos explícitos de funciones que no sean **pr**.
Construiremos ahora una función que no es **pr** aprovechándonos del resultado del último lema.

Sea $f_1, f_2, ..., f_n, ...$ una enumeración de todas las funciones **pr** de $\mathbb{N}$ en $\mathbb{N}$ y consideremos la función $h(x) = f_x(x)$ y veamos que h no puede ser **pr**. En efecto, supongamos que la función $g(x) = f_x(x) + 1$ es **pr**, luego tendríamos que para todo $x \in \mathbb{N}$, $g(x) = f_x(x) + 1 = f_n(x)$ para algún $n \in \mathbb{N}$. Tomando $x = n$ tendríamos que $f_n(n) + 1 = f_n(n)$ lo cual es una contradicción. Luego g así definida no es **pr** y como la función constante 1 es **pr** entonces por la Proposición 1.2, $f_x(x)$ no es **pr**.

1.4. Minimización

Si a las operaciones ya conocidas de *recurrencia primitiva* y *composición* de las funciones **pr** añadimos una nueva operación llamada *minimización* entonces obtendremos las funciones *recursivas*, es decir que las funciones recursivas son las que surgen de aplicar un número finito de veces las reglas conocidas y la nueva regla. Esta nueva operación trabaja de la siguiente manera.

Primero diremos que una función $f(x_1, ..., x_k, y)$ es regular para y si para todo $(n_1, ..., n_k)$ existe un m tal que $f(n_1, ..., n_k, m) = 0$, de esta manera podemos definir una nueva función $h(x_1, ..., x_k) = \mu y(f(x_1, ..., x_k, y) = 0)$ donde $\mu y(f(x_1, ..., x_k) = 0)$ es el mínimo y tal que $f(x_1, ..., x_k, y) = 0$. A esta función h la llamaremos *minimización* de f con respecto a y.

Tenemos ahora los elementos para definir las funciones recursivas.

1.5. Funciones Recursivas

Definición 1.3. *Una función f es recursiva si es una función primitiva recursiva o puede obtenerse de las funciones primitivas recursivas por un número finito de aplicaciones de composición, recurrencia primitiva y minimización.*

CAPÍTULO 2

FUNCIÓN DE ACKERMANN

Veamos ahora una función especial en el sentido de que esta va a ser recursiva pero no **pr**. Esta función recibe el nombre de *FUNCIÓN DE ACKERMANN* y será de gran ayuda para el cumplimiento del objetivo general de este trabajo.

2.1. Definición

Definición 2.1. *La función de Ackermann es una función de* $\mathbb{N}^2$ *en* $\mathbb{N}$ *definida recursivamente de la siguiente manera:*

$$A(m,n)=\begin{cases} n+1 & si \quad m=0 \\ A(m-1,1) & si \quad m>0 \quad y \quad n=0 \\ A(m-1,A(m,n-1)) & si \quad m>0 \quad y \quad n>0. \end{cases}$$

Esta función tiene la cualidad de ser recursiva pero no primitiva recursiva.

Como ejemplo escribamos el cálculo de $A(2,1)$

$$\begin{aligned}
A(2,1) &= A(1, A(2,0)) \\
&= A(1, A(1,1)) \\
&= A(1, A(0, A(1,0))) \\
&= A(1, A(0, A(0,1))) \\
&= A(1, A(0,2)) \\
&= A(1,3) \\
&= A(0, A(1,2)) \\
&= A(0, A(0, A(1,1))) \\
&= A(0, A(0, A(0, A(1,0)))) \\
&= A(0, A(0, A(0, A(0,1)))) \\
&= A(0, A(0, A(0,2))) \\
&= A(0, A(0,3)) \\
&= A(0,4) \\
&= 5
\end{aligned}$$

2.2. Propiedades

Nota 2.1. *Notaremos* $A^n(p,q) = A(p, A(p, A(p, ..., A(p,q)\cdots)$. *Más precisamente* $A^2(p,q) = A(p, A(p,q))$ *y para* $n > 2$, $A^{n+1}(p,q) = A(p, A^n(p,q))$, *es decir que* $A^n(p,q)$ *resulta de aplicar* n *veces la función* A *situando los resultados en la segunda variable.*

Nota 2.2. *Veamos que* $A(m+1,n) = A^{n+1}(m,1)$ *para todo* $m, n \in \mathbb{N}$.

Demostración. Por inducción en n luego en m. Para $n = 0$ se tiene que $A(m+1, 0) = A(m, 1) = A^{0+1}(m, 1)$. Ahora supongamos que la igualdad se cumple para n, es decir

$$A(m + 1, n) = A^{n+1}(m, 1), \quad m \in \mathbb{N}$$

y comprobémoslo para $n + 1$, es decir

$$A(m + 1, n + 1) = A^{n+2}(m, 1), \quad m \in \mathbb{N}.$$

Para $m = 0$

$$\begin{aligned} A(1, n + 1) &= A(0, A(1, n)) \\ &= A(0, A^{n+1}(0, 1)) \\ &= A^{n+2}(0, 1). \end{aligned}$$

Ahora, si tenemos la validez para m, verifiquemos la proposición para $m + 1$:

$$\begin{aligned} A^{n+2}(m + 1, 1) &= A(m + 1, A^{n+1}(m + 1, 1)) \\ &= A(m + 1, A(m + 2, n)) \\ &= A(m + 2, n + 1). \end{aligned}$$

Así que la propiedad se cumple para $n + 1$ con cualquier m, y la inducción general nos permite concluir que la propiedad es válida para todo $m, n \in \mathbb{N}$. □

Proposición 2.1. *Para cada $m, n \in \mathbb{N}$, $A(m, n) > n$. Es decir, la función de Ackermann toma siempre un valor mayor que la segunda variable de la pareja en donde se evalúa.*

Demostración. Por doble inducción, veamos que para todo $m \in \mathbb{N}$ se cumple que $A(m, n) > n$ para todo $n \in \mathbb{N}$.
Para $m = 0$ tenemos que $A(0, n) = n + 1 > n$.
Como primera hipótesis inductiva supongamos que la proposición es válida para m, es decir

$$A(m, k) > k \text{ para todo } k \in \mathbb{N}$$

y comprobemos que

$$A(m+1,k) > k \text{ para todo } k \in \mathbb{N}:$$

para $k = 0$ tenemos que $A(m+1,0) > 0$ pues por definición $A(m,n)$ es siempre un sucesor.

Ahora como segunda hipótesis de inducción supongamos que

$$A(m+1,n) > n$$

y comprobemos que

$$A(m+1,n+1) > n+1.$$

En efecto

$$\begin{aligned} A(m+1,n+1) &= A^{n+2}(m,1) \\ &= A(m, A^{n+1}(m,1)) \\ &\geq A^{n+1}(m,1)+1 \\ &= A(m+1,n)+1 \\ &> n+1. \end{aligned}$$

Concluimos entonces que la función de Ackermann toma siempre un valor mayor que la segunda variable. □

Proposición 2.2. *Si $p, q \in \mathbb{N}$ con $p > q$ entonces para todo $m, n \in \mathbb{N}$ $A^p(m,n) > A^q(m,n)$. Es decir que la aplicación reiterada de la función de Ackermann produce cada vez mayores valores.*

Demostración. Dado que $p > q$, existe un natural $t > 0$ tal que $p = q + t$. Si $t = 1$ tenemos que $p = q + 1$, luego

$$A^p(m,n) = A^{q+1}(m,n) = A(m, A^q(m,n)) > A^q(m,n).$$

Si $A^{q+t}(m,n) > A^q(m,n)$ entonces

$$\begin{aligned} A^{q+(t+1)}(m,n) &= A^{(q+t)+1}(m,n) \\ &= A(m, A^{q+t}(m,n)) \\ &> A^{q+t}(m,n) \\ &> A^q(m,n). \end{aligned}$$

□

Proposición 2.3. *Para todos $m, n \in \mathbb{N}$, $A^n(m,1) > n$. Es decir que al aplicar n veces la función de Ackermann a $(m,1)$ (en la segunda variable) se obtendrá un valor mayor que n (el número de veces que se aplica Ackermann).*

Demostración. Por inducción en n. Veamos que se cumple para $n = 1$, es decir que $A(m,1) > 1$ para todo $m \in \mathbb{N}$.
Si $m = 0$, $A(0,1) = 2 > 1$. Ahora supongamos que $A(m,1) > 1$ y comprobemos que $A(m+1,1) > 1$. En efecto

$$\begin{aligned} A(m+1,1) &= A^2(m,1) \\ &= A(m, A(m,1)) \\ &> A(m,1) \\ &> 1. \end{aligned}$$

Por otro lado supongamos que $A^n(m,1) > n$ para todo $m \in \mathbb{N}$ y comprobemos que $A^{n+1}(m,1) > n+1$. En efecto

$$\begin{aligned} A^{n+1}(m,1) &= A(m, A^n(m,1)) \\ &\geq A^n(m,1) + 1 \\ &> n+1. \end{aligned}$$

□

Proposición 2.4. $A(m+1,n) \geq A(m,n+1)$.

Demostración. Para $n = 0$ tenemos $A(m+1,0) = A(m,1)$. Para $m = 0$ tenemos $A(0,n+1) = n+2 = A^{n+1}(0,1) = A(1,n)$. Supongamos ahora que $m, n \neq 0$ $A(m+1,n) := A(m, A(m+1,n-1))$ pero $A(m+1,n-1) > n-1$ por la Proposición 2.1 de donde se tiene una de las siguientes igualdades

- $A(m+1,n-1) = n$
- $A(m+1,n-1) = n+p$ para $0 < p \in \mathbb{N}$.

Pero $A(m+1,n-1) = A^n(m,1) > n$ por la Proposición 2.3, por lo que tenemos que $A(m+1,n-1) = n+p$, de donde

$$\begin{aligned}
A(m+1,n) &:= A(m, A(m+1,n-1)) \\
&= A(m, n+p) \\
&= A^{n+p+1}(m-1,1) \\
&\geq A^{n+2}(m-1,1) \\
&= A(m, n+1).
\end{aligned}$$

□

Proposición 2.5. *Para cada $m, n \in \mathbb{N}$, $A(m+1,n) > A(m,n)$. Es decir que la función de Ackermann es creciente en la primera variable.*

Demostración. Veamos que para todo $m \in \mathbb{N}$ se cumple que

$$A(m+1,n) > A(m,n) \text{ para todo } n \in \mathbb{N},$$

- Si $m = 0$, tenemos $A(1,n) = A^{n+1}(0,1) = n+2 > n+1 = A(0,n)$
- Supongamos que

  $$A(m+1,n) > A(m,n) \text{ para todo } n \in \mathbb{N} \text{ (hipótesis inductiva 1).}$$

  Debemos comprobar que $A(m+2,k) > A(m+1,k)$ para todo $k \in \mathbb{N}$

- Para $k = 0$

$$\begin{aligned} A(m+2,0) &:= A(m+1,1) \\ &> A(m,1) \\ &= A(m+1,0), \end{aligned}$$

- Ahora supongamos que

  $$A(m+2,k) > A(m+1,k) \text{ (hipótesis inductiva 2)}$$

  y comprobémoslo para $k+1$

$$\begin{aligned} A(m+2,k+1) &= A^{k+2}(m+1,1) \\ &= A(m+1, A^{k+1}(m+1,1)) \\ &> A^{k+1}(m+1,1) \\ &= A(m+2,k) \\ &\geq A(m+1,k+1). \end{aligned}$$

Por lo tanto podemos concluir que la función de Ackermann es creciente en la primera variable. $\square$

Proposición 2.6. *Para cada $m, n, p \in \mathbb{N}$, $A(m, n+1) > A(m, n)$ y consecuentemente si $n > p$ se tiene que $A(m, n) > A(m, p)$. Es decir que la función de Ackermann es creciente en la segunda variable.*

Demostración. Para $m = 0$ tenemos que

$$A(0, n+1) = n+2 > n+1 = A(0, n)$$

ahora veamos para m un sucesor

$$A(m, n+1) := A(m-1, A(m, n)) > A(m, n)$$

$\square$

2.3. La función de Ackermann no es pr

Aunque no lo mostramos en este trabajo, la función de Ackermann es recursiva, y el no ser **pr** la hace una función especial que además tiene la particularidad de determinar una frontera para las funciones primitivas recursivas en un sentido que explicaremos más adelante.

Definición 2.2. *Sean $f, g : \mathbb{N} \to \mathbb{N}$. Diremos que f* ***mayoriza a*** *g, y escribiremos $f >> g$, si $f(n) > g(n)$ para casi todo $n \in \mathbb{N}$, es decir, si $|\{m : f(m) \leq g(m)\}|$ es finito, o, lo que es equivalente, si hay un $k \in \mathbb{N}$ tal que para todo $n > k$ se da $f(n) > g(n)$.*

Proposición 2.7. *Sean $f, g, h : \mathbb{N} \to \mathbb{N}$. Si $f >> g$ y $g >> h$, entonces $f >> h$.*

Demostración. Como $f >> g$, hay un k_1 tal que para todo $n > k_1$ $f(n) > g(n)$, y como $g >> h$, hay un k_2 tal que para todo $n > k_2$ $g(n) > h(n)$. Así tomando $k = \text{máx}(k_1, k_2)$ tenemos que $f >> h$. □

Nota 2.3. *Fijando m en la primera variable podemos ver la función de Ackermann como una función de una variable y escribir $A_m(n)$ para referirnos a $A(m, n)$. A las funciones resultantes de fijar m en la función de Ackermann las llamaremos funciones ackermannianas o incluso funciones de Ackermann.*

Proposición 2.8. *$A_m(n)$ es* ***pr*** *para todo $m \in \mathbb{N}$.*

Demostración. Para $m = 0$ tenemos que $A_m(n) = A_0(n) = A(0, n) = S(n)$ que es **pr** por definición.

Supongamos que $A_m(n)$ es **pr** y comprobemos que $A_{m+1}(n)$ es **pr**. En efecto

$$A_{m+1}(n) = A^{n+1}(m, 1) = A_m A_m \cdots A_m(1)$$

Así A_{m+1} resulta de componer $n + 1$ veces A_m y como esta es **pr** por hipótesis de inducción y la composición de **pr** es **pr** obtenemos que $A_{m+1}(n)$ es **pr**. □

Lema 2.1. *Sea $f : \mathbb{N} \to \mathbb{N}$ una función **pr**. Entonces existe un $k \in \mathbb{N}$ tal que $A_k >> f$. Esto es, cada función **pr** es mayorizada por una función ackermanniana.*

Demostración. Veamos que se cumple para las funciones **pr** base.
Para la función constante cero tenemos

$$Z(n) = 0 < n + 2 = A_1(n), \text{para todo } n \in \mathbb{N}$$

por tanto $Z << A_1$.
Para la función sucesor tenemos

$$S(n) = n + 1 < n + 2 = A_1(n), \text{para todo } n \in \mathbb{N}$$

por tanto $S << A_1$.
Para la función proyección, que no es más que la identidad tenemos que también es acotada por la función A_1. Así concluimos que todas las funciones **pr** base son acotadas por algún A_k.
Ahora supongamos que f y g son **pr** y que existen $k, t \in \mathbb{N}$ tales que $f << A_k$ y $g << A_t$. Veamos que bajo composición la función obtenida es acotada por una ackermanniana.

$$(f \circ g)(n) = f(g(n)) << A_k$$

por tanto se cumple para la composición.
Veámoslo ahora para el esquema de recurrencia primitiva. Si tenemos f, g primitivas recursivas (en este caso dom$g = \mathbb{N}^2$) y existen $k, t \in \mathbb{N}$ tales que $f << A_k$ y $g << A_t$, el esquema de recurrencia primitiva es el siguiente:

$$\begin{cases} h(0) = f(0) \\ h(S(n)) = g(n, h(n)), \end{cases}$$

tomando $s = \text{máx}\{k, t\}$ entonces tenemos que

$$h << A_s.$$

Por lo tanto toda función **pr** esta mayorizada por una función de Ackermann. $\square$

A partir de las funciones de Ackermann de una variable es posible construir una nueva función a la que llamaremos «diagonal de Ackermann», tomando las parejas $(n, A_n(n))$. Esta función es especial como veremos en la siguiente proposición.

Proposición 2.9. *La función $f(n) = A_n(n)$ no es* ***pr****.*

Demostración. Supongamos que f es **pr**, luego por el Lema 2.1 tendremos que existe un $k \in \mathbb{N}$ con $A_k >> f$. Esto es, existe un $k' \in \mathbb{N}$ tal que para todo $n > k'$, $A_k(n) > f(n) = A_n(n)$. Tomando $m > \max(k, k')$ tendríamos que $A_k(m) > f(m) = A_m(m)$, lo cual, por la proposición 7 es una contradicción. Entonces concluimos que f así definida no es **pr**. $\square$

CAPÍTULO 3

SUCESIONES DE GOODSTEIN

3.1. Las Sucesiones

Definición 3.1. *Dados dos números naturales $m > 0$ y $n > 1$, denotamos por $m_{(n}$ la expresión del número m en base n, es decir,*

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

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

Ejemplo 3.1. $21_{(2} = 2^4 + 2^2 + 1$ *y* $261_{(2} = 2^8 + 2^2 + 1$

Definición 3.2. *Dados dos números naturales $m > 0$ y $n > 1$, la expresión del número m en base pura n, notada $m_{[n}$ es:*

$$m_{[n} = m \quad si\ m < n\ y$$

$$m_{[n} = \sum_{1 \leq i \leq k} a_i \cdot n^{e_{i[n}} \quad en\ otro\ caso$$

Ejemplo 3.2. $21_{[2} = 2^{4_{[2}} + 2^{2_{[2}} + 1 = 2^{2^2} + 2^2 + 1$ *y* $261_{[2} = 2^{8_{[2}} + 2^{2_{[2}} + 1 = 2^{2^{3_{[2}}} + 2^2 + 1 = 2^{2^{2+1}} + 2^2 + 1.$

Definición 3.3. *Sea $m > 0$, $n \geq 2$, y $x \geq n$ o $x = \omega$. Definimos las operaciones que denotaremos por $m^x_{(n}$ y $m^x_{[n}$ al resultado de cambiar todas las apariciones de n por x en la expresión en base n (o base pura n) de m.*

Ejemplo 3.3. $21^3_{[2} = 3^{3^3} + 3^3 + 1$ *y* $21^\omega_{(2} = \omega^4 + \omega^2 + 1$

Definición 3.4. *(Sucesiones débiles de Goodstein). Sea m un número natural hagamos*

$$m_0 = m_{(2}$$

y construyamos cualquier elemento de la sucesión de la siguiente manera

$$m_{k+1} = (m_k)^{k+3}_{(k+2} - 1$$

Las sucesiones de esta manera construidas son llamadas sucesiones débiles de Goodstein.

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

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

Ejemplo 3.4. *Tomemos $m = 21$, la sucesión débil de Goodstein en base 2 así:*

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

Definición 3.5. *Sean $m \in \mathbb{N}$ y $n \geq 2$. La sucesión fuerte de Goodstein comenzando por m en base n se define recursivamente del siguiente modo:*

$$m_0 = m_{[2}$$

y para cada $k \geq 0$,

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

Ejemplo 3.5. *Tomemos $m = 7$ y $n = 2$ para la sucesión fuerte de Goodstein, así:*

$m_0 = 2^2 + 2^1 + 1 = 7$

$m_1 = 3^3 + 3^1 + 1 - 1 = 27 + 3 = 30$

$m_2 = 4^4 + 4 - 1 = 4^4 + 3 = 256 + 3 = 259$

$m_3 = 5^5 + 3 - 1 = 3125 + 2 = 3127$

$\vdots$

A continuación presentamos el objeto de estudio de este trabajo, es decir el *Teorema de Goodstein*. También presentamos inicialmente una versión débil del mismo.

Teorema Débil de Goodstein: Sea m_i la sucesión 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.

Teorema de Goodstein: Sea m_i la sucesión fuerte 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 Axiomática de Peano.

La demostración de estos teoremas utiliza los números ordinales y sus propiedades. En líneas generales, una sucesión de Goodstein se puede transformar en una sucesión de ordinales infinitos de la cual se puede comprobar que es decreciente y acota a la sucesión inicial. Como toda sucesión decreciente de ordinales llega a cero, las sucesiones de Goodstein llegan a cero. Un desarrollo completo se presenta en [9].

CAPÍTULO 4

SUCESIONES FUNDAMENTALES

En 1897 *Cantor* define las sucesiones fundamentales que convergen hacia un ordinal límite α. Si λ es un ordinal mayor o igual que ω y $\langle \alpha_\gamma \,|\gamma < \lambda\rangle$ es una sucesión transfinita de ordinales de longitud λ, escribimos

$$\alpha = \sup\{\alpha_\gamma \mid \gamma < \lambda\} = \lim_{\gamma\to\lambda} \langle\alpha_\gamma \mid \gamma < \lambda\rangle.$$

Llamamos a α el límite de la sucesión y decimos que la sucesión converge a α. En particular

$$\omega \cdot 2 = \lim_{n\to\omega} \langle \omega + n \,|n < \omega\rangle\,.$$

$$\omega^\omega = \lim_{n\to\omega} \langle \omega^n \,|n < \omega\rangle\,.$$

Pero también tenemos que las sucesiones $\langle n \cdot 2 \,|n < \omega\rangle$, $\langle n^2 \,|n < \omega\rangle$, $\langle 2^n \,|n < \omega\rangle$ convergen a ω. Estamos interesados en que dado un ordinal límite podamos referirnos a una sucesión particular que converja a él. Dicha sucesión la llamaremos *sucesión fundamental* y tendrá longitud ω. Para describir la sucesión fundamental del ordinal λ usaremos la notación $\{\lambda\}\,(n)$ para referirnos al término n-ésimo de la misma e incluiremos todos los ordinales en la siguiente definición.

Definición 4.1. *Sea* $\alpha \leq \epsilon_0$. *La* ***sucesión fundamental de*** α *es la función* $\{\alpha\} : \omega \to \epsilon_0$ *definida por*

(α0) $\{0\}(n) = 0$.

(α1) $\{\alpha + 1\}(n) = \alpha$.

(α2) $\left\{\omega^{\delta+1} \cdot (\gamma + 1)\right\}(n) = \omega^{\delta+1} \cdot \gamma + \omega^{\delta} \cdot n$.

(α3) $\left\{\omega^{\delta} \cdot (\gamma + 1)\right\}(n) = \omega^{\delta} \cdot \gamma + \omega^{\{\delta\}(n)}$, *si* δ *es un ordinal límite.*

(α4) $\{\epsilon_0\}(0) = 1$ *y* $\{\epsilon_0\}(n + 1) = \omega^{\{\epsilon_0\}(n)}$.

Ejemplo 4.1.

- $\{\omega\}(n) = \{\omega^{0+1} \cdot (0 + 1)\}(n) = \omega^{0+1} \cdot 0 + \omega^0 \cdot n = n$, *aplicando ($\alpha$2).*
- $\{\omega + 1\}(n) = \omega$ *y en general* $\{\omega + m + 1\}(n) = \omega + m$.
- $\{\omega \cdot 2\}(n) = \{\omega^{0+1} \cdot (1 + 1)\}(n) = \omega^{0+1} \cdot 1 + \omega^0 \cdot n = \omega + n$.
- $\{\omega^\omega\}(n) = \{\omega^\omega \cdot (0 + 1)\}(n) = \omega^\omega \cdot 0 + \omega^{\{\omega\}(n)} = \omega^n$.

A continuación listamos algunas propiedades de las sucesiones fundamentales.

Proposición 4.1. *Si* $\alpha > 0$, *entonces* $\{\alpha\}(n) < \alpha$.

Demostración. Para (α1) tenemos

$$\{\alpha + 1\}(n) = \alpha < \alpha + 1.$$

Para (α2) tenemos

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

Para ($\alpha 3$) supongamos que se cumple para todo $\alpha' < \alpha$ es decir $\{\alpha'\}(n) < \alpha'$ y comprobémoslo para α. En efecto

$$\begin{aligned}\{\alpha\}(n) &= \left\{\omega^{\delta} \cdot (\gamma + 1)\right\}(n) \\ &= \omega^{\delta} \cdot \gamma + \omega^{\{\delta\}(n)} \\ &< \omega^{\delta} \cdot \gamma + \omega^{\delta} \qquad (3) \\ &= \omega^{\delta} \cdot (\gamma + 1)\end{aligned}$$

La relación (3) se explica porque siendo $\alpha = \omega^{\delta} \cdot (\gamma + 1)$ entonces $\delta < \alpha$, de donde $\{\delta\}(n) < \delta$, implicando que $\omega^{\{\delta\}(n)} < \omega^{\delta}$. Por lo tanto la proposición se cumple para todo $\alpha > 0$. $\square$

Proposición 4.2. *Sean $\alpha, \beta < \epsilon_0$ y supongamos que $\alpha >> \beta > 0$. Entonces $\{\alpha + \beta\}(n) = \alpha + \{\beta\}(n)$.*

Demostración. Procedemos por inducción sobre β. Sea $\beta = \gamma + 1$ un sucesor, entonces

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

Caso límite. Si $\beta = \omega^{\delta+1}(\gamma + 1)$, entonces $\alpha + \beta = \omega^{\delta+1}(\frac{\alpha}{\omega^{\delta+1}} + \gamma + 1)$ y por tanto

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

Para el otro caso límite tenemos que $\beta = \omega^\delta(\gamma+1)$ con δ un ordinal límite, luego

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

□

Proposición 4.3. *Sean $n \in \mathbb{N}$ y $\lambda < \epsilon_0$ un ordinal límite. Entonces $\{\lambda\}(n+1) > \{\lambda\}(n)$. Es decir, la sucesión fundamental de un ordinal límite no cero es estrictamente creciente.*

Demostración. Veamos que se cumple para ω,

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

Ahora supongamos que λ es de la forma $\lambda = \omega^{\delta+1}\cdot(\gamma+1)$, luego,

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

Para el siguiente caso límite con $\lambda = \omega^\delta\cdot(\gamma+1)$ y δ límite, suponemos que se cumple para $\delta' < \delta$ y veamos que se cumple para δ. Así,

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

pues por hipótesis inductiva $\{\delta\}(n+1) > \{\delta\}(n)$. □

Corolario 4.1. *Sean $\alpha < \lambda \leq \epsilon_0$, con λ límite entonces:*

- *hay un mínimo $k \in \omega$ tal que $\{\lambda\}(k) > \alpha$, y por tanto*

- *para cada* $n \geq k$ *tenemos que* $\{\lambda\}(n) > \alpha$.

Observación 4.1. *Si* $\lambda < \epsilon_0$ *es un ordinal límite, de acuerdo con lo comentado al presentar las sucesiones fundamentales tenemos*

$$\lim_{n \to \omega} \{\lambda\}(n) = sup \{\{\lambda\}(n) : n \in \mathbb{N}\} = \lambda.$$

CAPÍTULO 5

FUNCIONES O, G y P

Necesitamos poder referirnos a las sucesiones de Goodstein introduciendo una terminología especial. En este capítulo presentamos unas funciones que nos permitirán describir las sucesiones de Goodstein y hacemos dicha descripción.

5.1. Función O

Definición 5.1. *Para cada $k > 1$, 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 5.1. *Una consecuencia inmediata de la definición de o y O es que si*

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

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

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

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

Ejemplo 5.1.

- $o_2(261) = \omega^8 + \omega^2 + 1$ *pues* $21_{(2} = 2^8 + 2^2 + 1$ *y*
- $O_2(21) = \omega^{\omega^{\omega}} + \omega^{\omega} + 1$ *pues* $21_{[2} = 2^{2^2} + 2^2 + 1$.

5.2. Función G

Definición 5.2. *Sea* $n \in \omega$ *y* $\alpha < \epsilon_0$. *Definimos*

a) $G_n(0) = 0$,

b) $G_n(\alpha + 1) = G_n(\alpha) + 1$, *y*

c) $G_n(\alpha) = G_n(\{\alpha\}(n))$ *para todo límite* $\alpha \neq 0$.

Ahora mostraremos algunos ejemplos para ver un poco más claro el comportamiento de la función G, que dicho a grandes rasgos lo que hace es pasar de ordinales a enteros.

Ejemplo 5.2.

- $G_n(1) = G_n(0+1) = G_n(0)+1 = 1$ *y en general* $G_n(m) = m$ *para todo* $m < \omega$.
- $G_n(\omega) = G_n(\{\omega\}(n)) = G_n(n) = n$.
- $G_n(\omega \cdot 2) = G_n(\{\omega \cdot 2\}(n)) = G_n(\omega + n) = 2 \cdot n$.

Proposición 5.1. *Si* $n > 0$ *y* $\alpha < \epsilon_0$, *entonces* $G_n(\alpha) = 0$ *si y sólo si* $\alpha = 0$

Demostración. Si $\alpha = 0$ por definición de G tenemos $G_n(\alpha) = 0$. Ahora debemos probar que si $G_n(\alpha) = 0$ entonces $\alpha = 0$, o equivalentemente si $\alpha > 0$ entonces $G_n(\alpha) > 0$. En efecto, si α es un sucesor tenemos $G_n(\alpha) = G_n(\beta+1) = G_n(\beta)+1 > 0$. Por otro lado si α es un ordinal límite y suponiendo que la proposición se cumple para todo $\alpha' < \alpha$ entonces $G_n(\alpha) = G_n(\{\alpha\}(n))$ así por hipótesis inductiva tenemos que $G_n(\alpha) > 0$ $\square$

Proposición 5.2. *Si* $\alpha >> \beta$, *entonces* $G_n(\alpha + \beta) = G_n(\alpha) + G_n(\beta)$.

Demostración. Por inducción en β. Caso $\beta = 0$

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

Supongamos que se cumple para β y comprobemos para $\beta + 1$,

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

Para el caso β límite supongamos que la proposición es verdadera para todo $\beta' < \beta$. Además, notemos que si $\alpha >> \beta$, α es ordinal límite entonces $\alpha + \beta$ también lo es, luego

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

$\square$

Proposición 5.3. *Sea* $\lambda = \omega^\delta \cdot m < \epsilon_0$*, con* $m \in \omega$*. Entonces* $G_n(\lambda) = G_n(\omega^\delta) \cdot m$*.*

Demostración. Por doble inducción sobre δ y m

Para $\delta = 0$ tenemos

$$G_n(\lambda) = G_n(m) = m = 1 \cdot m = G_n(1) \cdot m = G_n(\omega^0) \cdot m, \text{para todo } m < \omega.$$

Para $\delta = \alpha + 1$ un sucesor, comprobemos que se cumple la proposición para todo $m \in \omega$. Empecemos con $m = 0$

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

Supongamos que $G_n(\omega^{\alpha+1} \cdot p) = G_n(\omega^{\alpha+1}) \cdot p$ y calculemos

$$\begin{aligned}
G_n(\lambda) &= G_n(\omega^{\alpha+1} \cdot (p+1)) \\
&= G_n(\left\{\omega^{\alpha+1} \cdot (p+1)\right\}(n)) \\
&= G_n(\omega^{\alpha+1} \cdot p + \omega^\alpha \cdot n) \\
&= G_n(\omega^{\alpha+1} \cdot p) + G_n(\omega^\alpha \cdot n) \\
&= G_n(\omega^{\alpha+1}) \cdot p + G_n(\left\{\omega^{\alpha+1}\right\}(n)) \\
&= G_n(\omega^{\alpha+1}) \cdot p + G_n(\omega^{\alpha+1}) \\
&= G_n(\omega^{\alpha+1})(p+1).
\end{aligned}$$

Entonces $G_n(\omega^{\alpha+1} \cdot m) = G_n(\omega^{\alpha+1}) \cdot m$ para todo $m < \omega$.

Ahora veamos para δ un ordinal límite. Con $m = 0$ el resultado es trivial; ahora supongamos que se cumple para p y probemos para $p + 1$ así:

$$\begin{aligned}
G_n(\omega^\delta \cdot (p+1)) &= G_n(\left\{\omega^\delta \cdot (p+1)\right\}(n)) \\
&= G_n(\omega^\delta \cdot p + \omega^{\{\delta\}(n)}) \\
&= G_n(\omega^\delta \cdot p) + G_n(\omega^{\{\delta\}(n)}) \\
&= G_n(\omega^\delta) \cdot p + G_n(\left\{\omega^\delta\right\}(n)) \\
&= G_n(\omega^\delta) \cdot p + G_n(\omega^\delta) \\
&= G_n(\omega^\delta)(p+1)
\end{aligned}$$

□

Proposición 5.4. *Sea* $0 < \alpha < \epsilon_0$ *y* $n > 0$. *Entonces* $G_n(\omega^\alpha) = n^{G_n(\alpha)}$.

Demostración. Por inducción en α. Para $\alpha = 0$

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

Ahora por inducción supongamos que se cumple para un β y probemos para $\beta + 1$

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

En el caso de que α sea un ordinal límite supongamos que la propiedad se cumple para todo $\alpha' < \alpha$, luego

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

□

Lema 5.1. *Sea* $\alpha < \epsilon_0$. $G_n(\alpha)$ *se obtiene tomando la representación de* α *en forma normal de Cantor y reemplazando todas las apariciones de* ω *por* n.

Demostración. Veamos α en forma normal de Cantor

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

Por la Proposición 5.2, $G_n(\alpha) = G_n(\omega^{\alpha_1} \cdot a_1) + \cdots + G_n(\omega^{\alpha_n} \cdot a_n)$, luego por la Proposición 5.3, $G_n(\alpha) = G_n(\omega^{\alpha_1}) \cdot a_1 + \cdots + G_n(\omega^{\alpha_n}) \cdot a_n$ y finalmente por la

Proposición 5.4 tenemos

$$G_n(\alpha) = n^{G_n(\alpha_1)} \cdot a_1 + \cdots + n^{G_n(\alpha_n)} \cdot a_n$$

□

Proposición 5.5. *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

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

Demostración. Es inmediato dándonos cuenta de que lo que hace la función O es cambiar las apariciones de n por ω mientras que lo que hace la función G es lo contrario cambiando las apariciones de ω por n. □

5.3. Función P

Definición 5.3. *Sea $\alpha < \epsilon_0$ y $n < \omega$. El* ***n-anterior de*** *α se define mediante*

a) $P_n(0) = 0$

b) $P_n(\alpha + 1) = \alpha$

c) $P_n(\lambda) = P_n(\{\lambda\}(n))$ *para λ límite.*

Ejemplo 5.3.

- $P_n(m + 1) = m$ *para todo $m, n \in \mathbb{N}$.*
- $P_5(\omega^3) = P_5(\{\omega^3\}(5)) = P_5(\omega^2 \cdot 5) = P_5(\{\omega^2 \cdot 5\}(5)) = P_5(\omega^2 \cdot 4 + \omega \cdot 5) = P_5(\omega^2 \cdot 4 + \omega \cdot 4 + 5) = \omega^2 \cdot 4 + \omega \cdot 4 + 4.$
- $P_3(\omega^4) = P_3(\omega^3 \cdot 3) = P_3(\omega^3 \cdot 2 + \omega^2 \cdot 3) = P_3(\omega^3 \cdot 2 + \omega^2 \cdot 2 + \omega \cdot 3) = P_3(\omega^3 \cdot 2 + \omega^2 \cdot 2 + \omega \cdot 2 + 3 = \omega^3 \cdot 2 + \omega 2 \cdot 2 + \omega \cdot 2 + 2.$

Teorema 5.1. *Sean $\alpha < \epsilon_0$ y $n \in \mathbb{N}$. Entonces*

$$G_n P_n(\alpha) = P_n G_n(\alpha)$$

Demostración. Por inducción sobre α. Si $\alpha = 0$ tenemos:

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

Ahora por inducción sobre β supongamos que se cumple para β y probemos para $\beta + 1$,

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

Por inducción transfiníta supongamos que se cumple para todo $\alpha' < \alpha$, así.

$$\begin{aligned} G_n P_n(\alpha) &= G_n P_n(\{\alpha\}(n)) \\ &= P_n G_n(\{\alpha\}(n)) \\ &= P_n G_n(\alpha) \end{aligned}$$

□

5.4. Construcción de las sucesiones de Goodstein a partir de las funciones O, G y P

Empecemos la sucesión de Goodstein partiendo de un natural $m = m_0$ en pura base n. Sabemos que cualquier término siguiente de la sucesión (término k) será el anterior pasado de la base $n + k$ a la base $n + k + 1$ y restándole 1. De esta manera siendo m_0 el primer elemento y haciendo $\alpha = O_n(m_0)$ tendremos que,

$$m_1 = P_{n+1} G_{n+1}(\alpha),$$

que por el Teorema 5.1 es,

$$m_1 = G_{n+1} P_{n+1}(\alpha).$$

Ahora tendremos que aplicarle exactamente el mismo tratamiento a este nuevo número (m_1). Esto es, aplicarle la función O_{n+1} pues este último quedó en esta base, luego pasarlo a la base siguiente aplicando G_{n+2} y finalmente restándole 1, que para nuestro caso seria aplicar P_{n+2}. Así tendremos,

$$\begin{aligned} m_2 &= P_{n+2}G_{n+2}O_{n+1}(m_1) \\ &= P_{n+2}G_{n+2}O_{n+1}G_{n+1}P_{n+1}(\alpha) \\ &= P_{n+2}G_{n+2}P_{n+1}(\alpha) \\ &= G_{n+2}P_{n+2}P_{n+1}(\alpha) \end{aligned}$$

En general y siguiendo los mismos pasos de construcción tendremos que cualquier elemento de la sucesión podrá ser obtenido con dichas funciones. Es decir,

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

El Teorema de Goodstein afirma que existe un k' tal que $m_{k'} = 0$, esto es

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

lo que por la Proposición 5.1 es equivalente a decir que existe un k tal que

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

CAPÍTULO 6

JERARQUÍA DE HARDY

En este capítulo presentamos una familia de funciones que permitirán determinar el valor de k en la expresión

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

La existencia de este k está garantizada por la validez del teorema de Goodstein.

6.1. Funciones de Hardy

Definición 6.1. *Para cada $\alpha \leq \epsilon_0$, definimos una función $H_\alpha : \omega \to \omega$ del siguiente modo*

a*)* $H_0(n) = n$

b*)* $H_{\alpha+1}(n) = H_\alpha(n+1)$

c*)* $H_\alpha(n) = H_{\{\alpha\}(n)}(n)$ *si α es límite.*

Ejemplo 6.1.

- $H_1(n) = H_0(n+1) = n+1$, *y en general* $H_m(n) = n+m$.
- $H_\omega(n) = H_{\{\omega\}(n)}(n) = H_n(n) = 2n$.
- $H_{\omega+1}(n) = H_\omega(n+1) = 2(n+1)$, *y en general* $H_{\omega+m}(n) = 2(n+m)$.
- $H_{\omega\cdot 2}(n) = H_{\{\omega\cdot 2\}(n)}(n) = H_{\omega+n}(n) = 2(n+n) = 2^2 n$.
- $H_{\omega\cdot 2+m}(n) = H_{\omega\cdot 2}(n+m) = 2^2(m+n)$.
- $H_{\omega\cdot 3}(n) = H_{\{\omega\cdot 3\}(n)} = H_{\omega\cdot 2+n}(n) = 2^2(n+n) = 2^3 n$.
- *En general* $H_{\omega\cdot m}(n) = 2^m n$.
- $H_{\omega^2}(n) = H_{\{\omega^2\}(n)}(n) = H_{\omega\cdot n}(n) = 2^n n$.
- $H_{\omega^2+m}(n) = H_{\omega^2}(n+m) = 2^{n+m}(n+m)$.

Teorema 6.1. *Sean* $0 < \alpha < \epsilon_0$ *y* $0 < n < \omega$. *Entonces*

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

en donde $\mu k[P_k P_{k-1} ... P_{n+1}(\alpha) = 0]$ *representa el número* k *que permite que* $P_k P_{k-1} ... P_{n+1}(\alpha) = 0$ *partiendo de escribir* m_0 *en base* n *y hacer* $\alpha = O_n(m_0)$.

Demostración. Por inducción sobre α:
Dado que α no puede ser 0 el primer caso inductivo será para $\alpha = 1$. De aquí tenemos que $P_{n+1}(\alpha) = 0$ para cualquier $n \in \omega$ y por tanto $k = n+1$. Por otro lado $H_1(n+1) = n+2$ y $H_1(n+1) - 1 = n+1$.
Ahora por inducción supongamos que se cumple para β, es decir

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

y comprobémoslo para $\beta + 1$, es decir, existe un k' tal que

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

Pero $P_{k'} P_{k'-1} ... P_{n+1}(\beta+1) = P_{k'} P_{k'-1} ... P_{n+2}(\beta)$ pues $P_{n+1}(\beta+1) = \beta$ de donde por hipótesis inductiva tendremos que $H_\beta(n+2) - 1 = k'$ pero $H_\beta(n+2) = H_{\beta+1}(n+1)$ de donde obtenemos el resultado.

Ahora si α es límite tendremos $P_k P_{k-1} ... P_{n+1}(\alpha) = P_k P_{k-1} ... P_{n+1}(\{\alpha\}(n+1)) = 0$ y por tanto $H_{\{\alpha\}(n+1)}(n+1) - 1 = k$ es decir, $H_\alpha(n+1) - 1 = k$.
De manera análoga para las sucesiones débiles de Goodstein se tiene la misma fórmula con $\alpha = o_n(m_0)$. $\square$

Proposición 6.1. *Si* $\epsilon_0 > \alpha >> \beta \geq 0$, *entonces* $H_{\alpha+\beta}(n) = H_\alpha H_\beta(n)$.

Demostración. Por inducción en β. Para $\beta = 0$,

$$H_{\alpha+0}(n) = H_\alpha(n) = H_\alpha H_0(n).$$

Por inducción supongamos que se cumple para β y comprobémoslo para $\beta + 1$,

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

Finalmente supongamos que β es límite, así como $\alpha >> \beta$ entonces $\alpha + \beta$ es límite. Por hipótesis de inducción supongamos que se cumple para todo $\beta' < \beta$ y probemos que se cumple para β,

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

$\square$

Ejemplos

Mostramos algunos valores del número de pasos que se requieren para que una sucesión de Goodstein llegue a cero. Anotamos inicialmente que si k es el valor que permite que la composición $P_k P_{k-1} ... P_{n+1}(\beta)$ sea cero, entonces el correspondiente término de la sucesión es m_{k-2}.

a) Caso $m = 4$ empezando en base 2, sucesión 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 $21 = 23 - 2$.

b) Caso $m = 5$ empezando en base 2, sucesión 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 $m_{61} = 0$.

c) Caso $m = 7$, empezando en base 2, sucesión 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 $m_{2045} = 0$.

d) Caso $m = 8$, empezando en base 2, sucesión débil

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

e) Caso $m = 4$, empezando en base 2, sucesión fuerte

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

Proposición 6.2. *Para cada $k, m < \omega$, $m > 0$ se cumple $H_{\omega^k \cdot m}(n) = H^m_{\omega^k}(n)$.*

Demostración. Por doble inducción sobre k y m. Si $k = 0$ tenemos que

$$H_m(n) = m + n = H_1^m(n) \quad \text{para todo } m.$$

Ahora por hipótesis inductiva supongamos que dado un k fijo la fórmula propuesta es válida para todo $m > 0$. Comprobemos entonces para $k + 1$
Si $m = 1$

$$H_{\omega^{k+1} \cdot 1}(n) = H^1_{\omega^{k+1}}$$

Como segunda hipótesis inductiva supongamos válida la fórmula para $k+1$ y m y comprobemos para $k+1$ y $m+1$.

$$\begin{aligned} H_{\omega^{k+1}\cdot(m+1)}(n) &= H_{\{\omega^{k+1}\cdot(m+1)\}(n)}(n) \\ &= H_{\omega^{k+1}\cdot m+\omega^k\cdot n}(n) \\ &= H_{\omega^{k+1}\cdot m}H_{\omega^k\cdot n}(n) \\ &= H^m_{\omega^{k+1}}H_{\omega^{k+1}}(n) \\ &= H^{m+1}_{\omega^{k+1}}(n) \end{aligned}$$

El principio de inducción nos permite concluir que la fórmula también es válida con $k+1$ para todo $m>0$ y por lo tanto es válida para todo k y todo $m>0$. □

Proposición 6.3. *Para cada $k \in \omega$ se cumple $H_{\omega^{k+1}}(n) = H^n_{\omega^k}(n)$.*

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

Proposición 6.4. *Sean $n \in \omega$ y $\alpha \leq \epsilon_0$. Entonces $H_\alpha(n+1) > H_\alpha(n)$.*

Demostración. Por inducción en α. Si $\alpha = 0$,

$$H_0(n+1) = n+1 > n = H_0(n)$$

Supongamos que se cumple para β y comprobémoslo para $\beta+1$

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

Para el caso límite supongamos por inducción que se cumple para todo $\lambda' < \lambda$ y veamos que se cumple para λ,

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

$\square$

Proposición 6.5. *Si $\alpha < \beta \leq \epsilon_0$, entonces $H_\alpha << H_\beta$.*

Demostración. Inducción en β con α fijo. Primero supongamos que β es exactamente el sucesor de α, es decir $\beta = \alpha + 1$, así

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

y como $H_\alpha(n) < H_\beta(n)$ para todo n entonces $H_\alpha << H_\beta$.
Ahora supongamos que β es un sucesor más grande que el sucesor de α, esto es $\beta = \gamma + 1 > \alpha + 1$ y por hipótesis inductiva supongamos que se cumple para γ y comprobémoslo para $\gamma + 1$. En efecto

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

de donde podemos concluir que $H_\beta >> H_\alpha$.
Finalmente supongamos que $\alpha < \beta$ con β límite. Luego por el corolario 4.1 tenemos que existe un $k \in \mathbb{N}$ tal que para todo $n > k$, $\alpha < \{\beta\}(n)$. Ahora por inducción supongamos que se cumple para $\alpha < \{\beta\}(n) < \beta$ es decir $H_{\{\beta\}(n)} >> H_\alpha$ si $n > k$. Pero $H_{\{\beta\}(n)} >> H_\alpha$ implica que existe un $k' \in \mathbb{N}$ tal que para todo $m > k'$ $H_{\{\beta\}(n)}(m) > H_\alpha(m)$.
Tomando $\overline{k} = \max\{k, k'\}$ tendremos

$$H_\beta(n) = H_{\{\beta\}(n)}(n) > H_\alpha(n)$$

para todo $n > \overline{k}$, de donde concluimos que $H_\beta >> H_\alpha$. $\square$

6.2. H_{ω^k} es Ackermanniana

En esta sección veremos que la función H_{ω^k} es una variación de la función de Ackermann, de la cual mostramos en el capítulo 2 que su diagonal no es **pr**.

Definición 6.2. *Para cada $k < \omega$ definamos $HA_k : \omega \to \omega$ del siguiente modo:*

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

Proposición 6.6. *Para cada $k, n < \omega$,*

a) $HA_0(n) = n + 1$.

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

Demostración.

a) $HA_0(n) = H_{\omega^0}(n) = H_1(n) = H_0(n+1) = n + 1$.

b) $HA_{k+1}(n) = H_{\omega^{k+1}}(n) = H^n_{\omega^k}(n) = HA_k^n(n)$

□

Proposición 6.7.

a) $HA_1(n) = 2n$.

b) $HA_2(n) = 2^n n$.

Demostración.

a) $HA_1(n) = H_\omega(n) = H_n(n) = n + n = 2n$ por ejemplo 6.1.

b) $HA_2(n) = H_{\omega^2}(n) = H_{\{\omega^2\}(n)}(n) = H_{\omega \cdot n}(n) = 2^n n$ por ejemplo 5.

□

Proposición 6.8. *Para cada $m, n < \omega$, $n > 0$ tenemos que $HA_m(n) > n$. Esto es, el valor de la función HA_k siempre es mayor que su argumento.*

Demostración. Por inducción en m. Para $m = 0$ tenemos

$$HA_0(n) = n + 1 > n.$$

Supongamos que la proposición es válida para m y comprobémosla para $m+1$. Así, $HA_{m+1}(1) = HA_m^1(1) > 1$ y si $HA_{m+1}(n) > n$ entonces

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

El principio de inducción garantiza la validez de lo propuesto. □

Corolario 6.1. *Sean $p, q < \omega$ con $p > q$. Entonces $HA_m^p(n) > HA_m^q(n)$. Es decir que la aplicación reiterada de las funciones de Hardy produce valores cada vez mayores.*

Demostración. Como $p > q$ entonces existe un $t < \omega$ tal que $p = t + q$, luego

$$\begin{aligned}
HA_m^p(n) &= HA_m^{t+q}(n) \\
&= HA_m^t(HA_m^q(n)) \\
&> HA_m^q(n).
\end{aligned}$$

Por lo tanto concluimos que la función HA_m es mayor entre más veces se componga. □

Proposición 6.9. *Para cada* $m, n < \omega$

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

es decir que la función HA_m *es creciente para todo* m.

Demostración. Por inducción en m. Si $m = 0$ tenemos

$$HA_0(n+1) = n+2 > n+1 = HA_0(n)$$

ahora supongamos que se cumple para m y comprobemos que se cumple para $m+1$. En efecto

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

□

Proposición 6.10. *Para cada* $n > 1$, $HA_n >> A_{n+1}$. *Es decir que la función* HA_n *siempre mayorizará a la función Ackermanniana* A_{n+1}.

Demostración. Por inducción sobre n. Como $n > 1$ empezaremos nuestro caso base con $n = 2$, de donde

$$\begin{aligned} HA_2(m) &= 2^m m \\ &> 2^{m+3} - 3 \\ &= 2^m 8 - 3 \\ &= A_3(m). \end{aligned}$$

Supongamos que se cumple para n, es decir que existe un $k < \omega$ tal que

$$HA_n(m) > A_{n+1}(m)$$

para todo $m > k$ y comprobemos para $n+1$.

En efecto, como $HA_n(m) > A_{n+1}(m)$ para $m > k$ entonces $HA_nHA_n(m) > HA_nA_{n+1}(m)$ y como $A_{n+1}(m) > m > k$ tendremos

$$\begin{aligned} HA_n^2(m) &> HA_nA_{n+1}(m) \\ &> A_{n+1}A_{n+1}(m) \\ &= A_{n+1}^2(m). \end{aligned}$$

Ahora si $HA_n^t(m) > A_{n+1}^t(m)$ entonces

$$\begin{aligned} HA_n^{t+1}(m) &= HA_n^t(HA_n(m)) \\ &> A_{n+1}^t(HA_n(m)) \\ &> A_{n+1}^t(A_{n+1}(m)) \\ &= A_{n+1}^{t+1}(m). \end{aligned}$$

En particular tenemos que $HA_n^m(m) > A_{n+1}^m(m)$ para todo $m > k$.

Por otra parte tomando $m > A_{n+1}(1)$ tendremos que

$$A_{n+1}(m) > A_{n+1}^2(1).$$

Finalmente y tomando

$$m > \text{máx}\{2, k, A_{n+1}(1)\}$$

obtendremos que

$$\begin{aligned} HA_{n+1}(m) &= HA_n^m(m) \\ &> A_{n+1}^m(m) \\ &= A_{n+1}^{m-1}A_{n+1}(m) \\ &> A_{n+1}^{m-1}A_{n+1}^2(1) \\ &= A_{n+1}^{m+1}(1) \\ &= A_{n+2}(m). \end{aligned}$$

□

Proposición 6.11. *Si $f : \omega \to \omega$ es una función* ***pr****, existe un $k < \omega$ tal que $HA_k >> f$.*

Demostración. En el capítulo 2, Lema 2,1 de este trabajo vimos que si $f : \omega \to \omega$ es una función **pr** entonces existía un $k < \omega$ tal que $A_k >> f$. Por la Proposición 6.10 tenemos que $HA_j >> A_k$ con $j = k - 1$ y por la Proposición 2.7 podemos concluir que $HA_k >> f$. □

Proposición 6.12. *La función $f(n) = H_{\omega^\omega}(n) = H_{\omega^n}(n) = HA_n(n)$ no es* ***pr****.*

Demostración. Por contradicción supongamos que f es **pr**. De esta manera y por la Proposición 6,11 existe un k tal que $HA_k >> f$, equivalentemente que existe un k' tal que para todo $n > k'$

$$HA_k(n) > f(n) = HA_n(n).$$

Tomando $n > \max\{k, k'\}$ tendremos que

$$f(n) = HA_n(n) < HA_k(n)$$

lo cual es una contradicción en virtud de la proposición 6.5 pues $n > K$ implica $\omega^n > \omega^k$.

Por lo tanto podemos concluir que la función f así presentada no es una función **pr**.
□

Para el resto del trabajo necesitamos referirnos a los sistemas **AP** y **APR**. El sistema **AP** es la Axiomática de Peano, la cual permite describir las propiedades usuales de los números naturales. Estas se pueden desarrollar a partir de un conjunto de axiomas establecidos por *Giuseppe Peano* que involucra básicamente la constante 0, las nociones de sucesor, suma, producto y el principio de inducción.

El sistema **APR** es el sistema en el cual se pueden describir las funciones primitivas recursivas y se puede considerar como el mismo sistema **AP** en donde hay restricciones en el uso de cuantificadores. Si una función no es primitiva recursiva entonces no se puede demostrar en **APR** que es total (su dominio es ω).

Teorema 6.2. *Sea $m < \omega$ y denotemos por m_i su correspondiente sucesión débil de Goodstein en base $n > 1$. La función*

$$f(m) = \mu k(m_{k-2} = 0)$$

*no es **pr**.*

Demostración. Supongamos por contradicción que f es **pr**. Como

$$\begin{aligned} f(m) &= \mu k(m_k = 0) \\ &= H_\alpha(n+1) - 1 \end{aligned}$$

donde $\alpha = o_n(m_0)$ y la función constante 1 es **pr** entonces $H_\alpha(n+1) = f(m) + 1$ sería **pr**. Pero recordando que la función o lo que hace es cambiar las apariciones de la base n por ω tendremos por la Proposición 6.5 que H_α no es **pr**. Por esta contradicción concluimos que f no es una función **pr**. Por lo tanto el teorema débil de Goodstein no es demostrable en **APR**. □

CAPÍTULO 7

LA AXIOMÁTICA DE PEANO NO DEMUESTRA EL TEOREMA DE GOODSTEIN

En este capítulo presentamos el objetivo principal de este trabajo con el apoyo del teorema de *Wainer* ([8], [7]).

Hemos visto que el teorema de Goodstein puede ser representado por una función f en el sentido que el teorema es válido si y sólo si la función es total ($\mathrm{dom} f = \omega$). Para referirnos a una función que representa un teorema demostrable en **AP** decimos que ella es demostrablemente recursiva. Los resultados siguientes garantizan que la función que representa el teorema de Goodstein no es demostrablemente recursiva.

Teorema 7.1. *(Wainer) 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 $H_\alpha >> f$.

Corolario 7.1. *$H_{\epsilon_0}(n)$ mayoriza a todas las funciones demostrablemente recursivas, y por tanto*

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

Demostración. Una consecuencia inmediata de la proposición 6.5 es que si $\alpha < \epsilon_0$ entonces $H_\alpha << H_{\epsilon_0}$ y en virtud del teorema de Wainer tendremos que H_{ϵ_0} no puede ser demostrablemente recursiva y por tanto

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

□

Nota 7.1. *En palabras, la fórmula del Teorema 7.1 expresa que con la Axiomática de Peano se puede demostrar que para cada ordinal $\alpha < \epsilon_0$, la función H_α es total. En cuanto a la fórmula del Corolario 7.1, esta expresa que con la Axiomática de Peano no se puede demostrar que la función H_{ϵ_0} es total.*

Corolario 7.2. *Sea $m < \omega$, $n > 1$ y denotemos por m_i su correspondiente sucesión (fuerte) de Goodstein comenzando por m en base n; entonces*

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

Es decir que si $f(m) = \mu k(m_{k-2} = 0) = H_\alpha(n+1) - 1$, de la Axiomática de Peano no se puede deducir que esta función es total.

Demostración. Por el Teorema 6.1, $k = H_\alpha(n+1) - 1$, donde $\alpha = O_n(m)$. Pero como podemos elegir m de modo que α sea tan grande como queramos entonces $f(m) = \mu k(m_k = 0)$ no puede estar mayorizada por ningún H_β. La única función que mayoriza a $f(m)$ es H_{ϵ_0} y de esta manera $f(m)$ no puede ser demostrablemente recursiva. Por lo tanto en **AP**, **EL TEOREMA DE GOODSTEIN ES UN TEOREMA NO DEMOSTRABLE**. □

BIBLIOGRAFÍA

[1] Blasco Jose María. Notas sobre el Teorema de Goodstein. Mayo de 2005. Universidad de Barcelona.

[2] Caicedo Xavier F. *Elementos de lógica y calculabilidad*. Departamento de matemáticas, Universidad de los Andes. Bogotá. 1989. Editorial una empresa docente.

[3] Caicedo Andrés Eduardo. *Goodstein's Function*. California Institute of Technology, Pasadena, USA. 2007.

[4] E. A. Cichon. *A short proof of two Recently Discovered Independence Results Using Recursion Theoretic Methods*. Proceedings of the American Mathematical Society. (1983). 704-706.

[5] Gallego Castaño Enrique. *Técnicas de demostración de indecidibilidad e inseparabilidad en teorías formales*. Universidad Complutence de Madrid. Madrid mayo de 2001.

[6] Karel Hrbacek, Thomas Jech. *Introduction to set theory*. Third Edition. Editorial BOARD. University of Wisconsin, Milwaukee. editorial BOARD.

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

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

[9] Celis, Monica. *Teorema de Goddstein : Un Problema de Teoría de Números Resuelto con Teoría de Conjuntos*. Tesis de grado, Universidad del Cauca (2010).