Los Teoremas de Incompletitud de Gödel: Parte III: Incompletitud

Guillermo Morales Luna

Departmento de Computación
CINVESTAV-IPN

gmorales@cs.cinvestav.mx

2-o Encuentro Nacional de Epistemología y Matemáticas, Zacatecas

In Memoriam Guillermo Moreno

Contenido

Contenido

Aritmética de Peano

Signatura AP_1 de la Aritmética de Peano.

Constantes	:	Nullus	-	número cero
		I	-	número uno
		II	-	número dos
		$\vdots$		$\vdots$
		MCMXCVIII	-	número mil novecientos noventa y ocho
		$\vdots$		$\vdots$
Funciones	:	Addere	-	suma (binaria)
		Multiplicare	-	multiplicación (binaria)
Relaciones	:	$=$	-	igual a (binaria)
	:	$<$	-	menor que (binaria)

Signatura AP de la Aritmética de Peano.

Constantes	:	0	-	número cero
Funciones	:	s	-	sucesor (unaria)
Relaciones	:	$=$	-	igual a (binaria)

En AP, la relación de desigualdad queda:

$$(x \leq y) \equiv \exists z(x + z = y).$$

Con esto, sea P^- el conjunto de los siguientes axiomas propios:

$$\begin{array}{c|c}
s(x) \neq 0 & x + 0 = x \\
x \neq 0 \rightarrow s(0) \leq x & x + s(y) = s(x + y) \\
s(x) = s(y) \rightarrow x = y & x + y = y + x \\
 & (x + y) + z = x + (y + z) \\
\hline
x \cdot 0 = 0 & (x \leq y) \vee (y \leq x) \\
x \cdot s(y) = x \cdot y + y & x \cdot (y + z) = x \cdot y + x \cdot z \\
x \cdot y = y \cdot x & x + y = x + z \rightarrow y = z \\
(x \cdot y) \cdot z = x \cdot (y \cdot z) &
\end{array}$$

Sea $AP = P^- \cup EI$, donde EI es el esquema de inducción: Para cualquier fórmula ϕ,

$$\phi(0, \mathbf{x}) \wedge \forall x(\phi(x, \mathbf{x}) \rightarrow \phi(s(x), \mathbf{x})) \rightarrow \forall x(\phi(x, \mathbf{x})).$$

Estructuras-*AP*

Ejemplo

$(\mathbb{N}, id)$ es una estructura-AP, donde $\mathbb{N}$ es el conjunto de números naturales e id es la interpretación usual de los símbolos aritméticos.

Ejemplo

El conjunto de funciones de los naturales en los naturales $\mathbf{N} = \mathbb{N}^{\mathbb{N}}$ es una estructura-AP con la interpretación de los símbolos "punto-a-punto":

Cero 0	:	$\Phi(0) = \mathbf{0}$, donde $\mathbf{0} : n \mapsto 0$ es la función cero,
Sucesor s	:	$\Phi(s) : f \mapsto f'$, donde $f' : n \mapsto s(f(n))$ es la función $f + 1$,
Suma $+$	:	$\Phi(+) : (f, g) \mapsto f + g$, donde $f + g : n \mapsto f(n) + g(n)$ es la función suma punto-a-punto,
Igualdad $=$	:	$\Phi(=) = \{(f, g) \vert \forall n : f(n) = g(n)\}$, es decir, dos funciones son iguales si coinciden en cada punto.

Presentaremos una tercer estructura de AP. El filtro de Frèchet $\mathcal{F} = \{\{m \in \mathbb{N} | m \geq n\}\}_{n \in \mathbb{N}}$ es, en efecto, un filtro.

Ejemplo

*Sea $\mathcal{U}$ un ultrafiltro en $\mathbb{N}$ que extienda al filtro de Frèchet y sea $\sim_{\mathcal{U}}$ la relación en **N** definida como*

$$f \sim_{\mathcal{U}} g \;\Leftrightarrow\; \{n \in \mathbb{N} | f(n) = g(n)\} \in U.$$

*$\sim_{\mathcal{U}}$ es una relación de equivalencia congruente con las operaciones de **N** y por tanto $\mathbb{N}^* = \mathbf{N}/\sim_{\mathcal{U}}$ es una estructura-AP.*

Por ejemplo, la fórmula de la aritmética de Peano

$$\phi_0 \equiv \forall x(x \neq 0 \rightarrow \exists y(s(y) = x)$$

que asevera que todo elemento no nulo posee un antecesor es válida en $\mathbb{N}$, no lo es en **N** pues la función $x \mapsto (x \bmod 2)$ es no-nula mas no posee antecesor alguno. Sin embargo, ϕ_0 sí es verdadera en $\mathbb{N}^*$.

Veremos aquí que la aritmética de Peano no es completa. Para esto, codificaremos a la aritmética dentro de la misma aritmética y propondremos un enunciado tal que ni él ni su negación son demostrables en AP.

Para cada $n \in \mathbb{N}$ construímos el n-ésimo numeral como $\mathbf{n} = s^n(0) = \underbrace{s(\cdots s(}_{n \text{ veces}} 0) \cdots)$. Una relación $A \subset \mathbb{N}^k$ se dice representable en AP si existe una fórmula bien formada $\phi_A(x_1, \ldots, x_k)$ tal que para cualesquiera $n_1, \ldots, n_k \in \mathbb{N}$ se tiene que rigen las implicaciones

$$
\begin{array}{rcl}
(n_1, \ldots, n_k) \in A & \to & AP \vdash \phi_A(\mathbf{n}_1, \ldots, \mathbf{n}_k) \\
(n_1, \ldots, n_k) \notin A & \to & AP \vdash \neg\phi_A(\mathbf{n}_1, \ldots, \mathbf{n}_k)
\end{array}
$$

Una función $\mathbb{N}^n \to \mathbb{N}$ es representable si su gráfica lo es.

El concepto de demostrabilidad es muy algorítmico, por lo cual una demostración puede verse como un método de cálculo o de comprobación. Así pues, el resultado siguiente aparece de manera muy natural, aunque en este texto omitiremos su demostración.

Teorema (Gödel)

Una función es representable si y sólo si es recursiva. Una relación es representable si y sólo si es recursiva.

Enumeración de Gödel

Especiales:	$($	$\mapsto$	3	$) \mapsto 5$
	$,$	$\mapsto$	7	$\neg \mapsto 9$
	$\to$	$\mapsto$	11	$\forall \mapsto 13$
Variables:	x_j	$\mapsto$	$7+8j$	
Constantes:	c_j	$\mapsto$	$9+8j$	
Funciones:	f_j^n	$\mapsto$	$11+8(2^n\cdot 3^j)$	
Relaciones:	R_j^n	$\mapsto$	$13+8(2^n\cdot 3^j)$	
Cadenas:	$\xi_0\xi_1\cdots\xi_k$	$\mapsto$	$2^{g(\xi_1)}3^{g(\xi_2)}\ldots p_k^{g(\xi_k)}$	
Cadenas de cadenas:	$\sigma_0\sigma_1\cdots\sigma_k$	$\mapsto$	$2^{g(\sigma_1)}3^{g(\sigma_2)}\ldots p_k^{g(\sigma_k)}$	

(donde p_k es el k-ésimo número primo.)

Definamos las siguientes relaciones en $\mathbb{N}$:

1. *Fbf* (Fórmula bien formada):

$$Fbf(n) \ \Leftrightarrow \ \exists \phi \text{ Fbf} : n = g(\phi)$$

2. *AxL* (Axioma lógico):

$$AxL(n) \ \Leftrightarrow \ \exists \phi \text{ Fbf} : (\phi \text{ axioma lógico}) \wedge (n = g(\phi))$$

3. *AxP* (Axioma propio):

$$AxP(n) \ \Leftrightarrow \ \exists \phi \text{ Fbf} : (\phi \text{ axioma propio}) \wedge (n = g(\phi))$$

4. *Demos* (Demostración):

$$Demos(n) \ \Leftrightarrow \ \exists \Delta \in (\text{Fbf})^* : (\Delta \text{ demostración}) \wedge (n = g(\Delta))$$

5. *Dmble* (Demostrable):

$$Dmble(n) \ \Leftrightarrow \ \exists \Delta \exists m : \begin{array}{l} m = g(\Delta) \wedge Demos(m) \wedge \\ n = (\text{exponente del máximo primo que} \\ \quad \text{divide a } m) \end{array}$$

6. *Sust* (Sustitución):

$$Sust(m,n,p,q) \;\Leftrightarrow\; \exists \phi, x, t : \begin{array}{l} \phi \text{ es una fórmula que involucra a la variable } x, \\ t \text{ es un término}, \\ n = g(\phi), p = g(x), q = g(t), \text{ y} \\ m = g(\phi(x \leftarrow t)). \end{array}$$

7. *Inst* (Instanciación):

$$Inst(m,n) \;\Leftrightarrow\; \exists \phi(x) : n = g(\phi(\mathbf{m})).$$

8. *Cump* (Cúmplese):

$$Cump(m,n) \;\Leftrightarrow\; \exists \Delta, \phi(x) : \begin{array}{l} \Delta \text{ es una prueba de } \phi(\mathbf{m}), \text{ y} \\ n = g(\Delta). \end{array}$$

Proposición

Las relaciones anteriores son todas recursivas y por ende son representables en AP.

Tenemos entonces que para cualesquiera $m, n \in \mathbb{N}$:

$$\begin{array}{rcl} AP \vdash Cump(\mathbf{m}, \mathbf{n}) & \Leftrightarrow & Cump(m, n) \text{ se cumple} \\ & \Leftrightarrow & \text{para alguna fórmula } \phi(x),\ n \text{ codifica una} \\ & & \text{demostración de } \phi(\mathbf{m}), \\ AP \vdash \neg Cump(\mathbf{m}, \mathbf{n}) & \Leftrightarrow & Cump(m, n) \text{ no se cumple} \\ & \Leftrightarrow & n \text{ no codifica demostración alguna de} \\ & & \phi(\mathbf{m}), \text{ para ninguna fórmula } \phi(x). \end{array}$$

Hagamos

$\alpha_1(x_1) \equiv \forall x_2(\neg Cump(x_1, x_2))$: ningún "enunciado" de la forma $\phi(x_1)$ es demostrable, Sean $p = g(\alpha_1(x_1))$ y $\alpha \equiv \alpha_1(\mathbf{p})$.

Se ve que α asegura que ningún enunciado de la forma $\phi(\mathbf{p})$ es demostrable,
en particular, para $\phi = \alpha_1$, asevera que $\alpha_1(\mathbf{p})$ no es demostrable,
es decir, que α mismo no es demostrable.
α es un enunciado que se refiere a sí mismo y asevera su propia indemostrabilidad.

Si AP fuese consistente, entonces $AP \nvdash \alpha$.

Una teoría T, que posea un modelo que incluya a $\mathbb{N}$, es consistente-ω si para cualquier fórmula $\phi(x)$, dado que para cada $n \in \mathbb{N}$ se tuviera que $T \vdash \phi(\mathbf{n})$ entonces necesariamente $T \not\vdash \neg\forall x : \phi(x)$.

Si T es consistente-ω entonces es también consistente, a secas.

Si AP fuese consistente-ω, entonces $AP \not\vdash \neg\alpha$.

Teorema (Primero de Incompletitud de Gödel)

Si AP fuese consistente-ω entonces ha de ser incompleta.

Teorema (Segundo de Incompletitud de Gödel)

En AP no puede demostrarse su propia consistencia.

1. Si H es un conjunto inconsistente de fórmulas bien formadas entonces la teoría de H, *Teoría*(H), coincide con el conjunto de todas las fórmulas bien formadas. En otras palabras, en una teoría inconsistente cualquier cosa es demostrable.

2. Un enunciado ϕ, con número de Gödel $n = g(\phi)$, es demostrable en AP si y sólo si $AP \vdash Dmble(\mathbf{n})$ y es indemostrable en AP si y sólo si $AP \vdash \neg Dmble(\mathbf{n})$.

3. En AP se puede mostrar que 0 es distinto a $1 = s(0)$. La negación de esta desigualdad es $\phi_0 \equiv 0 = s(0)$. Así pues, tendremos que AP es consistente si y sólo si no se puede demostrar ϕ_0. Sea pues $n_0 = g(\phi_0)$ y sea $Con \equiv \neg Dmble(\mathbf{n}_0)$. El Segundo Teorema de Incompletitud de Gödel equivale a mostrar que, en efecto, $AP \not\vdash \neg Dmble(\mathbf{n}_C)$, donde $n_C = g(Con)$.

4. De acuerdo con la regla modus ponens, si $n_{12} = g(\phi_1 \rightarrow \phi_2)$, $n_1 = g(\phi_1)$ y $n_2 = g(\phi_2)$ entonces

$$AP \vdash (Dmble(\mathbf{n}_{12}) \wedge Dmble(\mathbf{n}_1) \rightarrow Dmble(\mathbf{n}_2))$$

5. Además tenemos que todo lo demostrable es demostrablemente demostrable, es decir, si $n_1 = g(\phi_1)$ y $n_2 = g(Dmble(\mathbf{n}_1))$ entonces

$$AP \vdash (Dmble(\mathbf{n}_1) \rightarrow Dmble(\mathbf{n}_2))$$

6. Por todo lo anterior, para probar el Segundo Teorema de Incompletitud basta ver que *Con* es demostrablemente equivalente en AP al enunciado α demostrado indemostrable en el Primer Teorema de Incompletitud.

Utilicemos la notación $\phi(\lceil\xi\rceil)$ para denotar a la fórmula $\phi(\mathbf{n})$ donde $n = g(\xi)$.

Veamos primero $AP \vdash \alpha \rightarrow Con$:

$$\begin{array}{rcl} AP \vdash (0 = s(0)) \rightarrow \alpha & \Rightarrow & AP \vdash Dmble(\lceil (0 = s(0)) \rightarrow \alpha \rceil) \\ & \Rightarrow & AP \vdash Dmble(\lceil (0 = s(0)) \rceil) \rightarrow Dmble(\lceil \alpha \rceil) \\ & \Rightarrow & AP \vdash \neg Dmble(\lceil \alpha \rceil) \rightarrow \neg Dmble(\lceil (0 = s(0)) \rceil) \\ & \Rightarrow & AP \vdash \alpha \rightarrow Con \end{array}$$

pues $AP \vdash \alpha \rightarrow \neg Dmble(\lceil \alpha \rceil)$.

Recíprocamente, veamos $AP \vdash Con \to \alpha$:

$$
\begin{aligned}
& AP \vdash Dmble(\ulcorner\alpha\urcorner) \to Dmble(\ulcorner Dmble(\ulcorner\alpha\urcorner)\urcorner) \\
\Rightarrow\quad & AP \vdash Dmble(\ulcorner\alpha\urcorner) \to Dmble(\ulcorner\neg\alpha\urcorner) \\
\Rightarrow\quad & AP \vdash Dmble(\ulcorner\alpha\urcorner) \to Dmble(\ulcorner\alpha \wedge \neg\alpha\urcorner) \\
\Rightarrow\quad & AP \vdash Dmble(\ulcorner\alpha\urcorner) \to Dmble(\ulcorner 0 = s(0)\urcorner) \\
\Rightarrow\quad & AP \vdash \neg Dmble(\ulcorner 0 = s(0)\urcorner) \to \neg Dmble(\ulcorner\alpha\urcorner) \\
\Rightarrow\quad & AP \vdash Con \to \alpha
\end{aligned}
$$

$\square$

Contenido

Los teoremas que hemos visto hasta ahora indemostrables en la aritmética de Peano son enunciados autoreferentes.
Veremos un teorema de “tipo aritmético” que independiente en la aritmética de Peano, es decir, tal que ni él ni su negació son demostrables en AP.

Representación formal en base m

Sea $m \geq 2$. Para cada $a \in N$ definimos $rp_m(a)$ como sigue:

$$\begin{array}{llll}
\text{i)} & a \leq m^m - 1 & \Rightarrow & \exists! a_0, \ldots, a_{m-1} \in [0, m-1] : \\
 & & & a = \sum_{i=0}^{m-1} a_i \cdot m^i \\
 & & \Rightarrow & rp_m(a) = \sum_{i=0}^{m-1} a_i \cdot m^i \\
\text{ii)} & a \geq m^m & \Rightarrow & \exists! a_0, \ldots, a_{\lceil \log_m(a) \rceil - 1} \in [0, m-1] : \\
 & & & a = \sum_{i=0}^{\lceil \log_m(a) \rceil - 1} a_i \cdot m^i \\
 & & \Rightarrow & rp_m(a) = \sum_{i=0}^{\lceil \log_m(a) \rceil - 1} a_i \cdot m^{rp_m(i)}
\end{array}$$

Ejemplo

Para $m = 2$ *y* $a = 100$ *tenemos*

$$a = 1100100_2 = 2^6 + 2^5 + 2^2,$$

luego

$$rp_2(100) = 2^{2^2+2} + 2^{2^2+1} + 2^2.$$

Escribamos $rp(a, m) = rp_m(a)$.
Con esta notación denotaremos por $rp(a, k|m)$ al resultado de sustituir a m por k en $rp(a, m)$.

Sucesión de Goodstein

Para $a \in N$ y $m \geq 2$ dados, definiremos a la sucesión de Goodstein $S(a, m) = \{s_n(a, m)\}_{n\geq 0}$ de manera recursiva. Para ello nos auxiliaremos de la sucesión $B(a, m) = \{b_n(a, m)\}_{n\geq 0}$ definida igualmente de manera recursiva. Explícitamente, hacemos

$$
\begin{array}{rlcl}
 & b_0 = m & ; & s_0 = a \\
\forall n \geq 0 : & b_{n+1} = b_n + 1 & ; & s_{n+1} = rp(s_n, b_{n+1} | b_n) - 1
\end{array}
$$

Ejemplo

Para $m = 2$ *y* $a = 100$ *tenemos* $rp_2(100) = 2^{2^2+2} + 2^{2^2+1} + 2^2$.

Los primeros términos de la sucesión de Goodstein son:

$$
\begin{array}{rcl}
s_0(100,2) & = & 2^{2^2+2} + 2^{2^2+1} + 2^2 \\
 & = & 100 \\
s_1(100,2) & = & 3^{3^3+3} + 3^{3^3+1} + 3^3 - 1 \\
 & = & 3^{3^3+3} + 3^{3^3+1} + 2 \cdot 3^2 + 2 \cdot 3 + 2 \\
 & = & O(3^{27}) \\
s_2(100,2) & = & 4^{4^4+4} + 4^{4^4+1} + 2 \cdot 4^2 + 2 \cdot 4 + 1 \\
 & = & O(2^{512}) \\
\vdots & & \vdots
\end{array}
$$

Sorpresivamente tenemos que ... ¡la sucesión de Goodstein converge a cero!

Teorema (de Goodstein)

$\forall a \forall m \exists n: \; s_n(a, m) = 0.$

El teorema se cumple en $\mathbb{N}$: el modelo estándar de los números naturales. Sin embargo no es demostrable en la aritmética de Peano, pues, en términos de (a, m), el mínimo n que anula a la sucesión de Goodstein crece vertiginosamente rápido.

Función de Goodstein

Definimos a la función G como

$$G : (a, m) \mapsto G : (a, m) = \min\{n | s_n(a, m) = 0\}.$$

Puede probarse que la diagonal de G "domina" a cualquier función recursiva, es decir:

$$\forall f \in \{\text{funciones recursivas}\}\exists n_0 : \; n \geq n_0 \; \rightarrow \; f(n) < G(n, n),$$

con fines de la exposición aquí, y sin entrar en detalles técnicos, podemos pensar que las funciones recursivas son precisamente las funciones efectivamente computables. Se tiene, en consecuencia, que:

- G no puede ser recursiva y
- el Teorema de Goodstein no es demostrable formalmente, pues
  - una demostración formal de él daría un algoritmo para calcular G, y no puede existir tal algoritmo pues la función que calcularía tal algoritmo estaría acotada a la larga por G.

Supongamos que el número a es de la forma $a = a_i \cdot m^i$, donde $i < m$, con $a_i < m$.
Al calcular la sucesión de Goodstein, el término que le sigue a a es precisamente

$$\begin{aligned} a_i \cdot (m+1)^i - 1 &= (a_i - 1) \cdot (m+1)^i + \\ &\quad (m+1)^i - 1 \\ &= (a_i - 1) \cdot (m+1)^i + \\ &\quad m \cdot (m+1)^{i-1} + \cdots + m \cdot (m+1) + m \end{aligned}$$

Así pues

- se ha decrementado en uno el dígito más significativo de la expresión formal, aunque
- se han "restablecido" los demás dígitos a sus máximos valores posibles. Sin embargo,
  - estos dígitos son estrictamente menores que la base actual,
  - no se modificarán más al calcular la sucesión: ¡Sólo pueden decrecer!
- Al cabo de un cierto número de iteraciones los dígitos menos significativos se anularán.
- En este momento el término actual es de la forma inicial pero se ha decrementado en una unidad el dígito más significativo.

Algunos valores explícitos de la función

Calcularemos valores para argumentos de la forma $(a \cdot m^i, m)$ donde $a \in [1, m-1]$, $i \in [0, m-1]$ y $m \geq 2$.
Definamos

$$\begin{array}{rcl} p(i,a,m) & = & \min\{k | s_k(a \cdot m^i, m) = 0\}, \\ q(i,a,m) & = & \min\{k | s_k(a \cdot m^i, m) = (a-1)\cdot(m+k)^i\}. \end{array}$$

Entonces incialmente, para $i = 0$, se tiene $q(0, a, m) = 1$ y $p(0, a, m) = a$.
Recursivamente, para $i \geq 1$, los valores de q y de p se calculan según

```
s := 1 ;
for j = 0 to i − 1 do
    {r := p(j, m, m + s) ;
    s := s + r } ;
q(i, a, m) := s
```

```
s := 0 ;
for b = 0 to a − 1 do
    {r := q(i, a − b, m + s) ;
    s := s + r } ;
p(i, a, m) := s
```

Equivalentemente, se tiene las recurrencias siguientes:

$$\left\{\begin{array}{rcl} q(0,a,m) & = & 1 \\ q(i,a,m) & = & q(i-1,a,m)+p(i-1,m,m+q(i-1,a,m)) \end{array}\right.$$

y

$$\left\{\begin{array}{rcl} p(0,a,m) & = & a \\ \left\{\begin{array}{l} p(i,1,m) \\ p(i,a,m) \end{array}\right. & \begin{array}{c} = \\ = \end{array} & \begin{array}{l} q(i,1,m) \\ q(i,a,m)+p(i,a-1,m+q(i,a,m)) \end{array} \end{array}\right.$$

De aquí se puede ver que q es "constante respecto a m",

$$\forall a:\ q(i,a,m)=q(i,1,m).$$

Proposición

Supongamos que $h_i : N \longrightarrow N$ *es una función tal que* $\forall a, m: \; q(i, a, m) = h_i(m) - m$. *Entonces*

1. $p(i, a, m) = h_i^a(m) - m.$
2. $q(i + 1, a, m) = h_i^{m+1}(m) - m.$

Tan sólo para ilustrar los crecimientos de las funciones h_i observamos:

$$\begin{aligned} h_0(m) &= m+1 \\ h_1(m) &= 2m+1 \\ h_2(m) &= 2^{m+1}(m+1)-1 \end{aligned}$$

Para ilustrar el crecimiento de h_3 veamos las primeras iteraciones de h_2:

$$\begin{aligned} h_2^2(m) &= 2^{1+m+2^{1+m}(1+m)}(1+m)-1 \\ h_2^3(m) &= 2^{1+m+2^{1+m}(1+m)+2^{1+m+2^{1+m}(1+m)}(1+m)}(1+m)-1 \\ h_2^4(m) &= 2^{1+m+2^{1+m}(1+m)+2^{1+m+2^{1+m}(1+m)}(1+m)+2^{1+m+2^{1+m}(1+m)+2^{1+m+2^{1+m}(1+m)}(1+}} \end{aligned}$$

Pues bien

$$h_3(m) = h_2^{m+1}(m).$$

Los crecimientos de h_i con $i \geq 4$ son ciertamente inimaginables.

$G(a, m)$ **con** $a < m^m$

Hemos visto que si a es de la forma $a = a_i \cdot m^i$ entonces $G(a, m) = p(i, a_i, m)$.
Ahora, si $a < m^m$ tenemos que $\exists a_0, \ldots, a_{m-1} \in [0, m-1]$ tales que $a = \sum_{i=0}^{m-1} a_i \cdot m_i$.
En este caso, $G(a, m)$ es el número de veces que hay que aplicar la construcción de Goodstein para anular a todos los dígitos a^i. Teniendo en cuenta que en cada iteración se incrementa la base, vemos que $G(a, m)$ se calcula mediante el algoritmo siguiente:

$$\boxed{\begin{array}{l} s := 0 \ ; \\ \textbf{for } i = 0 \textbf{ to } m-1 \textbf{ do} \\ \quad \{r := p(i, a_m, m+s) \ ; \\ \quad s := s + r \ \} \ ; \\ G(a, m) := s \end{array}}$$

Contenido

En la primera mitad del siglo XIX Catalan conjeturó que las únicas potencias sucesivas en los naturales son 8 y 9. En otras palabras:

Conjetura de Catalan

$$\forall x, n, y, m: \; x^n - y^m = 1 \Leftrightarrow x = 3 \wedge n = 2 \wedge y = 2 \wedge m = 3.$$

Hasta ahora la conjetura de Catalan ha permanecido abierta.
Sin embargo ha habido “algunos avances”.

Proposición (Tijdeman, 1970)

Si $(x, n, y, m) \in N_2^4$ *es una solución de la ecuación de Catalan entonces existe una constante* C *efectivamente computable, tal que* $\max(x, n, y, m) \leq C$.

El problema entonces es estimar la constante C.

Proposición (Langevin, 1976)

La constante C *satisface la desigualdad* $C \leq exp(exp(exp(exp(730))))$.

Ya que $\exp(x) = 10^{\log(e^x)} = 10^{x \cdot \log(e)}$ y $\log(e) = 0.4342944819033\ldots$

$\exp(730)$	se escribe (en decimal) con casi $\frac{730}{2}$ dígitos,
$\exp(\exp(730))$	tiene una longitud (en decimal) que se escribe con casi $\frac{730}{2}$ dígitos,
$\exp(\exp(\exp(730)))$	tiene una longitud (en decimal) cuya longitud se escribe con casi $\frac{730}{2}$ dígitos,
$\exp(\exp(\exp(\exp(730))))$	tiene una longitud (en decimal) cuya longitud tiene una longitud cuya longitud se escribe con casi $\frac{730}{2}$ dígitos,

El número de átomos en el Universo es "apenas" del orden de 10^{100}. Luego, si contamos un "Universo" por cada átomo del Universo tendremos 10^{200} átomos. A esta cantidad habría que multiplicarla por 10^{65} para obtener sólo la primera cantidad de la lista anterior.

Proposición (Baker, 1982)

Para soluciones x, n, y, m de la ecuación de Catalan, con los cuatro números mayores o iguales que 3, se ha de tener necesariamente que

$$\max(x, y) \leq \min\left\{exp\left(exp\left((5n)^{10} m^{10m^3}\right)\right), exp\left(exp\left((5m)^{10} n^{10n^3}\right)\right)\right\}.$$

Fijos n y m, para buscar las posibles soluciones (x, y) utilizando una CRAY se necesitaría una cantidad de tiempo comparada con la cual toda la edad del Universo equivaldría a un mero parpadeo.
Sin embargo, ¡¡todo lo involucrado es computable!!

Contenido

Referencias

- Barwise (ed): *Handbook of Mathematical Logic*, Studies in Logic and the Foundations of Mathematics, Vol. 90. North-Holland Publishing Co., 1977.
- Bell, Machover: *Introduction to Mathematical Logic*, North-Holland, 1978.
- Bell, Slomson: *Models and Ultraproducts: An Introduction*, North-Holland, 1969.
- Cuena: *Lógica Informática*, Alianza Informática, 1987.
- Chang, Lee: *Symbolic Logic and Mechanical Theorem Proving*. Academic Press, 1973.
- Davis: *The Undecidable. Basic Papers on Undecidable Propositions, Unsolvable Problems and Computable Functions*. Raven Press, 1965.
- Enderton, *A Mathematical Introduction to Logic*, Academic Press, 1972.
- Gabbay, Hogger, Robinson, (editors): *Handbook of Logic in Artificial Intelligence and Logic Programming*, Oxford University Press, 1993.

- Gödel, Kurt. 1931. On formally undecidable propositions of *Principia mathematica* and related systems I. In Gödel, 1986, pp. 145-195. Originally published as "Über formal unentscheidbare Sätze der *Principia mathematica* und verwandter Systeme I", *Monatshefte für33 Mathematik und Physik*, 38, pp. 173-198.
- Gödel, Kurt. 1986. *Collected Works*, vol. I. Oxford University Press.
- Hamilton: *Logic for Mathematicians*. Cambridge University Press, 1978.
- Hintikka, J. *Knowledge and belief*, Cornell University Press, 1962.
- Jech, T., *Set Theory*, Academic Press, 1978.
- Kleene: *Introduction to Metamathematics*. Wolters-Noordhoff, 1980.
- Kleene: *Mathematical Logic*. Wiley, 1976.
- Manin: *A Course in Mathematical Logic*. Springer-Verlag, 1977.

- Mendelson: *Introduction to Mathematical Logic*. Van Nostrand (Third Edition), 1987.
- Paris, J., *The uncertain reasoner's companion - a mathematical perspective*, Cambridge University Press, 1994.
- Robinson: *Logic: Form and functions: The Mechanization of Deductive Reasoning*. North-Holland, 1979.
- Shoenfield: *Mathematical Logic*, Addison-Wesley Publishing Co., 1967.
- Smorynski: What's New in Logic?, *Math. Intelligencer*, 7, no. 3, 53–54, 1985.
- van Heijenoort, Jean (ed.). 1967. *From Frege to Gödel: A Source Book in Mathematical Logic*, 1879-1931. Harvard University Press, Cambridge, MA.