7 2y

Universidad Nacional Autónoma de México

FACULTAD DE CIENCIAS

LA SOLUCION DEL DECIMO PROBLEMA DE HILBERT Y SU RELACION CON EL TEOREMA DE GODEL

Tesis que presenta

JOSE JORGE MAX FERNANDEZ DE CASTRO TAPIA

para obtener el título de

M A T E M A T I C O

México, D. F., septiembre de 1988

I N D I C E

INTRODUCCION

En agosto de 1900, en el II Congreso Internacional de matemáticos, celebrado en París, el alemán David Hilbert planteó 23 problemas desde entonces conocidos universalmente. Pretendía anticipar y, en buena medida, determinar, los temas y alcances prevenibles del desarrollo de las Matemáticas para el siglo que comenzaba. El presente trabajo tiene relación con dos de estos 23 problemas: el segundo, a) que puede enunciarse como el de "la no contradicción de los axiomas de la Aritmética", y el décimo b) que se refiere a "la posibilidad de resolver una ecuación diofantina", y cuyos enunciados textuales son, respectivamente:

a) Demostrar que los axiomas de la Aritmética no son contradictorios; i.e. demostrar que, basándose en los axiomas, no se podrá jamás llegar a resultados contradictorios por medio de un número finito de deducciones lógicas.

b) Se da una ecuación de Diofanto con un número arbitrario de incógnitas y coeficientes enteros racionales; se pide encontrar un método por medio del cual, a través de un número finito de operaciones, se pueda distinguir si la ecuación es resoluble en números enteros racionales.

Treinta años más tarde, el matemático checoslovaco Kurt Gödel demostró en su famoso "teorema de incompletud", la imposibilidad de resolver satisfactoriamente el 2° problema, que aquí enunciamos en a). Sin embargo, con base en la teoría contenida en dicho teorema diversos autores como S. Kleene, Martin Davis, Julia Robinson y otros, hicieron aportaciones significativas para la evolución conceptual del décimo problema, aquí señalado como b) mismo que fue finalmente resuelto por Matiyasèvic, en 1970.

Lo que tratamos en las páginas siguientes es de demostrar el teorema de Gödel partiendo de la solución del décimo problema de Hilbert, b) que también exponemos. La vinculación de ambos temas la encontramos sugerida en diversos artículos (véase bibliografía, Nos. 4,6 y 8) y nuestra contribución es el desarrollo detallado de dicha relación, todo ello dentro de un marco que rebasa en amplitud dichos temas y que es el de la teoría de la calculabilidad.

El autor agradece al maestro Carlos Torres Alcaraz su generosa guía y auxilio, y a la candidata a doctor Yolanda Torres Falcón la revisión que hizo del 5° capítulo y los consejos recibidos para su elaboración.

CAPITULO I

ALGORITMOS DE MARKOV

El décimo problema de Hilbert consiste en hallar un procedimiento efectivo para responder a una cierta clase de preguntas. Si se pretendiera demostrar que tal procedimiento existe, bastaría exhibir uno que cumpliera con las condiciones exigidas. En cambio, si se trata, como es realmente el caso, de probar que 'está condenada al fracaso toda tentativa de resolver así el problema', es necesario definir matemáticamente, y con todo rigor lo que significan las palabras 'procedimiento efectivo' ó 'cálculo' o bien 'algoritmo'. En 1900 aludían a una noción ordinaria en la práctica de todo matemático, a algo frecuente en su trabajo cotidiano, pero no a un concepto claro y exacto. Sólo después de que Gödel demostró, en 1931, su célebre teorema de incompletud, fue posible elaborar una teoría que definiera satisfactoriamente tales términos. En este primer capítulo expondremos en sus líneas mas elementales esa teoría que permitió la solución definitiva del problema sucodicho.

El primer ejemplo de lo que es un algoritmo nos viene de la Aritmética. Un cálculo aritmético es una forma mecánica de manipular signos de acuerdo a reglas fijas. Se parte de ciertos datos, y después de un número de pasos, que puede ser muy grande, pero que siempre es finito, se llega al resultado. Un algoritmo es un instructivo detallado que permite realizar una operación compleja, digamos sumar o multiplicar, sabiendo hacer otra mas sencilla, como el reconocimiento de signos ó del lugar que éstos ocupan en una expresión, y del reemplazo de unos por otros. Usamos casi indistintamente 'cálculo' ó 'algoritmo'. Si bien este último término alude mas al instructivo, a las reglas fijas de que estamos hablando, mientras que el primero se refiere mas al seguimiento o puesta en marcha de ese instructivo. La palabra 'procedimiento' recoge bien ambos sentidos.

En principio para cada algoritmo puede construirse una máquina que lo realice. Así que la pregunta por el poder de los procedimientos algorítmicos es la pregunta por la naturaleza y el alcance de las máquinas calculadoras o digitales.

En los años treintas, fueron dadas varias definiciones matemáticas de lo que es un algoritmo: las máquinas de Turing, las de Post, la calculabilidad λ de Church, los algoritmos de Markov. Todas ellas resultaron equivalentes. La tesis de Church afirma que corresponden adecuadamente esas caracterizaciones de la calculabilidad, a lo que, desde un punto de vista intuitivo, se entiende con la palabra 'algoritmo'. Obviamente que la tesis de Church no puede ser probada. La situación es similar a la que se da en Análisis cuando se pasa de la vaga noción de area bajo una curva al concepto preciso de integral de una función, o cuando se equipara la idea que tenemos de continuidad de una curva con la definición respectiva con épsilons y deltas. Sin embargo, en todos estos casos hay buenas razones para aceptar la definición que se propone. Lo mismo ocurre con la tesis de Church. Mas adelante habiendo estado en contacto directo con cierta clase de algoritmos discutiremos algunos elementos que se aducen en su apoyo.

En este capítulo estudiaremos los algoritmos de Markov Esta presentación seguirá muy de cerca a la que hace Mendelson (1964), que a su vez se aproxima mucho a la de Markov (1954). Haremos primeramente, algunas consideraciones relativas al lenguaje a emplear. En seguida vendrá la definición de los algoritmos normales o de Markov, con algunos ejemplos que no sólo aclararán el sentido de los términos, sino que serán útiles en el desarrollo posterior de la Teoría. Veremos algunas convenciones notacionales y de elección de alfabeto que permitirán el uso de algoritmos para el cálculo de funciones numéricas comunes. Algunos ejemplos harán plausible la idea de que las funciones Markov calculables abarcan todas las operaciones importantes de la Aritmética elemental. Finalmente demostraremos que la clase de estas funciones es cerrada bajo composición y minimalización.

Visto desde un cierto ángulo, un algoritmo es una regla de transformación de expresiones de un cierto lenguaje. Estas expresiones no son sino sucesiones de un número por lo común pequeño de símbolos, que adecuadamente combinados producen una cantidad enorme de 'palabras'. Podemos considerar al espacio en blanco que separa una palabra de otra como un símbolo más del lenguaje. Para fijar ideas asumimos que los símbolos de cualquier alfabeto están tomados de la sucesión $a_0, a_1, a_2, \ldots$

Definicion 1.1 Un alfabeto A es un subconjunto finito o numerable del conjunto $\{a_0, a_1, a_2, \ldots\}$.
Una palabra de A es una sucesión finita o vacía de elementos de A. Si $P = a_{j_1} a_{j_2} \ldots a_{j_n}$ con $j_i \in \mathbb{N}$ (donde no todos los a_{j_i}'s son necesariamente distintos) llamamos a n la longitud de P y la denotamos $\ell(p)$. En particular la palabra vacía tiene longitud 0.

No es necesario trabajar con alfabetos muy grandes porque todo lo que en ellos puede hacerse es susceptible de 'traducción' a un alfabeto de tan sólo 2 letras o símbolos. Denotaremos con W_A (o W simplemente si A se sobreentiende) al conjunto de todas las palabras de un alfabeto A.

Una operación elemental entre dos palabras X y Y es la yuxtaposición que denotaremos por XY. Desde luego que $\Lambda X = X\Lambda = X$ (Λ es la palabra vacía) y $\ell(XY) = \ell(X) + \ell(Y)$

Definición 1.2 Una palabra P ocurre en una palabra Q si existen S y $T \in W$

tales que $q = spr$ donde s ó r pueden ser la palabra vacía.

En este contexto un algoritmo es una función efectivamente calculable que tiene por dominio a un subconjunto de W y con valores en W*. La mayoría de los algoritmos se descomponen en unos cuantos pasos muy sencillos. La idea de Markov es que todos pueden construirse partiendo de una operación: la substitución de una palabra por otra. Antes de dar la definición precisa de algoritmo normal o de Markov vamos a describir su significado desde un punto de vista operativo.

El esquema de un algoritmo normal U es una lista finita de la forma

$$
\begin{array}{l}
P_1 \rightarrow (\cdot)\, q_1 \\
P_2 \rightarrow (\cdot)\, q_2 \\
\vdots \qquad\quad \vdots \\
P_n \rightarrow (\cdot)\, q_n
\end{array}
$$

donde $P_1, q_1, P_2, q_2, \ldots P_n, q_n \in W$ y $P_n = q_n = \Lambda$. Las expresiones $P_i \rightarrow (\cdot) q_i$ se llaman producciones. Unas son simples $P_i \rightarrow q_i$, y otras son terminales $P_i \rightarrow \cdot q_i$. La notación $P_i \rightarrow (\cdot) q_i$ representa cualquiera de estos dos casos, es decir, denota a $P_i \rightarrow q_i$ ó a $P_i \rightarrow \cdot q_i$. El punto indicará la instrucción de finalizar el proceso después de realizar la operación correspondiente. Diremos de P_i que es el antecedente de la producción y de q_i que es el consecuente. Este esquema es una prescripción para calcular los valores de $U: V \subset W \rightarrow W$. Equivale a: Dada una palabra P busque la P_i de índice menor en el esquema que ocurra en P (alguna tiene que haber pues $P_n = \Lambda$ ocurre en toda palabra; $P = \Lambda P$). Substituya la primera ocurrencia (de izquierda a derecha) de esa P_i en P por q_i. Llamemos al resultado de esa substitución P'. Si la producción hallada $P_i \rightarrow (\cdot) q_i$ es terminal, entonces el proceso habrá terminado y $U(P) = P'$. Si es simple, el proceso debe repetirse para P'. Ahora bien, hay dos posibilidades: 1) que después de realizados varios pasos se tenga la palabra R y que la producción $P_j \rightarrow \cdot q_j$ sea la de índice menor en U tal que su antecedente ocurre en R. Entonces el valor de U para P ($U(P)$) será el resultado de reemplazar la primera ocurrencia de P_j

*Suponemos aquí un alfabeto dado fijo.

en R por q_j. Diremos que P está en el dominio de U o que U se aplica a P. Ó 2) que no sea ese el caso, sino que el proceso se reitere para siempre. Diremos entonces que U no calcula para P.

Ejemplo 1 Sea $A = \{a_0, a_1\}$. Considere el esquema

$$U: \quad a_0 \to .\, a_1$$
$$a_1 \to a_0$$
$$\Lambda \to .\, \Lambda$$

y $U(a_1 a_0 a_1) = a_1 a_1 a_1$ pues el primer renglón de la tabla o esquema nos indica efectuar en $a_1 a_0 a_1$ la substitución de a_0 por a_1 y detenernos

$U(a_1 a_1 a_1) = a_1 a_1 a_1$ (observe que aquí se aplica primero la segunda producción de U, obteniéndose el resultado parcial $a_0 a_1 a_1$ que a su vez se transforma en $a_1 a_1 a_1$ por efecto de la primera producción).

$U(a_1 a_0) = a_1 a_1$ y $U(a_0 a_0) = a_1 a_0$

El efecto del algoritmo determinado por este esquema es el de transformar cada palabra que contenga por lo menos una ocurrencia de a_0 en la palabra que resulta al reemplazar la ocurrencia mas a la izquierda de a_0 por a_1 las demás palabras quedan inalteradas al aplicarles U

Ejemplo 2. Sea $A = \{a_0, a_1, a_2\}$. Considere el esquema

$$U: \quad a_1 \to \Lambda$$
$$\Lambda \to .\, \Lambda$$

$U(a_0 a_0 a_2) = a_0 a_0 a_2$, $U(a_1 a_1 a_0) = a_0$, $U(a_0 a_1 a_2 a_1 a_2) = a_0 a_2 a_2$

El efecto del algoritmo normal correspondiente a este esquema es el de borrar en las palabras toda ocurrencia de a_1.

Ejemplo 3 Sea $A = \{a_0, \dots, a_n\}$. Considere

$$U: \Lambda \to .\, a_3$$
$$\Lambda \to .\, \Lambda$$

$U(P) = a_3 P$ para cualquier palabra P

Ejemplo 4 Sea $A = \{a_0, a_1, a_2, a_3\}$ y U determinado por:

$$a_0a_1 \to a_1a_0$$
$$a_0a_2 \to a_2a_0$$
$$a_0a_3 \to a_3a_0$$
$$a_0a_0 \to a_0$$
$$a_0 \to \cdot a_0$$
$$\Lambda \to a_0$$
$$\Lambda \to \cdot\Lambda$$

Este esquema puede abreviarse así

$$a_0\xi \to \xi a_0 \quad (\xi \in A - \{a_0\})$$
$$a_0a_0 \to a_0$$
$$a_0 \to \cdot a_0$$
$$\Lambda \to a_0 \;.$$
$$\Lambda \to \cdot\Lambda$$

(Siempre que usemos tales abreviaturas se entenderá que éstas representan a las correspondientes producciones dadas en cualquier orden)

$U(a_1a_2a_0a_3a_1) = a_1a_2a_3a_1a_0$, $U(a_3a_2a_0) = a_3a_2a_0$, $U(a_3a_2) = a_3a_2a_0$

$U(a_0a_1a_0a_0a_2) = a_1a_2a_0$

El efecto de U es el de agregar por la derecha a_0 a cualquier palabra no terminada en a_0, y eliminar toda otra ocurrencia de este símbolo.

Ejemplo 5. Sea $A = \{a_0, a_1, a_2\}$ y U definido por

$$a_0 \to a_1$$
$$a_1 \to a_0$$
$$a_2 \to \cdot a_2a_2$$
$$\Lambda \to \cdot\Lambda$$

A diferencia de los otros ejemplos, en éste U no está definido para todo elemento de W_A; sólo se aplica a palabras que no contengan a_0 ni a_1. $U(a_2a_2) = a_2a_2a_2$ y $U(\Lambda) = \Lambda$

Consideremos una producción $P_i \to (\cdot)q_i$ como una función f_i que se aplica exclusivamente a palabras P en las que P_i ocurre y sea

$f_i(P)$ es el resultado de substituir la primera ocurrencia de P_i en P por Q_i. (Notación: sea $\overline{\overline{n}} = \{1, 2, \dots, n\}$ para cada número natural $n > 0$)

Definición 1.3 El algoritmo normal o de Markov U determinado por el esquema

$$f_1 : P_1 \to Q_1$$
$$f_2 : P_2 \to Q_2$$
$$\vdots \qquad \vdots$$
$$f_n : P_n \to Q_n$$

donde f_n es terminal y $P_n = Q_n = \Lambda$, es la función $U : D \subset W \to W$, tal que dadas las palabras P y Q de A, $U(P) = Q$ si y sólo si existe una sucesión $W_1, W_2, \dots, W_m \in W$ con las siguientes propiedades

1) $W_1 = P$ y $W_n = Q$

2) Para cada $i \in \overline{\overline{m-1}}$ sea j_i el menor número que pertenece a $\overline{\overline{n}}$ tal que f_{j_i} se aplica a W_i, entonces $f_{j_i}(W_i) = W_{i+1}$

3) Si $i \in \overline{\overline{m-2}}$, f_{j_i} es simple.

4) $f_{j_{m-1}}$ es terminal

Definición 1.4. Si A y B son 2 alfabetos, B es extensión de A si $A \subseteq B$. Por un algoritmo sobre A entendemos un algoritmo en una extensión de A

Eventualmente, y por conveniencia, emplearemos letras distintas de las a_i's como símbolos de un alfabeto.

Ejemplo 6 Sea $A = \{a_0, \dots a_n\}$ y U el algoritmo con esquema

$$\xi \to \cdot\Lambda \qquad \xi \in A$$
$$\Lambda \to \cdot\Lambda$$

U borra la primera letra de toda palabra no vacía

* Nuevamente suponemos un alfabeto dado fijo A; y del algoritmo U aquí definido diremos que es un algoritmo en A.

Ejemplo 7 Sea A un alfabeto arbitrario $\{a_0, a_1, \ldots, a_n\}$ y α, β, γ tres letras que no pertenecen a A. Sea U el algoritmo normal en el alfabeto $B = A \cup \{\alpha, \beta, \gamma\}$ dado por:

a)	$\alpha\xi \to \xi\gamma\beta\xi$	$\xi \in A$
b)	$\beta\eta\xi \to \xi\beta\eta$	$\xi, \eta \in A \cup \{\gamma\}$
c)	$\beta\xi \to \gamma\xi$	$\xi \in A$
d)	$\gamma\gamma\gamma \to \gamma\gamma$	
e)	$\gamma\gamma\xi \to \xi\gamma\gamma$	$\xi \in A$
f)	$\gamma\xi \to \alpha\xi$	$\xi \in A$
g)	$\gamma\gamma \to .\Lambda$	
h)	$\Lambda \to \alpha$	
i)	$\Lambda \to .\Lambda$	

Para cualquier palabra P, $U(P) = PP$. Veámoslo en el caso particular $P = a_0a_1a_2$. Indicaremos el efecto de U sobre P, paso a paso, del siguiente modo:

$$a_0a_1a_2 \xrightarrow{(h)} \alpha a_0a_1a_2 \xrightarrow{(a)} a_0\gamma\beta a_0a_1a_2 \xrightarrow{(b)} a_0\gamma a_1\beta a_0a_2 \xrightarrow{(b)} a_0\gamma a_1a_2\beta a_0 \xrightarrow{(c)}$$

$$a_0\gamma a_1a_2\gamma a_0 \xrightarrow{(f)} a_0\alpha a_1a_2\gamma a_0 \xrightarrow{(a)} a_0a_1\gamma\beta a_1a_2\gamma a_0 \xrightarrow{(b)\ldots} a_0a_1\gamma a_2\gamma a_0\beta a_1 \xrightarrow{(c)}$$

$$a_0a_1\gamma a_2\gamma a_0\gamma a_1 \xrightarrow{(f)} a_0a_1\alpha a_2\gamma a_0\gamma a_1 \xrightarrow{(a)} a_0a_1a_2\gamma\beta a_2\gamma a_0\gamma a_1 \xrightarrow{(b)}$$

$$a_0a_1a_2\gamma\gamma\beta a_2a_0\gamma a_1 \xrightarrow{(b)\ y\ (c)} a_0a_1a_2\gamma\gamma a_0\gamma a_1\gamma a_2 \xrightarrow{(e)} a_0a_1a_2a_0\gamma\gamma\gamma a_1\gamma a_2 \xrightarrow{(d)}$$

$$a_0a_1a_2a_0\gamma\gamma a_1\gamma a_2 \xrightarrow{(e)\,(d)\ y\ (g)} a_0a_1a_2a_0a_1a_2$$

Sea N el alfabeto que sólo contiene las letras a_0 y a_1, que también escribiremos como $*$ y $|$ respectivamente.

Notación: Con cada natural n asociemos la expresión $\bar{n} = \underbrace{||\ldots|}_{(n+1)\text{ trazos}}$

Así $\bar{3} = ||||$ y $\bar{0} = |$

y a cada m-ada de números naturales $(n_1, n_2, n_3, \ldots, n_m)$ la repre-

sentamos por $\overline{(n_1, n_2, \ldots, n_m)} = \bar{n}_1 * \bar{n}_2 * \ldots * \bar{n}_m$. Vg. $\overline{(3,0,1)} = 1111 * 1 * 11$.
Llamaremos 'numerales' a las expresiones $\bar{n}$ $(n \geq 0)$

Ejemplo 8. En N considere el esquema

$$U: \begin{array}{l} \Lambda \to \cdot 1 \\ \Lambda \to \cdot \Lambda \end{array}$$

Dada cualquier palabra P en N, $U(P) = 1P$ y $U(\bar{n}) = \overline{n+1}$

Ejemplo 9. En N el esquema

$$\begin{array}{l} 11 \to 1 \\ 1 \to \cdot 1 \\ \Lambda \to \cdot \Lambda \end{array}$$

Definición 1.5 Dos algoritmos U y B sobre un alfabeto A son completamente equivalentes en A si para cada palabra de A ó $U(P) = B(P)$ ó ninguno de los dos es aplicable a P.
Que U y B son completamente equivalentes en A significa que no es posible distinguirlos por su efecto sobre las palabras de A

Ejemplo 10 Sea U definido en $M = \{a_1, a_2, \alpha\}$ por

$$\begin{array}{l} \alpha a_1 \to a_2 \alpha \\ \alpha a_2 \to a_2 \alpha \\ \alpha \to \cdot \Lambda \\ \Lambda \to \alpha \\ \Lambda \to \cdot \Lambda \end{array}$$

$U(a_1 a_2 a_1) = a_2 a_2 a_2$. U transforma cada palabra de $\{a_1, a_2\}$ en la que se obtiene al substituir en ella todas las ocurrencias del símbolo a_1 por a_2.

Definición 1.6 Dado un algoritmo U sobre un alfabeto A, sea

$$U^A = \{X \in W_A \mid U \text{ es aplicable a } X\}.$$

U^A es el dominio de U en A.

Definición 1.7 Sea U un algoritmo de Markov sobre un alfabeto M tal que $N \subseteq M$. Entonces para cada natural n mayor que cero, asociamos a U una función n-aria $f_U^n(x_1, \ldots, x_n)$ de la siguiente manera. Dada una $(m_1, \ldots, m_n)$, sea $\alpha_1 = \overline{(m_1, \ldots, m_n)}$; existen 2 posibilidades:

a) que $\alpha_1 \in U^M$ y $U(\alpha_1) = \overline{\omega}$ para algún $\omega \in \mathbb{N}$. En este caso definimos

$$f_U^n(m_1, \ldots, m_n) = \omega$$

b) que no suceda a), es decir que $\alpha_1 \notin U^M$ ó que $U(\alpha_1)$ no sea el numeral de un número. Entonces diremos que $(m_1, \ldots, m_n)$ no está en el dominio de f_U^n

Definición 1.8 Una función parcial de m argumentos naturales f y con valores en $\mathbb{N}$, es parcialmente Markov calculable si existe un algoritmo normal U sobre N que satisface que:

1) $\{(\omega_1, \ldots, \omega_m) \in \mathbb{N}^m \mid U \text{ se aplica a } \overline{(\omega_1, \ldots, \omega_m)}\} = \text{Dominio de } f$

2) $f(\omega_1, \ldots, \omega_m) = f_U^m(\omega_1, \ldots, \omega_m)$ para cada $(\omega_1, \ldots, \omega_m) \in$ Dominio de f.

Si, además, f es total, decimos simplemente que es Markov-calculable

Ejemplo 11. En N considere el algoritmo U definido por

$$\begin{aligned} * &\to * \\ || &\to .| \\ | &\to .| \\ \Lambda &\to .\Lambda \end{aligned}$$

$U(\overline{n+1}) = \overline{n}$ y $U(\overline{0}) = \overline{0}$. Entonces la función

$$Pd(x) = \begin{cases} x-1 & \text{si } x>0 \\ 0 & \text{si } x=0 \end{cases}$$

es Markov calculable. En este caso U es sólo aplicable a numerales. En varios de los ejemplos siguientes aparecen producciones del tipo $* \to *$ que tienen por objeto delimitar el dominio de aplicación del algoritmo a la dimensión de que se trate. Así, en el caso de las funciones 'proyección' $\Pi_i^n(x_1, \ldots, x_n) = x_i$ el algoritmo dado tiene por dominio en N a palabras de la forma $\overline{(m_1, \ldots, m_n)}$ con $m_i \in \mathbb{N}$. Ello no es necesario, de acuerdo a la definición, para demostrar que esas funciones son Markov calculables, pero lo incluimos para satisfacer definiciones mas rigurosas aunque en el fondo equivalentes, como la original de Markov. Los ejemplos 8 y 9 demuestran que las funciones $f(x)=x+1$ y $g(x)=0$ son Markov calculables.

Ejemplo 12. Sean $\alpha_1,\ldots,\alpha_{2k}$ símbolos no pertenecientes a N. Para $i\in\bar{k}$ sea S_i la lista

$$\alpha_{2i-1}* \to \alpha_{2i-1}*$$
$$\alpha_{2i-1}| \to \alpha_{2i}|$$
$$\alpha_{2i}| \to \alpha_{2i}$$
$$\alpha_{2i}* \to \alpha_{2i}$$

y S_i'

$$\alpha_{2i-1}* \to \alpha_{2i-1}*$$
$$\alpha_{2i-1}| \to \alpha_{2i}|$$
$$\alpha_{2i}| \to |\alpha_{2i}$$
$$\alpha_{2i}* \to \alpha_{2i+1}$$

Si $1\le j\le k$ considere el algoritmo U_j^k de esquema:

$$S_1$$
$$\vdots$$
$$S_{j-1}$$
$$S_j'$$
$$S_{j+1}$$
$$\vdots$$
$$S_{k-1}$$
$$\alpha_{2k-1}* \to \alpha_{2k-1}*$$
$$\alpha_{2k-1}| \to \alpha_{2k}|$$
$$\alpha_{2k}| \to \alpha_{2k}$$
$$\alpha_{2k}* \to \alpha_{2k}*$$
$$\alpha_{2k} \to \cdot\Lambda$$
$$\Lambda \to \alpha_1$$
$$\Lambda \to \cdot\Lambda$$

Si $j\geq k$, considere U_k^k dado por

$$S_1$$
$$\vdots$$
$$S_{k-1}$$
$$\alpha_{2k-1}* \to \alpha_{2k-1}*$$
$$\alpha_{2k-1}| \to \alpha_{2k}|$$
$$\alpha_{2k}| \to |\alpha_{2k}$$
$$\alpha_{2k}* \to \alpha_{2k}*$$
$$\alpha_{2k} \to \cdot\Lambda$$
$$\Lambda \to \alpha_1$$
$$\Lambda \to \cdot\Lambda$$

Entonces U_j^k sólo es aplicable a expresiones de la forma $\overline{(n_1, \ldots, n_k)}$ y $U_j^k \overline{(n_1, \ldots, n_k)} = \overline{n_j}$. Los esquemas están diseñados de tal modo que el algoritmo parcial definido por S_i se enfrente al i-ésimo bloque de trazos borrándolos todos, así como al símbolo $*$. En cambio, S_j' salta los trazos y borra $*$.

Ahora volvamos a la cuestión planteada al principio: ¿Es correcta esta definición de función calculable? ¿Corresponde a lo que por ello se entiende en Matemáticas? Eso es lo que afirma la Tesis de Church. Se fundamenta en los siguientes hechos:

1) Si f es Markov calculable y U es el algoritmo respectivo, para conocer el valor que f asigna a cualquier argumento n basta manipular la expresión $\bar{n}$ de acuerdo al esquema de U. Este indica de modo determinístico todos los pasos a realizar. Cada uno de tales pasos consiste en buscar la primera expresión de una lista finita que ocurre dentro de una sucesión de signos dada, y luego en operar una substitución, lo que es un proceso completamente mecánico.

2) Para una gran variedad de funciones de la Aritmética, para las que hay consenso en considerarlas como intuitivamente algorítmicas, se ha hallado el algoritmo normal que calcula sus valores. Eso mismo haremos para algunos casos muy importantes, en lo que resta del capítulo

3) Las caracterizaciones de la Calculabilidad dadas independientemente por Church, Post, Turing, y Markov resultaron equivalentes, como lo demostró en 1936 Kleene. Supongamos que tenemos dos 'instructivos' U y U' para calcular, respectivamente, la función f, según dos de esas caracterizaciones. La prueba de Kleene consistió en mostrar un procedimiento algorítmico, en el sentido informal de la palabra, para construir U' a partir de U y viceversa.

Al margen de otras cuestiones que pueden alegarse a favor ó en contra de la Tesis de Church estos tres resultados dan materia suficiente para afirmar que la definición de la clase de las funciones Markov calculables es natural e interesante y que éste es uno de los pocos conceptos absolutos hallados en la investigación en torno al Fundamento de las Matemáticas. Por lo pronto, da pie a una teoría muy rica y de gran belleza como tendremos, en parte, ocasión de ver mas adelante. El primero de los muchos resultados sorprendentes que aparecen en su desarrollo es, precisamente, la naturalidad e independencia del concepto de función calculable. Sin embargo, esta teoría, tal y como aquí la vamos exponiendo, es de poca utilidad práctica porque deja de lado cuestiones como las que se refieren al tiempo con que se lleva a cabo un cálculo o al espacio que requiere.

Ahora bien, otra cosa que debe ser observada surge de las definiciones 1.7 y 1.8: que no hay modo de saber si un número n pertenece al dominio D_f de una función f Markov calculable. Porque supongamos que hay una máquina que tiene por objeto seguir las instrucciones del algoritmo U que calcula f (es decir, una máquina programada según el esquema de U). Si al darle por dato la expresión $\bar{n}$, después de un tiempo se detiene, entonces $n \in D_f$. Pero durante el intervalo en que la máquina está en acción, no podemos determinar, salvo en algunos casos, si se detendrá o no. Veremos en un capítulo subsiguiente cómo está encerrada aquí una autorreferencia, porque este 'no podemos determinar' significa 'a través de procedimientos algorítmicos'.

Ejemplo 13 La adición. Sea U el algoritmo en N con esquema:

(1) $*\,| \to |\,*$

(2) $*\,* \to *\,*$

(3) $* \to \Lambda$

(4) $||\to .|$

(5) $\Lambda \to .\Lambda$

U en N sólo es aplicable a palabras de la forma $\overline{(n,m)}$ y el siguiente diagrama indica su efecto:

$$\underbrace{||\ldots|}_{(n+1)\ \text{Trazos}} * \underbrace{||\ldots|}_{(m+1)\ \text{Trazos}}$$

aplicación reiterada de (1)

$$\to \underbrace{|||\ldots||\ldots|}_{(n+m+2)} *$$

(3)

$$\to \underbrace{|||\ldots||\ldots|}_{(n+m+2)}$$

(4)

$$\to \underbrace{|||\ldots||\ldots|}_{(n+m+1)\ \text{trazos}} = \overline{m+n}$$

Entonces $U(\overline{m,n}) = \overline{m+n}$

Ejemplo 14. El siguiente es el esquema del algoritmo que calcula $f(x,y) = (x+1)(y+1)$. Es más sencillo que el que corresponde a la multiplicación $f(x,y) = x \cdot y$ a causa de nuestra convención notacional, y que esta última función es calculable resultará de este ejemplo por un corolario posterior. Puesto que

$$(x+1)(y+1) = \underbrace{(y+1) \cdots (y+1)}_{(x+1)\ \text{veces}}$$

ante la expresión $\underbrace{||\ldots|}_{(x+1)\ \text{trazos}} * \underbrace{||\ldots|}_{(y+1)\ \text{trazos}}$ nuestro algoritmo comenzará borrando un trazo de la izquierda y repitiendo el bloque de trazos de longitud $y+1$ tantas veces como trazos queden en el 1er bloque. Usaremos para ello varios símbolos que no pertenecen a N ($\alpha, n, \omega, \beta, \kappa, \epsilon, m$). Explicaremos paso a paso el efecto de las producciones del esquema. Primero aparece 'α' (con la penúltima producción)

$$(1)\quad \alpha \underbrace{||\ldots|}_{(x+1)\ \text{trazos}} * \underbrace{||\ldots|}_{(y+1)\ \text{trazos}}$$

la primera producción $\alpha|| \to \epsilon\omega$ suprime un trazo y marca otro | con ϵ, que indica que todo el segundo bloque de trazos debe repetirse después de poner la marca *

$$(2)\ \epsilon\,\omega\ \underbrace{11\ldots\ 1}_{(X-1)} * \underbrace{11\ldots\ 1}_{(Y+1)}$$

siguen las producciones $\left.\begin{array}{l}\omega 1 \to 1\omega \\ \omega * \to *\omega\end{array}\right\}$ ω salta

$1\omega \to n\alpha *\ \}$ llega al final y reemplaza un 1 por el símbolo n indicando que va a copiar ese trazo al final de la expresión. Eso lo hace α.

$$(3)\ \epsilon 11.\quad 1 * \underbrace{11\ldots\ 1}_{Y\ \text{trazos}} n\alpha *$$

$\left.\begin{array}{l}\alpha * \to * \alpha \\ \alpha 1 \to 1\alpha \\ \alpha \to 1B\end{array}\right\}$ α avanza hasta el final agrega el 1 correspondiente a n e introduce B

$$(4)\ \epsilon 11\ldots\quad 1 * \underbrace{11\ldots 1}_{Y\ \text{trazos}} n * 1B$$

$\left.\begin{array}{l}1B \to B1 \\ *B \to B*\end{array}\right\}$ B retrocede.

$1nB \to n1\alpha\ \}$ hasta hallar n. El proceso se repite

$*nB \to *K1\ \}$ Excepto que todo el bloquo haya sido copiado.

$$(5)\ \epsilon \underbrace{11\ldots\ 1}_{(X-1)} * \underbrace{11\ldots\ 1}_{Y\ \text{trazos}} nB * 1 \qquad \text{B retrocede}$$

$$(6)\ \epsilon 11\ldots\quad 1 * \underbrace{11\ldots\ 1}_{(Y-1)} n1\alpha * 1$$

Se restaura el 1, n se coloca un lugar a la izquierda y el ciclo se reinicia...

$$(7)\ \epsilon 11\ldots 1 * K \underbrace{11\ldots\ 1}_{(Y+1)} * \underbrace{11\ .1}_{(Y+1)}$$

hasta que el bloque se ha terminado. Aparece K

$$\left.\begin{array}{l} 1{*}K \rightarrow 1K{*} \\ 11K \rightarrow 1K1 \end{array}\right\}$$ K retrocede

$\epsilon 1K \rightarrow \epsilon\omega$ } un trazo desaparece del primer bloque y se marca otro con ϵ para volver a comenzar

$\epsilon{*}K \rightarrow m$ } excepto que se haya acabado el primer bloque. Aparece m.

8) $\epsilon 1K \underbrace{11\ldots 1}_{(x-2)} * \underbrace{11\ldots 1}_{(y+1)} * \underbrace{11\ldots 1}_{(y+1)\text{ trazos}}$ K retrocede

(9) $\epsilon\omega \underbrace{11\ldots 1}_{(x-2)} * \underbrace{11\ldots 1}_{(y+1)} * \underbrace{11\ldots 1}_{(y+1)}$ vuelve a iniciarse el proceso

hasta que:

10) $\epsilon{*}K \underbrace{\underbrace{11\ldots 1}_{(y+1)} * \underbrace{11\ldots 1}_{(y+1)} * \ldots\ldots * \underbrace{11\ldots 1}_{(y+1)\text{ trazos}}}_{(x+1)\text{ veces}}$

11) $m11\ldots 1 * 11\ldots 1 * 11\ldots 1 * \ldots\ldots * 11\ldots 1$

$$\left.\begin{array}{l} m1 \rightarrow 1m \\ m{*} \rightarrow m \end{array}\right\}$$ m avanza borrando el símbolo * y

$m \rightarrow \cdot 1$ desaparece al final agregando un trazo (por nuestra convención notacional)

$\Lambda \rightarrow a$ Producción que introduce 'a'

$\Lambda \rightarrow \cdot\Lambda$

Es, con mucho, el algoritmo mas complejo de cuantos hemos visto hasta aquí. Falta agregar al principio la producción

$$a1{*}1 \rightarrow \cdot 11$$

para el caso en que los argumentos sean ambos el 0.

Con abreviaturas el esquema de $\mho$ queda así

$$a|*| \to .||$$
$$a|| \to \varepsilon\omega$$
$$\omega\xi \to \xi\omega \qquad \xi \text{ en } N$$
$$|\omega \to n\alpha *$$
$$\alpha\xi \to \xi\alpha \qquad \xi \text{ en } N$$
$$\alpha \to |B$$
$$\xi B \to B\xi \qquad \xi \text{ en } N$$
$$|nB \to n|\alpha$$
$$*nB \to *K|$$
$$|\xi K \to |K\xi \qquad \xi \text{ en } N$$
$$\varepsilon|K \to \varepsilon\omega$$
$$\varepsilon * K \to m$$
$$m| \to |m$$
$$m* \to m$$
$$m \to .|$$
$$\Lambda \to a$$
$$\Lambda \to :\Lambda$$

Ejemplo 16. El esquema que se da a continuación corresponde al algoritmo $\mho$ de la función

$$f(x,y) = \begin{cases} x-y & \text{si } x > y \\ 0 & \text{si } y \geq x \end{cases}$$

o substracción propia. $\mho$ opera cancelando sucesivamente trazos de cada extremo de la expresión $||\ldots|*||\ldots|$ hasta terminar con el segundo bloque, o si el de la izquierda es menor aparece una letra K que borra todos los trazos, excepto uno. Como siempre $\mho$ está definido sobre N. Sea $\mho$ definido por

(a) $\quad i| \to \alpha \quad$ Se introduce α y desaparece un $|$

(b) $\quad \alpha| \to |\alpha \quad$ α salta...

(c) $\quad \alpha*| \to *B| \quad$ hasta hallar $*$; se transforma en B

(d) $\quad \alpha* \to .|| \quad$ excepto que el 2º bloque se haya terminado

(e)	$B11 \to 1B1$	B busca el final de la expresión..
(f)	$B1 \to C$	borra un 1; introduce C
(g)	$1C \to C1$	C retrocede y...
(h)	$1{*}C \to 1D{*}$	al hallar $*$ se convierte en D
(i)	${*}C \to K$	salvo que el primer grupo se haya acabado
(j)	$11D \to 1D1$	D salta hacia la izquierda.
(k)	$1D \to i1$	Se reinicia el ciclo
(l)	$K11 \to K1$	K borra todo trazo, menos el último.
(m)	$K1 \to .1$	
(n)	$K \to .1$	
(ñ)	$\Lambda \to i$	se introduce i
(o)	$\Lambda \to .\Lambda$	

Para ilustrar el comportamiento de U con la expresión $\overline{(m,n)}$, suponga primero $m > n$. Sea $K = m - n$. Denotemos $\overline{m} = \underbrace{11..1}_{(m+1)\text{ veces}}$ con 1^{m+1} $(m \geq 0)$. Entonces $\overline{(m,n)} = 11^m * 11^n$

(ñ) $11^m * 11^n$
(a) $i\,11^m * 11^n$
(b) $\alpha 1^m * 11^n$
(c) $1^m \alpha * 11^n$
$1^m * B11^n$
(e) $1^m * 11^{n-1}B1$
(f) $1^m * 11^{n-1}C$
(g) $1^m * C11^{n-1}$
(h) $1^m D * 1^n$
(j) $1D\,1^{m-1} * 1^n$
(k) $i\,1^m * 1^n$

(a) $\alpha\, 1^{m-1} * 11^{n-1}$
⋮
$1^K * B1$
(f) $1^K * C$
(h) $1^K D *$
(j) $1D1^{K-1} *$
(k) $i\,11^{K-1} *$
(a) $\alpha\, 1^{K-1} *$
(b) $1^{K-1} \alpha *$
(d) $1^{K-1}11 = \overline{K}$

y si $m < n$

$11^m * 11^n$
⋮
$i1^m * 11^{n-1}$
⋮

$i1 * 11^K$
(b) $\alpha * 11^K$
(c) $*B11^K$
(e) $*1^K B1 \to$

$$
\begin{aligned}
&\xrightarrow{(f)} \\
(g)\ &\ * 1^{K} C \\
(i)\ &\ * C 1^{K} \\
(k)\ &\ K 1^{K} \\
(l)\ &\ K 1^{K-1} \\
(m)\ &\ K 1 \\
&\ 1 = \bar{0}
\end{aligned}
$$

En caso de igualdad $(\bar{m} = \bar{n})$ es análogo, salvo que en él se aplica en lugar de (k) y (m) la producción (n)

Hasta ahora comprobar que algunas funciones elementales de la Aritmética son Markov calculables ha sido bastante complicado. Veinte producciones se requirieron para formar el esquema de la multiplicación. A continuación y en el siguiente capítulo mostraremos técnicas muy ingeniosas que, desde un punto de vista mas general y abstracto pero constructivo, permiten 'producir' a partir de ciertas funciones otras nuevas de las que puede afirmarse que son Markov calculables sin que sea necesario, aunque siempre es posible, exhibir el esquema de cada una de ellas.
El primer problema que surge aquí es el de hallar un algoritmo normal que realice la composición de otros dos, definidos en un mismo alfabeto. A éstos llamémosles U y B y al alfabeto A. Se trata entonces de encontrar el esquema de un algoritmo H sobre A, tal que $H = B \circ U$. Obviamente que

$$H^{A} = \{x \in W_{A} \mid x \in U^{A} \text{ y } U(x) \in B^{A}\}.$$

Para ello debemos conectar las producciones terminales de U con las 'iniciales' de B. Pero, además, hace falta transformar el lenguaje de tal manera que se impida el que, una vez que U operó, sus producciones vuelvan a ser aplicables trastornando la acción de B. Para cada símbolo $b \in A$, sea $\bar{b}$ un nuevo símbolo $(\bar{b} \notin A)$ llamado el correlato de b. Sea $\bar{A}$ el alfabeto formado por los correlatos de los elementos de A, y α y β' dos símbolos que no pertenecen a $A \cup \bar{A}$. Denotamos por S_U al esquema de U salvo que en lugar del punto en las producciones terminales aparece α y S_B al esquema de B, excepto que cada símbolo es reemplazado por su correlato, cada punto terminal por B', y las producciones de la forma $\Lambda \to Q$ y $\Lambda \to \cdot Q$ (con $Q \in W_A$) son substituidas por $\alpha \to \alpha Q$ y $\alpha \to \alpha B' Q$ respectivamente.

El esquema

(1) $\xi\alpha \to \alpha\xi$ (ξ en A)

(2) $\alpha\xi \to \alpha\bar{\xi}$ (ξ en A)

(3) $\bar{\xi}\eta \to \bar{\xi}\bar{\eta}$ (ξ, η en A)

(4) $\bar{\xi}B' \to B'\bar{\xi}$ (ξ en A)

(5) $B'\bar{\xi} \to B'\xi$ (ξ en A)

(6) $\xi\bar{\eta} \to \xi\eta$ (ξ, η en A)

(7) $\alpha B' \to \cdot\Lambda$

$\quad \mathfrak{S}_B$

$\quad \mathfrak{S}_U$

$\quad \Lambda \to \cdot\Lambda$

determina el algoritmo H. Está diseñado de modo que ninguna operación de B opere antes que todas las de U

Si $P \in W_A$ — P

[Si $U(P) =$ $a_{j_1} \dots a_{j_n}$]

$a_{j_1} a_{j_2} \dots a_{j_i} \alpha a_{j_{i+1}} \dots a_{j_n}$ — α ocurre en el sitio en que se haya realizado la ultima substitución de U

$\alpha a_{j_1} a_{j_2} \dots a_{j_n}$

$\alpha \bar{a}_{j_1} a_{j_2} \dots a_{j_n}$

$\alpha \bar{a}_{j_1} \bar{a}_{j_2} \dots \bar{a}_{j_n}$

[Si $B(a_{j_1} \dots a_{j_n}) =$ $a_{k_1} \dots a_{k_e}$]

$\alpha \bar{a}_{k_1} \dots \bar{a}_{k_m} B' \bar{a}_{k_{m+1}} \dots \bar{a}_{k_e}$ — B' señala donde se efectuó el último reemplazo de B.

$\alpha B' \bar{a}_{k_1} \bar{a}_{k_2} \dots \bar{a}_{k_e}$

$\alpha B' a_{k_1} \bar{a}_{k_2} \dots \bar{a}_{k_e}$

$\alpha B' a_{k_1} a_{k_2} \dots a_{k_e}$

$a_{k_1} a_{k_2} \dots a_{k_e}$

Denotaremos por $B\sigma U$ al algoritmo determinado por H

Definición 1.9 Sean A y B dos alfabetos, $a_1,..,a_k$ símbolos de A y $q_1,..,q_k$ palabras de B. El algoritmo normal $\mathrm{sub}^{a_1,\dots,a_k}_{q_1,\dots,q_k}$, definido a continuación, asocia a cada palabra de A, el resultado de substituir en ella cada ocurrencia de a_i por la correspondiente q_i. Su esquema es:

$$\begin{array}{ll}
\alpha a_i \rightarrow q_i\alpha & i \in \bar{\bar{k}} \\
\alpha \xi \rightarrow \xi\alpha & \xi \in A-\{a_1,..,a_k\} \\
\alpha \rightarrow \cdot\Lambda & \\
\Lambda \rightarrow \alpha & \\
\Lambda \rightarrow \cdot\Lambda &
\end{array}$$

donde α es un símbolo que no pertenece a A ni a B

Ejemplo 17. El algoritmo U^n definido en $N \cup \{\alpha_1,..,\alpha_n\}$ $(\alpha_i \notin N)$ por el esquema

$$\begin{array}{ll}
** \rightarrow ** & \\
\alpha_i | \rightarrow |\alpha_i & i \in \bar{\bar{n}} \\
\alpha_i * | \rightarrow *\alpha_{i+1}| & i \in \overline{\overline{n-1}} \\
\alpha_i * \rightarrow \alpha_i * & i \in \bar{\bar{n}} \\
\alpha_i \rightarrow \alpha_i & i \in \overline{\overline{n-1}} \\
\alpha_n \rightarrow \cdot\Lambda & \\
\Lambda \rightarrow \alpha_1 & \\
\Lambda \rightarrow \cdot\Lambda &
\end{array}$$

se aplica en N sólo a palabras de la forma $(\bar{m}_1 * \bar{m}_2 * \dots * \bar{m}_n)$ y $U^n(\bar{m}_1 * \bar{m}_2 * \dots * \bar{m}_n) = \bar{m}_1 * \bar{m}_2 * \dots * \bar{m}_n$

Definición 1.10 Dados un algoritmo normal U en un alfabeto A, y una extensión B de A, la extensión natural $U^{\#B}$ de U a B, es el algoritmo determinado en B por el esquema de U
En particular si $P \in W_B - W_A$ y $q \in W_A$ entonces $U^{\#B}(P) = P$ y $U^{\#B}(qP) = U(q)P$

todos estos resultados de carácter técnico van finalmente encaminados a mostrar el alcance de lo que puede calcularse a través de los algoritmos normales. Mas tarde tocará también hallar sus limitaciones

teorema 1.1 Sean U_1 y U_2 algoritmos normales y sea A la unión de sus alfabetos. Entonces hay un algoritmo normal B sobre $A\cup\{*\}$ llamado la yuxtaposición de U_1 y U_2 tal que

$$B(P) = U_1^{\#A}(P) * U_2^{\#A}(P) \quad \text{para } P\in W_A$$

Demostración Sea $A=\{a_1,\ldots,a_n\}$ y $\bar{A}=\{\bar{a}_1,\ldots,\bar{a}_n\}$ el conjunto de los correlatos de los elementos de A. Considere el algoritmo $C_{\bar{A}A}$ dado por

$$\xi\bar{\xi} \to \bar{\xi}\xi \quad \xi\in A$$
$$\Lambda \to .\Lambda$$

y similarmente $C_{A\bar{A}}$ con esquema

$$\bar{\xi}\xi \to \xi\bar{\xi} \quad \xi\in A$$
$$\Lambda \to .\Lambda$$

Entonces, por ejemplo $C_{A\bar{A}}(a_1\bar{a}_2a_1\bar{a}_3a_2) = a_1a_1a_2\bar{a}_2a_3$ y

$C_{A\bar{A}}(\bar{a}_{j1}\ldots\bar{a}_{jm}, a_{j1},\ldots,a_{jm}) = a_{j1}\ldots a_{jm}\bar{a}_{j1}\ldots\bar{a}_{jm}$

Sea D el algoritmo en $A\cup\bar{A}\cup\{*\}$ con esquema

$$*\bar{\xi} \to \bar{\xi}* \quad \xi \text{ en } A$$
$$*\xi \to .*\xi$$
$$\Lambda \to *$$
$$\Lambda \to .\Lambda$$

Claramente $D(\bar{P}P) = \bar{P}*P$ $(P\in W_A)$ Denotemos por $\bar{U}_1$ el algoritmo obtenido por reemplazar en el esquema de U_1 cada símbolo a por $\bar{a}$

Entonces

$$B = Sub^{\bar{a}_1,\ldots,\bar{a}_n}_{a_1,\ldots,a_n} \circ D \circ \bar{U}_1^{\#A} \circ C_{\bar{A}A} \circ U_2^{\#A} \circ C_{A\bar{A}} \circ Sub^{a_1,a_2,\ldots,a_n}_{a_1\bar{a}_1,a_2\bar{a}_2,\ldots,a_n\bar{a}_n}$$

Indiquemos el efecto sucesivo de cada una de estas operaciones que componen B, sobre una $P=a_{j1}\ldots a_{jk}$ de A del siguiente modo

$$
\begin{array}{ll}
 & a_{j_1} a_{j_2} \dots \quad a_{j_k} \\
\mathrm{Sub}^{a_1,\dots,a_n}_{a_1\bar{a}_1,\dots,a_n\bar{a}_n} & \\
 & a_{j_1}\bar{a}_{j_1} a_{j_2}\bar{a}_{j_2} \dots \quad a_{j_k}\bar{a}_{j_k} \\
C_{A\bar{A}} & \\
 & a_{j_1} a_{j_2} \dots a_{j_k} \bar{a}_{j_1} \bar{a}_{j_2} \dots \bar{a}_{j_k} \ (= P\bar{P}) \\
U_2^{\#A} & \\
 & U_2^{\#A}(P)\,\bar{P} \\
C_{\bar{A}A} & \\
 & \bar{P}\,U_2^{\#A}(P) \\
\bar{U}_1^{\#A} & \\
 & U_1^{\#A}(\bar{P})\,U_2^{\#A}(P) \\
D & \\
 & U_1^{\#A}(\bar{P}) * U_2^{\#A}(P) \\
\mathrm{Sub}^{\bar{a}_1,\dots,\bar{a}_n}_{a_1,\dots,a_n} & \\
 & U_1^{\#A}(P) * U_2^{\#A}(P)
\end{array}
$$

Corolario 1.2. Sean $U_1,\dots,U_k$ algoritmos normales y A la unión de sus alfabetos. Hay un algoritmo normal B sobre $A\cup\{*\}$ tal que

$$B(P) = U_1^{\#A}(P) * U_2^{\#A}(P) * \dots * U_k^{\#A}(P) \qquad P\in W_A$$

donde $U_i^{\#A}$ es la extensión natural de U_i a A. En este caso decimos que B es la yuxtaposición de los algoritmos $U_1,\dots,U_k$

Ahora demostraremos dos importantes teoremas concernientes a la clase de las funciones Markov calculables: El primero asegura que es cerrada bajo composición. El segundo establece lo mismo respecto a otra operación entre funciones que definiremos mas adelante: la minimalización.

Definición 1.11. Una función $H:\mathbb{N}^m\to\mathbb{N}$ se dice obtenida por substitución de las funciones $f(x_1,\dots,x_n)$ $(f:\mathbb{N}^n\to\mathbb{N})$ y $g_1(x_1,\dots,x_m),\dots,g_n(x_1,\dots,x_m)$ $(g_i\ \mathbb{N}^m\to\mathbb{N})$

$$\text{Si} \quad H(x_1,\dots,x_m) = f(g_1(x_1,\dots,x_m),\dots,g_n(x_1,\dots,x_m)) \quad (*)$$

y el dominio de $H = \{x\in\mathbb{N}^m \mid (g_1(x),\dots,g_n(x))\in \mathrm{Dom}\, f\}$

Es ésta una generalización multidimensional de la composición $f\circ g$ de dos funciones

Teorema 1.3 Si $f(x_1,\dots,x_n)$ y $g_1(x_1,\dots,x_m),\dots,g_n(x_1,\dots,x_m)$ son (parcialmente) Markov calculables y $H(x_1,\dots,x_m)$ está dada por $(*)$, entonces H es (parcialmente) Markov calculable

Demostración Denotemos con $U_f, U_{g_1},\dots,U_{g_n}$ los algoritmos sobre

$N = \langle *, 1 \rangle$ que calculan $f, g_1, \ldots, g_n$ respectivamente, y por B al algoritmo yuxtaposición de $U_{g_1}, \ldots, U_{g_n}$, es decir

$$B(P) = U_{g_1}(P) * U_{g_2}(P) * \ldots * U_{g_n}(P)$$

[No se olvide que $U^{\#}_{g_i}(P) = U_{g_i}(P)$ si $P = \bar{n}$ $n \in \mathbb{N}$]

Considérese que

$$H(x_1, \ldots, x_m) = U_f(\overline{U_{g_1}(x_1, \ldots, x_m), \ldots \ldots, U_{g_n}(x_1, \ldots, x_m)})$$
$$= U_f \circ B(\overline{x_1, \ldots, x_m})$$

Entonces $U_f \circ B$ es el algoritmo que calcula H.

Ahora estamos capacitados para probar de un modo indirecto la calculabilidad de ciertas funciones para las que sería fastidioso dar su esquema detallado. Sin embargo, ese esquema puede construirse a través de los procedimientos que el teorema anterior y el siguiente suministran. A título de ejemplo, demostraremos que la multiplicación es Markov-calculable. Sean

$$H(x,y) = (x+1)(y+1), \quad G(x,y) = x \dot{-} y$$
$$f'(x,y) = x+y \quad \text{y} \quad S(x) = x+1$$
$$x \cdot y = H(x,y) \dot{-} (x+y+1) = G(H(x,y), S \circ f'(x,y))$$

Análogamente es Markov calculable toda función polinomial con coeficientes enteros positivos

Para ampliar aún mas nuestro 'repertorio' de funciones calculables* emplearemos el recurso de definición de nuevas funciones llamado minimalización. Por ahora parecerá muy artificial. Poco a poco irá apareciendo su utilidad

Definición 1.12. Una función $f(x_1, \ldots, x_n)$ ($f: \mathbb{N}^n \to \mathbb{N}$) está definida por minimalización de la función $H(y, x_1, \ldots, x_n)$ de $n+1$ argumentos, si f asocia a $(x_1, \ldots, x_n)$ el menor número y para el cual $H(y, x_1, \ldots, x_n) = 0$ si tal número existe; de otra manera $f(x_1, \ldots, x_n)$ no está definida.

Si la función f, así definida, es total, H se dice regular.

*En adelante tomaremos 'calculable' y 'Markov calculable' como sinónimos escribimos

$$f(x_1,\dots,x_n) = \min_y \{H(y,x_1,\dots,x_n)=0\}$$

Teorema 1.4 Si $H(y,x_1,\dots x_n)$ es Markov calculable entonces

$$f(x_1,\dots,x_n) = \min_y \{H(y,x_1,\dots,x_n)=0\}$$

es parcialmente Markov calculable.

Demostración Sean K,α,α_1,B,C,D símbolos no en $\{*,1\}$ y U el algoritmo normal tal que

$$U(y,x_1,\dots,x_n) = K\,\overline{(f(y,x_1,\dots,x_n),y,x_1,\dots,x_n)}$$

representemos por $\mathcal{S}_U$ al esquema de U, excepto que sus puntos terminales han sido reemplazados por α.

Concidere el algoritmo U' dado por

(a)	$\xi\alpha \to \alpha\xi$	$\xi \in N \cup \{K\}$
(b)	$\alpha K \to \alpha_1$	
(c)	$\alpha_1 11 \to B11$	
(d)	$B1 \to B$	
(e)	$B* \to 1$	
(f)	$\alpha_1 1* \to C$	
(g)	$C1 \to 1C$	
(h)	$C* \to D$	
(i)	$D\xi \to D$	$\xi \in N$
(j)	$D \to \cdot\Lambda$	
(k)	$\mathcal{S}_U$	
(l)	$\Lambda \to \cdot\Lambda$	

Para ver el efecto de U' supongamos que para $(x_1,\dots,x_n)$ fijos

$$f(i,x_1,\dots,x_n) = r_i \neq 0 \qquad i \in \overline{y-1}$$

$$y\ f(y,x_1,\dots,x_n) = 0 = r_y$$

y que empezamos a calcular $\overline{(w,x_1,\dots,x_n)}$ con $0 < w < y$

$$\downarrow (x)$$

$$K(\bar{r}_i * \bar{i} * \bar{x}_1 * \alpha \bar{x}_2 * \ldots * \bar{x}_n)$$ aparece por ahí alguna ocurrencia de α

$$\downarrow (a)$$

$$K\alpha\,(\overline{r_i, i, x_1, \ldots, x_n})$$

$$\downarrow (a)\ y\ (b)$$

$$\alpha_1(\overline{r_i, i, x_1, \ldots, x_n})$$

$$\begin{tikzcd}[column sep=small]
& \alpha_1(\overline{r_i, i, x_1, \ldots, x_n}) \arrow[dl, "\text{Si } r_i \neq 0"'] \arrow[dr, "\text{Si } i = y"] & \\
B(\overline{r_i, i, x_1, \ldots, x_n}) \arrow[d, "(c)\ (d)"] & & C(\overline{y, x_1, \ldots, x_n}) \arrow[d, "(f)\ (g)"] \\
B*(\overline{i, x_1, \ldots, x_n}) \arrow[d, "(e)"] & & \bar{y}C*(\overline{x_1, \ldots, x_n}) \arrow[d, "(h)"] \\
(\overline{i+1, x_2, \ldots, x_n}) \arrow[d, "(k)\ (a)"] & & \bar{y}D(\overline{x_1, \ldots, x_n}) \arrow[d, "(i)\ (j)"] \\
K\alpha(\overline{r_{i+1}, i+1, x_1, \ldots, x_n}) & & \bar{y}
\end{tikzcd}$$

y sea $\mathcal{B}$ el algoritmo con esquema

$$\Lambda \to .1*$$
$$\Lambda \to .\Lambda$$

entonces $\mathcal{U}' \circ \mathcal{B}$ calcula f

También es facil observar que:

Corolario 1.5. Si $H(y, x_1, \ldots, x_n)$ es regular y Markov calculable, entonces

$$f(x_1, \ldots, x_n) = \min_y [H(y, x_1, \ldots, x_n) = 0]$$

es Markov calculable.

CAPITULO II
FUNCIONES RECURSIVAS

En este capítulo trataremos un procedimiento general de definición de funciones numéricas que está estrechamente relacionado con la calculabilidad y que ha sido ya esbozado en el capítulo anterior. Vimos dos operaciones entre funciones que preservan la propiedad de ser Markov-calculables. Esto nos permitió asegurar que la multiplicación es calculable,* sin necesidad de mostrar el esquema de su algoritmo. Ahora intentaremos hacer eso mismo de un modo más sistemático y ordenado.

Llamaremos a una función 'recursiva' si puede ser obtenida por un número finito de aplicaciones de tres esquemas de definición, a saber: composición, minimalización y recursión (que aún no hemos definido), partiendo de unas cuantas funciones básicas denominadas 'iniciales'.

Las funciones recursivas fueron tratadas por Gödel en su monografía de 1931. Su intención era caracterizar la Aritmética que sólo requiere de métodos finitarios. Desde entonces han sido materia de muchos trabajos importantes. Sin embargo, los métodos, las pruebas y las definiciones siguen siendo, esencialmente, las ideadas por Gödel

Al final de este capítulo demostraremos que las funciones recursivas son exactamente las mismas que las funciones Markov calculables. Una vez realizado éste trabajo dispondremos de los instrumentos suficientes para ingresar al Tema

*Recuérdese que hemos asumido ya la tesis de Church.

central de este escrito: las limitaciones de la calculabilidad.

Daremos primeramente una correspondencia biunívoca entre los números naturales y las parejas ordenadas de números naturales que jugará un papel muy señalado en todo lo que sigue. Enumeremos los pares en este orden:

$$\underbrace{(0,0)}\ \underbrace{(0,1)\ (1,0)}\ \underbrace{(0,2)\ (1,1)\ (2,0)}\ \underbrace{(0,3)\ (1,2)\ (2,1)\ (3,0)}\ldots$$

El n-ésimo grupo estará formado por los n pares (x,y) cuya suma $x+y$ es $n-1$: $(0,n-1), (1,n-2), \ldots\ (n-2,1), (n-1,0)$. Entonces (x,y) vendrá después de x parejas dentro del $(x+y+1)$-ésimo bloque. Sea $J(x,y)$ el lugar de (x,y) en esta lista, considerando $J(0,0)=0$

$$\therefore\ J(x,y) = 1+2+3+\ldots\ +(x+y)+x = \frac{(x+y)(x+y+1)}{2} + x$$

ó $$J(x,y) = \frac{1}{2}\left((x+y)^2+3x+y\right)$$

Evidentemente que $(x+y)(x+y+1)$ es siempre par. Por ello $J(x,y)$ es siempre un entero.

Considérese la función triangular

$$T(n) = 1+2+3+\ldots\ +n = \frac{n(n+1)}{2}$$

como es creciente, para cada $z \in \mathbb{N}$ hay un único $n \geq 0$ tal que

$$T(n) \leq z < T(n+1) = T(n)+n+1.$$

o $z = T(n)+x$ donde $0 \leq x < n+1$

y sea $y = n-x \geq 0$.

Es decir, que para cada z existen únicos x y $y \in \mathbb{N}$ para los cuales

$$z = T(x+y)+x = \frac{(x+y)(x+y+1)}{2} + x$$

Por lo tanto la función $J(x,y)$ es biyectiva y tiene funciones inversas $K(z)$ y $L(z)$ determinadas de forma que

$$J(K(z), L(z)) = z$$

y $\quad K(J(x,y)) = x \quad$ y $\quad L(J(x,y)) = y$

($(K(z), L(z))$ es la z-ésima pareja en el orden dado. A partir de J puede darse una función de n argumentos J^n que proporcione una correspondencia 1-1 entre $\mathbb{N}^n$ y $\mathbb{N}$. Por ejemplo definimos

$$J^3(x,y,z) = J(J(x,y), z)$$

y sus inversas $I_1^3(z) = K(K(z))$, $I_2^3(z) = L(K(z))$ y $I_3^3(z) = L(z)$

También utilizaremos frecuentemente la función $\mathrm{Rem}(x,y)$ de Gödel y, relacionada con ella, una formulación distinta del Teorema Chino del Residuo que aquí simplemente enunciamos.

Teorema 2.1 Si $b_0, b_1, \ldots\ b_n \in \mathbb{N}$ son primos relativos dos a dos entonces existe $z \in \mathbb{N}$ t.

$$\begin{aligned} z &\equiv a_0 \pmod{b_0} \\ z &\equiv a_1 \pmod{b_1} \\ &\vdots \\ z &\equiv a_n \pmod{b_n}. \end{aligned}$$

y para $a, b \in \mathbb{N}$ definimos $\mathrm{Rem}(a,b)$ como el residuo de dividir a entre b, si $b \neq 0$, y $\mathrm{Rem}(a,0) = 0$. Así $\mathrm{Rem}(3,2) = 1$ y $\mathrm{Rem}(4,0) = 4$.

Demostraremos que $\mathrm{Rem}(x,y)$ es una función que tiene la propiedad de 'decodificar' sucesiones finitas de números que previamente han sido codificados.

Teorema 2.2 Dados $n+1$ números $a_0, a_1, \ldots\ , a_n$ existen $a, b \in \mathbb{N}$ tales que

$$\begin{aligned} a_0 &= \mathrm{Rem}(a, 1+b) \\ a_1 &= \mathrm{Rem}(a, 1+2b) \\ &\vdots \\ a_n &= \mathrm{Rem}(a, 1+(n+1)b) \end{aligned}$$

Demostración sea b un número mayor que cualquier a_i y múltiplo de $n!$ Para $i \neq j$ tenemos que $(1+(1+i)b, 1+(1+j)b) = 1$ pues, suponiendo que $j > i$, si p es un número primo y

$$p \mid (1+(1+j)b) \text{ y } p \mid (1+(1+i)b) \text{ entonces } p \mid 1+(1+j)b - (1+(1+i)b) = j-i$$

y como $p \nmid b$, $p \mid j-i$, así que $p < n$ y $p \mid b$ lo que es imposible

Aplicando el teorema chino existe $a \in \mathbb{N}$ tal que

$$a \equiv a_i \pmod{1+(1+i)b} \quad \text{para todo } i \ (i \leq n)$$

Por otra parte $a_i < 1+(1+i)b$ como el lector podrá comprobar □

Aquí puede apreciarse la utilidad de las funciones $J(x,y)$ y sus inversas, pues la pareja (a,b) puede representarse con un sólo número $J(a,b)$. Definimos

$$t_i(u) = Rem(K(u), 1+(1+i)L(u)) \quad i,u \in \mathbb{N}$$

Corolario 2.3 Para cada sucesión de números naturales $a_0, a_1, \ldots, a_n$ existe $u \in \mathbb{N}$ tal que $t_i(u) = a_i$ para todo i $(0 \leq i \leq n)$

Dem. Sea $u = J(a,b)$ en el teorema anterior.

En el capítulo previo mostramos que varias funciones son Markov-calculables. Sin embargo, no fue posible hacer lo mismo para funciones como la exponenciación $f(x,y) = x^y$ de la que cualquiera admitiría su calculabilidad. Pues para conocer su valor en un determinado argumento basta reiterar determinadas veces una operación que ya sabemos calculable: la multiplicación

$$x^y = x^{y-1} \cdot x = x^{y-2} \cdot x \cdot x = \ldots = \underbrace{x \cdot x \cdots x}_{y \text{ veces}}$$

Algo similar ocurre con la función $n!$ que se calcula según la fórmula:

$$0! = 1$$
$$n! = n \cdot (n-1)!$$

De este tipo de funciones en las que el valor para un argumento dado se determina por el valor que la función asigna al argumento anterior se dice que están definidas por recursión. En lo que sigue escribiremos $x^{(n)}$, $y^{(m)}$, etc en lugar de $(x_1, \ldots, x_n)$ y $(y_1, \ldots, y_m)$

Definición 2.1 Una función $H(X^{(n+1)})$, $H: \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ está definida por recursión de la funciones $f(X^{(n)})$ y $g(X^{(n+2)})$ de n y $n+2$ argumentos respectivamente si

$$H(x_1, \ldots, x_n, 0) = f(x_1, \ldots, x_n)$$

$$\text{y} \quad H(x_1, \ldots, x_n, y+1) = g(x_1, \ldots, x_n, y, H(x_1, \ldots, x_n, y)) \quad (y \geq 0)$$

a $(x_1, \ldots x_n)$ se les llama 'parámetros de la recursión'.

Claro está que n puede ser 0, en cuyo caso $H(0)$ es una constante

$$H(0) = K$$

$$\text{y} \quad H(y+1) = g(y, H(y)).$$

Llamaremos iniciales a las funciones de la siguiente lista:

a) $S(x) = x+1$

b) $C_0(x) = 0$

c) $\Pi_i^n(X^{(n)}) = x_i$ con $1 \leq n$, $1 \leq i \leq n$.

y recursivas a las que de ellas pueden generarse por un número finito de aplicaciones sucesivas de los tres esquemas de definición mencionados. Otra definición equivalente es:

Definición 2.2. Una función f es parcial recursiva si existe una sucesión $f_1, \ldots, f_n$ de funciones con las siguientes propiedades: 1) $f_n = f$, 2) cada f_i $(1 \leq i \leq n)$ es ó a) inicial, ó b) se define de funciones anteriores en la lista por (b.1) recursión ó (b.2) composición ó (b.3) minimalización.

Si en el último inciso agregamos la exigencia de que la minimalización sea de funciones regulares, las funciones así obtenidas serán totales y se llamarán simplemente 'recursivas'.

Si, en cambio, suprimimos del todo el inciso (b.3) nos queda la definición de función recursiva primitiva (R.P)

El hecho de disponer de las funciones 'proyección' (es decir de las Π_i^n) nos libra de usar todas las variables que parecen requerir los esquemas de definición. Por ejemplo, si $f(x,y) = x+y$

$f(x,0)=x$

y $f(x,y+1)=h(f(x,y))$ donde $h(x)=x+1$

Según la fórmula de recursión h debería ser una función de tres variables. Eso se remedia fácilmente. Sea

$$H(x,y,z)=h\circ\Pi_3^3(x,y,z)=h(z)$$

entonces $f(x,0)=\Pi_1^1(x)=x$

y $f(x,y+1)=H(x,y,f(x,y))=h(f(x,y))$

En lo sucesivo estos desarrollos quedarán sobreentendidos en la mayoría de los casos.

Teorema 2.4. Son recursivo primitivas las funciones:

1) $C_k^n(x^{(n)})=k$ siendo k una constante

pues $C_k^n(x^{(n)})=\underbrace{S\circ S\circ\ldots\circ S}_{k\text{ veces}}\circ C_0\circ\Pi_1^n(x^{(n)})$

(Se comienza con la función $c_0(\Pi_1^n(x^{(n)})$ y se aplica k veces la función sucesor (i.e. $s(x)=x+1$), en cada caso se obtiene una función R.P.

2) $f(x,y)=x+y$

3) $f(x,y)=x\cdot y$ pues $f(x,0)=0$

y $f(x,y+1)=x+f(x,y)$

4) $f(x,y)=x^y$ ya que $f(x,0)=1$

y $f(x,y+1)=x\cdot f(x,y)$

5) $Pd(x)=\begin{cases}0 & \text{si } x=0\\ x-1 & \text{si } x\neq 0\end{cases}$ $\quad Pd(0)=0$, $\quad Pd(y+1)=y$

6) $\overline{sgn}(x)=\begin{cases}1 & \text{si } x=0\\ 0 & \text{si } x\neq 0\end{cases}$ $\quad \overline{sgn}(x)=0^x$

7) $sgn(x)=\begin{cases}0 & \text{si } x=0\\ 1 & \text{si } x\neq 0\end{cases}$ $\quad sgn(x)=\overline{sgn}(\overline{sgn}(x))$

8) $x\dot{-}y=\begin{cases}x-y & \text{si } x>y\\ 0 & \text{si } y\geq x\end{cases}$ $\quad x\dot{-}0=x$, $\quad x\dot{-}(y+1)=Pd(x\dot{-}y)$

9) $f(x,y)=|x-y|=(x\dot{-}y)+(y\dot{-}x)$

10) $f(n)=n!$ $\quad 0!=1$

y $(n+1)!=n!\cdot(n+1)$

11) $Rem(x,y)$ pues $Rem(0,x)=0$

y $Rem(y+1,x) = S(Rem(y,x))\cdot sgn(|x - S(Rem(y,x))|)$

12) $B(x^{(n)},z) = \sum_{t\le z} A(x^{(n)},t) = A(x^{(n)},0) + A(x^{(n)},1) + \dots + A(x^{(n)},z)$

Si $A(x^{(n)},t)$ es R.P. pues

$$B(x^{(n)},0) = A(x^{(n)},0)$$

$$y \quad B(x^{(n)},y+1) = B(x^{(n)},y) + A(x^{(n)},y+1)$$

y lo mismo ocurre con $D(x^{(n)},z) = \prod_{t\le z} A(x^{(n)},t)$

13) Si definimos $H(x^{(n)},y^{(m)}) = \sum_{t\le f(y^{(m)})} A(x^{(n)},t)$, y $A(x^{(n)})$

y $f(y^{(m)})$ son recursivas (primitivas) también lo es $H(x^{(n)},y^{(m)})$ ya que $H(x^{(n)},y^{(m)}) = B(x^{(n)},f(y^{(m)}))$ donde B es la función definida en 12)

Análogamente el producto $\prod_{t\le f(y^{(m)})} A(x^{(n)},t)$ es recursivo (primitivo) si A y f lo son.

14) Sea

$$H(x^{(n)},y^{(m)}) = \begin{cases} \sum_{t< f(y^{(m)})} A(x^{(n)},t) & \text{si } f(y^{(m)}) \ne 0 \\ 0 & \text{si } f(y^{(m)}) = 0 \end{cases}$$

entonces $H(x^{(n)},y^{(m)}) = C(x^{(n)},y^{(m)})$

donde $C(x^{(n)},0) = 0$

$$y \quad C(x^{(n)},y+1) = \sum_{t\le y} A(x^{(n)},t)$$

es decir que $H(x^{(n)},y^{(m)})$ es recursiva (primitiva) si $A(x^{(n)},t)$ y $f(y^{(m)})$ lo son.

15) $$W(x^{(n)},y^{(m)}) = \begin{cases} \prod_{t< f(y^{(m)})} A(x^{(n)},t) & \text{si } f(y^{(m)}) \ne 0 \\ 1 & \text{si } f(y^{(m)}) = 0 \end{cases}$$

es recursiva (primitivo) si $A(x^{(n+1)})$ y $f(y^{(m)})$ lo son

16) $f(u,v,x^{(n)}) = \sum_{u<t<v} A(x^{(n)},t)$ es recursiva (primitiva)

si $A(x^{(n+1)})$ lo es, porque

$$\sum_{u<t<v} A(x^{(n)},t) = \sum_{t<v} A(x^{(n)},t) \dot{-} \sum_{t\le u} A(x^{(n)},t)$$

lo mismo puede decirse del producto

$$\prod_{u<t<v} A(x^{(n)}, t) = \begin{cases} A(x^{(n)}, u+1)\cdot \qquad \cdot A(x^{(n)}, v-1) & \text{Si } u<v \\ 1 & \text{Si } v\le u \end{cases}$$

16) $D(x)$ = número de divisores de x si $x \neq 0$, y $D(0)=0$

pues

$$D(x) = \sum_{t\le x} \overline{sgn}\,(Rem(x,t)).$$

El esquema de derivación de una función recursiva a partir de las iniciales puede considerarse como un instructivo abreviado para el cálculo efectivo de sus valores. Por ejemplo, en el inciso 1) debimos haber puesto la siguiente lista para demostrar la recursividad de la suma

$$\left.\begin{array}{ll} 1. & f_1(x) = x \\ 2 & f_2(x) = Sx \\ 3 & f_3(x,y,z) = z \end{array}\right\} \text{iniciales}$$

4. $f_4(x,y,z) = f_2 \circ f_3(x,y,z) = S(z)$ composición de 2 y 3.

5 $f_5(x,0) = f_1(x)$

$f_5(x,y+1) = f_4(x,y,f_5(x,y)) = S(f(x,y))$ recursión con 1 y 4.

Esta derivación es una guía para hallar el resultado de cualquier suma. Para ilustrarlo calculemos $2+2$

$$\begin{aligned} 2+2 &= f_5(2,\,1+1) \\ &= f_4(2,1,f_5(2,1)) \\ &= f_4(2,1,f_4(2,0,f_5(2,0))) \\ &= f_4(2,1,f_4(2,0,f_1(2))) \\ &= f_4(2,1,f_4(2,0,2)) \\ &= f_4(2,1,f_2\circ f_3(2,0,2)) \\ &= f_4(2,1,f_2(2)) \\ &= f_4(2,1,3) \\ &= f_2\circ f_3(2,1,3) \\ &= f_2(3) = 4 \end{aligned}$$

La misma afirmación es válida para los casos en que se emplea la minimalización de funciones regulares. Para hallar la $Min_y\{f(x^{(n)},y)=0\}$ basta calcular $f(x^{(n)},0)$, $f(x^{(n)},1)\ldots$ hasta encontrar un cero, a sabiendas de que ésto ocurrirá en un número finito de pasos.

Así que, por lo menos intuitivamente, las funciones recursivas son calculables. Mas adelante lo demostraremos rigurosamente identificando, como ya lo hemos hecho aquí varias veces, la calculabilidad de funciones numéricas con la de Markov. también probaremos el inverso.

El hecho de que en la teoría se haga poco uso de la minimalización producirá en el lector la impresión de que es un procedimiento prescindible en el tratamiento de la calculabilidad. Tampoco la empleó Gödel en su artículo de 1931. Sin embargo, es necesaria en este contexto porque resulta que hay funciones calculables, en muy diversos sentidos, que no son recursivo primitivas

Definición 2.3 Una relación n-aria $A\subseteq\mathbb{N}^n$ (o conjunto si $n=1$) es recursiva (primitiva) si su función característica

$$C_A(X)=\begin{cases}0 & \text{si } X\in A\\ 1 & \text{si } X\notin A\end{cases}$$

es recursiva (primitiva).

Ejemplos. Son recursivo primitivas las siguientes relaciones

1) la relación $x=y$

pues $f(x,y)=|x-y|$ es su función característica

2) $A=\{(x,y)\mid x\leq y\}$ $\quad C_A(x,y)=sgn\,(x\dot{-}y)$

3) la relación $A=\{(x,y)\mid x \text{ divide a } y\}$

$C_A(x,y)=sgn\,(Rem\,(y,x))$

4) Dado $z\in\mathbb{N}$ fijo la relación $x\equiv y\ (\mathrm{mod}\ z)$

5) $C_A(x,y)=sgn\,|Rem\,(x,z)-Rem\,(y,z)$

Teorema 2.5 Si $R(x^{(n)})$ y $T(x^{(n)})$ son relaciones recursivas (primitivas) también lo son las relaciones $(R\vee T)(x^{(n)})$, $(R\wedge T)(x^{(n)})$,

$(\sim R)(X^{(n)})$, $(R \to T)(X^{(n)})$ definidas del siguiente modo:

$$(R \vee T)(X^{(n)}) \leftrightarrow R(X^{(n)}) \text{ ó } T(X^{(n)})$$

$$(R \wedge T)(X^{(n)}) \leftrightarrow R(X^{(n)}) \text{ y } T(X^{(n)})$$

$$(\sim R)(X^{(n)}) \leftrightarrow X^{(n)} \notin R$$

$$(R \to T)(X^{(n)}) \longleftrightarrow X^{(n)} \notin R \text{ o } X^{(n)} \in T$$

Demostración $C_{R \vee T}(X^{(n)}) = C_R(X^{(n)}) \cdot C_T(X^{(n)})$

$C_{\sim R}(X^{(n)}) = 1 \dot{-} C_R(X^{(n)})$ y $(R \to T)(X^{(n)}) \equiv ((\sim R) \vee T)(X^{(n)})$, etc.

Por ejemplo $\{(x,y,z) \mid x|y \text{ y } x<z\}$ es recursivo primitiva

Otra forma de generar relaciones o funciones recursivas de las ya conocidas es a través de los cuantificadores acotados $\exists_{T \leq x}$, $\forall_{y \leq x}$ y del operador μ-acotado. Si $R(X^{(n)}, y)$ es una relación $(n+1)$-aria definimos

$$A(X^{(n)}, z) \equiv \exists_{y<z} R(X^{(n)}, y) \leftrightarrow R(X^{(n)}, 0) \text{ o } R(X^{(n)}, 1), \quad \text{o } R(X^{(n)}, z-1)$$

su función característica está dada por el producto

$$C_A(X^{(n)}, z) = \prod_{T<z} C_R(X^{(n)}, t)$$

Análogamente

$$U(X^{(n)}, z) \equiv \forall_{y<z} R(X^{(n)}, y) \leftrightarrow R(X^{(n)}, 0), R(X^{(n)}, 1), \ldots \quad \text{y } R(X^{(n)}, z-1)$$

$$\text{ó } U(X^{(n)}, z) \leftrightarrow \sim \exists_{y<z} \sim R(X^{(n)}, y)$$

Asimismo usaremos los cuantificadores $\exists_{y \leq z}$ y $\forall_{y \leq z}$ como equivalentes a

$$\exists_{y<z+1} \text{ y } \forall_{y<z+1} \text{ respectivamente.}$$

Es evidente que la clase de las relaciones recursivas (primitivas) es cerrada bajo la acción de los cuantificadores acotados.

Ejemplos. Son R.P.

1) El predicado ó relación 1-aria $P(x)$: x es primo, pues

$$P(x) \leftrightarrow x > 1 \wedge \forall_{y<x} (y = 1 \vee y \nmid x)$$

2) La relación $A(x,y) \leftrightarrow (x,y)=1$ ya que $A(x,y) \leftrightarrow \underset{t<xy}{\forall} (t=0 \vee x \not| t \vee y \not| t)$ porque si denotamos con

$H(x,y,z)$ a la relación $\underset{t<z}{\forall} (t=0 \vee x \not| t \vee y \not| t)$ entonces

$A(x,y) \leftrightarrow H(x,y,f(x,y))$ donde $f(x,y)=x\cdot y$

3) La función $\pi(n)=$ número de primos $\leq n$

$\pi(n)=\sum_{t\leq n} \overline{sg}n\, c_P(t)$ donde c_P es la función característica del predicado $P(x)$

A continuación introduciremos el operador μ-acotado.

Definición 2.4 Sea $R(x^{(n)},y)$ una relación. Con la expresión $\mu_{y<z} R(x^{(n)},y)$ designamos a la función $f(x^{(n)},z)$ de $(n+1)$-variables tal que

$$f(x^{(n)},z)=\mu_{y<z}R(x^{(n)},y)=\begin{cases}\text{la menor } y<z \text{ para la cual } R(x^{(n)},y), \text{ si existe tal } y.\\ \\ z \qquad \text{en otro caso}\end{cases}$$

que es recursiva primitiva, si R lo es. Eso se prueba de la siguiente manera. Supongamos que t_0 es el menor número menor que z para el cual $(x^{(n)},t_0)\in R$; entonces el producto

$$\prod_{u\leq t} c_R(x^{(n)},u)=\begin{cases}1 & \text{si } t<t_0\\ \\ 0 & \text{si } t\geq t_0\end{cases}$$

Por ello

$$(*) \quad \sum_{t<z}\left(\prod_{u\leq t} c_R(x^{(n)},u)\right)=t_0$$

y si no hay tal t_0 $\quad \prod_{u\leq t} c_R(x^{(n)},u)=1$ para toda $t<z$

entonces $\sum_{t<z}\left(\prod_{u\leq t} c_R(x^{(n)},u)\right)=\sum_{t<z} 1 = z$

es decir que la expresión $(*)$ es igual a $\mu_{y<z} R(x^{(n)},y)$

De forma similar, 'preserva' la recursividad (primitiva) el operador

$$\mu_{y\leq h(z^{(m)})}\, R(x^{(n)},y) = \begin{cases} \text{la menor } y \leq h(z^{(m)}) \text{ para la cual } R(x^{(n)},y) \\ \quad \text{si hay tal } y \\ h(z^{(m)})+1 \quad \text{en otro caso} \end{cases}$$

$\mu_{y\leq h(z^{(m)})} R(x^{(n)},y)$ es una función $S(x^{(n)}, z^{(m)})$ de $(n+m)$ argumentos definida por composición

$$S(x^{(n)}, z^{(m)}) = f(x^{(n)}, h(z^{(m)})+1) = \mu_{y< h(z^{(m)})+1}\, R(x^{(n)},y)$$

Ejemplos. Son recursivo primitivas las siguientes funciones

1) $pr(x)$ es el x-ésimo número primo en orden ascendente

$Pr(0) = 2$

$pr(x+1) = \mu_{y\leq pr(x)!+1}\,(pr(x)<y \wedge P(y))$

(nótese que empezamos a contar en 0)

2) $e(x,i)$ = exponente del i-ésimo factor en la descomposición de x en factores primos. Así, por ejemplo, $e(2^2\cdot 3\cdot 5^4, 2)=4$. Y definimos arbitrariamente $e(0,i)=0$

$e(x,i) = \mu_{y<x}\,(pr(i)^y \mid x \wedge pr(i)^{y+1} \nmid x)$

3) $Co(n,m)$ = cociente de dividir n entre m, si $m\neq 0$, y $Co(n,0)=0$

$Co(n,m) = (\mu_{y\leq n}[(m(y+1))>n])\cdot sgn(m)$

4) $f(n,m) = [\sqrt[m]{n}\,]$ = mayor entero menor o igual que $\sqrt[m]{n}$ si $m\neq 0$, y $f(n,0)=0$

$f(n,m) = (\mu_{y\leq n}(m^{y+1}>n))\cdot sgn(m)$.

5) $J(x,y)$ pues

$J(x,y) = Co((x+y)^2+3x+y, 2)$

6) $K(z)$ y $L(z)$ ya que

$K(z) = \mu_{x\leq z} \underset{y\leq z}{\exists}\; z=J(x,y)$

y

$L(z) = \mu_{y\leq z} \underset{x\leq z}{\exists}\; z=J(x,y)$

Teorema 2.6 Sean $R_1,\ldots,R_m$ m relaciones n-arias tales que para cada $x^{(n)}$ estrictamente uno de los enunciados $R_1(x^{(n)}), R_2(x^{(n)}),\ldots,R_m(x^{(n)})$ es verdadero, $g_1(x^{(n)}),\ldots,g_m(x^{(n)})$

m funciones n-arias y

$$f(x^{(n)}) = \begin{cases} g_1(x^{(n)}) & \text{si } R_1(x^{(n)}) \\ \\ g_m(x^{(n)}) & \text{si } R_m(x^{(n)}) \end{cases}$$

entonces $f(x^{(n)})$ es recursiva (primitiva) si $R_1, \ldots, R_m$ y $g_1, \ldots, g_m$ lo son

Dem. $f(x^{(n)}) = g_1(x^{(n)}) \cdot \overline{sgn}\, c_{R_1}(x^{(n)}) + \ldots \qquad + g_m(x^{(n)}) \cdot \overline{sgn}\, c_{R_m}(x^{(n)})$ ∘

Ejemplo. La función

$$\max(a,b) = \begin{cases} a & \text{si } a > b \\ \\ b & \text{si } b \geq a \end{cases}$$

es recursivo primitiva.

Es frecuente hallar en Teoría de Números funciones f definidas de tal modo que $f(0)$ está dado explícitamente y $f(y+1)$ está expresado en términos no sólo de $f(y)$ sino de uno o mas de los valores precedentes $f(t)$ $(t \leq y)$. A este tipo de definición se le llama recursión por curso de valores.

Por ejemplo sea

$$f(0) = 2$$
$$f(1) = 3$$
$$\text{y } f(x+2) = f(x+1) \cdot f(x)$$

En general dada una función $f(x^{(n)}, y)$ sea

$$\tilde{f}(x^{(n)}, z) = \prod_{t < z} (pr(t))^{f(x^{(n)}, t)}$$

entonces $\tilde{f}(x^{(n)}, z)$ es una cifra que contiene 'codificados' todos los valores de f hasta $z-1$. De $\tilde{f}$ puede obtenerse f con ayuda de la función $e(n, i)$

$$f(x^{(n)}, y) = e(\tilde{f}(x^{(n)}, y+1), y)$$

Teorema 2.7 Si $f(x^{(n)}, y) = h(x^{(n)}, y, \tilde{f}(x^{(n)}, y))$ entonces $f(x^{(n)}, y)$ es recursiva (primitiva) si $h(x^{(n)}, y, z)$ lo es

Dem. $\tilde{f}(x^{(n+1)})$ es recursiva (primitiva) pues

$$\tilde{f}(X^{(n)},0)=1$$
$$\tilde{f}(X^{(n)},y+1)=\tilde{f}(X^{(n)},y)\cdot pr(y)^{h(X^{(n)},y,\tilde{f}(X^{(n)},y))}$$

y f se obtiene de $\tilde{f}$ por composición
$$f(X^{(n)},y)=e(\tilde{f}(X^{(n)},y+1),y)$$

Corolario 2.8. Sean $H(X^{(n+2)})$ y $R(X^{(n+1)})$ dos relaciones tales que $R(X^{(n)},y)\leftrightarrow H(X^{(n)},y,\tilde{C}_R(X^{(n)},y))$ entonces $R(X^{(n)},y)$ es recursiva primitiva si $H(X^{(n+2)})$ lo es

Demostración. $C_R(X^{(n)},y)=C_H(X^{(n)},y,\tilde{C}_R(X^{(n)},y))$ □

En lo que sigue emplearemos con frecuencia la recursión por curso de valores dando por sobreentendidas las aplicaciones del teorema 2.7 y el corolario 2.8, en cada caso particular.

Ejemplo. Más adelante veremos que la resolución de ecuaciones Pell genera las sucesiones

$$f(0)=0$$
$$f(1)=1$$
$$f(n+2)=2a\,f(n+1)-f(n) \quad \text{donde } a\in\mathbb{N} \text{ y } a>1$$

o bien

$$f(n)=((2a\,f(n\dot{-}1)\dot{-}f(n\dot{-}2))\dot{-}1)\cdot sgn(n\dot{-}1)+\overline{sgn}(1\dot{-}n)$$

$$=((2\cdot a\cdot e(\tilde{f}(n),n\dot{-}1)\dot{-}e(\tilde{f}(n),n\dot{-}2))\dot{-}1)\cdot sgn(n\dot{-}1)+\overline{sgn}(1\dot{-}n)$$

Sea

$$h(x,y)=((2\cdot a\cdot e(y,x\dot{-}1)\dot{-}e(y,x\dot{-}2))\dot{-}1)\cdot sgn(x\dot{-}1)+\overline{sgn}(1\dot{-}x)$$

$h(x,y)$ es R.P. ∴ lo es asimismo $f(n)=h(n,\tilde{f}(n))$

Ahora iniciamos un proceso que conducirá a demostrar que las funciones Markov-calculables son recursivas. La técnica que seguiremos llamada aritmetización se debe originalmente a Gödel. Primeramente definimos una función g que a cada uno de los elementos básicos de la teoría de los algoritmos de Markov hace corresponder un número non de la siguiente manera

$\rightarrow$	$\rightarrow\cdot$	a_0	a_1	a_2 ...	
3	5	7	9	11 ...	y $g(a_i)=2i+7$

y si $\alpha = \alpha_0 \ldots \alpha_n$ es una sucesión formada con símbolos de esa lista, asignamos a α el número

$$g(\alpha) = \prod_{i=0}^{n} pr(i)^{g(\alpha_i)}$$

Así, por ejemplo, a la expresión

$$a_0 a_2 \rightarrow \cdot\, a_1$$

corresponde el número

$$2^7 \cdot 3^{11} \cdot 5^5 \cdot 7^9$$

Similarmente si $s = s_0 s_1 \ldots s_n$ es una sucesión de expresiones sea

$$g(s) = \prod_{i=0}^{n} pr(i)^{g(s_i)}$$

v.g.

$$g(a_0 a_1 \rightarrow,\ a_1 \rightarrow \cdot\, a_2,\ a_3) = 2^{2^7 \cdot 3^9 \cdot 5^3} \cdot 3^{2^9 \cdot 3^5 \cdot 7^{11}} \cdot 5^{2^{13}}$$

Nótese en el caso de a_3, cómo un simple símbolo puede también ser considerado como una expresión y entonces le corresponde otro número bajo la función g. Por ello si α es el vacío concebido en tanto que símbolo (o ausencia de símbolos) definimos $g(\alpha)=1$, mientras que como palabra g le asigna el número 2^1. Llamamos, en general a $g(u)$ el número de Gödel de u y si $g(u)=n$, escribimos $\exp(n)=u$

La correspondencia que g establece es biunívoca sobre su rango. Eso se prueba fácilmente observando que por el teorema fundamental de la Aritmética a dos expresiones distintas (o sucesiones de expresiones) no les puede asignar g un mismo número; y que si u es una expresión y v una sucesión de expresiones, entonces

$$g(u) = 2^n \cdot x \qquad x>0 \quad \text{con } n \text{ non}$$

$$\text{y} \quad g(v) = 2^m \cdot x \qquad x>0 \quad \text{con } m \text{ par}$$

Por supuesto que no todo número es el número de Gödel de una expresión, símbolo o sucesión de expresiones. Es importante resaltar que dado un número natural hay un procedimiento efectivo para determinar si pertenece al rango de g y de ser así de qué elemento del dominio proviene. Asimismo lo hay para hallar la imagen de cualquier expresión o símbolo.

Una vez definida g, por cada relación entre palabras o sucesiones de palabras existe un predicado numérico entre los respectivos números de Gödel. Por ejemplo si $R(\mathrm{X},\mathrm{Y})$ es la relación X ocurre en Y entonces sea

$$\tilde{R}(n,m) = \{(n,m)\in \mathbb{N}^2 \mid exp(n) \text{ ocurre en } exp(m)\}.$$

A continuación enlistaremos una serie de predicados y funciones de este tipo, de los que, además, se demostrará que son recursivo primitivos.

1) $\ell(x) = \mu_{y<x}[e(x,y)=0 \wedge \forall_{i<x} e(x,y+i)=0]$

Si x es un número de Gödel, es decir, si pertenece al rango de g entonces $\ell(x)$ = número de ocurrencias de símbolos en $exp(x)$. Vg.
$\ell(2^3\cdot 3^2\cdot 5^7)=3$ y $\ell(1)=0$

2) $GN(x) \equiv \forall_{y<\ell(x)} e(x,y)\neq 0$

$GN(x)$ es verdadera si y sólo si x es un número de la forma $x=\prod_{i=0}^{n} pr(i)^{a_i}$ con $0<a_i\in\mathbb{N}$

3) $x*y = x\cdot \prod_{j<\ell(y)} pr(\ell(x)+j)^{e(y,j)}$

Si $x=g(M)$ y $y=g(N)$ donde M y N son expresiones o sucesiones de expresiones entonces $x*y=g(MN)$. La operación $*$ corresponde a la yuxtaposición entre palabras. Obsérvese que $x*1=1*x=x$

4) $SB(x) \leftrightarrow \exists_{y<x}\, x=2y+7$

$SB(x)$ si x es el número de Gödel de un símbolo del alfabeto $\{a_0,a_1,a_2,\ldots\}$

5) $W(x) \leftrightarrow x=2^1 \vee GN(x) \wedge \forall_{y<\ell(x)} SB(e(x,y))$

$W(x)$ se cumple si x es el número de Gödel de una palabra; $exp(2^1)$ es el vacío considerado como palabra.

6) $PRI(x) \leftrightarrow \exists_{u<x} \exists_{v<x} (W(u) \wedge W(v) \wedge x = u * 2^3 * v)$

PRI(x) sii exp(x) es una producción simple

7) $PRT(x) \leftrightarrow \exists_{u<x} \exists_{v<x} (W(u) \wedge W(v) \wedge x = u * 2^5 * v)$

PRT(x) se satisface sii x es el número de Gödel de una producción terminal

8) $PRO(x) \leftrightarrow PRI(x) \vee PRT(x)$

PRO(x) $\leftrightarrow$ x es el número de Gödel de una producción

9) $gd(n) = \prod_{i=0}^{n} pr(i)^9$

gd(n) = número de Gödel de $\overline{n}$

10) $gd^m(n_1, \ldots, n_m) = gd(n_1) * 2^7 * gd(n_2) * \ldots * 2^7 * gd(n_m)$

$gd^n(n_1, \ldots, n_m)$ = número de Gödel de $\overline{(n_1, \ldots, n_m)}$

11) $AI(x) \leftrightarrow GN(x) \wedge (\forall_{u<\ell(x)} PRO(e(x,u)) \wedge e(x, \ell(x) \dot{-} 1) = 2^1 \cdot 3^5 \cdot 7^1$

AI(x) se cumple si y sólo si x es el número de Gödel del esquema de un algoritmo (en lo que sigue identificaremos frecuentemente a un algoritmo con cualquiera de sus esquemas)

12) $PPR(x,y) \leftrightarrow PRO(y) \wedge \exists_{u<y} ((y = x * 2^3 * u) \vee (y = x * 2^5 * u))$

PPR(x,y) se satisface si exp(y) es una producción y el número de Gödel de su antecedente es x

13) $SPR(x,y) \leftrightarrow PRO(y) \wedge \exists_{u<y} ((y = u * 2^3 * x) \vee (y = u * 2^5 * x))$

SPR(x,y) es verdadero si y sólo si exp(x) es la segunda palabra de la producción exp(y)

14) $ppr(y) = \mu_{x<y}\, PPR(x,y)$

Si $exp(y)$ es una producción, $ppr(y)$ es el número de Gödel de su antecedente. Similarmente definimos

$$spr(y) = \mu_{x<y}\, SPR(x,y)$$

15) $OCC(x,y) \leftrightarrow W(x) \wedge W(y) \wedge \exists_{u<y} \exists_{v<y}\ y = u * x * v$

$OCC(x,y)$ se da si $exp(x) = X$ y $exp(y) = Y$ son palabras y X ocurre en Y

16) $SUBST(x,y,z,m) \leftrightarrow W(x) \wedge W(y) \wedge W(z) \wedge W(m) \wedge$

$$\wedge \exists_{u<x} \exists_{v<x}\ x = u * y * v \ \wedge\ m = u * z * v \ \wedge\ \sim OCC(y,u)$$

17) $SUBST(x,y,z,m)$ se cumple si y sólo si $x, y, z,$ y m son números de Gödel de palabras X, Y, Z y M respectivamente y M se obtiene al substituir la primera ocurrencia (de izquierda a derecha) en X de Y por Z.

17) $L^{S}SUB(x,y,z) \leftrightarrow PRI(z) \wedge SUBST(x, ppr(z), spr(z), y)$

$L^{S}SUB(x,y,z)$ se satisface si $exp(x)$ es una palabra y z el número de Gödel de una producción simple de la forma $P \to Q$ donde P ocurre en $exp(x)$; y $exp(y)$ se obtiene al substituir en $exp(x)$ la ocurrencia mas a la izquierda de P por Q. Análogamente definimos $L^{T}SUB(x,y,z)$ que se cumple en las mismas condiciones que la anterior, salvo que $exp(z)$ debe ser terminal.

18) $SCONS(x,y,z) \leftrightarrow A\ell(z) \wedge \exists_{u<\ell(z)}\ L^{S}SUB(x,y,e(z,u)) \wedge$

$$\forall_{v<u} \sim OCC(e(z,v), x)$$

$SCONS(x,y,z)$ es verdadera si x y y son números de Gödel de palabras X y Y, y z el del esquema de un algoritmo Z y Y resulta de X por una aplicación simple de Z. Asimismo definimos el predicado $TCONS(x,y,z)$ de manera obvia.

19) $DER(y,z) \leftrightarrow AI(z) \wedge GN(y) \wedge$

$\underset{u<\ell(y)\dot{-}2}{\forall}$ $SCONS(e(y,u), e(y,u+1), z) \wedge TCONS(e(y,\ell(y)\dot{-}2), e(y,\ell(y)\dot{-}1), z)$

$DER(y,z)$ se satisface cuando y es el número de Gödel de una sucesión de palabras $U_0, U_1, \ldots$ U_k $(k \geq 0)$, z es el esquema de un algoritmo Z y cada U_{i+1} resulta de U_i (con $0 \leq i < k$) por la aplicación de la primera producción simple del esquema $exp(z)$ aplicable a U_i, excepto U_k que proviene de U_{k-1} por efecto de una producción terminal de Z. En otras palabras, $DER(y,z)$ significa que $e(y,\ell(y\dot{-}1))$ es el resultado de transformar $e(y,0)$ de acuerdo al algoritmo Z.

20) $CORN(x) = \sum_{u<\ell(x)} CU(x,u)$ donde $cu(x,n)$ es la función característica del predicado $e(x,n) \neq 9$. Si x es el número de Gödel de una expresión α $CORN(x)$ es el no. de ocurrencias en α del símbolo S_1. $CORN(\bar{n}) = n+1$

21) $U(x) = corn(e(x, \ell(x)\dot{-}1)) \dot{-} 1$

Si x es el número de Gödel de una sucesión de expresiones $\alpha_1, \alpha_2, \ldots, \alpha_k$, $U(x)$ es el número de ocurrencias del símbolo S_1 menos uno.

22) $C(x) \leftrightarrow x > 1 \wedge \underset{u<\ell(x)}{\forall} e(x,u) = 9$

$C(x)$ se cumple si $exp(x)$ es una expresión formada exclusivamente con el símbolo S_1

23) $T^n(z, X^{(n)}, y) \leftrightarrow DER(y,z) \wedge e(y,0) = gd^n(X^{(n)}) \wedge C(e(y,\ell(y)\dot{-}1))$

$T^n(z, X^{(n)}, y)$ se satisface si y sólo si el algoritmo con esquema z calcula $\overline{X^{(n)}} = e(y,0)$ dando por resultado $e(y,\ell(y)\dot{-}1)$ La recursividad primitiva de los predicados $T^n(z, X^{(n)}, y)$ $(n \geq 1)$ es la base para la demostración de las mas importantes proposiciones que en adelante veremos. La primera de ellas es la siguiente:

Teorema 2.9 Una función $f: \mathbb{N}^n \to \mathbb{N}$ es Markov-calculable si y sólo si hay un número z_0 tal que

$$f(x^{(n)}) = U(\min_y T^n(z_0, x^{(n)}, y))$$

Demostración. Si f es Markov-calculable hay un algoritmo B que satisface que

$$\overline{f(x^{(n)})} = B(\overline{x^{(n)}})$$

y que es aplicable en $N = \{0,1\}$ y en dimensión n sólo a aquellos $x^{(n)}$ para los cuales $x^{(n)} \in \mathrm{Dom} f$. Sea z_0 el número de Gödel del esquema de B, entonces $\min_y T^n(z_0, x^{(n)}, y)$ está definida para $x^{(n)}$ si y solamente si B calcula para $x^{(n)}$ (i.e. $x^{(n)}$ al transformarse según las instrucciones de B, da por resultado una expresión de la forma $\bar{n}$ $(n \geq 0)$). Por la definición de algoritmo normal y del predicado $T^n(x^{(n+2)})$ si $T^n(z_0, x^{(n)}, y_0)$, entonces $y_0 = \min_y T^n(z_0, x^{(n)}, y)$ y $e(y_0, \ell(y_0) \dot{-} 1) = B(\overline{x^{(n)}})$, por lo tanto $U(y_0) = f(x^{(n)})$

Inversamente, si $f(x^{(n)}) = U(\min_y T^n(z_0, x^{(n)}, y))$ entonces $\exp(z_0)$ es el esquema de un algoritmo normal B que calcula un valor numérico para $\overline{(x^{(n)})}$ si y sólo si $x^{(n)} \in \mathrm{Dom} f$; y además por la definición de $T^n(x^{(n+2)})$ y de $U(x)$, $\overline{f(x^{(n)})} = B(\overline{x^{(n)}})$. Por ello si $f(x^{(n)})$ está definida por la ecuación de arriba, entonces es calculable con el algoritmo B.

Corolario 2.10 Cada función (parcialmente) Markov-calculable es (parcial) recursiva.

Dem. Sólo falta observar que si f es total y calculable y z_0 el correspondiente número que cumple el enunciado del teorema, entonces el predicado $T^n(z_0, x^{(n)}, y)$ es regular y, por ende, $U(\min_y T^n(z_0, x^{(n)}, y))$ es recursiva.

Una vez que el inverso del corolario 2.10 haya sido demostrado, podremos inferir del Teorema 2.9 que en la obtención de una función recursiva a partir de las iniciales se requiere aplicar a lo mas una sola vez el operador minimalización. Pero que este esquema es necesario en la generación de muchas funciones calculables lo muestra un argumento que aquí simplemente esbozamos. Los algoritmos normales pueden enlistarse siguiendo el número de Gödel de sus correspondientes esquemas. A cada función recursiva primitiva de una variable asociemos, de los algoritmos que la calculan, el primero que aparezca en la lista. Entonces el orden en los algoritmos induce un orden en las funciones. Esta enumeración es efectiva. Supongamos que $f_1(t), f_2(t), f_3(t), \ldots$ es la lista de las funciones recursivo-primitivas de un argumento. Sea $f(t)$ una función definida de este modo

$$(*)\ f(t) = f_t(t) + 1$$

$f(t)$ es, obviamente, calculable, pero si para algún valor de i se diera el caso de que $f(t) = f_i(t)$, se llegaría a la contradicción

$$f(i) = f_i(i) = f_i(i) + 1$$

Es decir, que f con todo y ser calculable no está incluida en la lista, y por ello no es recursiva primitiva.

Aparentemente el mismo argumento es aplicable a las funciones recursivas. Empero, no es ese el caso, pues en él, los miembros de la igualdad (*) no necesariamente estarían definidos (de hecho sabemos que no lo estarían). No se olvide que el empleo sin restricciones del operador minimalización produce frecuentemente funciones cuyo dominio no es todo $\mathbb{N}$.

Un ejemplo particular de función que no es R. P. para la que sí es posible construir un algoritmo que la calcule es la función exponencial generalizada de Ackermann de 3 variables:

$$f(0,x,y) = x+y$$

$$f(1,x,y) = x \cdot y$$

$$f(2,x,y) = x^y$$

$$\vdots$$

y $f(z+1,x,y)$ = resultado de aplicar y a sí mismo $x-1$ veces bajo la operación $f(z,x,y)$.

Apéndice

Teorema toda función recursiva es Markov-calculable

Dem. Hemos probado que las funciones

$S(x) = x+1$ $\qquad f(x,y) = x+y$

$\Pi_i^n(x^{(n)}) = x_i$ $\qquad g(x,y) = x \dot{-} y$

$C_0(x) = 0$ $\qquad h(x,y) = x \cdot y$

son Markov-calculables exhibiendo en cada caso el esquema de uno de los algoritmos que la calculan. También sabemos que las funciones de la lista que damos a continuación son calculables puesto que están definidas de las seis anteriores por las operaciones de composición y minimalización

1) $C_K(x) = K \quad K \in \mathbb{N}$

$$C_K(x) = \underbrace{S \circ S \quad S}_{K \text{ veces}}(C_0(x))$$

2) $\overline{sgn}(x) = 1 \dot{-} x$

3) $sgn(x) = \overline{sgn}(\overline{sgn}(x))$

4) $|x-y| = (x \dot{-} y) + (y \dot{-} x)$

5) $pd(x) = x \dot{-} 1$

6) $C_{x>y}(x,y)$ la función característica de la relación $x > y$

$C_{x>y}(x,y) = \overline{sgn}(x \dot{-} y)$

7) $Rem(x,y) = x \dot{-} y \cdot \min\{(z+1)y > x\}$

8) $C_{x=y}(x,y) = sgn|x-y|$

9) $\left[\frac{x}{2}\right] = \min_y \{2(y+1) > x\}$

10) $K(x)$ y $L(x)$. Sea $t(n) = \left[\frac{n(n+1)}{2}\right]$. Recordemos que si $J(x,y) = z$ entonces $x = z - t(n)$ donde n es el mayor número tal que $z \geq t(n)$ y $y = n - x$

$\therefore$ Sea $h(z) = \min_n \{t(n+1) > z\}$

y $\quad K(z) = z \dot{-} t(h(z))$

$\quad L(z) = h(z) \dot{-} K(z)$

11) $C_A(z, x^{(n)})$ la función característica del predicado

$\forall_{y \leq z} R(x^{(n)}, y)$ si $C_R(x^{(n)}, y)$ es calculable pues

$$\forall_{y \le z} R(x^{(n)}, y) \leftrightarrow z+1 = \min_w \{ c_R(x^{(n)}, w) = 1 \vee w = z+1 \}$$

lo que equivale a decir que $z+1$ es el primer número para el que puede fallar la relación R. Entonces

$$C_A(z, x^{(n)}) = \operatorname{sgn} | (z+1) - \min_w \{ 1 = c_R(x^{(n)}, w) \vee w = z+1 \} |$$
$$= \operatorname{sgn} | (z+1) - \min_w \{ |1 - c_R(x^{(n)}, w)| \cdot | z+1 - w | = 0 \} |$$

Lema Si $H(x^{(n)}, 0) = f(x^{(n)})$

y $H(x^{(n)}, y+1) = g(x^{(n)}, y, H(x^{(n)}, y))$

entonces $H(x^{(n+1)})$ es Markov-calculable si f y g lo son

Dem. Para cada selección de $x^{(n)}$ y y existe un número w tal que

$$t_i(w) = H(x^{(n)}, i) \quad 0 \le i \le y$$

por lo tanto

$$H(x^{(n)}, y) = t_y(\min_w t_0(w) = f(x^{(n)}) \wedge$$
$$\wedge \forall_{z \le y-1} [t_{z+1}(w) = g(x^{(n)}, z, t_z(w))] \quad \square$$

Con este lema y los resultados del capítulo 1 queda demostrado el teorema. En lo que sigue identificaremos 'recursivo' con 'calculable'

CAPITULO III
PREDICADOS SEMICALCULABLES

Llegamos ahora al tema central de este escrito: las limitaciones o, mas bien, las fronteras de la calculabilidad y de los procedimientos recursivos. No habremos de tratarlo sino muy someramente. Sin embargo, de los resultados que aquí demostraremos, derivarán el Teorema de Gödel, y la solución del décimo problema de Hilbert. Comenzaremos con la definición de predicados que en caso de no ser calculables (o recursivos) están, por lo menos, muy próximos a serlo

Definición 3.1 Un conjunto $A \subseteq \mathbb{N}$ es recursivamente enumerable si es vacío o es el rango de una función f parcialmente calculable (o recursiva).

Intuitivamente un conjunto satisface la definición 3.1 si hay un procedimiento efectivo para enumerar o hacer una lista de sus elementos. Por ejemplo, del conjunto de los números primos puede hacerse una lista con el procedimiento conocido como la Criba de Eratóstenes. En este caso, como en casi todos los que aparecen en la Teoria Elemental de Números, se trata de un conjunto que además es recursivo. El siguiente teorema proporciona una gran cantidad de ejemplos

Teorema 3.1 Si un conjunto $A \subseteq \mathbb{N}$ es recursivo entonces es recursivamente enumerable

Dem. Daremos 2 demostraciones. El caso $A = \phi$ es trivial.

1) Sea $A \neq \phi$, $C_A(x)$ su función característica y sea

$$f(x) = (\overline{sgn}\, C_A(x)) \cdot x + (sgn\, C_A(x)) \cdot s$$

donde s es un elemento particular de A. Entonces $f(x)$ es recursiva y el rango de f es A.

2) Si A es finito, digamos $A = \{a_0, a_1, \ldots a_n\}$ la función

$$f(x) = \begin{cases} a_i & \text{si } x = i \\ & \\ a_n & \text{si } x \geq n \end{cases}$$

es recursiva y su rango es A

Si A es infinito sea

$$f(0) = \min_y [C_A(y) = 0]$$
$$f(x+1) = \min_y [C_A(y) = 0 \text{ y } f(x) < y] \quad \square$$

La primera demostración es constructiva mientras que la segunda no lo es, pues no puede siempre saberse con métodos finitos si un conjunto del que sólo se tiene la función característica recursiva es o no finito.

A diferencia de lo que ocurre con la recursividad, en la obtención de todos los conjuntos recursivamente enumerables basta con las operaciones de composición y recursión. Esto en sí es un indicio de que algún conjunto recursivamente enumerable no es recursivo.

Teorema 3.2 Si $A \neq \phi$ es recursivamente enumerable entonces es el rango de una función recursiva primitiva

Dem. Sea $F(x^{(n)})$ tal que el rango de F es A y supongamos que F no es recursiva primitiva. Entonces F es de la forma

$$F(x^{(n)}) = H(\min_y (B(x^{(n)}, y) = 0))$$

donde H y B son recursivo primitivas. Sea $C(x^{(n)}, t)$ la función característica del predicado

$$\exists_{z \leq t} B(x^{(n)}, z) = 0$$

y sea $G(x^{(n)}, y) = H(\overline{sgn}(C(x^{(n)}, y)) \cdot \mu_{t \leq y} B(x^{(n)}, t) = 0 + C(x^{(n)}, y) \cdot K)$

donde $K = \min_y \{B(z^{(n)}, y) = 0\}$ siendo $z^{(n)}$ un elemento particular del dominio de F. $G(x^{(n)}, y)$ es R. P. y su rango es A. $\square$

Probaremos finalmente que el inverso del Teorema 3.1 no es válido a través de un contraejemplo de carácter constructivo. Los conceptos de recursividad y de enumerabilidad recursiva sólo difieren tratándose de conjuntos infinitos. En este caso la relación entre uno y otro corresponde aproximadamente a la que existe entre las nociones clásicas de infinito actual e infinito potencial. En efecto, un conjunto recursivamente enumerable no está completamente dado sino que va generándose paulatinamente y sus elementos aparecen uno a uno después de periodos de tiempo mas o menos largos, en virtud de procedimientos algorítmicos. Por otro lado un conjunto recursivo está ya íntegramente 'ante nosotros' a través de su función característica que es una prueba selectiva de pertenencia. Sin embargo, los conceptos de recursividad y enumerabilidad recursiva estan 'muy cerca' de ser equivalentes como lo muestran los Teoremas que siguen

Teorema 3.3 Un conjunto A es recursivo si y sólo si A y A^c son recursivamente enumerables.

Dem. Si A es recursivo, A^c también lo es, así la implicación $(\Rightarrow)$ se da por el Teorema 3.1

Inversamente si $f(x)$ y $g(x)$ son dos funciones recursivo primitivas tales que

$$A = \text{rango de } f \quad y \quad A^c = \text{rango de } g$$

considere la función recursiva (total)

$$H(x) = \min_y (x = f(y) \vee x = g(y))$$

entonces $C_A(x) = \operatorname{sgn} |x - f \circ H(x)|$ $\square$

En la demostración pudimos suponer que las funciones f y g que enumeran A y A^c respectivamente, son de una variable ya que dada, por ejemplo, una función de dos argumentos $w(x,y)$, su rango coincide con el de la función $h(z) = w(K(z), L(z))$ de una sola variable y que es recursiva primitiva si ω lo es.

Teorema 3.4 Cada conjunto A infinito y recursivamente enumerable contiene un subconjunto recursivo infinito

Demostración. Sea $f(x)$ recursiva y tal que A= rango de f. Definimos $g(x)$ de este modo

$$g(0) = f(0)$$

$$g(x+1) = f(\min_y (f(y) > g(x)))$$

g es recursiva (i.e. total porque el rango de f es infinito). Además g es creciente (si $x<y$, $g(x)<g(y)$). Sea B el rango de g. B es, obviamente, un subconjunto infinito de A; también es recursivo, pues para saber si un número x pertenece a B basta generar la sucesión $g(0), g(1), g(2), \ldots$ hasta que aparezca un elemento mayor que x. Entonces $x \in B$ si y sólo si ha aparecido ya en la lista. Más formalmente sea

$$h(x) = \min_y \{g(y) > x\} \text{ ; } h \text{ es recursiva (total)}$$

$$\text{y } x \in B \leftrightarrow \exists_{y<h(x)} \; x = g(y) \qquad \square$$

A continuación veremos una caracterización distinta de la enumerabilidad recursiva que permitirá extender el concepto a dimensiones mayores y estudiar sus propiedades mas interesantes. Antes se requiere probar que tal extensión es acorde a nuestra definición original

Teorema 3.5 Un conjunto $A \subseteq \mathbb{N}$ es recursivamente enumerable si y sólo si es el dominio de una función parcial recursiva.

Dem. Sea $f(x)$ la función recursiva cuyo rango es A y z_0 el número que satisface que

$$f(x) = U(\min_y T(z_0, x, y))$$

Así que

$$v \in A \leftrightarrow \exists_x \exists_y \; T(z_0, x, y) \wedge U(y) = v$$

o equivalentemente

$$v \in A \leftrightarrow \exists_{z} T(z_0, K(z), L(z)) \wedge U(L(z)) = v$$

llamemos $C_T(z, v)$ a la función característica del predicado $T(z_0, K(z), L(z)) \wedge U(L(z)) = v$ que es, claro está, recursiva

$v \in A \leftrightarrow v$ pertenece al dominio de la función

$$h(x) = \min_z \{C_T(z, x) = 0\}.$$

$(\Leftarrow)$ Si A es el dominio de la función

$$f(x) = U(\min_y T(z_0, x, y))$$

entonces $x \in A \leftrightarrow \exists_{y} T(z_0, x, y)$

denotemos con $\alpha(x) = 1$ a la función constante 1 y con $C_T(x, y)$ a la característica del predicado $T(z_0, x, y)$.

A es el rango de la función

$$h(x) = \alpha(\min_y T(z_0, x, y)) \cdot x \quad \text{que es recursiva.} \ \square$$

Definición 3.2 Un conjunto $A = \{x^{(n)} \mid P(x^{(n)})\}$ es recursivamente enumerable si es el dominio de una función parcial recursiva. En ese caso, el predicado $P(x)$ que lo define se llama semicalculable.

Los predicados semicalculables provienen de los recursivos al prefijar a éstos uno o varios cuantificadores existenciales

Teorema 3.6 Si $R(x^{(n)}, y^{(m)})$ $(n, m \geq 1)$ es un predicado recursivo entonces $\{x^{(n)} \mid (\exists y^{(m)}) R(x^{(n)}, y^{(m)})\}$ es un conjunto recursivamente enumerable

Demostración Para $m=1$ $\{x^{(n)} \mid (\exists y) R(x^{(n)}, y)\}$ es el dominio de la función $\min_y C_R(x^{(n)}, y) = 0$

Para $m \neq 1$, podemos emplear, como en el teorema anterior la funciones $J(x, y)$, $I(z)$, $D(z)$; por ejemplo, si $m = 2$ y $R(x^{(n)}, x, z)$ es recursiva también lo es $R(x^{(n)}, K(w), L(w))$ y

$$(\exists y)(\exists z) R(x^{(n)}, y, z) \leftrightarrow (\exists w) R(x^{(n)}, K(w), L(w))$$

Teorema 3.7 Sea $R(x^{(n)})$ un predicado semicalculable, entonces existe un predicado recursivo $P(y, x^{(n)})$ tal que

$$R(x^{(n)}) \leftrightarrow (\exists y) P(y, x^{(n)})$$

Dem. Si f es una función recursiva y su dominio es $\{x^{(n)} \mid R(x^{(n)})\}$, sea z_0 como en el teorema 3.5 el número que cumple

$$f(x^{(n)}) = U(\min_y T^n(z_0, x^{(n)}, y))$$

Así que $R(x^{(n)}) \leftrightarrow (\exists y)\, T^n(z_0, x^{(n)}, y)$. $\square$

En la siguiente discusión identificaremos a un algoritmo de Markov con cualquiera de sus esquemas, y a éstos a su vez, con sus números de Gödel. Así la expresión 'el algoritmo w' (con $w \in \mathbb{N}$) significará el algoritmo normal cuyo esquema tiene a w por número de Gödel

Para cada dimensión n y cada número z denotaremos con W_z^n al conjunto $\{x^{(n)} \mid (\exists y)\, T^n(z, x^{(n)}, y)\}$ es decir, al dominio de la función que el algoritmo z define en n dimensiones. Escribiremos W_z en lugar de W_z^1

Corolario 3.8. Un conjunto $A \subseteq \mathbb{N}^n$ $(n \geq 1)$ es recursivamente enumerable si y sólo si existe un número z_0 tal que

$$A = W_{z_0}^n$$

Mencionemos de paso un resultado interesante que surge de la aritmetización de la teoría de los algoritmos normales. Nos referimos a la existencia de un algoritmo universal. La función

$$h(z,x) = U(\min_y T(z,x,y))$$

es parcialmente calculable. Sea U el algoritmo que la calcula. Entonces al aplicar el algoritmo z a $\overline{x}$, el numeral de x, se obtiene el mismo valor que al aplicar U a $\overline{(z,x)}$

$$U\overline{(z,x)} = z(\overline{x}) \quad (\text{ó } \exp(z)\,(\overline{x}))$$

y un lado de la ecuación estará definido si y sólo si el otro lo está. Es obvio que el algoritmo U puede asimismo emplearse en el cálculo de funciones n-arias.

Intuitivamente el predicado $\exists_y T(z,x,y)$ es verdadero si el algoritmo z transforma a $\overline{x}$ en un valor numérico. Si z es fijo

$\exists_{y} T(z,x,y)$ define a W_z. Si, en cambio, es x la que permanece constante y z la que varía, el predicado caracteriza a aquellos algoritmos que tienen a $\bar{x}$ en su dominio o que calculan para $\bar{x}$. El conjunto formado por estos algoritmos es recursivamente enumerable de acuerdo con el teorema 3.6. Formando un cuadrado imaginario entre los valores que z va tomando y aquéllos por los que x corre consideremos los elementos de su diagonal. Sea W el conjunto $\{x \mid (\exists y)\ T(x,x,y)\}$ ó

$$x \in W \leftrightarrow \text{el algoritmo } x \text{ calcula para } x \leftrightarrow x \in W_x$$

Este planteamiento, que recuerda el de la paradoja de Russell, hace natural la pregunta por las propiedades de W^c

Teorema 3.9 $W^c = \{x \mid \sim(\exists y)\ T(x,x,y)\}$ no es recursivamente enumerable.

Dem. Si lo fuera, por el corolario 3.8 existiría z_0 tal que

$$W^c = W_{z_0} = \{x \mid (\exists y)\ T(z_0,x,y)\}$$

o bien $\sim(\exists y)\ T(x,x,y) \leftrightarrow (\exists y)\ T(z_0,x,y)$

pero si en lugar de x se pone z_0, se llega a una contradicción. □

Corolario 3.10 W no es recursivo (aunque sí recursivamente enumerable)

Evidentemente si para algún número y $W_y \subset W^c$ entonces tiene que haber un elemento de W^c que no pertenezca a W_y. Otra característica importante de W^c es que tal elemento puede hallarse efectivamente para cada conjunto $W_y \subset W^c$. Más claramente:

Definición 3.3 Un conjunto A es productivo si existe una función recursiva $f(x)$ tal que para toda x si W_x está contenido en A, entonces $f(x) \in A$ pero $f(x) \notin W_x$.

Teorema 3.11. W^c es productivo

Dem. Sea $f(x) = x$. Supongamos que $W_y \subset W^c$ y que

$$y \in W_y \subset W^c = \{x \mid \sim(\exists w)\ T(x,x,w)\}; \text{ se sigue que}$$

$$\sim(\exists w)\ T(y,y,w) \therefore y \notin W_y \ \text{ß}$$

y si $y \in W \to (\exists w)\ T(y,y,w) \leftrightarrow y \in W_y \subset W^c$ Así que si $W_y \subset W^c$,

$Y \notin W_Y$ y $Y \in W^c$ □

Una primera y nada despreciable consecuencia del corolario 3.10 es la solución negativa del problema de la 'parada' de los algoritmos de Markov, que consiste en determinar si hay un procedimiento finito que decida, dado un algoritmo H y una palabra m cualesquiera, si H se aplica o calcula para m. Podemos tratar esta cuestión transformándola en otra equivalente. Dado un algoritmo, o más bien, su número de Gödel z, definamos el predicado

$$P_z(n) \leftrightarrow exp(n) \text{ es una palabra a la que } z \text{ se aplica.}$$

Entonces el problema de la parada se convierte en la pregunta ¿Son recursivos los predicados $P_z(n)$? Veremos que, por lo menos, hay uno que no. Sea z_0 tal que

$$\{x \mid (\exists y)\, T(x,x,y)\} = W_{z_0} = \{x \mid (\exists y)\, T(z_0,x,y)\}$$

Ahora bien, si el conjunto de números de Gödel de palabras a las que z_0 se aplica, $\{n \mid P_{z_0}(n)\}$, fuese recursivo, asimismo lo sería W_{z_0} pues $W_{z_0} = \{x \mid P_{z_0}(gd(x))\}$

y la función $gd(x)$ = número de Gödel de $\bar{x}$, es recursiva □

Si aceptamos, como hasta aquí lo hemos hecho, la tesis de Church, el argumento anterior demuestra que el problema de la parada para los algoritmos normales tiene una solución negativa. Esto no debería resultar sorprendente después del corolario 3.10.

Debemos hacer notar que todos los teoremas de este capítulo han sido establecidos por medio de pruebas de carácter finitario o constructivo. Así, por ejemplo, aunque sería muy tedioso elaborar el esquema del algoritmo universal, la demostración de su existencia, así como la teoría misma en que se encuentra enmarcada, contienen mas o menos explícitamente las reglas que tendría que seguir quien se propusiera llevar a cabo esta labor. Y al decir 'reglas' nos referimos de nuevo a lo que intuitivamente se acepta como algorítmico y que hemos intentado caracterizar rigurosamente. Claro está, que ésta caracterización sólo es

válida en los casos de cuestiones numéricas o de aquéllas que, siendo relativas a expresiones lingüísticas pueden transformarse en numéricas, como ocurrió con el problema de la 'parada'. Allí la pregunta original se modificó en otra referente a la recursividad de un predicado numérico, gracias al artificio de la aritmetización.
De cualquier manera, la tarea de hallar el esquema del algoritmo universal, o de cualquier otro postulado en los teoremas, se asemeja, en muchos aspectos, a la faena de realizar un cálculo siguiendo el esquema de un algoritmo. En ambos casos está prescrita una actividad que requiere de un tiempo finito, pero indefinidamente largo, y además esa prescripción es determinística porque nada deja al azar, ni al ingenio del ejecutante, etc. Así que hay una cierta semejanza entre nuestro objeto de estudio y los procedimientos admitidos de demostración que hemos empleado.

Veamos otro resultado significativo que se consigue al aplicar el argumento diagonal de Cantor al conjunto de funciones totales Markov-calculables.

Teorema 3.12. El conjunto

$$A = \{z \mid (\forall x)(\exists y)\, t(z,x,y)\}$$

no es recursivamente enumerable

Dem. Supongamos que $A = W_{z_0}$ para algún z_0. Es decir

$$A = W_{z_0} = \{w \mid (\exists y)\, t(z_0, w, y)\}$$

De aquí que $z \in A \leftrightarrow (\forall x)(\exists y)\, t(z,x,y) \leftrightarrow (\exists y)\, t(z_0, z, y)$ $(*)$

Poniendo $z = z_0$

$$z_0 \in A \leftrightarrow (\forall x)(\exists y)\, t(z_0, x, y) \leftrightarrow (\exists y)\, t(z_0, z_0, y) \qquad (*)(*)$$

Por $(*)$ $z \in A \leftrightarrow (\exists y)\, t(z_0, z, y)$

Supongamos que $z_0 \in A$ o que $(\exists y)\, t(z_0, z_0, y)$

entonces por $(*)(*)$ $(\exists y)\, t(z_0, 0, y) \Rightarrow 0 \in A$

$(\exists y)\, t(z_0, 1, y) \Rightarrow 1 \in A$

$(\exists y)\, t(z_0, 2, y) \Rightarrow 2 \in A$

$\vdots \qquad \vdots$

y análogamente si $z \notin A$, entonces $0 \notin A, 1 \notin A, \ldots$ etc. lo cual implicaría que $A = \emptyset$ o $A = \mathbb{N}$. Eso es imposible porque cada algoritmo normal con número de Gödel z genera la función

$$f(x) = U(\min_y T(z, x, y))$$

y entonces toda función Markov-calculable sería total o no lo sería ninguna □

Se ha probado, además, que los conjuntos definidos con la negación o la cuantificación universal de un predicado semicalculable pueden no ser recursivamente enumerables. Sin embargo, hay otras operaciones lógicas bajo las cuales la clase de los predicados semicalculables es cerrada, como se demuestra a continuación.

Teorema 3.13 Si $P(x^{(n)})$ y $Q(x^{(n)})$ son predicados semicalculables también lo son $P(x^{(n)}) \vee Q(x^{(n)})$ y $P(x^{(n)}) \wedge Q(x^{(n)})$ *

Dem. Sabemos que hay dos predicados recursivos $R(y, x^{(n)})$ y $S(y, x^{(n)})$ tales que

$$P(x^{(n)}) \leftrightarrow (\exists y)\, R(y, x^{(n)})$$

$$\text{y} \quad Q(x^{(n)}) \leftrightarrow (\exists y)\, S(y, x^{(n)})$$

Entonces

$$P(x^{(n)}) \wedge Q(x^{(n)}) \leftrightarrow (\exists y)(\exists \omega)\, [R(y, x^{(n)}) \wedge S(y, x^{(n)})]$$

$$\text{y} \quad P(x^{(n)}) \vee Q(x^{(n)}) \leftrightarrow (\exists y)\, [R(y, x^{(n)}) \vee S(y, x^{(n)})]$$

Teorema 3.14. Si $P(y, x^{(n)})$ es semicalculable, asimismo lo es

$$T(x^{(n)}, z) \leftrightarrow \forall_{y \leq z}\, P(y, x^{(n)}).$$

Dem. $T(x^{(n)}, z)$ es verdadero si existe una sucesión $\omega_0, \omega_1, \omega_2, \ldots \omega_z$ que satisface $R(\omega_y, y, x^{(n)})$ para toda $y \leq z$. Nuevamente la función $S(i, y)$ que es recursiva nos permite codificar esta sucesión con un solo número U. Por ello

$$T(x^{(n)}, z) \leftrightarrow (\exists u)(\forall_{y \leq z})\, R(S(y, u), y, x^{(n)})$$ el cual es claramen-

* Equivalentemente: Si A y B son conjuntos recursivamente enumerables, también lo son $A \cap B$ y $A \cup B$

te un predicado semicalculable. $\square$

CAPITULO IV
EL DECIMO PROBLEMA DE HILBERT

Inicialmente el décimo problema de Hilbert consistía en hallar un procedimiento que aplicado a cualquier ecuación polinomial diofantina determinara si tenía solución en enteros. Con el tiempo, el desarrollo de la teoría que hemos expuesto en los anteriores capítulos permitió transformar el problema en otro mas elemental: establecer si ese procedimiento existe. Este planteamiento que hubiera resultado muy ambiguo en 1900, es preciso para nosotros una vez aceptada la tesis de Church. En esos términos fue hallada la solución por Matiyasèvic en 1970, aunque, como hemos comentado en la Introducción, su trabajo es sólo la coronación de una serie de esfuerzos realizados por diversos matemáticos entre los que cabe mencionar a Julia Robinson y a Martin Davis. La solución es de carácter negativo. Eso significa que se ha probado "la imposibilidad de resolver el problema sirviéndose de las hipótesis tales como nos han sido dadas o interpretadas" (Hilbert) En éste capítulo expondremos esa solución no siguiendo el orden histórico, tan complejo, que la materia tomó en su evolución, sino otro mas lógico y sistemático.

Cuando hablemos aquí de las raíces de un polinomio diofantino nos referiremos a raices naturales, y no enteras. La razón es que el problema propuesto por Hilbert es equivalente en ambos casos (resolver uno es resolver el otro) y el primer enfoque es mas sencillo. Pues el polinomio $P(x_1, \ldots x_n) = 0$ tiene raices enteras si y sólo si una de las ecuaciones $P(\pm x_1, \pm x_2, \ldots, \pm x_n) = 0$ tiene solución en números naturales; y viceversa, $P(x_1, \ldots, x_n) = 0$ tiene solución en naturales si y sólo si $P(u_1^2 + v_1^2 + w_1^2 + z_1^2, \ldots, u_n^2 + v_n^2 + w_n^2 + z_n^2) = 0$ tiene raices enteras; y ésto por el teorema de Lagrange que establece que cada número natural es la suma de a lo mas cuatro cuadrados

Definición 4.1 Por un polinomio entenderemos una función ($\mathbb{N} \to \mathbb{Z}$) de la forma

$$\sum_{\substack{0 \le i_1 \le n_1 \\ 0 \le i_2 \le n_2 \\ \vdots \\ 0 \le i_k \le n_k}} a_{i_1 i_2 \ldots i_k} X_1^{i_1} X_2^{i_2} \ldots X_k^{i_k}$$

donde los coeficientes $a_{i_1 i_2 \ldots i_k}$ son números enteros y las variables X^{i_j} tienen por rango a los números naturales (incluido el 0)

Por ejemplo

$3X^2y - 27X$, $Xy^3 + z$ son polinomios y los consideramos como funciones de x, y, z con dominio $\mathbb{N}$ y rango $\mathbb{Z}$

Sea $P(y_1, \ldots y_k, x_1, \ldots x_n)$ un polinomio. En vez de examinar una ecuación polinomial o diofantina de la forma

$$P(a_1, \ldots a_k, x_1, \ldots x_n) = 0$$

donde $a_1, \ldots a_k$ son números naturales fijos (llamados parámetros) y buscar sus raices, invertiremos el problema estudiando las propiedades de los conjuntos 'diofantinos' que definimos a continuación.

Definición 4.2 Un subconjunto A de $\mathbb{N}^n$ $(n \geq 1)$ es diofantino si existe un polinomio $P(X^{(n)}, y^{(m)})$ con $m \geq 0$, tal que

$$A = \{ X^{(n)} \mid (\exists y^{(m)}) \; P(X^{(n)}, y^{(m)}) = 0 \}$$

también llamaremos diofantino al predicado $R(X^{(n)})$ que satisface

$$R(X^{(n)}) \leftrightarrow (\exists y^{(m)}) \; P(X^{(n)}, y^{(m)}) = 0$$

Ejemplos. Son diofantinos los siguientes conjuntos y relaciones

1) el conjunto de los números compuestos C, pues

$$X \in C \leftrightarrow (\exists y)(\exists z)\,(X = (y+2)(z+2))$$

2) el conjunto de los cuadrados perfectos A

$$X \in A \leftrightarrow (\exists y) \;\; X = y^2$$

3) Las relaciones de orden $\{(x,y) \mid x < y\}$ y $\{(x,y) \mid x \leq y\}$

$$X \leq y \leftrightarrow (\exists z)(X + z = y) \;\; y \;\; X < y \leftrightarrow (\exists z)\,(X + z + 1 = y)$$

4) la relación de divisibilidad $x|y$

$$x|y \leftrightarrow (\exists z)\ (xz=y)$$

5) la relación $(m,n)=1$

$$(m,n)=1 \leftrightarrow (\exists u)(\exists v)\ (mu=1+nv)$$

6) El complemento de A (cf. (2))

x no es un cuadrado perfecto $\leftrightarrow (\exists w)(\exists y)\ (w^2+1+y=x)$ y $(\exists z)(x+1+z=(w+1)^2)$

es decir x está entre 2 cuadrados consecutivos; en una sola ecuación

$$x\in A^c \leftrightarrow (\exists w)(\exists y)(\exists z)\ [(w^2+1+y-x)^2+(x+1+z-(w+1)^2)^2=0]$$

En este caso hemos empleado una técnica muy general que permite definir un conjunto diofantino por medio de un sistema de ecuaciones simultáneas $P_1=0,\ P_2=0, \ldots, P_n=0$, substituyéndolas por la sola ecuación equivalente $P_1^2+P_2^2+\ldots+P_n^2=0$. El siguiente ejemplo ilustra este método

7) $S=\{(x,y,z)\mid x=y^2 \text{ y } x<z\}$

$(x,y,z)\in S \leftrightarrow x=y^2$ y $(\exists w)\ (x+w+1-z=0)$ ó bien

$$(x,y,z)\in S \leftrightarrow (\exists w)\ [(x-y^2)^2+(x+w+1-z)^2=0]$$

Análogamente puede definirse un conjunto diofantino a través de un predicado del tipo $P_1=0 \vee P_2=0, \ldots \vee P_n=0$ remplazándolo por la sola ecuación $P_1\cdot P_2 \cdots P_n=0$. Por ejemplo:

8) $S=\{(x,y)\mid x|y \text{ ó } y>x^2\}$

$(x,y)\in S \leftrightarrow (\exists u)\ y=x\cdot u$ ó $(\exists v)\ (x^2+v+1=y)$

$$(x,y)\in S \leftrightarrow (\exists u)(\exists v)\ [(y-xu)\cdot(x^2+v+1-y)=0]$$

La clase de los predicados diofantinos es cerrada bajo las operaciones lógicas de conjunción, disyunción, y, por supuesto, cuantificación existencial. En cambio, la negación permite obtener a veces un conjunto diofantino a partir de otro, como en el inciso cuatro, pero no siempre es así

9) la relación $\{(x,y)\mid x\nmid y\}$

pues $x\nmid y$ si y sólo si existen números naturales u y v tales que $y=ux+v$ y $0<v<x$ ó $y>0$ y $x=0$ $\therefore$ $x\nmid y \leftrightarrow (\exists u)(\exists v)(\exists r)(\exists w)(\exists z)$

$$[(y-ux-v)^2+(v-r-1)^2+(x-v-w-1)^2]\cdot[x^2+(y-z-1)^2]=0$$

Definición 4.3 Una función f de n argumentos $(n\geq 1)$ $(f\ \mathbb{N}^n \to \mathbb{N}$;

es diofantina si

$$\{(x_1,\dots,x_n,y) \mid y = f(x_1,\dots,x_n)\}$$ es un conjunto diofantino

Ejemplos. Son diofantinas las funciones:

1) $J(x,y)=z$ y sus inversas $K(u)$ y $L(u)$:

$J(x,y)=z \leftrightarrow 2z = x^2+2xy+y^2+3x+y$ y

$K(u)=x \leftrightarrow (\exists y)\ J(x,y)=u$ y $L(u)=y \leftrightarrow (\exists x)\ J(x,y)=u$

2) $Rem(a,b)=z$ pues

$Rem(a,b)=z \leftrightarrow (\exists u)\ (a=bu+z) \wedge z<b$

3) $t_i(u)=r$

$t_i(u)=r \leftrightarrow (\exists x)(\exists y)(\exists z)[K(u)=x \wedge L(u)=y \wedge z=1+(1+i)y \wedge Rem(x,z)=r]$

Otro modo de escribir un predicado diofantino es a través de una ecuación del tipo

$$(\exists y^{(m)})\,[P(x^{(n)},y^{(m)}) = Q(x^{(n)},y^{(m)})]$$

donde P y Q son polinomios con coeficientes naturales (que no necesariamente dependen de todas las variables $x_1,\dots,x_n,y_1,\dots,y_m$; en ésto nuestra notación es la misma que la que empleamos en el capítulo dos para las variables de una fórmula). La igualdad entre paréntesis es un predicado recursivo. Por el teorema 3, concluimos que

Teorema 4.1 Todo conjunto diofantino es recursivamente enumerable.

Al final del capítulo habremos probado también el inverso de este teorema, con lo cual quedará resuelto definitivamente el décimo problema de Hilbert. Porque habremos establecido que existe un conjunto diofantino, y que es susceptible de ser hallado con métodos finitos, pero no recursivo. Y si no es posible determinar recursivamente qué elementos satisfacen la ecuación

$$(\exists y^{(m)})\ P(x,y^{(m)})=0$$

tampoco habrá un algoritmo que decida si $P(x_0,y^{(m)})=0$, para un x_0 arbitrario, tiene o no solución.

El proceso de prueba es, esencialmente, el estudio de algunas propiedades formales del lenguaje de los predicados diofantinos

Definición 4.4 Una fórmula aritmética es aquélla que se compone de ecuaciones de la forma $a=b$, $a+b=c$ y $a\cdot b=c$, con a, b y c variables o símbolos de números particulares, unidas por medio de los conectivos y cuantificadores lógicos usuales (acotados o no).

Por ejemplo la fórmula

$P\neq 1 \wedge \forall_{x<p} (x=1 \vee x \not| p)$ que expresa la condición de ser p un número primo, ó

$\forall_x \forall_y \exists_u (x+u=y \vee x=u+y)$ que simboliza una proposición verdadera para los números naturales.

Teorema 4.2 Cada relación $\{(x_1, \ldots x_n, y) \mid y= f(x_1,\ldots,x_n)\}$ donde f es una función recursiva puede ser definida con una fórmula aritmética en la cual los cuantificadores universales, si los hay, están acotados, y no ocurren signos de negación (llamaremos a una fórmula de ésta clase fórmula aritmética restingida)

Dem. El teorema se cumple para las funciones iniciales

pues $C_0(x)=y \leftrightarrow y=0$

$\Pi_i^n(x^{(n)})=y \leftrightarrow y=x_i$

$S(x)=y \leftrightarrow y=x+1$

y para $z=x\cdot y$, $z=x+y$ y $z=x\dot{-}y$ pues esta ecuación es equivalente a $(x\leq y \wedge z=0) \vee (y<x \wedge z+y=x)$. Así que:

$z=x\dot{-}y \leftrightarrow (\exists u) [((x+u)=y \wedge z=0) \vee (y+u+1=z \wedge z+y=x)]$

Como toda función recursiva se define a partir de estas seis utilizando minimalización y composición (ver apéndice cap. 2), mostraremos que estos esquemas preservan la condición del Teorema

a) Si $F(x^{(n)}) = g(h_1(x^{(n)}), h_2(x^{(n)}) \ldots , h_m(x^{(n)}))$, entonces

$F(x^{(n)})=z \leftrightarrow (\exists y_1) \ldots (\exists y_m) [h_1(x^{(n)})=y_1 \wedge \ldots \wedge h_m(x^{(n)})=y_m \wedge g(y^{(m)})=z]$

así que si $g, h_1, \ldots, h_m$ son definibles a través de fórmulas aritméticas restringidas, lo mismo ocurre con F.

b) Si $F(x^{(n)}) = \min_y [h(x^{(n)}, y)=0]$,

$$F(x^{(n)}) = z \leftrightarrow h(x^{(n)}, z) = 0 \ \wedge\ (\forall t < z)(\exists u)(h(x^{(n)}, t) = u+1)$$

∴ el teorema es válido para F si lo es para h. □

Aunque la demostración está ya completa, queremos ilustrar cómo proceder para hallar, directamente, una fórmula aritmética restringida que corresponda a una función recursiva definida por medio del esquema de recursión. Considérese la función $f(x) = x!$ que definimos así

$$f(0) = 1, \quad f(x+1) = (x+1)\, f(x).$$

Para una x fija, sea $a_i = f(i)$ $(0 \le i \le x)$. La sucesión $a_0, a_1, \ldots a_x$ se encuentra determinada completamente por las igualdades

$$a_0 = 1 \quad y \quad a_{j+1} = (j+1)\, a_j \quad (0 \le j < x)$$

Utilicemos la función $t_i(u)$ para representar con un solo número una sucesión finita de valores.

$$y = x! \leftrightarrow (\exists u)[(T_0(u) = 1 \wedge t_x(u) = y) \wedge (\forall v < x)\ (t_{v+1}(u) = (v+1)\, t_v(u))]$$

y sabemos que $t_v(u)$ es, a su vez, expresable por medio de un predicado aritmético

El resultado anterior se debe a Gödel. En 1951, Davis mostró que las fórmulas aritméticas restringidas pueden asimismo representarse con expresiones que son diofantinas salvo por un cuantificador universal acotado.

Teorema 4.3. Para cada conjunto A recursivamente enumerable hay un polinomio $P(x, y, u, x_1, \ldots, x_n) = 0$ tal que

$$A = \{x \mid (\exists y)(\forall u \le y)(\exists x_1 \le y) \ldots (\exists x_n \le y)\ P(x, y, u, x_1, \ldots, x_n) = 0\}$$

Demostración. A es el rango de una función $f(x^{(n)})$ recursiva. Por el teorema 4.2, existe una fórmula aritmética restringida que define a A. Esta fórmula se transformará en otra equivalente, del tipo requerido, si se le aplican algunas de las siguientes reducciones.

1) Suponiendo trivialmente que todas las variables cuantificadas son distintas, se colocan al principio de la expresión todos los cuantificadores conservando su orden relativo. Las conjunciones y disyunciones, así como las relaciones $x \le y$ y $x < y$, que aparecerán repetidamente a lo largo del proceso, se eliminarán en cada ocasión con las técnicas que ya hemos empleado, a saber:

$$A = 0 \wedge B = 0 \leftrightarrow A^2 + B^2 = 0$$

$$A=0 \lor B=0 \leftrightarrow A\cdot B=0$$

$$x<y \leftrightarrow (\exists u)\ (x+u=y),\ \text{etc.}$$

2) En una expresión del tipo

$$(\forall x\le w)(\exists a_1,\ldots,a_n)(\exists z)(\forall y\le z)(\exists b_1,\ldots,b_m)\,[P=0]$$

la inversión del orden en que se hallan los cuantificadores existenciales y universales, para poner estos últimos uno al lado del otro y luego 'fundirlos' en uno solo, puede realizarse si se toman ciertas precauciones. Para que la fórmula resultante sea equivalente a la que tenemos se requiere agregar a

$$(\forall x\le w)(\forall y\le\ )(\exists a_1,\ldots,a_n,z)(\exists b_1,\ldots,b_m)[P=0]$$

algunos otros cuantificadores que garanticen que para cada x las $a_1,\ldots a_n$ y z correspondientes sean las mismas y, además, que la variable x quede acotada por z. Para ello se emplea nuevamente la función $t_i(u)$, de este modo

$$(\forall x\le w)\,(\exists a_1,\ldots,a_n)(\exists z)\,(\forall y\le z)\,(\exists b_1,\ldots,b_m)\,[P=0] \leftrightarrow$$

$$(\exists u_1,\ldots,u_n,u_{n+1})\,(\forall x\le w)\,(\forall y\le T_x(u_{n+1}))\,(\exists a_1,\ldots,a_n)(\exists z)(\exists b_1,\ldots,b_m)\,(a_1=T_x(u_1)$$
$$\land\ a_2=T_x(u_2)\land\ldots\ \land a_n=T_x(u_n)\land z=T_x(u_{n+1})\land[P=0] \leftrightarrow$$

$$(\exists u_1\ldots,u_n,u_{n+1})\,(\forall x\le w)\,(\forall y\le u_{n+1})\,(\exists a_1,\ldots,a_n)(\exists z)\,(\exists b_1,\ldots,b_m)\ (a_1=T_x(u_1)\land$$
$$\ldots\ \land a_n=T_x(u_n)\land z=T_x(u_{n+1})\land[y>z\lor P=0].$$

3) En una fórmula tal como

$$(\forall x\le T)(\forall y\le u)(\exists z)\,[P=0]$$

se requiere 'absorver' en uno solo los dos cuantificadores universales. Procedemos de acuerdo a las equivalencias que se dan a continuación

$$(\forall x\le T)(\forall y\le u)(\exists z)\ [P=0] \leftrightarrow$$
$$(\forall w\le J(T,u))\ (\exists z)(\exists x)(\exists y)\,[K(w)=x\land L(w)=y\land\ (x>T\lor y>U\lor P=0)]$$
$$\leftrightarrow\ (\exists r)\,(\forall w\le r)\,(\exists z)(\exists x)(\exists y)\ [r=J(T,u)\land\ J(x,y)=w\land(x>T\lor y>U\lor$$
$$P=0)]$$

$J(T,U)$ sirve de cota porque $T\le J(T,U)$ y $U\le J(T,U)$

4) Una fórmula del tipo

$$(\exists z)(\exists x)(\exists y)\,(\forall x\le y)\,[P=0]$$

es equivalente a una expresión con un solo cuantificador existencial a la izquierda.

$(\exists z)(\exists t)(\exists y)(\forall x \le y)[P=0] \leftrightarrow$

$(\exists w)(\exists y)(\forall x \le y)(\exists t)(\exists z)\ [J(t,z)=w \wedge P=0] \leftrightarrow$

$(\exists s)(\forall x \le L(s))(\exists w)(\exists y)(\exists t)(\exists z)[J(t,z)=w \wedge s=J(w,y) \wedge P=0] \leftrightarrow$

$(\exists s)(\forall x \le s)(\exists w)(\exists y)(\exists t)(\exists z)[J(t,z)=w \wedge s=J(w,y) \wedge (x>y \vee P=0)]$

Aplicando reiteradamente las reducciones de los incisos 2), 3) y 4) llegamos, al fin, a una expresión de la forma

$$(\exists y)(\forall x \le y)(\exists u_1, \ldots, u_n)[P=0].$$

Ahora veremos cómo obtener de ésta una fórmula en que todos los cuantificadores a partir del universal estén acotados por una misma variable. Obsérvese que $(\exists y)(\forall x \le y)(\exists u_1, \ldots, u_n)[P=0]$ enuncia la existencia de un número finito de valores $u_1, \ldots, u_n$ (n para cada $x \le y$); así que hay una cota superior para todos ellos que designaremos con la variable z. Entonces

$(\exists y)(\forall x \le y)(\exists u_1, \ldots, u_n)[P=0] \leftrightarrow$

$(\exists y)(\exists z)(\forall x \le y)(\exists u_1 \le z) \ldots (\exists u_n \le z)[P=0] \leftrightarrow$

$(\exists t)(\forall x \le K(t))(\exists u_1 \le L(t)) \ldots (\exists u_n \le L(t))(\exists y \le t)[y=K(t) \wedge P=0] \leftrightarrow$

$(\exists t)(\forall x \le t)(\exists u_1 \le L(t)) \ldots (\exists u_n \le L(t))(\exists y \le t)[y=K(t) \wedge (x>y \vee P=0)] \leftrightarrow$

$(\exists t)(\forall x \le t)(\exists u_1 \le t) \ldots (\exists u_n \le t)(\exists y \le t)[y=K(t) \wedge (u_1 \le L(t) \wedge \ldots$
$\ldots u_n \le L(t) \wedge (x>y \vee P=0))] \leftrightarrow$

$(\exists t)(\forall x \le t)(\exists u_1 \le t) \ldots (\exists u_n \le t) \wedge (\exists y \le t)(\exists z \le t) \wedge [J(y,z)=t \wedge$
$(u_1 \le z) \wedge \ldots \wedge (u_n \le z) \wedge (x>y \vee P=0))]$ ▫

Este resultado es fácilmente generalizable a mayores dimensiones según se deduce del lema que sigue.

Lema 4.4 El conjunto $A \subseteq \mathbb{N}^n$ es recursivamente enumerable si y sólo si $B=\{m \mid (\exists x^{(n)})\ J(x^{(n)})=m \wedge x^{(n)} \in A\}$ lo es.

Demostración. El predicado que define a B es semicalculable por el Teorema 3.6

⇐ Análogamente $(x_1, \ldots, x_n) \in A \leftrightarrow (\exists m)(J(x_1, \ldots, x_n)=m \wedge m \in B)$ y este predicado es semicalculable

Corolario 4.5 Si un conjunto $A \subseteq \mathbb{N}^n$ es recursivamente enumerable, entonces existe un polinomio $P(x, y, u_1, \ldots, u_m)$ $(m \ge 0)$ tal que:

$$A = \{(x_1, \ldots, x_n) \mid (\exists k)(\forall y \le k)(\exists u_1 \le k) \ldots (\exists u_m \le k)\, P(k, y, u_1, \ldots, u_m, x_1, \ldots, x_n) = 0\}$$

A la expresión $(\exists k)(\forall y \le k)(\exists u_1 \le k) \ldots (\exists u_m \le k)[P=0]$ se le denomina la forma normal de Davis del conjunto recursivamente enumerable. Mas adelante probaremos que es equivalente a un predicado diofantino ordinario. Para ello se requiere que, previamente enfrentemos una cuestión muy ardua: la de saber si la relación $z = x^y$ es diofantina No es posible entran en todas las complejidades a que esta materia nos llevaría. Esbozaremos, sin embargo, la demostración de un resultado conocido como la hipótesis de Julia Robinson. Fue éste un punto intermadio en el camino históricamente recorrido entre el planteamiento de aquel problema y su solución definitiva.

Primeramente es necesario mostrar algunas propiedades de la ecuación

$$(*) \quad x^2 - dy^2 = 1$$

$$\text{con } d = a^2 - 1 \quad a > 1$$

que es un caso particular de las llamadas ecuaciones Pell. Considérense las sucesiones x_n, y_n que satisfacen para cada n la igualdad

$$(x_n + y_n\sqrt{d}) = (a + \sqrt{d})^n$$

en particular $x_0 = 1$, $y_0 = 0$

y $x_1 = a$, $y_1 = 1$ ambos pares son raices de la ecuación $(*)$

Y además

$$(x_n + y_n\sqrt{d})(a + \sqrt{d}) = (x_{n+1} + y_{n+1}\sqrt{d})$$
$$= (ax_n + dy_n) + (ay_n + x_n)\sqrt{d}$$

Así que: $x_{n+1} = ax_n + dy_n \quad (**)$

$y \quad y_{n+1} = ay_n + x_n$

Análogamente

$$(x_{n-1} + y_{n-1}\sqrt{d})(a + \sqrt{d}) = x_n + y_n\sqrt{d}$$

ó $$(x_{n-1} + y_{n-1}\sqrt{d}) = (x_n + y_n\sqrt{d})(a - \sqrt{d})$$
$$= (ax_n - dy_n) + (ay_n - x_n)\sqrt{d}$$

Por lo tanto

$$x_{n-1} = ax_n - dy_n$$
$$y_{n-1} = ay_n - x_n$$

Sumando miembro a miembro los dos sistemas obtenemos:

$$x_{n-1}+x_{n+1}=2ax_n \quad \text{ó} \quad x_{n+1}=2ax_n-x_{n-1}$$

$$\text{y} \quad y_{n-1}+y_{n+1}=2ay_n \quad \text{ó} \quad y_{n+1}=2ay_n-y_{n-1} \qquad (***)$$

En general si x y y son soluciones positivas de (*) y definimos x' y y' tales que

$$x'+y'\sqrt{d}=(x+y\sqrt{d})(a+\sqrt{d})$$

entonces

$$(x')^2-(y')^2d=(ax+dy)^2-d(ay+x)^2=$$

$$a^2x^2+2adxy+d^2y^2-da^2y^2-2adxy-dx^2=a^2(x^2-dy^2)-d(x^2-dy^2)=$$

$$a^2-d=1$$

de modo similar x'' y y'' son soluciones de (*) si x y y lo son y

$$(x''+y''\sqrt{d})=(x+y\sqrt{d})(a-\sqrt{d})$$

Podemos concluir que los números x_n y y_n son solución de (*); y que son las únicas soluciones positivas se desprende del siguiente argumento. Supongamos dos números positivos x y y tales que

a) $x^2-dy^2=1$

b) Para cada n $x_n\neq x$ y $y_n\neq y$

Las igualdades (**) muestran que $\{x_n\}$ y $\{y_n\}$ son sucesiones crecientes, por ello lo es tambien la sucesión $(x_n+y_n\sqrt{d})$ cuyo primer término es 1. Por lo tanto existe una $n\geq 0$ para la cual

$$x_n+y_n\sqrt{d}<x+y\sqrt{d}<x_{n+1}+y_{n+1}\sqrt{d}$$

multiplicando cada término de la desigualdad por la cantidad $a-\sqrt{d}$ que es positiva, pero menor que uno (pues $d=a^2-1$ y $a>1$) obtenemos

$$x_{n-1}+y_{n-1}\sqrt{d}<(x+y\sqrt{d})(a-\sqrt{d})<x_n-y_n\sqrt{d}$$

Si continuamos con el proceso hasta que n sea cero, deducimos la existencia de dos números x' y y' que son solución de (*) y tales que se da $1<x'+y'<a+\sqrt{d}$; sólo hace falta probar que esa situación es imposible.

Lema 4.6 No hay enteros x, y los cuales satisfagan (*) y simultáneamente las desigualdades

$$1<x+y\sqrt{d}<a+\sqrt{d}$$

Demostración. Si así fuera tendríamos que

$$1=(x+y\sqrt{d})(x-y\sqrt{d})=(a+\sqrt{d})(a-\sqrt{d})$$

y como $x+y\sqrt{d} < a+\sqrt{d}$ entonces $a-\sqrt{d} < x-y\sqrt{d}$

y de igual manera $x-y\sqrt{d} < 1$

por lo tanto $a-\sqrt{d} < x-y\sqrt{d} < 1$

o bien $-1 < -x+y\sqrt{d} < -a+\sqrt{d}$ que sumada con la desigualdad $1 < x+y\sqrt{d} < a+\sqrt{d}$ da por resultado

$0 < 2y\sqrt{d} < 2\sqrt{d}$ ó $0 < y < 1$ lo que es una contradicción □

Ahora, a partir de las identidades (**) y (***) es posible demostrar algunas propiedades de las sucesión $\{x_n\}$ y $\{y_n\}$.

Lema 4.7 (1) $y_n \equiv n \pmod{a-1}$ si $a > 1$

y (2) $x_n - y_n(a-s) \equiv s^n \pmod{2as-s^2-1}$

donde s es un natural cualquiera.

Dem. Tanto (1) como (2) se satisfacen trivialmente si $n=0$ ó $n=1$. Mostraremos que son válidas para $n+1$ suponiendo que lo son para n y $n-1$:

$$y_{n+1} = 2ay_n - y_{n-1} \equiv 2n-(n-1) = n+1 \mod (a-1) \text{ pues } a \equiv 1 \pmod{a-1}$$

y
$$\begin{aligned} x_{n+1} - y_{n+1}(a-s) &= 2ax_n - x_{n-1} - 2ay_n(a-s) + y_{n-1}(a-s) = \\ & 2a(x_n - y_n(a-s)) - (x_{n-1} - y_{n-1}(a-s)) \\ &\equiv 2as^n - s^{n-1} \mod (2as-s^2-1) \\ &= s^{n-1}(2as-1) \\ &\equiv s^{n+1} \pmod{2as-s^2-1} \text{ porque } 2as \equiv s^2+1 \pmod{2as-s^2-1} \end{aligned}$$

Lema 4.8. Para todo n a) $y_{n+1} > y_n \geq n$

y b) $x_{n+1} > x_n \geq a^n$ y $x_n \leq (2a)^n$

De las ecuaciones (**) se deriva que las sucesiones $\{x_n\}$ y $\{y_n\}$ son crecientes. De aquí que $y_n \geq n$ pues $y_0 = 0 \geq 0$

Por (**) y (***) $ax_n \leq x_{n+1} \leq 2ax_n$, y si $a^n \leq x_n < (2a)^n$ entonces $a^{n+1} \leq x_{n+1} < (2a)^{n+1}$. Y como (b) se satisface cuando $n=0$, por inducción es verdadera para todo n

Teorema 4.9 Si hay una relación diofantina $D = \{(u,v) \mid D(u,v)\}$ tal que

1) $D(u,v)$ implica $v \leq u^u$

2) Para cada k, existen u y v para los cuales se cumple $D(u,v)$ y $v > u^k$,

entonces la relación $r = s^t$ es diofantina.

Dem. Considere el sistema de ecuaciones diofantinas

(1) $S>0$, $T>0$

(2) $v=S+T+1$

(3) $w=2aS-S^2-1$

(4) $(X')^2-(v^2-1)(v-1)^2(y')^2=1$

(5) $X'>1$

(6) $w \geq vX'$

(7) $D(a,z)$

(8) $X<z$, $Y>0$

(9) $x^2-(a^2-1)y^2=1$

(10) $Rem(Y,a-1)=T$

(11) $Rem(x-(a-S)y,w)=r$

Mostraremos que dados cualesquiera números positivos r, S y T; $r=S^T$ si y solamente si el sistema (1)-(11) tiene solución en los restantes argumentos. Hasta aquí hemos denotado con X_n y Y_n a la n-ésima solución de la ecuación $X^2-(a^2-1)Y^2=1$ porque 'a' se sobrentendía; en rigor debimos escribir $X_n(a)$ y $Y_n(a)$.

Dem ☞ Supóngase primero que existen a, x, y, w, v, z, x' y y' que hacen verdaderas (1)-(11) para r, S y T dados. Como $X'>1$ (de (4)), $v>1$ por lo tanto $X'=X_m(v)$ y $Y'(v-1)=Y_m(v)$ para alguna $m>0$. Por eso $X' \geq v^m$ y $Y'(v-1) \equiv m \pmod{v-1}$ (lemas 4.7 y 4.8). De esta última igualdad derivamos: $m \equiv 0 \mod (v-1)$ y por ello $m \geq v-1$.
Por (6) $w \geq vX' \geq v \cdot v^m \geq v^v$ y por (2) y (3)

$$2aS-S^2-1 \geq (S+T+1)^{(S+T+1)} > S^T \quad (12)$$

Además $X<z$ (8) y $D(a,z)$ (7) implican que $z<a^a$ y que $X<a^a$ (13)
De $Y>0$ (8) y $X^2-(a^2-1)y^2=1$ (9) se sigue que hay algun número positivo $n<a$ tal que $X_n=X$ y $Y_n=Y$ ($n \geq a$ llevaría a contradecir (13) pues $X_n(a)=x \geq a^n \geq a^a$). Por (10) y es de la forma

$$y=p(a-1)+T \quad 0 \leq T < a-1 \text{ con } p \text{ un número natural}$$

ó bien $y \equiv T \pmod{a-1}$.

Además, de acuerdo con el lema 4.7, $Y \equiv n \pmod{a-1}$. Así que

$n \equiv T \pmod{a-1}$ pero $n<a$ y $T<a-1$ entonces $n=T$ (pues $T>0$)

Finalmente, de $X-y(a-S) \equiv S^n \pmod{2aS-S^2-1}$ (lema 4.7) y de (11), (3) y (12) concluimos que $r=S^T$

⇒) Inversamente sea $r = s^t$ con s y $t > 0$. La condición que el teorema impone a $D(u,v)$ de que para cada k exista una pareja $(u,v) \in D$ con $v \geq u^k$ garantiza que pueden elegirse números a y z (a suficientemente grande) que satisfagan:

$$t < a-1$$

$$D(a,z) \text{ y } z > a^{2t} \qquad (14)$$

$$\text{y } 2as - s^2 - 1 > (s+t+1)^{2(s+t+1)} \quad (15)$$

Sean $v = s+t+1$, $w = 2as - s^2 - 1$, $x' = x_{v-1}(v)$ y $y' = y_{v-1}(v)/v-1$, entonces

$$x' \leq (2v)^{v-1} \leq (v)^{2v-2} \quad \text{(lema 4.8)}$$

$$\text{y} \qquad x' \cdot v \leq v^{2v-2} \cdot v < v^{2v} \quad \text{ó} \quad x' \cdot v < 2as - s^2 - 1 = w \quad \text{por (15)}$$

Así que (1)-(7) son verdaderas. Tomemos $x = x_t(a)$ y $y = y_t(a)$, entonces

$x = x_t \leq (2a)^t \leq (a)^{2t} < z$ por (14) y el lema 4.8. también sabemos que $y \equiv t \pmod{a-1}$ (lema 4.7) y como $t < a-1$ se deduce (10). Por último

$$x - (a-s)y \equiv s^t = r \quad \text{(lema 4.7(b))}$$

$$\text{pero} \quad r = s^t < (s+t+1)^{2(s+t+1)} < w$$

concluimos que (11) se cumple □

El antecedente de la implicación que el teorema establece es conocido como la hipótesis de Julia Robinson. Gracias al argumento anterior, el problema original, relativo al carácter diofantino de la relación $z = x^y$, fue reemplazado por otro un poco mas sencillo o, tal vez, mas concreto; el de buscar una relación $D(u,v)$ que cumpliera las condiciones del teorema. Después de 20 años de permanecer abierta esta cuestión fue al fin resuelta por Matiyasĕvic quien, en 1971, utilizando la sucesión de los números de Fibonacci construyó una relación $D(u,v)$ que satisface la hipótesis de Julia Robinson.

Para evitar algunos desarrollos sencillos aunque largos, como los del teorema anterior, y no desviar la atención del lector de nuestra línea principal de argumentación, aceptaremos en adelante sin mayor prueba que la relación $r = x^y$ es diofantina. De hecho hubiéramos debido mostrar que la relación:

$$D = \{(u,v) \mid v = \chi_u(2) \wedge u > 3\}$$

cumple con las condiciones exigidas

Teorema 4.10 Las siguientes relaciones son diofantinas

$$z = \binom{n}{m} \qquad r = n! \qquad y \qquad z = \prod_{k=1}^{y} a + bk$$

Para demostrarlo en el primer caso es necesario hallar una propiedad que caracterice suficientemente al número $\binom{n}{m}$ y que sea expresable por medio de un predicado diofantino. Veremos que si u es un número mayor que 2^n y $0 < m \leq n$ entonces

$$\left[\frac{(u+1)^n}{u^m}\right] \equiv \binom{n}{m} \pmod u$$

(donde $[x]$ denota al mayor entero menor o igual a x)

En efecto

$$\frac{(u+1)^n}{u^m} = \sum_{i=0}^{m-1} \binom{n}{i} u^{i-m} + \sum_{i=m}^{n} \binom{n}{i} u^{i-m}$$

el segundo sumando es un entero, mientras que

$$\sum_{i=0}^{m-1} \binom{n}{i} u^{i-m} < u^{-1} \sum_{i=0}^{m-1} \binom{n}{i} < u^{-1} \sum_{i=0}^{n} \binom{n}{i} = u^{-1} \cdot 2^n < 1$$

entonces

$$\sum_{i=m}^{n} \binom{n}{i} u^{i-m} \leq \frac{(u+1)^n}{u^m} < \sum_{i=m}^{n} \binom{n}{i} u^{i-m} + 1$$

Es decir que

$$\left[\frac{(u+1)^n}{u^m}\right] = \sum_{i=m}^{n} \binom{n}{i} u^{i-m}$$

ó bien

$$\left[\frac{(u+1)^n}{u^m}\right] - \binom{n}{m} = \sum_{i=m+1}^{n} \binom{n}{i} u^{i-m}$$

observando que cada uno de los términos de esta suma es divisible entre u concluimos que

$$\left[\frac{(U+1)^n}{U^m}\right] \equiv \binom{n}{m} \pmod{U}$$

y además

$$\binom{n}{m} \leq \sum_{i=0}^{n} \binom{n}{i} = 2^n < U$$

Por lo tanto

$$Rem\left(\left[\frac{(U+1)^n}{U^m}\right], U\right) = \binom{n}{m}$$

De todo lo cual se deriva que

$$\binom{n}{m} = z \leftrightarrow (\exists u)(\exists v)(\exists w)\left[v = 2^n \wedge U > v \wedge w = \left[\frac{(U+1)^n}{U^m}\right] \wedge Rem(w,U) = z\right.$$

a su vez $w = \left[\frac{(U+1)^n}{U^m}\right] \leftrightarrow$

$$(\exists x)(\exists y)(\exists r)\left[T = U+1 \wedge x = T^n \wedge y = U^m \wedge yw \leq x < y(w+1)\right]$$

Ahora procederemos análogamente con las otras dos relaciones

Lema 4.11 Si r es un número mayor que $(2n)^{n+1}$

$$n! = \left[\frac{r^n}{\binom{r}{n}}\right]$$

prueba. Dado que

$$\frac{r^n}{r(r-1)\ldots(r-n+1)} \geq 1$$

$$n! \leq \frac{r^n}{\binom{r}{n}} = \frac{n!\,r^n}{r(r-1)\ldots(r-n+1)} = n!\left\{\frac{1}{(1-\frac{1}{r})\ldots(1-\frac{n-1}{r})}\right\} < \frac{n!}{(1-\frac{n}{r})^n}$$

(pues $1-n/r < 1-i/r$ con $0 \leq i \leq n-1$ y por ende

$$\left(1-\frac{n}{r}\right)^n < \prod_{i=0}^{n}\left(1-\frac{i}{r}\right) \quad)$$

Además si $n \neq 0$ (para $n=0$ es trivial) $0 < \frac{n}{r} < \frac{1}{2}$ (pues $r > 2^n \geq 2n$) De aquí que $2\left(\frac{n}{r}\right)^2 < \frac{n}{r}$ ó bien

$$1 < 1 + \left(\frac{n}{r}\right) - 2\left(\frac{n}{r}\right)^2 = \left(1 + 2\left(\frac{n}{r}\right)\right)\left(1-\frac{n}{r}\right)$$

y

$$\frac{1}{1-\left(\frac{n}{r}\right)} < 1 + 2\left(\frac{n}{r}\right)$$

$$y \quad \left(1+\frac{2n}{r}\right)^n = \sum_{j=0}^{n} \binom{n}{j}\left(\frac{2n}{r}\right)^j < 1 + \left(\frac{2n}{r}\right)\sum_{j=0}^{n}\binom{n}{j} = 1 + 2^n\left(\frac{2n}{r}\right)$$

pues $0 < \frac{2n}{r} < 1$. Así que

$$\frac{r^n}{\binom{r}{n}} < n!\left(1+2^n\left(\frac{2n}{r}\right)\right)^n < n! + \frac{n!\ 2^{n+1}\cdot n}{r} < n! + \frac{n^{n+1}\cdot 2^{n+1}}{r} < n! + 1$$

Así queda $n!$ caracterizado como el mayor entero menor o igual que $r^n/\binom{r}{n}$ siendo r cualquier número mayor que $(2n)^{n+1}$

$\therefore$ $m = n! \leftrightarrow (\exists a)(\exists b)(\exists c)(\exists d)(\exists f)[\ b = 2n+1 \wedge c = n+1 \wedge a = b^c \wedge d = a^n$ $\wedge\ f = \binom{a}{n} \wedge\ mf \leq d < (m+1)f$. Y de este predicado ya sabemos que es diofantino.

En cuanto a $z = (a+b)(a+2b)\ldots(a+by)$, que es una relación de a, b y y z, el siguiente lema proporciona la propiedad que requerimos

Lema 4.12. Si dos números q y u son tales que $bq \equiv a \pmod{u}$ entonces

$$\prod_{k=1}^{y}(a+bk) \equiv b^y\cdot y!\binom{q+y}{y} \pmod{u}$$

Prueba $b^y\cdot y!\binom{q+y}{y} = b^y(q+y)(q+y-1)\ldots(q+1) =$

$(bq+by)(bq+b(y-1))\ldots(bq+b) \equiv (a+by)\ldots(a+b) \pmod{u}$ $\square$

Ahora basta elegir u mayor que $\prod_{k=1}^{y} a+bk$ y de tal manera que la congruencia $bq \equiv a \pmod{u}$ tenga solución. Estos requisitos los cumple el número $b(a+by)^y+1$. Entonces $\prod_{k=1}^{y} a+bk$ es caracterizado como

$$\prod_{k=1}^{y} a+bk = Rem\left(b^y\cdot y!\binom{q+y}{y}, u\right) \quad \text{donde } u = b(a+by)^y+1$$

Así que $z = \prod_{k=1}^{y}(a+bk) \leftrightarrow \{(\exists m)(\exists p)(\exists q)(\exists r)(\exists s)(\exists t)(\exists u)(\exists v)(\exists w)(\exists x)$

$r = a+by \wedge s = r^y \wedge u = bs+1 \wedge bq = a+ut \wedge m = b^y \wedge v = y! \wedge w = q+y$ $\wedge\ x = \binom{w}{y} \wedge\ Rem(mvx, u) = z\}$

Una vez halladas las expresiones diofantinas correspondientes a las 3 relaciones anteriores estamos en condiciones de probar que los predicados diofantinos son cerrados bajo la operación lógica de cuantificación universal acotada, que es lo único que nos falta para tener el inverso del teorema 4.1. En efecto, hemos descrito, paso a paso, el modo de hallar para cada conjunto A recursivamente enumerable un polinomio P de tal manera que

$$X^{(n)} \in A \leftrightarrow (\exists u)(\forall y \le u)(\exists v_1 \le u) \ldots (\exists v_n \le u)\, P(u, y, v_1, \ldots v_n, X^{(n)}) = 0$$

Ahora veremos que ésta identidad es equivalente a un sistema de ecuaciones diofantinas. El lector puede convencerse, tanto de la plausibilidad de este proceso que transforma el predicado original en otro diofantino, como de la dificultad de realizarlo para un caso concreto no trivial. Así, por ejemplo, cada relación exponencial que aparezca en el desarrollo debe reemplazarse por un sistema de 12 ecuaciones diofantinas con 20 cuantificadores existenciales. Sin embargo, el procedimiento descrito es efectivo en el sentido en que hemos empleado esta palabra.

Teorema 4.13. Dado $P(u, y, v_1, \ldots, v_m, x_1, \ldots, x_n)$ un polinomio sea $Q(u, x_1, \ldots x_n)$ otro con las siguientes propiedades

(1) $Q(u, X^{(n)}) > u$

(2) Para cualesquiera $y, v_1, \ldots, v_m \le u$

$$|P(u, y, v_1, \ldots, v_m, x_1, \ldots, x_n)| \le Q(u, x_1, \ldots, x_n)$$

entonces $(\forall y \le u)(\exists v_1 \le u)(\exists v_2 \le u) \ldots (\exists v_m \le u)[P(u, y, v_1, \ldots, v_m, x_1, \ldots, x_n) = 0]$ (3)

Si y sólo si $(\exists T)(\exists c)(\exists a_1, \ldots, a_m)[T = Q(u, X^{(n)})! \wedge 1 + cT = \prod_{i=1}^{u} 1 + iT$

$$\wedge\ 1 + cT \mid P(u, c, a_1, \ldots, a_m, x_1, \ldots, x_n) \wedge 1 + cT \mid \prod_{j=1}^{u} (a_1 - j) \ldots \wedge 1 + cT \mid \prod_{j=1}^{u} (a_m - j) \quad (4)$$

Dem. $\Leftarrow$ Supongamos la condición (4). Para cada $y \le u$ sea P_y un factor primo de $1 + yT$ y llamemos v_i^y al residuo de dividir a_i entre P_y. Es decir

$$\operatorname{Rem}(a_i, P_y) = v_i^y$$

Por hipótesis $P_y \mid 1 + yT$, $1 + yT \mid 1 + cT$ y $1 + cT \mid \prod_{j=1}^{u} (a_k - j)$ por lo cual $P_y \mid \prod_{j=1}^{u} a_k - j$ y ya que P_y es primo $P_y \mid a_k - j$ para alguna $j = 1, \ldots, u$ o bien

$$j \equiv a_k \equiv v_k^y \pmod{P_y} \quad y \quad j \le u < P_y \quad \text{pues}$$

Si u fuera mayor o igual que p_y, dado que $\varphi(u, X^{(n)})! = T$ y por (1) p_y dividiría a T lo que es imposible, asimismo $v_k^y < p_y$, por lo tanto $v_k^y = j$ y $v_k^y < u$. Ahora mostraremos que

$$P(u, y, v_1^y, v_2^y, \dots, v_m^y, X^{(n)}) = 0 \qquad \text{para cada } y \le u$$

Primeramente obsérvese que

$p_y \mid y(1+cT)$ y $p_y \mid c(1+yT)$ y por ende $p_y \mid c-y$ ó

$c \equiv y \pmod{p_y}$. También $v_k^y \equiv a_k \pmod{p_y}$ para $k=1,\dots,m$

Por ello

$$P(u, y, v_1^y, \dots, v_m^y, X^{(n)}) \equiv P(u, c, a_1, \dots, a_m, X^{(n)}) \equiv 0 \pmod{p_y}$$

Además $p_y > \varphi(u, X^{(n)}) > |P(u, y, v_1^y, \dots, v_m^y, X^{(n)})|$ porque de otro modo p_y sería divisor de T

$\Leftarrow$) Nuevamente designemos con $v_1^y, \dots, v_m^y$ a los números, que para cada $y \le u$, satisfacen (3). Sean c y T tales que

$$\varphi(u, X^{(n)})! = T \quad \text{y} \quad 1 + cT = \prod_{i=1}^{u} 1 + iT$$

Como antes, $c \equiv y \mod 1+yT$ y los números $1+rT$ y $1+sT$ $(r,s \le u)$ son primos entre sí; porque si $p \mid 1+rT$ y $p \mid 1+sT$, entonces $p \mid r-s$ y eso implica que $p<u$ y que $p \mid T$ (por (1)) ⨳. Por lo tanto existen $a_1, \dots, a_m$ que solucionan el sistema de congruencias

$$\begin{aligned} a_j &\equiv v_j^1 \pmod{1+T} \\ a_j &\equiv v_j^2 \pmod{1+2T} \\ &\ \ \vdots \\ a_j &\equiv v_j^u \pmod{1+uT} \end{aligned} \qquad 1 \le j \le m$$

y $P(u, c, a_1, \dots, a_m, X^{(n)}) \equiv P(u, y, v_1^y, \dots, v_m^y, X^{(n)}) \equiv 0 \pmod{1+yT}$

ó bien

$$1+yT \mid P(u, c, a_1, \dots, a_m, X^{(n)})$$

y como los números $1+yT$ son primos entre sí, se concluye que

$$\prod_{y=1}^{u} (1+yT) = 1+cT \mid P(u, c, a_1, \dots, a_m, X^{(n)})$$

Por último $1+yT \mid a_j - v_j^y$ pues $a_j \equiv v_j^y \pmod{1+yT}$

y ya que $1 \le v_j^y \le u$,

para $j=1,\dots,m$, $1+yT \mid \prod_{i=1}^{u} (a_j - i)$ y más aún $1+cT \mid \prod_{i=1}^{u} (a_j - i)$

□

Si u fuera mayor o igual que P_y, dado que $\varphi(u, X^{(n)})! = T$ y por (1) P_y dividiría a T lo que es imposible; asimismo $v_k^y < P_y$, por lo tanto $v_k^y = j$ y $v_k^y < u$. Ahora mostraremos que

$$P(u, y, v_1^y, v_2^y, \ldots, v_m^y, X^{(n)}) = 0 \quad \text{para cada } y \leq u$$

Primeramente obsérvese que

$P_y \mid y(1+cT)$ y $P_y \mid c(1+yT)$ y por ende $P_y \mid c-y$ ó

$c \equiv y \pmod{P_y}$. También $v_k^y \equiv a_k \pmod{P_y}$ para $k=1, \ldots, m$

Por ello

$$P(u, y, v_1^y, \ldots, v_m^y, X^{(n)}) \equiv P(u, c, a_1, \ldots, a_m, X^{(n)}) \equiv 0 \pmod{P_y}$$

Además $P_y > \varphi(u, X^{(n)}) > |P(u, y, v_1^y, \ldots, v_m^y, X^{(n)})|$ porque de otro modo P_y sería divisor de T

$\Rightarrow$) Nuevamente designemos con $v_1^y, \ldots, v_m^y$ a los números, que para cada $y \leq u$, satisfacen (3). Sean c y T tales que

$$\varphi(u, X^{(n)})! = T \quad y \quad 1+cT = \prod_{i=1}^{u} 1+iT$$

Como antes, $c \equiv y \mod 1+yT$ y los números $1+rT$ y $1+sT$ $(r, s \leq u)$ son primos entre sí; porque si $p \mid 1+rT$ y $p \mid 1+sT$, entonces $p \mid r-s$ y eso implica que $p < u$ y que $p \mid T$ (por (1)) ✗. Por lo tanto existen $a_1, \ldots, a_m$ que solucionan el sistema de congruencias

$$\begin{array}{lll} a_j \equiv v_j^1 & \pmod{1+T} & \\ a_j \equiv v_j^2 & \pmod{1+2T} & 1 \leq j \leq m \\ \vdots & \vdots & \vdots \\ a_j \equiv v_j^u & \pmod{1+uT} & \end{array}$$

y $P(u, c, a_1, \ldots, a_m, X^{(n)}) \equiv P(u, y, v_1^y, \ldots, v_m^y, X^{(n)}) = 0 \pmod{1+yT}$

ó bien

$1+yT \mid P(u, c, a_1, \ldots, a_m, X^{(n)})$ y como los números $1+yT$ son primos entre sí, se concluye que

$$\prod_{y=1}^{u} (1+yT) = 1+cT \mid P(u, c, a_1, \ldots, a_m, X^{(n)})$$

Por último $1+yT \mid a_j - v_j^y$ pues $a_j \equiv v_j^y \pmod{1+yT}$

y ya que $1 \leq v_j^y \leq u$,

Para $j=1, \ldots, m$, $1+yT \mid \prod_{i=1}^{u} (a_j - i)$ y más aún $1+cT \mid \prod_{i=1}^{u} (a_j - i)$ $\square$

Teorema 4.14 Cada conjunto recursivamente enumerable es diofantino

Dem. Sólo falta mostrar cómo puede hallarse el polinomio Q que aparece en el antecedente del teorema anterior. Si $P(u, Y, v_1, \ldots, v_m, X^{(n)})$ es de la forma

$$P = \sum_{j=1}^{\ell} T_j \quad \text{donde} \quad T_j = K u^{\alpha} y^{\beta} v_1^{r_1} \ldots v_m^{r_m} x_1^{s_1} \ldots x_n^{s_n}$$

Sea $$U_j = |K|\, u^{\alpha+\beta+r_1+\ldots+r_m} x_1^{s_1} \ldots x_n^{s_n}$$

y sea $$Q(u, x_1, \ldots, x_n) = u + \sum_{j=1}^{\ell} U_j$$

entonces Q satisface trivialmente las condiciones (1) y (2). Esto completa la prueba. □

En el capítulo anterior demostramos que el conjunto

$$W = \{x \mid (\exists y)\, T(x, x, y)\}$$

es recursivamente enumerable, pero no recursivo. Por lo tanto, existe un polinomio $P(x, y^{(m)})$, efectivamente construible, tal que

$$x \in W \leftrightarrow (\exists y^{(m)})\, P(x, y^{(m)}) = 0$$

Supongamos que hubiera un algoritmo que ante cualquier ecuación polinomial diofantina decidiera si tiene o no raices naturales. Entonces podría tambien determinarse algorítmica o recursivamente la cuestión de si $x \in W$ ó no, contradiciendo lo que ya sabemos. Concluimos que:

Teorema 4.15 El décimo problema de Hilbert es insoluble.

CAPITULO V

EL TEOREMA DE GÖDEL

Una vez que ha quedado demostrada la solución negativa del décimo problema de Hilbert, veremos ahora cómo se relaciona con el célebre Teorema de Gödel. Este resultado, uno de los mas importantes en la historia de la Lógica, establece la imposibilidad de formalizar completamente la Matemática clásica, y en particular, la Teoría elemental de números. La versión que de él probaremos es un poco mas específica que la original, y es la siguiente.

Teorema 5.1 Para cada axiomatización formal y consistente de la teoría de números hay una ecuación diofantina, la cual no tiene solución en los naturales, pero tal que este hecho no puede probarse en la axiomatización dada.

En realidad, demostraremos el teorema 5.1 para una teoría de 1er orden singular, y dejaremos al lector interesado, el obtener, a través del análisis de la demostración, condiciones mas generales de validez que lo hacen extensible a otros sistemas formales.

Empecemos describiendo un sistema lo suficientemente poderoso, desde el punto de vista deductivo, como para contener teoremas que, bajo una cierta interpretación, correspondan a las mas relevantes proposiciones verdaderas de la Aritmética elemental. Para ello introduciremos entre sus axiomas, algunos que representan una formalización de los postulados que DedeKind en 1901, dió informalmente, para la aritmética y que podemos formular así:

1) 0 es un número natural

2) Si x es un número natural, hay otro número natural, denotado sx (llamado el sucesor de x)

3) $0 \neq Sx$ para cualquier número natural x

4) Si $Sx = Sy$, entonces $x = y$

5) Si el 0 tiene una propiedad P, y cada vez que un número x tiene esa propiedad, Sx la tiene, entonces todo número natural la tiene.

Estos principios son conocidos como los Axiomas de Peano. A continuación describiremos un sistema 'adecuado' para su formalización

Sea F la teoría de 1er orden que consta de los siguientes símbolos primitivos:

$)$, $($	paréntesis	símbolos lógicos y de agrupación
$\sim$ $\to$		
$x_0, x_1, x_2, \ldots$	variables	
a_0	una constante individual	
A_1^2	una letra predicativa	
f_1^2, f_2^2, f_1^1	y tres letras funcionales	

Definición 5.1 Una expresión de F es cualquier sucesión finita de símbolos de F

Desde aquí hacemos una convención que facilita la lectura de las fórmulas. En lugar de escribir, por ejemplo A_1^2xy, pondremos $x = y$, y asimismo reemplazaremos f_1^1x, f_1^2xy, f_2^2xy, por Sx, $x+y$, y $x \cdot y$ respectivamente. La constante a_0 simbolizará en F al número 0 y Sx a la función sucesor $S(x) = x+1$.

Las reglas para construir fórmulas mas complejas, a partir de los símbolos dados, están contenidos en forma recursiva en las definiciones de 'término', 'fórmula atómica' y 'fórmula bien formada'

Definición 5.2

1) a_0 es un término

2) x_i es un término $(i \geq 0)$

3) Si T_1 y T_2 son términos, también lo son $(T_1 + T_2)$, $(T_1 \cdot T_2)$ y ST_1

Definición 5.3 Si t_1 y t_2 son términos, $t_1 = t_2$ es una fórmula atómica.

Definición 5.4.

1) las fórmulas atómicas son fómulas bien formadas.

2) $(A \to B)$, $\sim A$, y $(x)A$ son fórmulas bien formadas si A y B lo son y x es una variable.

Abreviaremos la expresión "fórmula bien formada" con f.b.f.

Es posible, desde luego, introducir entre los símbolos primitivos algunos que representen otras operaciones lógicas como la conjunción o la disyunción, y otras relaciones numéricas. Habría entonces que complicar un poco la descripción de la sintaxis del sistema, y luego agregar nuevos axiomas a la lista que damos a continuación. Eso alargaría la prueba sin alterarla en nada esencial. Optamos por un camino mas breve

Si A es una f.b.f. y $x_{i_1}, \ldots, x_{i_n}$, n variables cualesquiera, la notación $Ax_{i_1} \ldots x_{i_n}$ (o bien $A(x_{i_1}, \ldots, x_{i_n})$ indicará que las variables que aparecen libres en A pertenecen al conjunto $\{x_{i_1}, \ldots, x_{i_n}\}$; en tanto que $At_1 \ldots t_n$ (o $A(t_1, \ldots t_n)$) denotará el resultado de reemplazar en A cada uno de los términos t_j por todas las ocurrencias libres de x_{i_j}. Con esta notación pasemos ahora a especificar los axiomas de S

Sean A, B y C f.b.fs, v una variable, y t un término. Son axiomas de F:

(1) $(A \to (B \to A))$

(2) $((A \to (B \to C)) \to ((A \to B) \to (A \to C)))$

(3) $((\sim B \to \sim A) \to (A \to B))$

(4) $((v)Av \to At)$ si t es libre para v en Av

(5) $(A \to (v)A)$ si v no aparece libre en A

(6) $((v)(A \to B) \to ((v)A \to (v)B))$

Estos axiomas junto con el 21) (Cf. mas adelante) aplicado a ellos, garantizan que entre los Teoremas de F se hallan necesariamente todas las fórmulas de F que sean universalmente válidas. Suponemos en el lector conocimiento de este hecho.

(7) $(x_1 = x_2 \to (x_1 = x_3 \to x_2 = x_3))$

(8) $(x_1 = x_2 \to Sx_1 = Sx_2)$

(9) $(Sx_1 = Sx_2 \to x_1 = x_2)$

(10) $\sim 0 = Sx_1$

(11) $(x_1 + 0) = x_1$

(12) $S(x_1 + x_2) = x_1 + Sx_2$

(13) $(x_1 \cdot 0) = 0$

(14) $(x_1 \cdot Sx_2) = ((x_1 \cdot x_2) + x_1)$

(15) $(x_1 + x_2) = (x_2 + x_1)$

(16) $(x_1 + (x_2 + x_3)) = ((x_1 + x_2) + x_3)$

(17) $(x_1 \cdot x_2) = (x_2 \cdot x_1)$

(18) $(x_1 \cdot (x_2 \cdot x_3)) = ((x_1 \cdot x_2) \cdot x_3)$

(19) $(x_1 \cdot (x_2 + x_3)) = ((x_1 \cdot x_2) + (x_1 \cdot x_3))$

(20) $A0 \to ((v)(Av \to ASv) \to (v)Av)$

(21) $(v)A$ es axioma, si A lo es.

En este segundo grupo de axiomas, una parte ((9), (10) y (20)) corresponde a los postulados de Peano antes referidos. Otra parte establece las propiedades elementales de la igualdad ((7) y (8)) y las definiciones recursivas de suma y multiplicación ((11), (12), (13) y (14)). Los axiomas (15), (16), (17), (18) y (19), no son, en rigor, independientes de los otros, sino que podrían suprimirse. En ese caso, aparecerían mas adelante como teoremas. Como es fácil imaginar, el incluirlos entre los axiomas tiene por objeto acortar un poco la demostración que veremos a lo largo del capítulo, y sin que, por ello, pierda ninguna validez.

La única regla de inferencia de F es el modus ponens: de A y $(A \to B)$ se sigue B. Abreviaremos la indicación de que esta regla ha sido aplicada con 'MP'.

Teorema 5.2 Si A es una f.b.f. y $\vdash_F A$, entonces $\vdash_F (x)A$ donde x es cualquier variable.

Demostración Supongamos que $A_1, \ldots, A_n = A$ es una prueba en F de A. Si A es un axioma, el resultado se sigue trivialmente por (21). Si, en cambio, A proviene de A_i y $A_j = (A_i \to A)$ por modus ponens. (con $i, j < n$) procedemos por inducción suponiendo verdadero el enunciado del teorema para A_i y A_j:

$$\vdash (x) A_i \quad y \quad \vdash (x)(A_i \to A)^{*}$$

y por ax. (6) y M.P. $\vdash ((x) A_i \to (x) A)$

y de nuevo por M.P. $\vdash (x) A$

Teorema 5.3. Si una f.b.f. Ax es teorema de F, asimismo lo es $A\tau$ donde τ es un término libre para x en Ax.

Dem. $\vdash Ax$ implica $\vdash (x) Ax$ como acabamos de ver y

$\vdash ((x) Ax \to A\tau)$ Ax (4).

$\therefore \vdash A\tau$ por M.P.

En particular en los axiomas 7 a 19 podemos substituir las variables por cualesquiera términos y obtener siempre teoremas.

El no tener F sino una regla de inferencia queda compensado por lo que el teorema 5.2 establece, a saber, la posibilidad de hallar nuevos teoremas aplicando la cuantificación universal a los ya obtenidos.

Además, no sólo sabemos que fórmulas como

$$(a_0 \cdot 0) = 0 \quad y \quad (x_1)(x_1 + 0) = x_1$$

son teoremas, sino también que podemos construir sus pruebas respectivas. Para ello bastaría seguir los pasos de alguna de las dos demostraciones anteriores para cada caso particular.

Otra propiedad de F que, con algunas restricciones y variantes, es válida para cualquier teoría de 1er orden es la que se enuncia en el siguiente teorema y su corolario.

Teorema 5.4. Si A y B son f.b.f.s y $A \vdash_F B$ entonces $\vdash_F (A \to B)$

Dem. Sea $W_1, \ldots W_n = B$ una deducción en F de B a partir de A. Por in-

* Escribimos simplemente $\vdash A$, en lugar de $\vdash_F A$.

ducción demostraremos que $\vdash A \to W_i^*$ para cada i $(1 \leq i \leq n)$.

Si $i=1$ y B es un axioma, entonces la siguientes es una prueba de $A \to B$ en F

1) W_1 ax.

2) $W_1 \to (A \to W_1)$ ax. (1)

3) $A \to W_1$ M.P. 1 y 2

Si $W_1 = A$, $\vdash A \to W_1$, pues es una prueba de F:

1) $A \to ((A \to A) \to A)$ ax. (1)

2) $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ ax. (2)

3) $(A \to (A \to A))$ ax. (1)

4) $(A \to (A \to A)) \to (A \to A)$ M.P. 1 y 2.

5) $A \to A$ MP 3 y 4.

Ahora bien si $i > 1$ y W_i es A ó es un axioma, procedemos como antes. En caso contrario W_i proviene de fórmulas anteriores en la sucesion, digamos W_j y $W_K = W_j \to W_i$ $(K, j < i)$ por modus ponens. Por hipótesis de inducción $\vdash A \to (W_j \to W_i)$ y $\vdash A \to W_j$. Además

$$\vdash (A \to (W_j \to W_i)) \to ((A \to W_j) \to (A \to W_i))$$

Así que $\vdash A \to W_i$ por 2 M.P.

Corolario 5.5. Si Γ es un conjunto de f. b. f.s y $\Gamma \cup \{A\} \vdash B$, entonces $\Gamma \vdash A \to B$.

Este resultado es conocido como el 'teorema de la deducción' que en F es válido sin restricciones

Se le denomina 'interpretación standurd' de F a la que tiene por dominio los números naturales y en la que los símbolos S, +, • se interpretan como las funciones sucesor $(x \mapsto x+1)$, suma y producto, respectivamente, a_0 como el número 0, y el predicado A_1^2 como la igualdad. La prueba de que esta interpretación es un modelo de F es incierta porque emplea argumentos de la Teoría de Conjuntos que no son muy legítimos dentro de la Metamatemática, debido en

* A veces, deliberadamente, suprimimos algunos paréntesis para facilitar la lectura de las fórmulas, cuando eso no da pie a ninguna confusión.

parte a que pueden considerarse mas 'fuertes' que aquello que se pretende probar, y en parte a que en dicha teoría subsisten problemas relativos a su consistencia, etc. Por ello en el teorema de Gödel aplicado a F, que vemos mas adelante, la consistencia de F aparecerá como una suposición o como el antecedente de una implicación.

Los términos son las expresiones de F que, de acuerdo a la interpretación standard representan números naturales. De entre ellos, a los que resultan mas simples, y que son como los nombres de los números en F, los llamaremos 'cifras'. Mas específicamente:

Definición 5.5

1) a_0 es cifra

2) Si w es cifra, también lo es sw.

Así, por ejemplo, al 5 corresponde en F la cifra $sssssa_0$.

Denotaremos a $\underbrace{ss\ldots s}_{n \text{ veces}}a_0$ con $\bar{n}$ $(n \geq 0)$

Teorema 5.6.

1) Si $n=m$, entonces $\vdash \bar{n}=\bar{m}$.

Primeramente veremos que $\vdash x_1=x_1$

1. $(x_1+0)=x_1 \rightarrow ((x_1+0)=x_1 \rightarrow x_1=x_1)$ Ax 7*

2 $(x_1+0)=x_1$ AX.1

3. $x_1=x_1$ 2 veces M.P.

Ahora el resultado se sigue del enunciado del Teorema 5.3 porque, evidentemente si $n=m$, $\bar{n}$ y $\bar{m}$ son el mismo término.

2) Si $n \neq m$, entonces $\vdash \bar{n} \neq \bar{m}$

Dem. Supóngase que $n>m$.

1. $\bar{m}=\bar{n}$ hipótesis

2. $(\bar{m}=\bar{n} \rightarrow \overline{m-1}=\overline{n-1})$ Ax 9*

3. $\overline{m-1}=\overline{n-1}$ M.P. 1 y 2.

⋮ ⋮

K) $\bar{0}=\overline{n-m}$ reiteradas aplicaciones de ax.9 y M.P.

* Aquí, como en otros casos mas adelante, debe sobreentenderse que estamos aplicando el teorema 5.3.

K) $\bar{0} = S\,\overline{n-m-1}$ otra forma de escribir K) $(n-m-1 \geq 0)$.

K+1) $\bar{0} \neq S\,\overline{n-m-1}$ Ax. 10.

K+2) $\bar{0} = S\,\overline{n-m-1} \wedge \bar{0} \neq S\,\overline{n-m-1}$ tautología

K+3) $\vdash \bar{n} = \bar{m} \rightarrow 0 = S\,\overline{n-m-1} \wedge 0 \neq S\,\overline{n-m-1}$ teo. 5.4.

K+4) $\bar{n} \neq \bar{m}$ tautología $(P \rightarrow (Q \wedge \sim Q)) \rightarrow \sim P$

3) Si $n+m=r$ entonces $\vdash \bar{n}+\bar{m}=\bar{r}$

Dem. por inducción sobre m.

Si $m=0$, $\bar{n}=\bar{r}$ y $\vdash \bar{n}+\bar{0}=\bar{r}$ AX. (11)

Supongamos que una prueba de F termina con la fórmula

K) $\bar{n}+\bar{m}=\bar{r}$; agreguemósle los siguientes pasos:

K+1) $\bar{n}+\bar{m}=\bar{r} \rightarrow S(\bar{n}+\bar{m})=S\bar{r}$ ax (8)

K+2) $S(\bar{n}+\bar{m})=S\bar{r}$ M.P. K) y K+1)

K+3) $S(\bar{n}+\bar{m})=(\bar{n}+S\bar{m})$ AX 12.

K+4) $S(\bar{n}+\bar{m})=(\bar{n}+S\bar{m}) \rightarrow (S(\bar{n}+\bar{m})=S\bar{r} \rightarrow \bar{n}+S\bar{m}=S\bar{r})$ AX. 7.

K+5) $S(\bar{n}+\bar{m})=S\bar{r} \rightarrow (\bar{n}+S\bar{m})=S\bar{r}$ M.P. K+3) y K+4)

K+6) $\bar{n}+S\bar{m}=S\bar{r}$ M.P K+2) y K+5)

pero $S\bar{m}=\overline{m+1}$ y $S\bar{r}=\overline{r+1}$

4) Si $n \cdot m = r$, entonces $\vdash \bar{n}\cdot\bar{m}=\bar{r}$

Dem. análoga a la de 3).

Siguiendo la práctica común en las exposiciones del Teorema de Gödel, entraríamos aquí en el estudio detallado de las características sintácticas de nuestro sistema formal F. El objetivo sería el de mostrar que sus axiomas y reglas de inferencia bastan para probar fórmulas que, en la interpretación standard, se traducen en las mas básicas e importantes proposiciones de la Aritmética. Por citar un ejemplo, veríamos que

$$(\sim y=0 \rightarrow ((x\cdot y)=(z\cdot y) \rightarrow x=z)$$

o que $(\sim x=0 \rightarrow (\exists y)(Sy=x))$

son Teoremas de F, (obviamente en esta última expresión el símbolo para el cuantificador existencial puede considerarse una mera abreviatura de $\sim(y)\sim$

Esta incursión, en el aspecto deductivo y formal del sistema, suele ser de utilidad en la prueba subsiguiente. Podemos, sin embargo, evitar este paso, así como el que se refiere a la representabilidad de las funciones recursivas, gracias a que hemos dejado establecida la solución del décimo problema de Hilbert. Claro que el probar teoremas de F tiene además un valor didáctico, que no desconocemos. En todo caso, recomendamos al lector interesado que consulte libros como el de Mendelson, o el de G. Hunter (Cf. la bibliografía al final) que emplean sistemas muy similares al nuestro. Procederemos aquí mas directamente, aprovechando, en buena parte, el material de los capítulos anteriores.

Se trata de mostrar que F es un sistema incompleto tanto sintáctica como semánticamente (suponiéndolo consistente). Es decir que en él puede hallarse efectivamente una fórmula verdadera, de acuerdo a la interpretación standard y tal que ni ella, ni su negación, sean teoremas de F.

Haremos uso nuevamente de la Aritmetización, técnica que en el capítulo II nos sirvió para construir predicados recursivos referentes a las operaciones con algoritmos normales. Análogamente comenzamos aquí definiendo una función g que asocie un número a cada uno de los símbolos elementales de F de la siguiente manera

)	(	$\sim$	$\rightarrow$	a_0	$=$	S	+	$\cdot$	x_0	x_1	
3	5	7	9	11	13	15	17	19	21	23	y $g(x_j) = 21 + 2j$ $(j \geq 2)$

Para cada expresión $w = s_0 s_1 \ldots s_n$ donde $s_0, \ldots, s_n$ son cualesquiera símbolos de F, definimos

$$g(w) = \prod_{j=0}^{n} pr(j)^{g(s_j)}$$

y, por último, a la sucesión de expresiones $e = c_0 \ldots c_n$, g hace corresponder el número

$$g(e) = \prod_{j=0}^{n} pr(j)^{g(c_j)}$$

en general llamaremos a $n = g(w)$ el número de Gödel de w, y en ese caso escribiremos $exp(n) = w$.

Desde luego que si pensamos como diferentes objetos del dominio a un símbolo considerado simplemente como tal, o como una expresión o como una sucesión de expresiones, entonces la función g es biunívoca sobre su rango; y la demostración de este hecho es análoga a la que se dió en el capítulo II a propósito de la función g allí definida. Debemos hacer notar, nuevamente, que el procedimiento que conduce de los símbolo o expresiones de F a sus números de Gödel, o viceversa, es efectivo.

Ahora a cada relación o propiedad R entre los elementos de nuestro sistema formal corresponde una relación $\tilde{R}$ entre sus respectivos números de Gödel. Por ejemplo, si $R(x_1, x_2, x_3)$ es un predicado metamatemático entre expresiones de F, tal como ser x_3 el resultado de aplicar modus ponens a x_1 y x_2, entonces sea

$$\tilde{R} = \{(n, m, w) \in \mathbb{N}^3 \mid R(\exp(n), \exp(m), \exp(w))\}$$

Daremos a continuación una serie de predicados y funciones relacionados con la sintaxis de F que son recursivo primitivos.

1) $VAR(X) \leftrightarrow \underset{Y<X}{\exists} (X = 21 + 2Y)$

VAR(X) si y sólo si X es el número de Gödel de una variable.

2) $VARE(X) \leftrightarrow \underset{Y<X}{\exists} (VAR(Y) \wedge X = 2^Y)$

VARE(X) se satisface si exp(X) es una expresión que consta de una sola variable

3) $NON(X) \leftrightarrow \underset{Y<X}{\exists} (X = 2Y + 3)$

NON(X) es verdadero si X es el número de Gödel de un símbolo primitivo de F.

4) $EX(X) \leftrightarrow GN(X) \wedge \underset{Y<\ell(X)}{\forall} NON(e(X,Y))$*

*Para la definición de GN(X), $\ell(X)$, etc. ver capítulo II

EX(X) se satisface si X es el número de Gödel de una expresión de F.

5) $Num(0) = 2^{11}$

$Num(y+1) = 2^{15} * Num(y)$

Num(y) es el número de Gödel de $\overline{y}$

6) $MP(X,Y,Z) \leftrightarrow EX(X) \wedge EX(Y) \wedge EX(Z) \wedge (Y = X * 2^{9} * Z)$

MP(X,Y,Z) se cumple si X, Y, Z son números de Gödel de expresiones $\mathfrak{X}$ $\mathfrak{Y}$ y $\mathfrak{Z}$, y $\mathfrak{Z}$ se sigue de $\mathfrak{X}$ y $\mathfrak{Y}$ por modus ponens.

7) $CFR(X) \leftrightarrow X = 2^{11} \vee \underset{Y<X}{\exists} (CFR(Y) \wedge X = 2^{15} * Y)$

CFR(X) es verdadero si X es el número de Gödel de una cifra.

8) $Sum(X,Y) = 2^{5} * X * 2^{17} * Y * 2^{3}$

Sum(X,Y) es el número de Gödel de la expresión (exp(X) + exp(Y))

9) $Mult(X,Y) = 2^{5} * X * 2^{19} * Y * 2^{3}$

Si $exp(X) = T_1$ y $exp(Y) = T_2$ son términos Mult(X,Y) es el número de Gödel de la expresión $(T_1 \cdot T_2)$

10) $Suc(X) = 2^{15} * X$

Suc(X) es el número de Gödel de la expresión S(exp(X))

11) $TERM(X) \leftrightarrow X = 2^{11} \vee VARE(X) \vee \Big(\underset{Y<X}{\exists}\ \underset{Z<X}{\exists}\ TERM(Y) \wedge TERM(Z) \wedge$

$(X = Sum(Y,Z) \vee X = Mult(Y,Z) \vee X = Suc(Y))\Big)$

TERM(X) se satisface si exp(X) es un término

12) $FMAT(X) \leftrightarrow \underset{Y<X}{\exists}\ \underset{Z<X}{\exists}\ TERM(Y) \wedge TERM(Z) \wedge X = Y * 2^{13} * Z$

$FMAT(X) \leftrightarrow$ X es el número de Gödel de una fórmula atómica

13) $\mathrm{Imp}(X,Y) = 2^5 * X * 2^9 * Y * 2^3$

Si $exp(X) = \mathfrak{X}$ y $exp(Y) = \mathfrak{Y}$ son f.b.f.s $\mathrm{Imp}(X,Y)$ proporciona el número de Gödel de la fórmula $(\mathfrak{X} \to \mathfrak{Y})$

14) $\mathrm{Neg}(X) = 2^7 * X$

Si $exp(X)$ es una fórmula, $\mathrm{Neg}(X)$ es el número de Gödel de su negación.

15) $\mathrm{Geni}(X,K) = 2^5 \cdot 3^{21+2K} \cdot 5^3 * X$

Si $exp(X) = A$, $\mathrm{Geni}(X,K)$ es el número de Gödel de $(X_K)A$

16) $\mathrm{Gen}(X,v) = \mathrm{Geni}(X, \mathrm{Co}(e(v,0) \dot{-} 21, 2))$

Si v es el número de Gödel de una expresión que consta de una sola variable X_K, y $exp(X) = A$, entonces $\mathrm{Gen}(X,v)$ es el número de Gödel de $(X_K)A$

17) $\mathrm{FMBF}(X) \leftrightarrow (\mathrm{FMAT}(X) \vee ((\exists_{Y<X} \mathrm{FMBF}(Y) \wedge X = \mathrm{Neg}(Y)) \vee (\exists_{Y<X} \exists_{Z<X} \mathrm{FMBF}(Y) \wedge$

$\mathrm{FMBF}(Z) \wedge X = \mathrm{Imp}(Y,Z)) \vee (\exists_{Y<X} \exists_{Z<X} \mathrm{VARE}(Y) \wedge \mathrm{FMBF}(Z) \wedge X = \mathrm{Gen}(Z,Y)))$

$\mathrm{FMBF}(X) \leftrightarrow$ $exp(X)$ es una fórmula bien formada.

18) $\mathrm{SUBST}_1(X,Y,T,v) \leftrightarrow \mathrm{TERM}(T) \wedge \mathrm{VARE}(v) \wedge \mathrm{TERM}(Y) \wedge ((Y = 2^{11} \wedge X = Y) \vee$

$(Y = v \wedge X = T) \vee (\mathrm{VARE}(Y) \wedge Y \neq v \wedge X = Y) \vee ((\exists_{w<Y} \exists_{u<X} \mathrm{SUBST}_1(u,w,T,v) \wedge$

$Y = \mathrm{suc}(w) \wedge X = \mathrm{suc}(u)) \vee (\exists_{w<Y} \exists_{z<Y} \exists_{u<X} \exists_{m<X} \mathrm{SUBST}_1(u,w,T,v) \wedge$

$\wedge\ \mathrm{SUBST}_1(m,z,T,v) \wedge ((Y = \mathrm{sum}(w,z) \wedge X = \mathrm{sum}(u,m)) \vee (Y = \mathrm{mult}(w,z) \wedge$

$X = \mathrm{mult}(u,m)))))$

$\mathrm{SUBST}_1(X,Y,T,v)$ es cierta si $exp(Y) = A$ es un término y $exp(X)$ es el resultado de substituir en A todas las ocurrencias de la variable con número de

Gödel v por el término exp(T).

19) $SUBST_2(X,Y,\tau,v) \leftrightarrow \exists_{u<X} \exists_{w<X} \exists_{r<Y} \exists_{s<Y}$ $TERM(u) \wedge TERM(v) \wedge X = u * 2^{13} * w \wedge$

$Y = r * 2^{13} * s \wedge SUBST_1(u,r,\tau,v) \wedge SUBST_1(w,s,\tau,v)$

$SUBST_2(X,Y,\tau,v)$ se satisface si exp(Y)= A es una fórmula atómica y exp(X) es el resultado de substituir en A, la variable con número de Gödel v en todas sus ocurrencias por el término con número de Gödel τ.

20) $SUBST_3(X,Y,\tau,v) \leftrightarrow (FMAT(Y) \wedge SUBST_2(X,Y,\tau,v)) \vee (FMBF(Y) \wedge$

$(\exists_{w<Y} \exists_{s<Y} \; Y = Neg(w) \wedge X = Neg(s) \wedge SUBST_3(s,w,\tau,v)) \vee (\exists_{w<Y} \exists_{s<Y} \exists_{r<X} \exists_{z<X}$

$Y = Imp(w,s) \wedge X = Imp(r,z) \wedge SUBST_3(r,w,\tau,v) \wedge SUBST_3(z,s,\tau,v)) \vee$

$(\exists_{z<Y} \exists_{w<Y} \exists_{r<X} \; VARE(z) \wedge Y = Gen(w,z) \wedge X = Gen(r,z) \wedge SUBST_3(r,w,\tau,v) \wedge v \neq z)$

$\vee (\exists_{z<Y} \; Y = Gen(z,v) \wedge X = Y))$.

$SUBST_3(X,Y,\tau,v) \leftrightarrow$ exp(X)= $\mathfrak{X}$ y exp(Y)= $\mathfrak{Y}$ son f.b.f.s., exp(τ)= T es un término, exp(v)= V una variable, y $\mathfrak{X}$ se obtiene al substituir en $\mathfrak{Y}$ todas las ocurrencias libres de V por T.

21) $LIB(Y,v) \leftrightarrow VARE(v) \wedge (TERM(Y) \wedge \sim SUBST_1(Y,Y,2^{21+2v},v)) \vee$

$(FMBF(Y) \wedge \sim SUBST_3(Y,Y,2^{21+2v},v))$.

$LIB(Y,v)$ es verdadera si Y es el número de Gödel de una fórmula o de un término que contiene libre a la variable con número de Gödel v.

22) $LI(X,v,t) \leftrightarrow TERM(t) \wedge VARE(v) \wedge FMBF(X) \wedge (FMAT(X) \vee$

$(\exists_{w<X} \; X = Neg(w) \wedge LI(w,v,\tau)) \vee (\exists_{Y<X} \exists_{z<X} \; X = Imp(Y,z) \wedge LI(Y,v,\tau) \wedge$

$LI(z,v,T) \vee (\exists_{w<x} \exists_{z<x} (VARE(w) \wedge X = Gen(z,w) \wedge ((w \neq z \rightarrow$

$((LI(z,v,T) \wedge \sim LIB(T,w)) \vee (LI(z,v,t) \wedge \sim LIB(z,v))))$

$LI(x,v,t)$ se cumple si $exp(x) = \mathbb{X}$ es una fórmula, $exp(v) = \mathbb{V}$ una variable, $exp(T) = T$ un término y T es libre para V en $\mathbb{X}$

23) a) $AX_1(X) \leftrightarrow \exists_{Y<X} \exists_{Z<X} FMBF(Y) \wedge FMBF(Z) \wedge X = Imp(Y, Imp(Z,Y))$

$AX_1(X) \leftrightarrow$ X es el número de Gödel de una instancia del esquema axiomático número uno

b) $AX_2(X) \leftrightarrow \exists_{Y<X} \exists_{Z<X} \exists_{W<X} FMBF(Y) \wedge FMBF(Z) \wedge FMBF(W) \wedge$

$X = Imp(Imp(Y, Imp(Z,W)), Imp(Imp(Y,Z), Imp(Y,W)))$

$AX_2(X) \leftrightarrow$ X es el número de Gödel de una instancia del esquema axiomático número 2.

c) $AX_3(X) \leftrightarrow \exists_{Y<X} \exists_{Z<X} FMBF(Y) \wedge FMBF(Z) \wedge$

$X = Imp(Imp(Neg(Y), Neg(Z)), Imp(Z,Y))$

$AX_3(X)$ es cierta si X es el número de Gödel de una instancia del esquema axiomático número 3.

d) $AX_4(X) \leftrightarrow \exists_{Y<X} \exists_{Z<X} \exists_{W<X} \exists_{r<X} FMBF(Y) \wedge VARE(Z) \wedge TERM(W) \wedge FMBF(r) \wedge$

$LI(Y,Z,W) \wedge X = Imp(Gen(Y,Z), r) \wedge SUBST_3(r,Y,W,Z)$

$AX_4(X) \leftrightarrow$ $exp(X)$ es una instancia del esquema axiomático no. 3.

e) $AX_5(X) \leftrightarrow \exists_{Z<X} \exists_{Y<X} VARE(Y) \wedge FMBF(Z) \wedge \sim LIB(Z,Y) \wedge X = Imp(Z, Gen(Z,Y))$

$AX_5(X) \leftrightarrow$ X es el número de Gödel de una instancia del esquema axiomático número 5.

f) $AX_6(X) \leftrightarrow \exists_{Z<X} \exists_{W<X} \exists_{Y<X}$ $VARE(Y) \wedge FMBF(Z) \wedge FMBF(W) \wedge$

$X = Imp(Gen(Imp(Z,W),Y), Imp(Gen(Z,Y), Gen(W,Y)))$

$AX_6(X) \leftrightarrow exp(x)$ es una instancia del esquema axiomático no. seis

g) $AX_{7-19}(X) \equiv x$ es el número de Gödel de alguno de los axiomas 7 a 19.

$AX_{7-19}(X)$ es recursivo porque es de la forma:

$X = a_7 \vee X = a_8 \vee \dots \vee X = a_{19}$ donde $exp(a_i)$ es el i-ésimo axioma $(7 \leq i \leq 19)$

h) $AX_I(X) \leftrightarrow \exists_{W<X} \exists_{r<X} \exists_{Y<X} \exists_{Z<X}$ $FMBF(Y) \wedge VARE(Z) \wedge SUBST_2(W, Y, 2^{11}, Z) \wedge$

$SUBST_3(r, Y, 2^{15} * Z, Z) \wedge X = Imp(W, Imp(Gen(Imp(Y,r),Z), Gen(Y,Z)))$

$AX_I(X) \leftrightarrow X$ es el número de Gödel de una instancia del esquema axiomático número 20.

24) $AX(X) \leftrightarrow AX_1(X) \vee AX_2(X) \vee \dots \vee AX_{7-19}(X) \vee AX_I(X) \vee$

$$\left(\exists_{Z<X} \exists_{W<X} VARE(Z) \wedge AX(W) \wedge X = Gen(W,Z)\right)$$

$AX(X)$ se satisface si X es el número de Gödel de un axioma de F

25) $PB(Y) \leftrightarrow \forall_{X<\ell(Y)} \left(AX(e(Y,X)) \vee \left(\exists_{r<X} \exists_{s<X} MP(e(Y,r), e(Y,s), e(Y,X))\right)\right)$

$PB(Y)$ es verdadera si Y es el número de Gödel de una prueba en F.

26) $PR(Y,X) \leftrightarrow PB(Y) \wedge e(Y, \ell(Y) - 1) = X$

$PR(Y,X) \leftrightarrow exp(Y)$ es una prueba de $exp(X)$

Una vez que hemos verificado el caracter recursivo de los anteriores predicados, y especialmente de $PR(Y,X)$ queda ya muy poco para concluir nuestra demostración. Supondremos ahora, no sólo la consistencia de F, que es suficiente para probar que una fórmula 'verdadera' no es teorema de F (i.e. la incompletud semántica), sino una hipótesis, aún mas fuerte, necesaria para probar que en F hay una fórmula indecidible, es decir, que ni ella ni su negación son demostrables. Nos referimos a la asunción de que F posee la propiedad llamada ω-consistencia, que definimos a continuación:

Definición 5.6 Una Teoría de 1er orden K, con los mismos símbolos que F, se dice ω-consistente, si para cada fórmula $A(x)$ de K, si $\vdash_K A(\bar{n})$ para cada número natural n, entonces no es Teorema de K $\sim(x)A(x)$

Teorema 5.7 Si F es ω-consistente, F es consistente.
Demostración. En F es teorema $\bar{n}=\bar{n}$, si F fuera inconsistente habría una prueba de $\sim(x)\,x=x$ (por la tautología $(A\to(\sim A\to B))$) por lo que F sería ω-inconsistente.

Antes de pasar a la demostración formal del teorema de Gödel para F, daremos una versión intuitiva de la misma, que podrá servir de guía en lo que sigue. Supóngase que hemos numerado los predicados de la forma $P(x_0,x_1,\ldots,x_n)=0$ donde P es un polinomio con coeficientes enteros. Veremos que si $P(a_0,a_1,\ldots,a_n)=0$ para ciertos números naturales $a_0,a_1,\ldots,a_n$, una fórmula equivalente $\tilde{P}(\bar{a}_0,\bar{a}_1,\ldots,\bar{a}_n)=\bar{0}$ [donde $\bar{a}_i$ es el numeral de a_i] es teorema de F. Consideremos el conjunto A de números naturales n para los que puede probarse en F que

$$\tilde{P}_n(\bar{n},x_1,\ldots x_m)=0$$

no tiene solución ($P_n(x_0,x_1,\ldots x_m)=0$ es el n-ésimo predicado en el orden dado y $\tilde{P}_n(x_0,\ldots x_m)=0$ es su equivalente formal); es decir que

(1) $n\in A \leftrightarrow \vdash_F (x_1)(x_2)\ldots(x_m)\sim\tilde{P}_n(\bar{n},x_1,\ldots,x_m)=0$ (m, desde luego, depende de n)

o bien

$$n\in A \leftrightarrow \vdash_F \sim\tilde{P}_n(\bar{n},x_1,\ldots,x_m)=0$$

Demostraremos que A es un conjunto recursivamente enumerable o diofantino, es decir que hay un predicado polinomial $P_k(x_0,\ldots,x_r)=0$ tal que

(2) $n\in A \leftrightarrow (\exists a_1,\ldots,a_r)P_k(n,a_1,\ldots,a_r)=0$

lo cual, a su vez, implica que en F se puede probar que

$$\tilde{P}_k(\bar{n},x_1,\ldots,x_r)=0 \text{ tiene solución}$$

mula indecidible, es decir, que ni ella ni su negación son demostrables. Nos referimos a la asunción de que F posee la propiedad llamada ω-consistencia, que definimos a continuación:

Definición 5.6 Una teoría de 1er orden K, con los mismos símbolos que F, se dice ω-consistente, si para cada fórmula $A(x)$ de K, si $\vdash_K A(\bar{n})$ para cada número natural n, entonces no es teorema de K $\sim(x)A(x)$.

Teorema 5.7 Si F es ω-consistente, F es consistente.
Demostración. En F es teorema $\bar{n}=\bar{n}$, si F fuera inconsistente habría una prueba de $\sim(x)\,x=x$ (por la tautología $(A\rightarrow(\sim A\rightarrow B))$) por lo que F sería ω-inconsistente.

Antes de pasar a la demostración formal del teorema de Gödel para F, daremos una versión intuitiva de la misma, que podrá servir de guía en lo que sigue. Supóngase que hemos numerado los predicados de la forma $P(x_0,x_1,\ldots,x_n)=0$* donde P es un polinomio con coeficientes enteros. Veremos que si $P(a_0,a_1,\ldots,a_n)=0$ para ciertos números naturales $a_0,a_1,\ldots,a_n$, una fórmula equivalente $\tilde{P}(\bar{a}_0,\bar{a}_1,\ldots,\bar{a}_n)=\bar{0}$ [donde $\bar{a}_i$ es el numeral de a_i] es teorema de F. Consideremos el conjunto A de números naturales n para los que puede probarse en F que

$$\tilde{P}_n(\bar{n},x_1,\ldots x_m)=0$$

no tiene solución ($P_n(x_0,x_1,\ldots x_m)=0$ es el n-ésimo predicado en el orden dado y $\tilde{P}_n(x_0,\ldots x_m)=0$ es su equivalente formal); es decir que

$$(1)\quad n\in A \leftrightarrow \vdash_F (x_1)(x_2)\ldots(x_m)\sim\tilde{P}_n(\bar{n},x_1,\ldots,x_m)=0$$ (m, desde luego, depende de n)

o bien

$$n\in A \leftrightarrow \vdash_F \sim\tilde{P}_n(\bar{n},x_1,\ldots,x_m)=0$$

Demostraremos que A es un conjunto recursivamente enumerable o diofantino, es decir que hay un predicado polinomial $P_k(x_0,\ldots,x_r)=0$ tal que

$$(2)\quad n\in A \leftrightarrow (\exists a_1,\ldots,a_r)P_k(n,a_1,\ldots,a_r)=0$$

lo cual, a su vez, implica que en F se puede probar que

$$\tilde{P}_k(\bar{n},x_1,\ldots,x_r)=0 \quad \text{tiene solución}$$

si en (1) y (2) ponemos K en lugar de n, y asumimos la consistencia de F, entonces concluimos que $P_K(K, x_1, \ldots, x_r) = 0$ no tiene solución, pero eso no puede probarse en F. Habremos hallado un enunciado que bajo la interpretación standard es verdadero, y que, sin embargo, no es teorema de F. Con ésto en mente veamos ahora la prueba formal.

Dada la naturaleza de nuestro sistema, en lugar de predicados

$$P(x_0, x_1, \ldots, x_m) = 0$$

donde P es un polinomio con coeficientes enteros, consideraremos equivalentemente identidades de la forma

$$R(x_0, x_1, \ldots x_m) = S(x_0, \ldots, x_m)^{*}$$

donde R y S son polinomios con coeficientes naturales. Estos polinomios, a su vez, serán concebidos ahora como expresiones linguísticas de un cierto tipo.

Sea f una función con dominio $\{X \mid X \text{ es un término de } F\}$ tal que

1) $f(x_i) = x_i \quad (i \geq 1)$
2) $f(\bar{n}) = n$
3) $f((\tau_1 + \tau_2)) = (f(\tau_1) + f(\tau_2))$
4) $f((\tau_1 \cdot \tau_2)) = (f(\tau_1) \cdot f(\tau_2))$
5) $f(S\tau_1) = (\tau_1 + 1)$

donde τ_1 y τ_2 son términos y en 5) τ_1 no es una cifra. Por la fórmula $(f(\tau_1) + f(\tau_2))$ debe entenderse una expresión linguística que incluye el símbolo $+$ y los 2 paréntesis, y así también en (4) y (5).

Por ejemplo, a

$$(((SSSa_0 + x_1) + (x_1 \cdot x_2)) + x_3)$$

corresponde bajo F la expresión algebraica

$$(((3 + x_1) \cdot (x_1 \cdot x_2)) + x_3)$$

Si, de manera obvia, extendemos f para que sea aplicable a fórmulas atómicas $(f(\tau_1 = \tau_2) = (f(\tau_1) = f(\tau_2))$ tendremos para cada una de ellas, un predicado polinomial (en un sentido mas amplio de la palabra 'polinomio') y para cada predicado polinomial 'co-

* Recuérdese que esta notación indica que las variables de P y de Q se hallan contenidas en el conjunto $\{x_0 \ldots x_m\}$

rrectamente escrito' habrá una fórmula atómica correspondiente. Así a

$$S((Sa_0 + x_2)\cdot(SSa_0 + x_1)) = x_3$$

corresponde el predicado polinomial*

$$((1 + x_2)(2 + x_1) + 1) = x_3$$

y de la fórmula original diremos que representa en F al predicado respectivo.

El Teorema 5.6 demuestra que si

$P(x_0, x_1, \ldots, x_n) = Q(x_0, \ldots, x_n)$ es un predicado polinomial y tenemos que $P(a_0, a_1, \ldots, a_n) = Q(a_0, \ldots, a_n)$ (con $a_i \in \mathbb{N}$), entonces la fórmula que representa este hecho en F $A(\bar{a}_1, \ldots, \bar{a}_n)$ es un teorema de F. Así por ejemplo, de $((3+0)+(3\cdot 3)) = 12$

se sigue que $\vdash_F ((\bar{3}+\bar{0})+(\bar{3}\cdot\bar{3})) = \overline{12}$

Obviamente, si enumeramos las fórmulas atómicas, quedan a su vez enumerados los predicados polinomiales. Esto lo logramos con la siguiente función h.

Sea $C_{AT}(X)$ la función característica del predicado FMAT(X). Definimos

$$h(x) = \overline{sgn}\, C_{AT}(x)\cdot x + C_{AT}(x)\cdot g(0=0)$$
$$= \overline{sgn}\, C_{AT}(x)\cdot x + C_{AT}(x)\cdot 2^{11}\cdot 3^{13}\cdot 5^{11}$$

El rango de h es el conjunto de fórmulas atómicas. Obsérvese que $h(x) = x$ si FMAT(x). Entonces h enumera los predicados polinomiales repitiendo tan sólo $(0=0)$ en el n-ésimo lugar cada vez que FMAT(n) es falso. Denotemos con $P_i(x_0 \ldots) = Q_i(x_0 \ldots)$ al predicado i-ésimo en este orden

Teorema 5.8 El conjunto A de números n tales que en F se prueba que $P_n(n, x_1, \ldots) = Q_n(n, x_1, \ldots)$ no tiene solución es recursivamente enumerable.

Dem. Aquí, por supuesto, 'probarse en F que $P_n(n, x_1, \ldots) = Q_n(n, x_1, \ldots)$ no tiene solución' significa que

* Llamamos ahora 'predicados polinomiales' a las imágenes bajo F de las fórmulas atómicas.

$$\vdash_F (x_1)\ldots(x_e) \sim \tilde{P}_n(\bar{n}, x_1, \ldots, x_e) = \tilde{Q}_n(\bar{n}, x_1, \ldots, x_e)$$

ó $\vdash_F \sim \tilde{P}_n(\bar{n}, x_1, \ldots, x_e) = \tilde{Q}_n(\bar{n}, x_1, \ldots, x_e)$

donde $\tilde{P}_n = \tilde{Q}_n$ es la imagen bajo f^{-1} de $P_n = Q_n$

Así que

$$n \in A \leftrightarrow FMAT(n) \wedge (\exists y)(\exists w)\ PR(Y, Neg(w)) \wedge$$
$$SUBST_3(w, n, Num(n), 2^{21})$$

Entonces A es recursivamente enumerable por el teorema □

A es, por lo tanto, un conjunto diofantino, y existe un predicado polinomial $P_J(x_0, \ldots, x_m) = Q_J(x_0, \ldots x_m)$ tal que

$$n \in A \leftrightarrow (\exists a_1, \ldots, a_m)\ P_J(n, a_1, \ldots, a_m) = Q_J(n, a_1, \ldots, a_m)$$

Es decir, si $n \in A$, hay ciertos números que son raices del predicado polinomial susodicho, y además, eso puede probarse en el sistema pues

si $n \in A \rightarrow \vdash_F P_J(\bar{n}, \bar{a}_1, \ldots, \bar{a}_m) = Q_J(\bar{n}, \bar{a}_1, \ldots, \bar{a}_m)$* [Para ciertos $a_1, \ldots, a_m \in \mathbb{N}$.]

Ahora bien, en F

$$\vdash (x_1)\ldots(x_m) \sim P_J(\bar{n}, x_1, \ldots, x_m) = Q_J(\bar{n}, x_1, \ldots, x_m) \rightarrow$$
$$\sim P_J(\bar{n}, \bar{a}_1, \ldots, \bar{a}_m) = Q_J(\bar{n}, \bar{a}_1, \ldots, \bar{a}_m)]$$

y por el ax(3) y M.P.

$$\vdash P_J(\bar{n}, \bar{a}_1, \ldots, \bar{a}_m) = Q_J(\bar{n}, \bar{a}_1, \ldots, \bar{a}_m) \longrightarrow$$
$$\sim (x_1)\ldots(x_m) \sim P_J(\bar{n}, x_1, \ldots, x_m) = Q_J(\bar{n}, x_1, \ldots, x_m)$$

Por ello si $n \in A$, entonces $\vdash \sim (x_1)\ldots(x_m) \sim P_J(\bar{n}, x_1, \ldots, x_m) = Q_J(\bar{n}, x_1, \ldots, x_m)$

Así que si J perteneciera a A, por un lado tendríamos que

$\vdash \sim P_J(\bar{J}, x_1, \ldots, x_m) = Q_J(\bar{J}, x_1, \ldots, x_m)$ ó equivalentemente

$$\vdash_F (x_1)\ldots(x_m) \sim P_J(\bar{J}, x_1, \ldots, x_m) = Q_J(\bar{J}, x_1, \ldots, x_m)$$

Y por otro

$$\vdash_F \sim (x_1)\ldots(x_m) \sim P_J(\bar{J}, x_1, \ldots, x_m) = Q_J(\bar{J}, x_1, \ldots, x_m)$$

contradiciendo la consistencia de F

Luego $J \notin A$ ó

$$\sim (\exists x_1)\ldots(\exists x_m)\ P_J(\bar{J}, x_1, \ldots, x_m) = Q_J(\bar{J}, x_1, \ldots x_m)$$

pero este enunciado no es un Teorema de F

* Aquí, por sencillez, identificamos $P_J = Q_J$ con $\tilde{P}_J = \tilde{Q}_J$

Además, como para cada número natural i

$$(x_2)\ldots(x_m)\sim P_j(j,i,x_2,\ldots,x_m)=q_j(j,i,x_2,\ldots,x_m)$$

por el teorema 5.6

$$\vdash (x_2)\ldots(x_m)\sim P_j(\bar{j},\bar{i},x_2,\ldots,x_m)=q_j(\bar{j},\bar{i},x_2,\ldots,x_m)$$

y si F es ω-consistente, es falso que

$$\vdash_F \sim(x_1)\ldots(x_m)\sim P_j(\bar{j},x_1,\ldots,x_m)=q_j(\bar{j},x_1,\ldots,x_m)$$

Teorema 5.9

(1) Si F es consistente, entonces la f.b.f.

$$(x_1)\ldots(x_m)\sim P_j(\bar{j},x_1,\ldots,x_m)=q_j(\bar{j},x_1,\ldots,x_m)$$

no es teorema de F

(2) Si F es ω-consistente, el enunciado

$$\sim(x_1)\ldots(x_m)\sim P_j(\bar{j},x_1,\ldots,x_m)=q_j(\bar{j},x_1,\ldots,x_m)$$

es indecidible en F

Como dijimos al principio del capítulo, el análisis de la prueba, que acabamos de dar, revelará que el teorema 5.9 es válido para teorías de 1er orden similares (en ciertos aspectos) a nuestro sistema, y, en particular, es aplicable a cualquier extensión consistente y axiomática (es decir, donde el predicado 'ser axioma' sea recursivo) de F. Quede esa tarea al lector interesado.

Bibliografía

(1) Davis, Martin

a) Computability and Unsolvability. Mc Graw Hill Company. New York 1958

(b) Mathematical Logic. Courant Institute. New York. 1969

(c) Unsolvable Problems. En Recursion Theory, compilación hecha por Y.N Moschovakis.

(d) Hilbert's tenth Problem is unsolvable. (la fotocopia de este artículo consultada por el autor carece de los datos de impresión; por lo cual se omiten)

(2) Kleene, S.C. Introducción a la Metamatemática. Ed. Tecnos Madrid 1974

(3) Gödel, Kurt. Obras completas. Alianza Editorial. Madrid. 1981

(4) Hunter, Geoffrey. Metalógica. Ed. Paraninfo. Madrid 1981

(5) Mendelson, Elliot. Introduction to Mathematical Logic. D. Van Nostrand. U.S.A. 1964

(6) Monk, J.D Mathematical Logic. Springer Verlag. New York. 1976.

(7) Robinson Julia Diophantine Decision Problems. (Igual caso que la referencia 1.(d))

8) Rogers, H Theory of Recursive Functions and Effective Computability. Mc Graw Hill. U.S.A. 1967.