NÚMEROS Ω DE CHAITIN, MÁQUINAS DE SOLOVAY E INCOMPLETEZ

Por:

DIEGO FERNANDO MANCO BERRÍO

REQUISITO PARA OPTAR AL TÍTULO DE MATEMÁTICO

ASESOR
CARLOS MARIO PARRA LONDOÑO
UNIVERSIDAD NACIONAL DE COLOMBIA SEDE MEDELLÍN

UNIVERSIDAD DE ANTIOQUIA

FACULTAD DE CIENCIAS EXACTAS Y NATURALES

DEPARTAMENTO DE MATEMÁTICAS

MARZO 2 0 1 2

AGRADECIMIENTOS

A mis padres Francisco Javier Manco Úsuga y María Magdalena Berrío Berío y al conjunto de mi familia. Al profesor Carlos Mario Parra por dirigir mi trabajo. Al profesor Johany Suárez por ayudarme a solucionar alguna duda cuando fue pertinente. A Alejandra Montes por ayudarme a transcribir parte del manuscrito cuando mi estado de salud me lo impedía.

ÍNDICE GENERAL

INTRODUCCIÓN

En este trabajo se prueba en detalle una sorprendente generalización del teorema de incompletez de Gödel cuya idea original se debe a Calude [Ca99] y Solovay [So99]. Para lograrlo introducimos brevemente al lector en la fascinante Teoría Algorítmica de la Información en los primeros dos capítulos. En el tercero y cuarto nos concentramos en nuestro resultado que se logra gracias a una previa caracterización de los números que llamaremos recursivamente enumerables aleatorios y teoremas basados en el concepto de complejidad algorítmica, que se deben a Chaitin y a Solovay entre otros.

Nos basaremos principalmente en [Ca02], aunque haremos frecuentes alusiones a otros artículos y textos.

Capítulo 1

Notación y resultados básicos

En este capítulo fijamos notación y mencionamos algunos resultados básicos que se usarán en lo que sigue.

1.1. Notación

Mencionamos la notación que se usará frecuentemente en el texto.
Denotamos por $\mathbb{N}$ al conjunto de números naturales, $\mathbb{N}_+$ al conjunto de los naturales positivos, $\mathbb{Q}$ al conjunto de números racionales y $\mathbb{R}$ al conjunto de números reales. Usaremos $\lfloor \alpha \rfloor$ para denotar la parte entera del número real α, por $\log_Q$ el logaritmo en base Q, además abreviamos por $\log(n)$ a $\lfloor \log_2(n+1) \rfloor$.
Fijamos un conjunto finito $A = \{a_1, ..., a_Q\}$, con $Q \geq 2$ y lo llamamos un alfabeto. Denotamos por A^* el conjunto de las cadenas finitas sobre A, ie, sucesiones de la forma $x = x_1...x_n$ con $x_i \in A$ para $1 \leq i \leq n$. Denotamos por λ la cadena vacía y escribimos $A^+ = A^* \setminus \{\lambda\}$. Si $x \in A^*$, $|x|_A$ es la longitud de x ($|\lambda|_A = 0$). Si el alfabeto está especificado y no hay lugar a confusión escribimos $|x|$ en vez de $|x|_A$. Cada orden total $<$ en el conjunto A, digamos $a_1 < a_2 < \cdots < a_Q$, induce naturalmente un orden total en A^* que llamamos orden de diccionario:

$$\lambda < a_1 < \cdots < a_Q < a_1a_1 < \cdots < a_1a_Q < \cdots < a_Qa_Q$$

$$< \cdots < a_1a_1a_1 < \cdots < a_1a_1a_Q < \cdots < a_Qa_Qa_Q < \cdots$$

Denotamos por $string_Q(n)$ la n-ésima cadena con respecto al orden de diccionario, si se sobrentiende a qué relación de orden hacemos referencia. $string_Q : \mathbb{N} \to A^*$ es una función biyectiva que satisface $|string_Q(n)| = \lfloor log_Q(n(Q-1)+1) \rfloor$. Si no hay ambigüedad escribimos $string$ en vez de $string_Q$.
Definimos en A^* la relación de orden $\leq_p$ de modo que $x \leq_p y$ sii existe $z \in A^*$ tal que $y = xz$.

Como es usual, decimos que $x <_p y$ sii $x \leq_p y \wedge x \neq y$. Decimos que dos cadenas x, y son comparables si $x \leq_p y$ o bien $y \leq_p x$.

Si $x, y \in S$ definimos la concatenación de x con y como $z = xy$. La concatenación de x con sí mismo i veces $x...x$ la denotamos x^i con $x^0 = \lambda$. Si $S, T \subseteq A^*$ definimos su concatenación ST como $\{xy/x \in S, y \in T\}$. Si $m \in \mathbb{N}$ escribimos $A^m = \{x \in A^*/|x| = m\}$. Si $a_i \in A$ entonces la cadena cuya única componente es a_i se denota $\langle a_i \rangle$.

Por A^ω denotamos el conjunto de funciones $f : \mathbb{N}_+ \to A$, ie, secuencias infinitas de la forma $\mathbf{x} = x_1...x_n....$ Si $\mathbf{x} \in A^\omega$ y $n \in \mathbb{N}_+$ denotamos por $\mathbf{x}(n)$ la cadena $x_1...x_n \in A^*$. Si $x \in A^*$ y $y \in A^\omega$ denotamos por xy su concatenación. Si $S \subseteq A^*$ decimos que

$$SA^\omega = \{x \in A^\omega/\exists n \in \mathbb{N}_+(\mathbf{x}(n) \in S)\}.$$

Si $x \in A^*$: $xA^\omega = \{x\}A^\omega$. Si $Q \in \mathbb{N}$, con $Q \geq 2$, denotamos por A_Q el alfabeto $\{0, 1, ..., Q-1\}$ con el orden $<$ usual. Una letra $a \in A_Q$ denota al tiempo el símbolo que se usa para obtener cadenas de números y su valor numérico i con $0 \leq i \leq Q-1$. En particular denotamos $\Sigma = A_2 = \{0, 1\}$, además $string_2 = bin$.

Una función parcial $\varphi : X \overset{\circ}{\to} Y$ es una función cuyo dominio es subconjunto Z de X. Si $dom(\varphi) = X$ decimos de φ que es total y escribimos $\varphi : X \to Y$. Si $x \in dom(\varphi)$ escribimos $\varphi(x) < \infty$, de lo contrario $\varphi(x) = \infty$. Si dos funciones parciales $\psi : X \overset{\circ}{\to} Y$ y $\phi : X \overset{\circ}{\to} Y$ tienen igual dominio y si para $x \in \text{dom}\phi$ $\phi(x) = \psi(x)$ entonces decimos que para $x \in X$ $\phi(x) \simeq \psi(x)$.

1.2. Computabilidad

Intuitivamente una función parcial $f : \mathbb{N} \overset{\circ}{\to} \mathbb{N}$ se dice parcial recursiva si se puede programar un algoritmo tal que dado el número natural n, determine si $f(n) < \infty$ y en tal caso calcule $f(n)$. Las investigaciones de Turing, Church, Kleene y otros matemáticos llevaron a diferentes formalizaciones de este concepto que han resultado ser equivalentes. La tesis de Church-Turing afirma que el concepto intuitivo se corresponde con cualquiera de las formalizaciones, por ejemplo las máquinas de Turing. Asumimos que el lector está familiarizado con alguna de estas formalizaciones.

Como es usual llamaremos a una función parcial, $\varphi : A^* \overset{\circ}{\to} A^*$, parcial recursiva (p.r.) si existe una función parcial recursiva $f : \mathbb{N} \overset{\circ}{\to} \mathbb{N}$ tal que

$$\varphi(x) \simeq string(f(string^{-1}(x))).$$

Una función recursiva $f : \mathbb{N} \to \mathbb{N}$ es una función total definida análogamente. Se pueden definir de manera análoga las nociones de función parcial recursiva y función recursiva para funciones de

la forma $f : (A^*)^n \overset{\circ}{\to} A^*$. Si $\varphi : (A^*)^n \overset{\circ}{\to} A^*$ escribimos $\varphi^{(n)} : (A^*)^n \overset{\circ}{\to} A^*$. Es usual fijar una gödelización de las máquinas de Turing de manera que $\phi_k^{(n)} : (A^*)^n \overset{\circ}{\to} A^*$ representa la función de n variables computada por la máquina de Turing con código k, $(k \in \mathbb{N}_+)$. Esta numeración permite probar los siguientes teoremas:

2.1 Teorema (Teorema s-m-n)**.** *Si $m, n \in N_+$ entonces existe una función total computable de $m+1$ variables s_m^n tal que*

$$\phi_e^{(m+n)}(\boldsymbol{x}, \boldsymbol{y}) \simeq \phi_{s_m^n(\boldsymbol{x},e)}^{(n)}(\boldsymbol{y}).$$

2.2 Teorema. *Para cada $n \in \mathbb{N}_+$ la función $\phi_U^{(n)}$ definida por $\phi_U^n(e, x_1, ..., x_n) \simeq \varphi_e^{(n)}(x_1, ..., x_n)$ es parcial computable.*

Enunciaremos un resultado de gran utilidad en la Teoría de Recursión:

2.3 Teorema (Teorema de la Recursión)**.** *Si $m \in \mathbb{N}_+$ y $f^{(1)}$ es total computable entonces existe un x, a veces llamado punto fijo de f, tal que $\phi_x^{(m)} = \phi_{f(x)}^{(m)}$*

Para consultar las pruebas de éstos y otros resultados, así como la definición precisa de una gödelización para las funciones parciales recursivas, recomendamos el texto de Cutland [Cu80].

1.3. Topología y Probabilidad en A^ω

Podemos ver que el conjunto $\{xA^\omega\}_{x \in A^*}$ es una base para alguna topología en A^ω. Consideraremos a A^ω dotado con esta topología, la cual coincide con la topología producto de ω copias de A que se han equipado, cada una, con la topología discreta (en la cual cada subcobnjunto es abierto). Como cada conjunto dotado de la topología discreta es compacto podemos usar el Teorema de Tychonoff para obtener que A^ω es compacto.

Se puede probar que cada función $\mu : \{xA^\omega\}_{x \in A^*} \to \mathbb{R}$ que satisface

$$\mu(A^\omega) = \mu(\lambda A^\omega) = 1,\ \forall_{x \in A^*} \left[\mu(xA^\omega) = \sum_{i=1}^{Q} \mu(xa_i A^\omega) \right],$$

se puede extender de modo único a una medida en la σ-álgebra de Borel de A^ω. Para ver los detalles recomendamos [Ca02], sección 1.4.
Utilizaremos la medida de probabilidad uniforme definida por

$$\mu(xA^\omega) = Q^{-|x|}.$$

Nos interesa el caso $Q = 2$. En ocasiones esta medida se denomina medida de Lebesgue, ya que identifica $x \in \Sigma^*$ con el racional en $[0, 1)$ cuya expansión binaria es x, y la secuencia $y \in \Sigma^\omega$ con el número real en $[0, 1]$ cuya expansión binaria es y. De esta forma el conjunto $x\Sigma^\omega$ se identifica con el intervalo $[x, x + 2^{-|x|})$.

1.4. Conjuntos libres de prefijos

Un subconjunto S de A^* se denomina libre de prefijos si dados $x, y \in S$, con $x \leq_p y$, se tiene $x = y$.

4.1 Ejemplo. Si $S \subseteq A^*$ el conjunto $\hat{S} = \{x \in S / \neg\exists y \in S(y <_p x)\}$ es claramente un conjunto libre de prefijos. Se puede ver fácilmente que $SA^\omega = \hat{S}A^\omega$.

4.2 Ejemplo. Si $x \in \Sigma^*$ definimos $\overline{x}$ insertando un cero antes de cada letra de x y agregando al final un uno. Hacemos $\overline{\lambda} = 1$. Definimos ahora la versión autolimitante de $x \in A^*$: $d(x) = \overline{bin(|x|)}x$. Es claro que $S = \{d(x)/x \in A^*\}$ es libre de prefijos.

Es interesante notar que si $S \subseteq \Sigma^*$ es libre de prefijos entonces cuando $x, y \in S$ se tiene que $x\Sigma^\omega \cap y\Sigma^\omega$ es vacío, o lo que es lo mismo, los intervalos de la forma $[x, x + 2^{-|x|})$ con $x \in S$ son disjuntos dos a dos.
Mostramos ahora una condición necesaria para que un conjunto sea libre de prefijos.

4.3 Teorema (Kraft)**.** *Si $S \subseteq A^*$ es libre de prefijos entonces $\sum_{s\in S} Q^{-|s|} \leq 1$.*

Demostración. Es fácil ver que $S \subseteq A^*$ es libre de prefijos sii para $x, y \in S$ con $x \neq y$: $xA^\omega \cap yA^\omega = \phi$. Si $S \subseteq A^*$ es libre de prefijos $\{xA^\omega\}_{x\in S}$ es una familia de conjuntos disjuntos dos a dos de modo que

$$\sum_{s\in S} Q^{-|s|} = \sum_{s\in S} \mu(sA^\omega) = \mu\left(\bigcup_{s\in S} sA^\omega\right) = \mu(SA^\omega) \leq \mu(A^\omega) = 1.$$

□

Si S es un conjunto libre de prefijos entonces definimos $\Omega_S = \mu(S) = \sum_{x\in S}(2^{-|x|}) \leq 1$.

Capítulo 2

Nociones básicas de la Teoría Algorítmica de la Información

La Teoría algorítmica de la Información mezcla elementos de la Teoría de la Información de Shannon y de la Teoría de Recursión. Esto se usa para definir la complejidad algorítimca de un elemento, que se mide por el tamaño en bits del programa más corto que lo computa. En la primera sección definimos las máquinas de Chaitin, las numeramos y probamos la existencia de máquinas de Chaitin universales, además definimos la complejidad algorítmica de un objeto. En la segunda sección definimos la probabilidad de parada de una máquina de Chaitin, lo cual nos ofrece una nueva perspectiva del famoso Problema de la Parada.

2.1. Máquinas de Chaitin

Una máquina de Turing con dominio $S \subseteq \Sigma^*$, es autolimitante cuando S es libre de prefijos. Se suele suponer que una máquina de este tipo recibe como entrada un programa con datos incluidos. En los lenguajes de programación usados en la práctica toda máquina es autolimitante pues toda cadena (programa y datos) para la cual la máquina busca su imagen (lo ejecuta) y para, contiene las instrucciones Begin y End, que hacen las veces de paréntesis izquierdo y paréntesis derecho en las expresiones matemáticas, una vez cerrado el primer paréntesis se sabe que la expresión terminó. Si una expresión continúa después del cierre del primer paréntesis la expresión se considera inválida. De manera análoga, las instrucciones de un programa no pueden continuar después del End correspondiente al primer Begin. Considerar conjuntos libres de prefijos como los dominios de las máquinas autolimitantes, o de Chaitin, puede parecer innecesario, sin embargo, es un punto clave en la teoría algorítmica de la información y según el propio Chaitin, creador de la misma, este detalle mantuvo esta área del conocimiento estancada por casi una década [Ch88].

Para el resto del texto fijamos $A_Q = \{0,1\} = \Sigma$ y $A_Q^* = \Sigma^* = \{0,1\}^*$.

1.1 Definición (Máquina de Chaitin)**.** Decimos que una función parcial recursiva $C : \Sigma^* \overset{\circ}{\to} \Sigma^*$ es una máquina de Chaitin si $dom(C) \subseteq \Sigma^*$ es un conjunto libre de prefijos. En tal caso escribimos $\Omega_C = \Omega_{dom(C)}$

En lo que sigue fijaremos una gödelización $\{ \phi_i / i \in \mathbb{N}\}$ de las funciones parciales recursivas $\phi : \Sigma^* \overset{\circ}{\to} \Sigma^*$. Según lo expuesto en el capítulo anterior, la función universal $\Phi : \mathbb{N} \times \Sigma^* \overset{\circ}{\to} \Sigma^*$ definida por $\Phi(n, s) \simeq \phi_n(s)$ es parcial recursiva. A través de esta función obtendremos una gödelización de las Máquinas de Chaitin. Es claro que podemos obtener una numeración recursiva sin repeticiones del dominio de Φ (i.e. una biyección recursiva total f t.q. $f : \mathbb{N} \overset{\circ}{\to} \mathbb{N} \times \Sigma^*$ con $ran(f) = dom(\Phi)$), digamos $\{(n_i, x_i) | i \in \mathbb{N}\}$. Ahora, definimos una nueva función Ψ como la restricción de Φ a cierto conjunto r.e. Tal conjunto es el rango de una función, θ, parcial recursiva, definida de la siguiente manera:

1. Haga $\theta(1) = (n_1, x_1)$.
2. Si se han definido $\theta(1), \ldots, \theta(i-1)$ y no existe $i < j$ tal que $n_i = n_j$ y x_i es compatible con x_j entonces imprima (n_j, x_j).
3. De lo contrario imprima $\theta(j - 1)$.

Se tiene que θ es una función total recursiva cuyo rango es r.e. La función Ψ es parcial recursiva, al ser la restrición de una función parcial recursiva a un subconjunto r.e. de su dominio $(ran(\theta))$. Podemos ahora definir:

$$\psi_n(x) \simeq \Psi(n, x)$$

Lo último llevará a una gödelización de las máquinas de Chaitin. Como es fácil probar:

- El dominio de ψ_n es libre de prefijos.

- Si el dominio de ϕ_n es libre de prefijos entonces $\psi_n = \phi_n$.

Hemos construído así una función universal que simula todos las máquinas de Chaitin y sólo máquinas de Chaitin. A partir de ésta podemos definir una noción que nos será útil en el último capítulo. Denotamos por D_n el dominio de Ψ_n y hacemos:

$$D_n[t] = \{s \in \Sigma : \exists j \leq t(n_j = n \wedge s_j = s \wedge \theta(j) = (n_j, s_j))\}.$$

Además de esto denotamos $\Omega_n = \Omega_{D_n}$. Estamos en condiciones de introducir la siguiente definición:

1.2 Definición (Máquina Universal de Chaitin)**.** Una máquina de Chaitin U se dice universal si para toda máquina de Chaitin C existe una constante c (que depende de ambas máquinas) tal que si $C(x) < \infty$ entonces existe una cadena x' tal que $U(x') = C(x)$ y $|x'| \leq |x| + c$

De lo anterior se sigue que:

1.3 Teorema. *Existe una máquina de Chaitin universal.*

Demostración. Considerando la función Ψ definida en la discusión anterior definamos:

$$U(0^i 1x) \simeq \psi_i(x)$$

Es claro que el dominio de U es libre de prefijos pues $dom(\psi_i)$ es siempre libre de prefijos. Es fácil ver que cumple además la propiedad de universalidad. □

Probamos un lema útil.

1.4 Lema. *Si U es una máquina de Chaitin universal entonces U es sobreyectiva.*

Demostración. Sean $x \in \Sigma^*$. Definimos la máquina $C(\lambda) = x$. Como U es universal existe y tal que $U(y) = C(\lambda) = x$. □

La idea de complejidad algorítmica se basa en el concepto de incompresibilidad de la información. Si pensamos, por ejemplo, en los primeros 700 millones de dígitos de π sabemos que contienen bastante información; sabemos además que podemos programar un algoritmo, de tamaño considerablemente menor a 700 millones de bits que al ser ejecutado sin entrada de datos, imprima los primeros 700 millones de bits de π y pare. La información de estos 700 millones de bits está pues codificada en el programa, comprimida por tanto. Podemos preguntarnos ahora cuál será el programa más compacto, de menor tamaño, tal que al ejecutarse sin entrada de datos imprime la cifra en cuestión y para. El tamaño de este programa será la complejidad algorítmica de Kolmogorov-Chaitin de dicha cadena, que será entonces el tamaño del programa más corto que la genera. A través de esta noción podremos definir en la siguiente sección el concepto de sucesión aleatoria.

1.5 Definición (Complejidad de Chaitin de una cadena)**.** Si $x \in \Sigma^*$ y C es una máquina de Chaitin definimos la complejidad de x con respecto C como:

$$H_C(x) \simeq \min\{|u| : u \in \Sigma^* \wedge C(u) = x\}.$$

El siguiente resultado es consecuencia directa de las definiciones anteriores.

1.6 Teorema. *Si C es una máquina de Chaitin y U una máquina de Chaitin universal entonces existe una constante c tal que si $x \in \Sigma^*$ entonces $H_U(x) \leq H_C(x) + c$.*

Ahora obtenemos de inmediato:

1.7 Corolario. *Si U y V son dos máquinass de Chaitin universales entonces existe una constante c tal que si $x \in \Sigma^*$ entonces $|H_U(x) - H_V(x)| \leq c$.*

2.2. Probabilidades de Parada

Definiremos en esta sección la probabilidad de parada de una máquina de Chaitin C. Primero definimos la probabilidad de parada de la máquina con salida x, ésto es, la probabilidad de que, escogida una cadena al azar, la máquina calcule, a partir de ésa cadena, la cadena x. Para ésto sumamos de cada entrada s tal que $C(s) = x$ su aporte a esta probabilidad ,$2^{-|s|}$, que es el inverso del número de programas de $|s|$ bits.

2.1 Definición (Probabilidad de Parada de una máquina de Chaitin con una cadena como salida)**.** Dada una máquina de Chaitin C definimos para $x \in \Sigma^*$ La probabilidad de parada de C con salida x como

$$P_C(x) = \sum_{u \in \Sigma^* : C(u) = x} 2^{-|u|}.$$

Para definir la probabilidad de parada de una máquina de Chaitin C sumamos cada probabilidad de parada con salida una cadena particular. Pretendemos recoger en esta definición el concepto intuitivo de la probabilidad de que dada una cadena al azar, la máquina pare.

2.2 Definición (Probabilidad de Parada de una máquina de Chaitin)**.** Definimos la probabilidad de parada de una máquina de Chaitin C como:

$$\sum_{x \in \Sigma^*} P_C(x) = \sum_{u \in dom(C)} 2^{-|u|} = \mu(domC\Sigma^\omega) = \Omega_C.$$

Se sabe que el problema de decidir si una máquina de Turing para o no es indecidible [Cu80]. Este problema es conocido como el Problema de la Parada. Al cambiar los dominios de nuestras máquinas a subconjuntos de Σ^*, libres de prefijos, encontramos una manera de cambiar el enfoque en el cual está planteado originalmente el problema, por otro en el cual en vez de decidir si la máquina para o no en una entrada dada, hallamos la probabilidad de que pare en una entrada escogida al

azar. Más adelante veremos la estrecha relación que conservan los dos enfoques cuando la máquina de Chaitin considerada es universal.
Presentamos una extensión del resultado de la desigualdad de Kraft que nos será útil. Para consultar la prueba de este resultado recomendamos el texto de Calude [Ca02], sección 4.1. Este resultado se conoce como el Teorema de Kraft-Chaitin.

2.3 Teorema. *Sea $\psi : \mathbb{N}_+ \overset{\circ}{\to} \mathbb{N}$ una función parcial recursiva cuyo dominio es $\{n \in \mathbb{N}_+ : n < m\}$ para algún $m \in \mathbb{N}$, o bien $\mathbb{N}$. Si $\sum_{i \in dom(\psi)} 2^{-\phi(i)} \leq 1$ entonces podemos construir (efectivamente) una función inyectiva recursiva $\theta : dom(\psi) \to \Sigma^*$ tal que:*
a) Para $n \in dom(\psi)$ se tiene $|\theta(n)| = \psi(n)$.
b) $ran(\theta)$ es un conjunto libre de prefijos.

Demostración. Definimos θ de la siguiente manera:

1. Haga $\theta(1) = 0^{\psi(1)}$

2. Si se ha definido $\theta(0), \ldots, \theta(n)$ y $\psi(n+1) < \infty$, entonces haga

$$\theta(n+1) = \min\{x \in \Sigma^{\psi(n+1)} : \forall i (1 \leq i \leq n) \Rightarrow \neg(x \leq_p \theta(i) \vee \ \theta(i) \leq_p x))\}$$

.

□

2.4 Teorema (Kraft-Chaitin)**.** *Sea $f : \mathbb{N}_+ \overset{\circ}{\to} \Sigma^* \times \mathbb{N}$ una función parcial recursiva cuyo dominio es $\{n \in \mathbb{N}_+ : n < m\}$ para algún $m \in \mathbb{N}$, o bien $\mathbb{N}$. Para $k \in dom(f)$ hagamos $f(k) = (x_k, n_k)$. Si*

$$\sum_{k=1}^{\infty} 2^{-n_k} \leq 1,$$

entonces podemos constuir efectivamente una máquina de Chaitin C tal que para $k \in dom(f)$, existe una cadena u_k, de tamaño n_k, tal que $C(u_k) = x_k$. Además $\Omega_C = \sum_{k=1}^{\infty} 2^{-n_k}$.

Demostración. La función parcialmente recursiva $\psi : dom f \to \mathbb{N}_+$ dada por $\psi(k) = n_k$ satisface las condiciones del anterior teorema. Definimos la máquina de Chaitin C como:

$$C(\theta(k)) = x_k.$$

□

2.3. Sucesiones Aleatorias

Basándose en trabajos anteriores, que intentaban capturar el verdadero sentido de aleatoriedad de una sucesión, Martin-Löf logró, en 1966, definir con éxito el concepto de sucesión aleatoria. Más adelante él mismo propuso definiciones equivalentes, una de las cuales adoptamos a continuación. La definición se basa en la idea de que un elemento aleatorio en un espacio muestral debe ser un elemento típico. Esta tipicidad debería poder ser verificada, en principio, por una máquina de Turing. En nuestra definición consideramos entonces todos los test r.e. que puedan escoger minorías en Σ^ω. Para ser más precisos consideramos conjuntos r.e. de la forma $E \subseteq \Sigma^* \times \mathbb{N}_+$, tal que cada nivel E_k es libre de prefijos y tal que su medida tiende a cero si $k \to \infty$, más precisamente $\mu(E_k\Sigma^\omega) \leq 2^{-k}$. De esta manera $\mu(\bigcap_{n\in\mathbb{N}_+} E_n) = 0$ y $\bigcap_{n\in\mathbb{N}_+} E_n$ es considerado una minoría, en otras palabras, un conjunto de medida cero construible, de modo que si **x** es una sucesión aleatoria, al ser un elemento típico, no puede estar en ninguna minoría y, por tanto, debe existir un n tal que $\mathbf{x} \notin E_n\Sigma^\omega$. Precisamos lo anterior:

3.1 Definición (Sucesión Martin-Löf aleatoria)**.** Una sucesión $\mathbf{x} \in \Sigma^\omega$ se dice Martin-Löf aleatoria si para todo conjunto r.e. $E \subseteq \Sigma^* \times \mathbb{N}_+$ tal que para $i \geq 1$, $E_i = \{x \in \Sigma^* : (x, i) \in E\}$ es libre de prefijos y

$$\mu(E_i\Sigma^\omega) < 2^{-i},$$

entonces existe k tal que $\mathbf{x} \notin E_kA^\omega$.

Otra definición fue propuesta más tarde por Gregory Chaitin y Clauss-Peter Schnorr. Ésta se basa en el hecho intuitivo de que una sucesión aleatoria debería ser tal que sus dígitos se generaran de manera impredecible. Cada programa especifica un patrón, por lo tanto la sucesión de los n primeros dígitos de x, si ésta es una sucesión aleatoria, debería ser cada vez más difícil de especificar, contener más información y por lo tanto ser más compleja. De lo contrario generaría patrones y sería posible predecir sus dígitos. Ya tenemos una forma de medir la complejidad de un objeto; para la siguiente definición fijamos una máquina universal de Chaitin U.

3.2 Definición (Sucesión Chaitin aleatoria)**.** Una sucesión $\mathbf{x} \in \Sigma^\omega$ se dice Chaitin-Schnorr aleatoria si existe una constante c tal que

$$H_U(\mathbf{x}(n)) \geq n - c.$$

Notemos que el hecho de que la sucesión sea aleatoria no depende de la escogencia de la máquina de Chaitin universal.
Estas definiciones son equivalentes. La prueba de este hecho se encuentra en [Ca02] sección 6.3.

3.3 Teorema. *Una sucesión $\boldsymbol{x} \in \Sigma^{\omega}$ es Martin-Löf aleatoria si y sólo si es Chaitin-Schnorr aleatoria.*

Se plantearon otras definiciones de aleatoriedad para sucesiones, como la de Solovay [So74] y la de Hertling y Weihrauch [HW98]. Todas ellas han resultado ser equivalentes a las dos presentadas en el texto. Esto ha llevado a la postulación de una tesis, al estilo de la Tesis de Church-Turing, que afirma que una sucesión es aleatoria si satisface alguna (y por lo tanto todas) las definiciones propuestas hasta el momento. Esta tesis se denomina la Hipótesis de Aleatoriedad. En el siguiente capítulo exhibimos ejemplos de sucesiones aleatorias.

Capítulo 3

Números reales r.e. aleatorios

En este capítulo definimos los números recursivamente enumerables (r.e.) aleatorios y damos una caracterización de los mismos como probabilidades de parada de máquinas de Chaitin universales. En la primera sección probamos un teorema que relaciona el Probrema de la Parada con los bits del número Ω_U. Más precisamente, si U es una máquina universal de Chaitin probamos que, de conocerse los primeros n bits de Ω_U, podríamos decidir si dada una cadena $s \in \Sigma^*$, con $|s| \leq n$, la computación de $U(s)$ para o no. Este resultado nos permite probar que la probabilidad de parada de una máquina de Chaitin universal es un número r.e. aeatorio. En la segunda sección probamos la esperada caracterización. Para hacerlo definimos la relación de dominación entre números reales y números tipo Ω, los cuales caracterizamos como probabilidades de parada de Máquinas de Chaitin universales.

3.1. Números Ω_U

En esta sección probaremos que la probabilidad de parada de una máquina de Chaitin universal es un número aleatorio en el sentido de que la sucesión que conforma su representación binaria es aleatoria. Por simplicidad en la notación escribimos Ω en vez de Ω_U dado que la prueba sólo usa propiedades generales de las máquinas de Chaitin universales. Por esta razón fijamos una máquina de Chaitin universal U.

Denotamos por $\Omega[n]$ la aproximación racional que consiste en los primeros n bits de la expansión binaria de Ω; en caso de que Ω tenga dos expansiones escogemos la que termina en infinitos ceros. Por $\Omega(i)$ denotamos el i-ésimo bit de $\Omega = 0.\Omega(1)\Omega(2)\ldots\Omega(n)\ldots$. Así $\Omega[n] = 0.\Omega(1)\Omega(2)\ldots\Omega(n)$. Con esta notación probamos un lema de utilidad:

1.1 Lema.

$$\Omega[n] \leq \Omega \leq \Omega[n] + 2^{-n}.$$

Demostración. Se sigue del siguiente hecho:

$$\Omega - \Omega[n] = \sum_{j \geq n+1}^{\infty} \Omega(j) 2^{-j} \leq \sum_{j \geq i+1}^{\infty} 2^{-j} = Q^{-i}.$$

□

Ahora probamos el teorema deseado.

1.2 Teorema. *Dado $\Omega[n]$, podemos decidir si $U(s) < \infty$, para los $s \in \Sigma^*$ con $|s| \leq n$.*

Demostración. Sea $f : \mathbb{N}_+ \to dom(U)$ una biyección computable. Definamos $\omega_k = \sum_{i=1}^{k} 2^{-|f(i)|}$. Calculemos k tal que $\Omega[n] < \omega_k$. Veamos que $U(s) < \infty$ si y sólo si $s \in \{f(1), \ldots f(k)\} = W_k$. Supongamos pues, por el absurdo, que $U(s) < \infty$ y $s \notin W_k$. Tendríamos entonces que

$$\Omega[n] \leq \Omega \leq \Omega[n] + 2^{-n} < \omega_k + 2^{-|s|} \leq \Omega,$$

lo cual es imposible. □

Conocer los primeros 10000 dígitos de Ω_U, permitiría decidir si los programas de longitud menor que 10000 bits paran o no. Es razonable pensar que, para un U adecuado, uno de estos programas busca un contraejemplo para la Conjetura de Goldbach, la Hipótesis de Riemann u otro problema matemático refutable por un contraejemplo que se halla mediante un algoritmo. Aún más, si algún programa que genera los teoremas de cierta teoría matemática tiene menos de 10000 bits, se podría decidir si cualquier afirmación de la teoría es cierta, falsa o indecidible. Sin embargo, aún si se conociera $\Omega[10000]$, hacer uso de esta información implicaría el empleo de recursos (tiempo y memoria) que superan la capacidad de los ordenadores actuales.

Es de notar además que, a través de este teorema, se tiende un puente entre nuestros dos puntos de vista sobre el problema de la parada (el clásico y el probabilista). En este sentido, es valioso citar aquí a Bennet, quien pone en contexto histórico y filosófico el último teorema:

"A través de la historia místicos y filósofos han buscado una llave compacta a la sabiduría universal, una fórmula finita o un texto que proporcionaría la respuesta a cada pregunta. El uso de la Biblia, el Corán, el libro adivinatorio I Ching y la tradición de libros secretos de Hermes Trimegisto y la cábala judía medieval ejemplifican esta creencia o esperanza. (...) En muchos sentidos Ω es un número cabalístico."[Be92]

Sin embargo, como se verá en el siguiente capítulo, nunca podremos conocer más que finitos bits de cualquier número Ω. A continuación definimos algunas nociones básicas.

Si U es una máquina universal de Chaitin, sabemos que su dominio es un conjunto r.e. Sea $f : \mathbb{N}_+ \to dom(U)$ una biyección computable. Como en la prueba anterior consideramos la secuencia

$$\omega_k = \sum_{i=1}^{k} 2^{-|f(i)|}.$$

Consideremos ahora la expansión binaria del número Ω_U (en caso de que Ω_U tenga expansión binaria finita la completamos con infinitos ceros)

$$\Omega_U = 0.\Omega(1)\Omega(2)...\Omega(n)...$$

Denotemos la sucesión de dígitos binarios de Ω_U por $r(\Omega_U)$. Es decir,

$$r(\Omega_U) = \Omega(1)\Omega(2)\ldots\Omega(n)\ldots \in \Sigma^{\omega}$$

Después de introducir estos conceptos, ofrecemos una prueba de la aleatoriedad de $r(\Omega)$ con base en la definición de aleatoriedad de Chaitin-Schnor.

1.3 Teorema. *La sucesión $r(\Omega)$ es aleatoria.*

Demostración. Definimos una máquina de Chaitin C tal que, al recibir como entrada un $x \in \Sigma^*$, realiza el siguiente procedimiento:

1. Compute $y := U(x)$
2. Compute el menor entero t (si existe) tal que $\omega_t \geq 0.y$
3. Imprima la menor cadena(en el orden de diccionario) que no pertenece al conjunto $\{U(f(1)), U(f(2)), \ldots U(f(t))\}$.

Si $x \in \Sigma^*$ y $C(x) < \infty$, entonces sea $y \in \Sigma^*$ la menor cadena (según el orden de diccionario) tal que $U(y) = U(x)$; es claro que $C(x) = C(y)$ y por lo tanto

$$H_C(C(x)) \leq |y| = H_U(x).$$

Por la universalidad de U existe una constante $c > 0$ tal que

$$H_U(C(x)) \leq H_C(C(x)) + c.$$

Ésto se da siempre que $C(x) < \infty$. Fijemos ahora $n \in \mathbb{N}_+$ y escojamos un $x \in \Sigma^*$ tal que

$$U(x) = 0.\Omega(1)\Omega(2)...\Omega(n).$$

Sabemos entonces que $M(x) < \infty$. Sea t el menor natural tal que $\omega_t \geq 0.\Omega(1)\Omega(2)...\Omega(n)$. Por un lema anterior

$$0.\Omega(1)\Omega(2)...\Omega(n) \leq \omega_t \leq \omega_t + \sum_{i=t+1}^{\infty} 2^{-|f(i)|} = \Omega \leq 0.\Omega(1)\Omega(2)...\Omega(n) + 2^{-n}$$

De modo que

$$\sum_{i=t+1}^{\infty} 2^{-f(i)} \leq 2^{-n}.$$

De ésto se sigue que si $i \geq t+1$, entonces $f(i) \geq n$. De la construcción de la máquina C se tiene que

$$n \leq H_U(M(x)) \leq H_M(M(x)) + c \leq H_U(U(x)) = H_U(0.\Omega(1)\Omega(2)...\Omega(n)) + c.$$

Lo anterior implica que $r(\Omega)$ es una sucesión aleatoria según la definición de Chaitin-Schnorr (2.3.2). □

Ahora introducimos una definición de aleatoriedad en el ámbito de los números reales. Consideramos sólo reales en el intervalo $[0, 1]$.

1.4 Definición (Real Aleatorio)**.** Un número real α se dice aleatorio si su expansión binaria forma una sucesión aleatoria.

Si un número tiene expansión binaria finita, la completamos con infinitos ceros.

Ahora, fijamos una numeración de los racionales en $[0, 1]$ por ejemplo la biyección $\upsilon : \mathbb{N} \to [0, 1] \cap \mathbb{Q}$ definida por $\upsilon(0) = 0$, $\upsilon(2n) = 1 + \upsilon(n)$ y $\upsilon(2n + 1) = 1/(1 + \upsilon(n))$. Hacemos esta consideración para introducir la siguiente:

1.5 Definición (Sucesión computable de racionales)**.** Una sucesión de racionales $a : \mathbb{N} \to \mathbb{Q}$ se dice computable si la función $f : \mathbb{N} \to \mathbb{N}$ definida por $f(x) = \upsilon^{-1}(a(x))$ es computable. Decimos entonces que la sucesión $(a_i)_{i\in\mathbb{N}}$ con $a_i = a(i)$ es computable.

A continuación introducimos la noción de número real recursivamente enumerable.

1.6 Definición (Número real r.e.)**.** Un número real se dice recursivamente enumerable (r.e.) si es el límite de una secuencia computable, no decreciente, de racionales.

Por ejemplo, si U es una máquina de Chaitin universal, entonces Ω_U es un número real r.e. puesto que $(\omega_k)_{k\in\mathbb{N}_+}$ es una sucesión computable de racionales con límite Ω_U.
Un real computable α es un número tal que existe una secuencia computable, no decreciente de racionales, digamos (a_n), tal que $|a_n - \alpha| \leq 2^{-n}$. Si computamos el número a_{n+1} podremos saber con certeza los primeros n bits de α. Éste no es el caso de los números r.e. puesto que a pesar de poder computar una aproximación tan buena como deseemos, no se sabe cuan cerca está la aproximación del límite.
De lo anterior se deduce lo siguiente.

1.7 Corolario. *Si U es una máquina de Chaitin universal entonces Ω_U es un número r.e. aleatorio.*

3.2. Caracterización de los números r.e. aleatorios

En esta sección abordamos la pregunta de si todos los números r.e. aleatorios son probabilidades de parada de máquinas universales de Chaitin. Para empezar introducimos la relación de dominación.

2.1 Definición (Dominación)**.** Decimos que el número real α domina al número real β y escribimos $\alpha \leq_{dom} \beta$ si existe una función parcial recursiva $f : \mathbb{Q} \overset{\circ}{\to} \mathbb{Q}$ y una constante $c > 0$ tal que, si $p \in \mathbb{Q}$ y $p < \alpha$, entonces $f(p) < \beta$ y además:

$$c(\alpha - p) \geq \beta - f(p).$$

Intuitivamente, si $\alpha \leq_{dom} \beta$ entonces α es menos aleatorio que β en el siguiente sentido: dada una aproximación computable de α entonces se obtiene una aproximación computable de β con un error similar. Esto implica que α debe ser más computable, y por lo tanto, más predecible que β. O equivalentemente, α debe ser menos aleatorio que β.
Es fácil probar entonces el siguiente resultado.

2.2 Lema. *Un real r.e.α domina a otro real r.e. β si existen secuencias recursivas no decrecientes (a_i) y (b_i), de racionales, tales que $\lim_{i\to\infty} a_i = \alpha$, $\lim_{i\to\infty} b_i = \beta$ y una constante $c > 0$ tal que, para todo $n \in \mathbb{N}$;*

$$c(\alpha - a_n) \geq \beta - b_n.$$

Queremos ahora definir un real r.e. tipo Ω, como aquel que domina a todos lo reales r.e. Intuitivamente, a la clase de los tipo Ω pertenecerán los números más aleatorios de entre los r.e.

2.3 Definición (Secuencia universal)**.** Una secuencia computable, creciente, de racionales (a_i) es universal si para todo secuencia computable y creciente de racionales (b_i), existe un número $c > 0$ tal que, para $n \in \mathbb{N}$: $c(\alpha - a_n) \geq \beta - b_n$.

Así introducimos la siguiente:

2.4 Definición. Un real es llamado tipo Ω si es el límite de una secuencia recursiva creciente de racionales.

Probamos ahora que si U es una máquina universal de Chaitin entonces Ω_U es un número tipo Ω, lo cual justifica su nombre.

2.5 Teorema. *Sea U una máquina de Chaitin universal. Toda secuencia recursiva, creciente, convergente con límite Ω_U es universal.*

Demostración. Sea (a_n) una secuencia de racionales recursiva y con límite Ω_U. Sea (b_n) una secuencia de racionales recursiva, creciente y convergente. Digamos que $\lim_{n\to\infty} b_n = \beta$.
Sea (x_i) una enumeración recursiva y sin repeticiones de $dom(U)$. Definamos, como es usual, $\omega_n = \sum_{i=1}^{n} 2^{-|x_i|}$. Es claro que ω_n es una sucesión creciente con límite Ω_U. Definamos por recursión una función g tal que $g(0) = \text{mín}\{j : \omega_j \geq a_0\}$ y

$$g(n) = \text{mín}\{j > g(n-1) : \omega_j \geq a_n\}.$$

Tenemos entoncces que $\Omega_U - a_n \geq \Omega_U - \omega_{g(n)}$. Por lo cual resta probar la afirmación del teorema para la sucesión $\omega_g(n)$. Definamos ahora una sucesión (y_i) de la siguiente manera: (y_i) es la mínima cadena, según el orden de diccionario, tal que $y_i \notin (\{U(x_j) : j \leq g(i)\} \cup \{y_j : j < i\})$.
Definamos ahora $n_i = \lfloor -log(b_{i+1} - b_i) \rfloor + 1$. Fácilmente obtenemos, para $i \in \mathbb{N}$, las desigualdades

$$2^{-n_i} \leq b_{i+1} - b_i \leq 2^{-(n_i - 1)}.$$

Debido a lo anterior

$$\sum_{i=0}^{\infty} 2^{-n_i} \leq \sum_{i=0}^{\infty} b_{i+1} - b_i = \beta - b_0 < 1.$$

Por el teorema de Kraft-Chaitin podemos definir una máquina de Chaitin C tal que para $i \in \mathbb{N}$, existe $u_i \in \Sigma^{n_i}$, tal que $C(u_i) = y_i$. Dado que U es una máquina universal sabemos que existe c tal que $H_U(y_i) \leq n_i + c$.
Escojamos para cada $i \in \mathbb{N}$ un $x_i' \in \{x_j : j > g(i)\}$ tal que $U(x_i') = y_i$ y $|x_i'| \leq n_i + c$. No hay

repeticiones en la numeración de los $x_i^{'}$ puesto que si $i \neq j$ entonces $y_i \neq y_j$ y por tanto $x_i^{'} \neq x_j^{'}$. Además, si $i \geq n$ entonces $x_i^{'} \in \{x_j : j > g(n)\}$. Por lo tanto tenemos que

$$\Omega_U - \omega_g(n) = \sum_{i=g(n)+1}^{\infty} 2^{-|x_i|} \geq \sum_{i=n}^{\infty} 2^{-|x_i^{'}|} \geq \sum_{i=n}^{\infty} 2^{-n_i-c} \geq 2^{-c-1} \sum_{i=n}^{\infty} (b_{i+1} - b_i) = 2^{-c-1}(\beta - b_n).$$

□

Definimos ahora una relación entre conjuntos libres de prefijos que nos permitirá establecer resultados sobre dominación entre las medidas de los mismos.

2.6 Definición (Simulación Fuerte)**.** Sean A, B conjuntos infinitos libres de prefijos. Decimos que A simula fuertemente a B, y escribimos $B \leq_{ss} A$, si existe una función parcial recursiva $f : \Sigma^* \overset{\circ}{\to} \Sigma^*$ tal que $dom(f) = A$, $ran(f) = B$ y una constante $c > 0$, tal que para $x \in A$, se tiene $|x| \leq |f(x)| + c$.

Inmediatamente obtenemos el siguiente resultado.

2.7 Lema. *La relación $\leq_{ss}$ es reflexiva y transitiva.*

Probamos ahora un teorema que relaciona simulación con dominación.

2.8 Lema. *Si $A, B \subseteq \Sigma^*$ son conjuntos r.e. libres de prefijos y $B \leq_{ss} A$, entonces $\mu(B\Sigma^*) \leq_{dom} \mu(A\Sigma^*)$.*

Demostración. Sean f y c como en la definición de simulación fuerte. Entonces, si $y \in B \setminus \{f(x_0), ..., f(x_n)\}$ existe $x \in A \setminus \{x_0, ..., x_n\}$ tal que $y = f(x)$ y $|x| \leq |y| + c$. Lo cual implica

$$\begin{aligned} \mu(B\Sigma^\omega) - \mu(\{f(x_0), \ldots, f(x_n)\}\Sigma^\omega) &= \mu((B \setminus \{f(x_0), \ldots, f(x_n)\})\Sigma^\omega) \\ &\leq 2^c(\mu((A \setminus \{x_0, \ldots, x_n\})\Sigma^\omega)) \\ &= 2^c(\mu(A\Sigma^\omega) - \mu(\{x_0, \ldots, x_n\}\Sigma^\omega). \end{aligned}$$

□

Ahora probamos una suerte de recíproco del teorema anterior.

2.9 Teorema. *Sea α un real r.e. y $B \subseteq \Sigma^\omega$ conjunto infinito, libre de prefijos y r.e.*
Si $\mu(B\Sigma^\omega) \leq_{dom} \alpha$ entonces podemos construir un conjunto $A \subseteq \Sigma^*$, libre de prefijos, infinito y r.e., tal que $\alpha = \mu(A\Sigma^\omega)$ y $B \leq_{ss} A$.

Demostración. Supongamos $\mu(B\Sigma^\omega \leq_{dom} \alpha)$ y sea (y_i) una enumeración recursiva de B. Sea a_n una secuencia positiva de racionales que converge a α. Por definición, existe una función recursiva $F : \mathbb{Q} \to \mathbb{Q}$ y una constante c tal que si $p < \alpha$ entonces $F(p) < \beta$ y $2^c(\alpha - p) \geq \mu(B\Sigma^\omega) - F(p)$ (de no cumplirse incrementamos c). Definamos ahora

$$f(n) = \text{mín}\{m : \sum_{i \leq m} 2^{-|y_i|} \geq F(a_n)\},$$

de modo que

$$2^c(\alpha - a_n) \geq \mu(B\Sigma^\omega) - \sum_{i=0}^{f(n)} 2^{-|y_i|}.$$

Asumimos, sin pérdida de generalidad, que

$$a_0 > \sum_{i=0}^{f(0)} 2^{-|y_i|-c}.$$

De no cumplirse lo anterior incrementamos c. Construiremos ahora una secuencia (n_i) de números naturales y una secuencia doble $(m_{i,j})_{i,j\geq 0}$ de elementos de $\mathbb{N} \cup \{\infty\}$. La secuencia (n_i) es tal que $n_i = |y_i| + c$.

Definimos $m_{i,j} = \infty$ para $i < f(0)$ y $j \in \mathbb{N}$. Definimos $(m_{f(0),j})$ de modo que:

$$\sum_{j=0}^{\infty} 2^{m_{-f(0),j}} = a_0 - \sum_{i=0}^{f(0)} 2^{-n_i}.$$

Consideramos una expansión infinita en la última expresión. Si $s \geq 1$ y se ha definido n_i y $m_{i,j}$ para $i \leq f(s-1)$, definimos $m_{i,j}$ para $f(s-1) < i < f(s)$ por casos:

A) Si

$$a_s \leq \sum_{i=0}^{f(s)} 2^{-n_i} + \sum_{i=0}^{f(s-1)} \sum_{j=0}^{\infty} 2^{-m_{i,j}},$$

entonces $m_{i,j} = \infty$ para $f(s-1) < i \leq f(s)$.

B) De lo contrario, hacemos $m_{i,j} = \infty$ para $f(s-1) < i < f(s)$ y definimos $m_{f(s),j}$ de manera que

$$\sum_{j=0}^{\infty} 2^{-m_{f(s),j}} = a_s - \left(\sum_{i=0}^{f(s)} 2^{-n_i} + \sum_{i=0}^{f(s-1)} \sum_{j=0}^{\infty} 2^{m_{i,j}} \right).$$

Ahora probamos la igualdad

$$\alpha = \sum_{i=0}^{\infty} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right).$$

Si para infinitos números s se cumple que

$$a_s = \sum_{i=0}^{f(s)} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right),$$

entonces se comprueba la igualdad deseada. Si por el contrario, la anterior igualdad sólo se cumple un número finito de veces entonces, puesto que

$$a_s < \sum_{i=0}^{f(s)} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right),$$

obtenemos

$$\alpha = \lim_{s\to\infty} a_s \leq \sum_{i=0}^{\infty} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right).$$

Consideremos el máximo $s_0 \in \mathbb{N}$ que satisface

$$a_{s_0} = \sum_{i=0}^{f(s_0)} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right).$$

Entonces, por la escogencia de c, tenemos que

$$\alpha - a_{s_0} \geq \sum_{i=f(s_0)+1}^{\infty} 2^{-|y_i|-c},$$

así que

$$\alpha \geq \sum_{i=0}^{\infty} \left(2^{-n_i} + \sum_{j=0}^{\infty} 2^{-m_{i,j}} \right).$$

Como el conjunto de los (i,j) tal que $m_{i,j} \neq \infty$ es recursivo e infinito, existe una biyección recursiva $h : \mathbb{N} \to \{(i,j) \in \mathbb{N}^2 : m_{i,j} \neq \infty\}$. Definimos una secuencia de números (r_i) como $r_{2i} = n_i$ y $r_{2i+1} = m_h(i)$. Puesto que $0 < \alpha \leq 1$, podemos construir una secuencia (x_i) de cadenas, sin repeticiones, tal que $A = \{x_i : i \in \mathbb{N}\}$ es libre de prefijos y $|x_i| = r_i$ para $i \in \mathbb{N}$. Es claro que $\alpha = \mu(A\Sigma^\omega)$. También se obtiene $B \leq_{ss} A$, al definir $g : A \to B$ tal que $g(x_{2i}) = y_i$ y $|g(x_{2i+1})| \geq |x_{2i+1}|$ (notemos que B es infinito). □

Estamos listos para probar que todo número tipo Ω es la probabilidad de parada de una máquina universal de Chaitin.

2.10 Teorema. *Para todo real α, tipo Ω, podemos construir una máquina de Chaitin universal U tal que $\alpha = \Omega_U$*

Demostración. Sea V una máquina de Chaitin universal. Puesto que Ω_V es un número r.e. y α es tipo Ω, se tiene que

$$\Omega_V = \mu(dom(V)\Sigma^\omega) \leq_{dom} \alpha.$$

Según el teorema anterior existe un conjunto infinito y libre de prefijos A, talque $\mu(A\Sigma^\omega) = \alpha$ y $dom(V) \leq_{ss} A$. Por lo tanto existe una función recursiva $f : A \to dom(V)$ sobreyectiva y una constante $c > 0$ tal que, para $x \in A$, $|x| \leq |f(x)| + c$. Definimos una máquina de Chaitin con dominio A, de modo que, para $x \in A$, $U(x) = V(f(x))$. Debido a que V es universal se sigue que U también lo es y además, $\Omega_U = \mu(A\Sigma^\omega) = \alpha$. □

Así obtenemos el siguiente resultado.

2.11 Corolario. *Un real es tipo Ω si y sólo si es la probabilidad de parada de una máquina universal de Chaitin.*

Ahora probamos que todos los números r.e. aleatorios son tipo Ω. Seguimos la prueba registrada en [KS01], Teorema 2.1.

2.12 Teorema. *Si α es un número real r.e. aleatorio y β es un real r.e. entonces $\beta \leq_{dom} \alpha$.*

Demostración. Sean (a_n) y (b_n) secuencias recursivas, no decrecientes que convergen a α y β respectivamente. Construiremos un test de Martin-Löf (A_n) tal que $\mu(A_n\Sigma^\omega) \leq 2^{-n}$. Debido a la aleatoriedad de α existirá un n tal que α no tiene ningún segmento inicial en A_n. En ese caso probaremos que $\alpha - a_s \geq 2^{-n}(\beta - b_s)$ para todo s. Construimos el test como sigue:
En lo siguiente denotaremos por $\langle a \rangle$ la expansión binaria de un racional a. Enumeramos el test por etapas. Sea $A_n[s]$ el conjunto finito de cadenas que ha sido agregado a A_n hasta la etapa s. Sea s_- la última etapa en la que hemos adicionado cadenas a A_n. Hacemos $A_n[0] = \phi$. Si $b_s \neq b_{s_-}$ y $\langle a_s \rangle \notin A_n[s]\Sigma^\omega$ agregamos cadenas: $d_1, \ldots, d_k$ tal que todo real (visto como secuencia) en el intervalo $[a_n, a_n + (b_s - b_{s_-})2^{-n})$, tiene como segmento inicial a uno de los d_i. En otras palabras agregamos el intervalo $[a_n, a_n + (b_s - b_{s_-})2^{-n})$ a $A_n\Sigma^\omega$; en caso contrario, definimos $A_n[s+1] = A_n[s]$.
$A_n = \bigcup_{s\in\mathbb{N}} A_n[s]$ es un conjunto libre de prefijos. Sean $t_1, ..., t_i, ...$ las etapas en las cuales hemos

agregado cadenas a A_n (notemos que este conjunto de etapas podría ser finito); tenemos:

$$\begin{aligned} 0 < \mu(A_n\Sigma^\omega) &= \mu\left(\bigcup_{s\in\mathbb{N}} A_n[s]\Sigma^\omega\right) \\ &= \sum_{i=1}^{\infty} \mu(A_n[t_i]\Sigma^\omega) \\ &= 2^{-n}\left(\sum_{j=0}^{\infty}(b_{t_{j+1}} - b_{t_j})\right) \\ &\leq 2^{-n}. \end{aligned}$$

Lo anterior se sigue pues la suma es telescópica y tiene límite $\beta - b_0$ si el conjunto de los t_i es infinito, o bien $b_{t_n} - b_0$ si t_n es el mayor de los t_i's.

Puesto que el conjunto $A = \{(x, n) : x \in A_n\}$ es r.e. entonces, como α es aleatorio, existe un n tal que $\alpha \notin A_n$. Notemos que si hemos adicionado $[a_n, a_n + (b_s - b_{s_-})2^{-n})$ a $A_n\Sigma^\omega$ entonces dado que α es aleatorio, y por tanto irracional, existe $a_t > a_n + (b_s - b_{s_-})$. Veamos que para todo s se cumple que $\alpha - a_s \geq 2^{-n}(\beta - b_s)$. Fijemos s. Sea t_0 la mayor etapa, menor que s, en la que agregamos algo a A_n. Sean $t_0, t_1, ...$ la secuencia de etapas (mayores o iguales que t_0) en las que hemos añadido algo a A_n.

Por construcción, para $k \geq 1$,

$$a_{t_{k+1}} > a_{t_k} + (b_{t_k} - b_{t_{k-1}})2^{-n}.$$

Así que

$$\sum_{k=1}^{\infty}(a_{t_{k+1}} - a_{t_k}) \geq \sum_{k=1}^{\infty}(b_{t_k} - b_{t_{k-1}})2^{-n} = 2^{-n}(\beta - b_{t_0}).$$

Pero como $t_0 \leq s \leq t_1$, obtenemos

$$\alpha - a_s \geq \alpha - a_{t_1} \geq 2^{-n}(\beta - b_{t_0}) \geq 2^{-n}(\beta - b_s).$$

□

Hemos obtenido la deseada caracterización, la cual consignamos en lo que sigue.

2.13 Corolario. *Un número real es r.e. aleatorio si y sólo si es la probabilidad de parada de una máquina de Chaitin universal.*

El anterior colorario nos permitirá, en la siguiente sección, dar una caracterización diferente de los números r.e. aleatorios; en esta ocasión obtendremos además, un sorprendente resultado de incompletez.

Capítulo 4

Máquinas de Solovay e Incompletez

En este capítulo ofrecemos otra caracterización de los números r.e. aleatorios en términos de máquinas de Solovay. Esto nos permitirá obtener sorprendentes resultados de incompletez relacionados con la probabilidad de parada de máquinas de Chaitin universales . En la primera sección probamos que ZFC, de ser aritméticamente sólida, sólo puede predecir un número finito de bits de la probabilidad de parada de una máquina de Chaitin universal. El objetivo de la segunda sección es mejorar dramáticamente este resultado al probar que para cada número r.e. aleatorio α, existe una máquina universal de Chaitin S, con $\alpha = \Omega_S$ y tal que ZFC sólo puede predecir los bits que preceden al primer cero de Ω_S. En caso de que α comience por cero se tendrá, en particular, una máquina de Chaitin universal S tal que ZFC no puede predecir ningún bit de Ω_S. Lo anterior, por supuesto, si ZFC es aritméticamente sólida.

4.1. Incompletez via Teoría Algorítmica de la Información

El interés por los límites del conocimiento ha capturado el interés de los filósofos desde la antigüedad, ejemplo de ello son algunos trabajos de Aristóteles y Kant. En el contexto de las matemáticas, a través de los trabajos de Hilbert,Gödel y Turing, entre otros, se obtuvieron sorprendentes resultados que ponían límites a lo conocible. La conocida frase, y epitafio, de Hilbert: ″Wir müsen wissen. Wir werden wissen″ (Debemos saber. Sabremos) resume en parte el proyecto de basar las matemáticas en un formalismo que fuese consistente y completo. Sin embargo sus esperanzas se vieron necesiariamente frustradas gracias a una de las mentes más geniales del pasado siglo, Kurt Gödel, quien en su famoso artículo de 1931, probó el primer teorema de incompletez, que afirma que todo sistema formal cuyo conjunto de axiomas sea recursivo (finitamente especificado), lo suficientemente rico para expresar la aritmética (o al menos cierta parte de ella) y sólida (tal que sus teoremas son ciertos en el model estándar de los naturales) tiene afirmaciones indecidibles

en dicho formalismo.
La afirmación utilizada en su famoso artículo era bastante anómala. Basados en la Teoría Algorítmica de la Información, Chaitin y otros, han generalizado en forma dramática el resultado de incompletez de Gödel encontrando sentencias indecidibles que ahora son simples afirmaciones sobre números naturales.
Dado que el conjunto de teoremas de las teorías consideradas es r.e. podemos medir su complejidad algorítmica como el tamaño del menor programa que, al ingresarse como entrada en cierta máquina universal de Chaitin, imprime los teoremas de la teoría. A través de esta noción Chaitin ha probado resultados impresionantes, como el hecho de que dada una teoría que satisfaga las condiciones del teorema de Gödel y una máquina de Chaitin universal U, existe una constante tal que la teoría no puede probar ningún teorema de la forma $H_U(x) > c$. Recientemente se han obtenido resultados de incompletez en la aritmética aún más sorprendentes. Por ejemplo Raatikainen [Ra98], construyó una máquina de Chaitin univerlsal tal que ZFC, de ser aritméticamente sólido y consistente, no puede probar ninguna afirmación de la forma $H_U(x) > 0$; el principal resultado de este capítulo, es otro teorema de incompletez, igualmente asombroso.
En esta sección probaremos un resultado, debido a Chaitin, esta vez en relación con los dígitos de los números r.e. aleatorios, que afirma que ZFC, de ser aritméticamente sólida y consistente, sólo puede predecir finitos bits de un número r.e. aleatorio. En la sigiuente sección probamos un resultado debido a Calude [Ca99], basado en un resultado de Solovay [So99], como ha sido mencionado al comienzo párrafos de este capítulo.

A continuación introducimos algunas nociones básicas. Para consultar más definiciones en materia de lógica recomentdamos, por ejemplo [Me87]. Por PA denotamos la Aritmética de Peano.

1.1 Definición. Una teoría T de primer orden se dice aritméticamente sólida si satisface las siguientes condiciones:

1. Existe una interpretación fija de PA en T (de modo que toda fórmula de PA tiene una traducción en el lenguaje de T).

2. Todo teorema de T que tenga traducción al lenguaje de PA es verdadero en el modelo estándar de PA.

Llamaremos a cada dígito de una sucesión un bit, como es usual, y empezaremos numerando desde el 0-ésimo bit.

1.2 Teorema. *Supongamos que ZFC es artiméticamente sólida y sea U un máquina universal de Chaitin. Entonces ZFC puede probar tan solo un número finito de afirmaciones de la forma:*

$$''el\ n\text{-}\acute{e}simo\ bit\ de\ \Omega_U\ es\ k''.$$

Demostración. Supongamos que ZFC predice k bits de Ω_U en las posiciones $i_1 < i_2 < \cdots < i_k$ y sean $\Omega(i_1), ..., \Omega(i_k)$ los bits que resultan de dicha predicción. Como ZFC es aritméticamente sólida es cierto que el j-ésimo bit de Ω es Ω_j para $j = i_1, \cdots, i_k$. Consideremos ahora

$$E_k = \{x_1\Omega_{i_1}x_2\Omega_{i_2}...x_k\Omega_{i_k} : \forall_{2\leq j\leq k}((|x_j| = i_j - i_{j-1} - 1) \wedge |x_1| = i_1 - 1\}.$$

Es claro entonces que

$$\mu(E_k\Sigma^\omega) = 2^{-i_k}2^{i_k-k} = 2^{-k}.$$

Ahora, puesto que $r(\Omega_U) \in E_k\Sigma^\omega$, si ZFC predice infinitos bits de Ω_U, tendríamos que Ω_U no es aleatorio, lo cual es absurdo. □

Si quisiéramos calcular los bits de un número real α que es r.e. aleatorio estaríamos limitados desde el comienzo. No obstante, puesto que existe una sucesión de racionales, computable, no decreciente y que converge a α, digamos (a_n), podemos hallar cotas inferiores para α. Aunque no podemos estar seguros de la precisión de estas cotas, sabemos que si la expansión binaria de algún a_n comienza por una cadena de unos, 1^i, entonces los primeros i bits de α son con seguridad todos 1. Ésto es una consecuencia de que α es irracional y por lo tanto no termina en una cadena infinita de $1's$. De esta manera obtenemos un procedimiento para hallar los bits de α (en expansión binaria) precentes al primer cero.
Si enmarcamos el anterior teorema en el contexto antes mencionado, por Bennet, el número que podría resolver algunos de los problemas más interesantes en matemáticas permanecerá desconocido. Continuando con la cita:
''El libro esotérico es, como Dios, simple pero indescriptible. (...) [Los números] Ω son en muchos sentidos números cabalísticos. Podemos saber de ellos a través de la razón, pero no pueden ser conocidos. Para conocerlos en detalle se debe aceptar su secuencia no computable de dígitos como palabras de un texto sagrado.''[Be92]

4.2. Números c.e. Aleatorios e Incompletez

Probamos primero un resultado técnico que nos será de utilidad:

2.1 Teorema. *Si $u, v \in \Sigma^*$ y $\boldsymbol{x} \in \Sigma^\omega$, las siguientes afirmaciones son equivalentes:*

1. *$u\boldsymbol{x}$ es una secuencia aleatoria.*

2. *$v\boldsymbol{x}$ es una secuencia aleatoria.*

Demostración. Si $v\mathbf{x}$ no es aleatoria veamos que $u\mathbf{x}$ no es aleatoria. Puesto que $v\mathbf{x}$ no es aleatoria existe un conjunto r.e. $T \subseteq \Sigma^* \times \mathbb{N}_+$ tal que cada sección T_n es libre de prefijos, $\mu(T_n) \leq 2^{-n}$ y $v\mathbf{x} \in \bigcap_{n\in\mathbb{N}_+} T_n$. Consideremos ahora el conjunto

$$A = \{(ub, m) \in \Sigma^* \times \mathbb{N}_+ : vb \in T_{m+|v|+1}\}.$$

Puesto que los T_n son libres de prefijos

$$\begin{aligned}\sum_{\{b:vb\in T_{m+|v|}\}} 2^{-|b|-|v|} &= \sum_{\{b:vb\in T_{m+|v|}\}} 2^{-|vb|} \\ &\leq \mu(T_{m+|v|}) \\ &\leq 2^{-|v|-m},\end{aligned}$$

así que

$$\sum_{\{b:vb\in T_{m+|v|}\}} 2^{-|b|} \leq 2^{-m}.$$

Obtenemos por lo tanto

$$\mu(A_m) = \sum_{\{b:vb\in T_{m+|v|}\}} 2^{-|ub|} = \sum_{\{b:vb\in T_{m+|v|}\}} 2^{-|u|}2^{-|b|} \leq 2^{-|u|-m} \leq 2^{-m}.$$

Así que A es un test de Martin-Löf. Veamos que $u\mathbf{x} \in \bigcap_{n\geq 1} A_m$. Si $m \geq 1$ entonces $v\mathbf{x} \in T_{m+|v|}\Sigma^\omega$ así que existe $t \in T_{m+|v|}$ tal que $t \leq_p vx$. Si $|t| < |v|$ entonces $2^{-|v|} < 2^{-|t|}$. Pero $2^{-|t|} \leq \mu(T_{m+|v|}\Sigma^\omega) \leq 2^{-m-|v|}$ así que $2^{-|v|} < 2^{-m-|v|}$ y, por tanto, $1 < 2^{-m}$, lo cual es imposible. Así que $|t| \geq |v|$ y obtenemos $t = vb$. Así $ub \in A_m$ y evidentemente $u\mathbf{x} \in A_m\Sigma^\omega$.
Es claro entonces que $u\mathbf{x} \in \bigcap_{m\geq 1} A_m\Sigma^\omega$ y por tanto no es aleatoria. □

Estamos listos para probar el teorema principal del texto:

2.2 Teorema. *Supongamos que ZFC es aritméticamente sólida y sea $i \geq 0$. Consideremos el real r.e. aleatorio*

$$\alpha = \alpha_0\alpha_1...\alpha_{i-1}0\alpha_{i+1}..., \text{ con } \alpha_0 = \alpha_1 = ... = \alpha_{i-1} = 1.$$

Entonces podemos construir una máquina universal de Chaitin, U, tal que

1. *PA prueba que S es universal.*

2. *ZFC no puede probar ningún teorema de la forma*

$$''el\ (n+i)\text{-}\acute{e}simo\ bit\ de\ \Omega_S\ es\ k''.$$

3. $\alpha = \Omega_S$.

Demostración. Probaremos primero el caso $i \geq 1$. Consideremos el real

$$0, \alpha_{i+1}\alpha_{i+2}...$$

Sabemos por el lema anterior que este número es aleatori y, puesto que α es r.e., se sigue que también es r.e. De manera que fijamos una máquina de Chaitin universal V, tal que

$$\Omega_V = 0, \alpha_{i+1}\alpha_{i+2}\ldots$$

y además, tal que PA prueba que V es universal.
Definimos una función parcial recursiva U en dos variables, $j \in \mathbb{N}$ y $s \in \Sigma$, de la siguiente manera:

1. Si $s = \lambda$ entre en un loop.

2. Si $s \in \{1, 01, 001, ..., 0^{i-1}1\}$ imprima 1.

3. Si $s = 0^{i+1}t$ calcule $V(t)$. De hallarlo, imprima $V(t)$.

4. Si $s = 0^i 1t$ continúe con el paso siguiente.

5. Liste los teoremas de ZFC, en un orden independiente de t y j, hasta encontrar uno de la forma
   $''el\ (n+i)\text{-}$ésimo $bit\ de\ \Omega_j\ es\ k''$.
   De encontrarlo fije los valores de n y k.

6. Si $|t| \neq n$ entre un loop.

7. Si $|t| = n$ fije el racional diádico r cuya expansión binaria es $1^i t\,\langle k \rangle$. Haga $r' = r + 2^{-(n+i+1)}$. Busque el menor entero m tal que $r < \Omega_j[m] < r'$. Si encuentra tal m continúe con el siguiente paso.

8. Si $s \in D_j[m]$ entre un loop.

9. Si $s \notin D_j[m]$ imprima 1.

Por el Teorema de la Recursión existe j tal que $\Phi_j(s) = U(j, s)$. Escribamos $S = \Phi_j$ y veamos que S es una máquina de Chaitin. Sean $s_1, s_2 \in domS$ tales que $s_1 \leq_p s_2$. Si s_1 pertenece a $\{1, 01, ..., 0^{i-1}1\}$, entonces, según la definición de nuestro algoritmo, s_1, s_2 están en el conjunto libre de prefijos

$$\{1, 01, ..., 0^{i-1}1\},$$

así que $s_1 = s_2$. Si $s_1 = 0^{i+1}t_1$ entonces $s_2 = 0^{i+1}t_2$ y $t_1 \leq_p t_2$, donde además t_1, t_2 pertenecen al dominio de V y por lo tanto $t_1 = t_2$. Si $s_1 = 0^i 1 t_1$ entonces $s_2 = 0^i 1 t_2$ y se han encontrado naturales n y k en el paso 5; estos números deben coincidir para t_1 y t_2 puesto que el orden en que se listaron los teoremas no depende del parámetro t. De esta manera $|t_1| = |t_2| = n$ y por tanto $s_1 = s_2$. Así concluimos que S es una máquina de Chaitin. De la universalidad de V se sigue la universalidad de S, aún más, la universalidad de S se puede probar en PA.
Sabemos ahora que $S = \Psi_j$. Probaremos ahora la parte más importante del teorema.
Supongamos que ZFC puede probar un teorema de la forma $''el\ (n+i)$-ésimo $bit\ de\ \Omega_j\ es\ k''$. Consideremos el primer teorema de esta forma listado por el algoritmo y fijemos n y k los enteros correspondientes a la afirmación. Como ZFC es aritméticamente sólida entonces la afirmación $''el\ (n+i)$-ésimo $bit\ de\ \Omega_j\ es\ k''$ es verdadera. Dado que Ω_S es irracional, escojamos r el único racional diádico con denominador 2^{n+i+1}, tal que:

$$r < \Omega_S < r + 2^{-(n+i+1)} = r'.$$

Puesto que $\{1, 01, ..., 0^{i-1}1\} \subseteq domS$, se tiene que $2^{-1} + \cdots + 2^{-i} < \Omega_U$, así que la expansión binaria de Ω_U empieza con 1^i. De manera que la expansión binaria de r es $1^i t\ \langle k \rangle$, donde t es una cadena de tamaño n. Hagamos $u = 0^i 1 t$ y consideremos la computación de $S(u)$. El algoritmo ejecuta el paso 5 y al listar los teoremas de ZFC se hallan los números n y k que fijamos. Tenemos $|t| = n$, de manera que el algoritmo procede al paso 7 para r y r' (los mismos ya fijados). Puesto que $r < \Omega_S < r + 2^{-(n+i+1)}$ la búsqueda del número m, en el mismo paso 7, tiene éxito. Si $s \in D_j[m]$ entonces $S(s)$ es indefinido, lo cual es imposible pues $D_j[m] \subseteq D_j$. Así que $s \notin D_j[m]$, entonces $S(s)$ está definido y D_j contiene, además de las cadenas en $D_j[m]$, una cadena s de tamaño $n + i + 1$, por lo cual $\Omega_j \geq \Omega_j[m] + 2^{-(n+i+1)} > r' > \Omega_j$. Lo cual es imposible.
De esta manera ZFC no puede probar ningún teorema de la forma $''el\ (n+i)$-ésimo $bit\ de\ \Omega_j\ es\ k''$. Ahora, es claro que

$$\Omega_S = 2^{-1} + 2^{-2} + \cdots + 2^{-i} + 2^{-(i+1)}\Omega_V = \alpha.$$

Para el caso $i = 0$ fijamos una máquina de Chaitin universal W tal que

$$\Omega_W = 0, \alpha_1\alpha_2...$$

y además, tal que PA prueba que W es universal. Al igual que en el caso anterior definimos una función parcial recursiva T en dos variables $j \in \mathbb{N}$ y $s \in \Sigma$ como sigue:

- Si $s = \lambda$ entre en un loop.
- Si $s = 0t$ calcule $W(t)$. De hallarlo, imprima $W(t)$.
- Si $s = 1t$ continúe con el paso siguiente.
- Liste los teoremas de ZFC, en un orden independiente de t y j, hasta encontrar uno de la forma
  $''el\ n$-ésimo $bit\ de\ \Omega_j\ es\ k''$.
  De encontrarlo fije los valores de n y k.
- Si $|t| \neq n$ entre un loop.
- Si $|t| = n$ fije r el racional diádico cuya expansión binaria es: $t\langle k \rangle$. Haga $r' = r + 2^{-(n+i+1)}$. Busque el menor entero m tal que $r < \Omega_j < r'$. Si encuentra tal m continúe con el siguiente paso.
- Si $s \in D_j[m]$ entre un loop.
- Si $s \notin D_j[m]$ imprima 1.

Por recursión, y argumentos similares a los anteriores, encontramos un j tal que $\Psi_j = U(j, s)$ con Ψ_j universal. Análogamente se muestra que ZFC no puede probar nigún teorema de la forma $''el\ n$-ésimo $bit\ de\ \Omega_j\ es\ k''$ y que $\alpha = \Omega_j$ □

De esta manera obtenemos una nueva caracterización de los números aleatorios r.e. como probabilidades de parada de máquinas de Solovay, para las cuales ZFC sólo puede predecir los bits anteriores al primer cero. Es interesante notar que en el caso $i = 0$, por ejemplo, sabemos que el primer bit de α es cero, pero ésto no se puede probar en ZFC. En general, se obtiene el siguiente resultado:

2.3 Teorema. *Si ZFC es aritméticamente sólido entonces para cada real aleatorio r.e. α, existe una máquina de Solovay S tal que $\alpha = \Omega_S$. Si*

$$\alpha = \alpha_0\alpha_1...\alpha_{i-1}0\alpha_{i+1}..., \text{ con } \alpha_0 = \alpha_1 = ... = \alpha_{i-1} = 1$$

la afirmación $''el\ i\text{-}ésimo\ bit\ de\ \Omega_S\ es\ 0''$ es cierta pero no se puede probar en ZFC.

Es preciso mencionar que, como observamos en la sección anterior, dado j se conoce un procedimiento para hallar los bits de Ω_j que preceden al primer cero. Suponemos ψ_j universal. Como es usual, podemos hallar una sucesión $\omega_k = \sum_{i=0}^{k} 2^{-|f(i)|}$, donde $f\mathbb{N}_+ \overset{\circ}{\to} \Sigma^*)$ es una biyección computable con rango $dom(\psi_j)$. Esta secuencia de racionales es estrictamente creciente y tiene límite Ω_j. Como se discutió en la anterior sección, si la expansión binaria de ω_k empieza por una cadena de unos, 1^i, entonces Ω_j empieza necesariamente por la misma cadena de unos. Para un k lo suficintemente grande, se conocerán con certeza los bits de Ω_U anteriores al primer cero.

A continuación probamos un resultado , debido a Chaitin, relacionado con el teorema de Jones Matiyasevich [JM84].

2.4 Teorema. *Dada una máquina universal de Chaitin U, existe una ecuación exponencial diofantina*

$$P(n, k, y_1, \ldots, y_m) = 0,$$

tal que para todo $k \geq 0$ la ecuación

$$P(n, k, y_1, \ldots, y_m) = 0,$$

tiene infinitas soluciones si y sólo si el n-ésimo bit de la expansión binaria de Ω_U es 1.

Que la ecuación sea diofantina exponencial significa que $P(n, k, y_1, \ldots, y_m)$ es un polinomio (de variables enteras no negativas) en el que se permite la exponenciación entre variables. En la prueba seguimos a [LV08], Lema 3.7.1.

Demostración. Sea $f : \mathbb{N} \to dom(U)$ una biyección computable. Como es usual consideremos la sucesión $\omega_k = \sum_{i=0}^{k} 2^{-|f(i)|}$. Es claro que el conjunto

$$R = \{(n, k) : \text{el n-ésimo bit } \omega_k \text{ es } 1\}$$

es r.e. Así que existe una ecuación diofantina $P(n, k, y_1, \ldots y_m) = 0$, según el Teorema de Jones-Matiyasevic [JM84], que tiene una solución si el n-ésimo bit de la expansión binaria de ω_k es 1 y

cero soluciones de lo contrario.
Si el n-ésimo bit de Ω_U es 1, entonces para infinitos k se tiene que el n-ésimo bit de ω_k es 1, por lo cual, la ecuación $P(n, k, y_1, \ldots y_m) = 0$ tiene infinitas soluciones que son tuplas $(k, y_1, \ldots y_m)$.
Si el n-ésimo bit de Ω_U es 0 entonces sólo para finitos k se tiene que el n-ésimo bit de ω_k es 1, por lo cual, sólo para finitos k la ecuación $P(n, k, y_1, \ldots y_m) = 0$ tiene solución, en cuyo caso es única, por lo tanto la ecuación $P(n, k, y_1, \ldots y_m) = 0$ tiene finitas soluciones. □

La combinación de los dos últimos teoremas nos permite enunciar el siguiente resultado.

2.5 Corolario. *Si ZFC es aritméticamente sólida entonces, para cada real aleatorio r.e. α, existe una máquina de Solovay S tal que $\alpha = \Omega_S$. Además, si*

$$\alpha = \alpha_0\alpha_1...\alpha_{i-1}0\alpha_{i+1}..., \text{ con } \alpha_0 = \alpha_1 = ... = \alpha_{i-1} = 1,$$

existe una ecuación diofantina

$$P(i, x, y_1, \ldots, y_m) = 0,$$

que tiene finitas soluciones, pero este hecho no se puede probar en ZFC.

Es interesante notar que Calude y otros han construido una máquina de Chaitin universal particular (que llamaremos U) y han hallado los 64 primeros bits de su probabilidad de parada (ver [Ca02] sección 8.7). Los bits son:

$$0000001000000100000110001000011010001111110010111011111010000010000.$$

De acuerdo con lo probado en este capítulo, si ZFC es aritméticamente sólida y U es una máquina de Solovay, ZFC sólo puede predecir los bits de Ω_U que preceden al primer cero. Por lo tanto, la máquina construida por Calude y otros no es una máquina de Solovay. De hecho, puesto que ZFC prueba que el primer bit de Ω_U es cero, es imposible construir una máquina de Solovay S, tal que $\Omega_U = \Omega_S$.
Por último notaremos que en este capítulo ZFC se puede remplazar por una teoría que contenga la aritmética, sea aritméticamente sólida, consistente y r.e. Escogimos ZFC porque esta teoría es el formalismo estándar de las matemáticas en la actualidad.
Es innegable el impacto que han tenido, en el ámbito matemático, los resultados de incompletez e independencia obtenidos en el último siglo, junto con las técincas mediante las cuales se han establecido dichos resultados. Ejemplos de afirmaciones independientes de gran relevancia se encuentran en diversas áreas: la Hipótesis del Continuo, la Conjetura de Kaplansky (todo homomorfismo algebraico de $C[0, 1]$a un espacio de Banach es continuo) y el problema de Whitehead (todo grupo de

Whitehead no contable es libre). Hasta el momento no hay un acuerdo sobre la manera de decidir estas cuestiones, o siquiera la pertinencia de las mismas. A este respecto escribe Gödel:

"...además de la intuición matemática existe otro (aunque sólo probable) criterio de veracidad para los axiomas matemáticos, a saber, su utilidad en matemáticas y, se podría añadir, en física (...) El caso más simple de una aplicación del criterio en discusion se da cuando algún (...) axioma tiene consecuencias verificables por computación para los números menores que un entero.

... los axiomas no necesitan ser evitentes por sí mismos, su justificación se basa (como en física) en el hecho de que hacen posible la deducción de algunas percepciones sensitivas. Pienso que (...) este punto de vista ha sido ampliamente justificado por desarrollos actuales y es de esperar que lo sea más en el futuro. Se ha visto que la solución a ciertos problemas aritméticos requiere asumir hechos que trascienden la aritmética (...) bajo estas circunstancias las matemáticas perderían en buena medida su " absoluta certeza" aunque debido a la influencia de la crítica moderna a los fundamentos, ésto ha sucedido ya en una gran escala"

A la luz de los resultados presentados en el texto nos preguntamos si no sería justo, de construirse una ecuación como la descrita en el teorema 2.5, asumir que tiene finitas soluciones aunque este hecho no pueda ser probado en ZFC y, de ser así, a qué otro tipo de afirmaciones sería válido aplicar el mismo criterio. Con esta pregunta, mucho menos arriesgada que la de Gödel, quien veía en el futuro la posibilidad de una matemática experimental, terminamos el texto.

BIBLIOGRAFÍA

[Be92] Bennet, C.H. *Chaitin's Omega* en *Fractal music, hypercards and more: mathematical recreations from Scientific American Magazine* 1st edition. WH Freeman and Company, 1992.

[Ca02] Calude, Cristian S. *Information and Randomness. An algorithmic perspective*. 2nd Edition, Revised and Extended. Springer, 2002.

[Ca99] Calude, Cristian S. *Chaitin Ω numbers, Solovay Machines and Incompletness* CDMTCS Reseach Report 114, 1999.

[C02] Calude, Cristian S. *Incompletness, Complexity, Randomness and Beyond.* CDMTCS Reseach Report 166.

[Ch88] Chaitin, G.J. *Randomness in arithmetic* en Scientific American 259, 1988

[Ch90] Chaitin, Gregory J. *Information, Randomness and Incompleteness: Papers on Algorithmic Information Theory.* World Scientific, Singapore. 2nd edition, 1990.

[Cu80] Cutland, Nigel. *An introduction to Recursive Function Theory*. Cambridge University Press, 1980.

[Gö81] Gödel, K. *Obras Completas*. Madrid. Alianza, 1981.

[HW98] Hertling P., Weihrauch K. *Randomness spaces* en *Automata, Languages and Programing*. Proc 25th Int. Coll, ICALP 98, 1998.

[JM84] Jones, J.P. Matiyasevic, Y. *Register machine proof of the theorem on exponential diophantine representation of the enumerable sets.* Journal of Symbolic Logic 49. 1989. pp. 818-829.

[KS01] Kucera, Antonín. Slaman, Theodore. *Randomness and recusrive enumerability* en SIAM J COMP Vol 31 No 1 pp. 199-111, 2001. pp. 569-586.

[LV08] Li, M. Vitányi, P.M. *An Introduction to Kolmogorov Complexity and its Applications.* 3rd edition Berlin. Springer-Verlag, 2008.

[Me87] Mendelson, E. *Introduction to Mathematical Logic*. Monterey: Wadsworth and Brooks/Cole 1987.

[Ra98] Raatikainen. *On interpreting Chaitin's incompletness theorem* Journal of Philosophic Logic 27. 1998

[So74] Solovay R.M. Draft of a paper (or series of papers) on Chaitin´s work... done for the most part during the period Sept.- Dec- 1974. Manuscript.

[So99] Solovay, Robert, M. *A Version of* Ω *for wich* ZFC *cannot predict a single bit*. CDMTCS Reseach Report 104, 1999.