Aleatoriedad, Incompletez e Independencia

por

Johany Alexis Suárez Ramírez

Trabajo presentado como requisito parcial
para optar al Título de

Magister en Matemáticas

Director: Carlos Mario Parra Londoño

Universidad Nacional de Colombia
Sede Medellín

Facultad de Ciencias

Escuela de Matemáticas

Septiembre 2006

Este trabajo hace parte del proyecto **Aleatoriedad y Lógica** (código QUIPÚ: 030802734)
financiado por la Dirección de Investigación, sede Medellín (DIME)
de la Universidad Nacional de Colombia.

Resumen

Basados en el trabajo de M. van Lambalgen, presentamos tres nociones distintas de aleatoriedad y estudiamos las relaciones entre ellas. Probamos el principio de homogeneidad y generalizamos el teorema de Chaitin-Schnorr. Luego, estudiamos las conexiones entre incompletez, complejidad y aleatoriedad. En particular, desarrollamos pruebas alternativas de dos teoremas clásicos de G. Chaitin: el teorema de incompletez y un teorema que relaciona números reales aleatorios con las ecuaciones diofantinas exponenciales.

Contenido

Agradecimientos

Agradezco a los profesores de la Escuela de Matemáticas por haberme ayudado a fortalecer mi formación matemática y a madurar como docente. En particular, quisiera agradecer a los profesores Volker Stallbohm, Carlos Mario Parra, Jorge Mejía, Jorge Cossio y Juan Diego Vélez y a la profesora Margarita Toro, de quienes tuve el privilegio y el placer de recibir clase. También quisiera agradecer a los profesores Pedro Isaza y Carlos Mejía por toda la ayuda y paciencia cuando los importune con asuntos burocráticos.

Agradezco a los profesores Carlos Cadavid (Universidad EAFIT), Luis Fernando Etcheverri (Universidad de Antioquia) y Juan Diego Vélez (Universidad Nacional) por haber accedido amablemente a ser jurados de mi tesis.

Agradezco profundamente al profesor Carlos Mario Parra por haber sido tanto el asesor de mis tesis de Pregrado y de Maestría como el mentor de mi formación como lógico durante los últimos seis años.

Por último, agradezco a mi esposa Catalina por haber iluminado e inspirado mis años de Maestría.

Introducción

El presente trabajo es una continuación del estudio de la teoría algorítmica de la información y de las relaciones entre aleatoriedad e incompletez iniciado en la monografía [Su03]. Así como dicha monografía se basa esencialmente en el texto de Calude [Ca02] y en algunos artículos de Chaitin, el actual trabajo se fundamenta en gran medida en la tesis doctoral [vL87a] y en los artículos [vL87b] y [vL89] del lógico holandés Michiel van Lambalgen. Como principales novedades de esta tesis destacamos que todos los resultados se enuncian para la complejidad autolimitante de Chaitin (van Lambalgen establece estos resultados con base en la complejidad de Kolmogorov) y para medidas computables arbitrarias (en [Ca02] y [Su03] sólo se considera la medida de Lebesgue). Por supuesto, esto nos ha llevado a modificar adecuadamente las pruebas ofrecidas por van Lambalgen.

En el capítulo 1 recogemos brevemente los prerrequisitos básicos para la compresión de los restantes capítulos. Suponemos que el lector está familiarizado con un primer curso de teoría de la recursión tal como se desarrolla en textos como [Ro67] o [Br94]. El segundo capítulo está dirigido a presentar las diferentes nociones de aleatoriedad propuestas por von Mises (sección 2.1), Martin-Löf (sección 2.2) y Chaitin (sección 2.4). En la sección 2.3, probamos el principio de homogeneidad y en la sección 2.5 mostramos que la noción de aleatoriedad de Martin-Löf coincide con la de Kolmogorov-Chaitin, lo cual generaliza el teorema de Chaitin-Schnorr. El capítulo 3 está dedicado a explorar las conexiones entre la incompletez sintáctica, la complejidad algorítmica y la aleatoriedad. Por último presentamos, a modo de conclusiones, un análisis detallado de las críticas que van Lambalgen presenta contra el uso de la teoría de la recursión en la definición de sucesión aleatoria y contra las interpretaciones epistemológicas que Chaitin hace de sus teoremas de incompletez.

Capítulo 1

Preliminares

En este capítulo introductorio, presentamos nuestra elección de la terminología, notación y resultados básicos que se usarán libremente a lo largo de la tesis.

1.1 Alfabetos y sucesiones

Si S es un conjunto finito, $\#S$ denota la cardinalidad de S. Un alfabeto es un conjunto finito $A = \{a_1, \ldots, a_Q\}$, donde $\#A = Q \geq 2$. El alfabeto binario $\{0, 1\}$ se denota por $\mathbf{2}$. A^* es el conjunto de todas las cadenas $x = x_1 x_2 \cdots x_n$ sobre A, incluyendo la cadena vacía λ. Dado $x \in A^*$, $|x|$ denota la longitud de x ($|\lambda| = 0$). Para $n \in \mathbb{N}$, $A^n = \{x \in A^* \mid |x| = n\}$. xy denota la concatenación de $x, y \in A^*$; en particular, x^k es la concatenación de x consigo misma k veces. La concatenación de $S, T \subseteq A^*$ es el conjunto $ST = \{st \mid s \in S \wedge t \in T\}$.

Todo orden total en A, digamos $a_1 < \cdots < a_Q$, induce un orden lexicográfico en A^*: $\lambda < a_1 < \cdots < a_Q < a_1 a_1 < a_1 a_2 < \cdots < a_Q a_Q < a_1 a_1 a_1 < \cdots$. Denotamos por $\mathsf{string}_Q(n)$ la n-ésima cadena de acuerdo al orden lexicográfico. Notemos que $\mathsf{string}_Q : \mathbb{N} \to A^*$ es una biyección tal que string_Q y string_Q^{-1} son *computables*; además, $\left|\mathsf{string}_Q(n)\right| = \lfloor \log_Q(n(Q-1)+1) \rfloor$. En particular, $\mathsf{bin}\,(n) := \mathsf{string}_2(n)$ y $|\mathsf{bin}\,(n)| = \lg n := \lfloor \log_2 (n+1) \rfloor$. Si no hay confusión sobre el alfabeto A, escribiremos $\mathsf{string}\,(n)$ en lugar de $\mathsf{string}_Q(n)$.

Dados $u, v \in A^*$, decimos que u es prefijo de v (lo que se denota $u \leq_p v$), si $v = uw$, para algún $w \in A^*$. Es claro que $\leq_p$ es un orden parcial en A^*. Decimos que $S \subseteq A^*$ es libre de prefijos, si dados $u, v \in S$ se tiene que $u \leq_p v$ implica $u = v$.

Podemos obtener un conjunto libre de prefijos del siguiente modo. Para $x \in \mathbf{2}^*$, $\underline{x}$ es la cadena que se obtiene al insertar un 0 antés de cada bit de x y al final un 1. Es claro que $|\underline{x}| = 2|x| + 1$. Definimos la versión autolimitante binaria de x por $d\,(x) := \underline{\mathsf{bin}(|x|)}\, x$. El conjunto $D_2 = \{d\,(x) \mid x \in \mathbf{2}^*\}$ es libre de prefijos y $|d\,(x)| = |x| + 2\lg|x| + 1$ (ejemplo 2.5 en [Ca02, 24]). Si reemplazamos 0 por a_1 y 1 por a_2, podemos considerar que la funcion bin toma valores en

$\{a_1, a_2\}^* \subset A^*$. Así, $D_A = \{d(x) \mid x \in A^*\}$ es un subconjunto libre de prefijos de A^*, donde $d(x) = \underline{\mathsf{bin}(|x|)}\, x$ es la versión autolimitante de $x \in A^*$.

A^ω denota el espacio de todas las sucesiones (infinitas) $\mathbf{x} = x_1 x_2 \cdots$, donde $x_k \in A$. El segmento inicial $\mathbf{x}(n)$ es el prefijo de $\mathbf{x}$ de longitud $n > 0$; es decir, $\mathbf{x}(n) = x_1 \cdots x_n \in A^*$. Para $S \subseteq A^*$, definimos $SA^\omega = \{\mathbf{x} \in A^\omega \mid (\exists n)\ (\mathbf{x}(n) \in S)\}$. Un cilindro es un conjunto de la forma $\{w\} A^\omega$ para algún $w \in A^*$; los cilindros se denotarán por wA^ω o por $\langle w \rangle$.

Dados $\mathbf{x} \in A^\omega$ y $w \in A^*$, escribimos $w <_p \mathbf{x}$ si existe n tal que $w = \mathbf{x}(n)$. Notemos que $SA^\omega = \{\mathbf{x} \mid (\exists u \in S)\ (u <_p \mathbf{x})\} = \bigcup_{u \in S} \langle u \rangle$ y $wA^\omega = \{\mathbf{x} \mid \mathbf{x}(|w|) = w\} = \{\mathbf{x} \mid w <_p \mathbf{x}\}$.

Topología y Medida en A^ω

Dotamos a A^ω con la topología τ generada por la familia de cilindros $\{\langle w \rangle\}_{w \in A^*}$. Por tanto, $\mathcal{V}$ es un abierto en A^ω sii existe $S \subseteq A^*$ tal que $\mathcal{V} = SA^\omega$. La topología τ coincide con la *topología producto* $\prod_{i=1}^{\infty} A$ que se obtiene al dotar a A con la topología discreta. Por el Teorema de Tychonoff, tenemos que (A^ω, τ) *es un espacio topológico compacto.*

Diremos que μ es una medida en A^ω si μ es una medida definida en $\mathcal{B}(A^\omega)$ tal que $\mu(A^\omega) = 1$, donde $\mathcal{B}(A^\omega)$ denota la σ-álgebra de Borel de A^ω; i.e., la menor σ-álgebra que contiene todos los conjuntos abiertos de A^ω. Las medidas en A^ω se caracterizan del siguiente modo. Sea $\mathcal{C}$ la clase de todas las uniones finitas disjuntas de elementos de $\mathcal{P} = \{\langle w \rangle\}_{w \in A^*} \cup \{\emptyset\}$. Se tiene que $\mathcal{C}$ es un álgebra de conjuntos (teorema 1.6 en [Ca02, 12]) y que la σ-álgebra generada por $\mathcal{C}$ coincide con $\mathcal{B}(A^\omega)$. Gracias al teorema de extensión de Carathéodory-Hahn ([Ba95, 101, 103], [Ry88, 295]) y al teorema 1.7 en [Ca02, 14], obtenemos el siguiente resultado.

Teorema 1.1 *Existe una biyección entre las medidas $\mu : \mathcal{B}(A^\omega) \to [0,1]$ en A^ω y las funciones $h : A^* \to [0,1]$ que satisfacen las siguientes dos propiedades*:

$$h(\lambda) = 1 \qquad y \qquad h(w) = \sum_{k=1}^{Q} h(wa_k), \quad \forall w \in A^*.$$

Así, las medidas en A^ω están completamente determinadas por sus valores en los cilindros. Esto es, a toda función h con las propiedades del teorema 1.1 está asociada una única medida μ en A^ω tal que $\mu(wA^\omega) = h(w)$, para todo $w \in A^*$.

Podemos definir una gran variedad de medidas en A^ω del siguiente modo. Sea $\mathbf{p} = (\overline{p}_n)_{n=1}^{\infty}$

una sucesión de Q-tuplas $\overline{p}_n = (p_1^{(n)}, \ldots, p_Q^{(n)}) \in [0,1]^Q$ tales que $\sum_{k=1}^{Q} p_k^{(n)} = 1$, para todo n. Definamos $h_{\mathbf{p}} : A^* \to [0,1]$ por $h_{\mathbf{p}}(\lambda) = 1$ y

$$h_{\mathbf{p}}(w) = \prod_{n=1}^{m} p_{k_n}^{(n)}, \qquad \text{si } w = a_{k_1} a_{k_2} \cdots a_{k_m} \in A^*, \text{ donde } a_{k_n} \in A.$$

Por el teorema 1.1, obtenemos una medida en A^ω, denotada por $\prod \mathbf{p}$, que llamaremos la medida producto inducida por la sucesión $\mathbf{p}$. Cuando $\mathbf{p}$ sea una sucesión constante $(\overline{p})_n$, denotaremos la medida producto correspondiente $\prod \mathbf{p}$ por $\mu_{\overline{p}}$. Como un caso particular, obtendremos la medida de Lebesgue λ_Q en A^ω al tomar el vector $\overline{p} = (\frac{1}{Q}, \ldots, \frac{1}{Q})$ (ver [Ha74, 159]).

Intuitivamente, la medida producto $\prod \mathbf{p}$ se genera mediante una sucesión de infinitos *ensayos de Bernoulli*, donde el n-ésimo ensayo corresponde al lanzamiento de un dado de Q caras para el cual la probabilidad de que caiga la k-ésima cara es $p_k^{(n)}$.

1.2 Teoría de la recursión

Una función parcial de X en Y es una función tal que $\mathrm{dom}(\varphi) \subseteq X$, lo que denotamos por $\varphi : X \xrightarrow{o} Y$. Si $\mathrm{dom}(\varphi) = X$, decimos que φ es total y escribimos $\varphi : X \to Y$. Cuando $x \in \mathrm{dom}(\varphi)$, escribimos $\varphi(x) \downarrow$ y decimos que $\varphi(x)$ converge; en caso contrario, escribimos $\varphi(x) \uparrow$ y decimos que $\varphi(x)$ diverge. Dadas dos funciones parciales $\varphi, \psi : X \xrightarrow{o} Y$, escribimos $\varphi \simeq \psi$ para indicar que $\mathrm{dom}(\varphi) = \mathrm{dom}(\psi)$ y que $\varphi(x) = \psi(x)$ para todo $x \in \mathrm{dom}(\varphi)$. Si $B \subseteq X$, denotamos por B^c el complemento $\{x \in X \mid x \notin B\}$ de B con respecto a X.

Una función $\varphi : \mathbb{N}^m \xrightarrow{o} \mathbb{N}$ es parcial recursiva (p.r.) si es computable por alguna maquina de Turing M. Cuando una función p.r. es total se dice que es recursiva. $\varphi_n^{(m)}$ denota la función p.r. de m variables computada por la maquina de Turing M_n con *índice* n. $B \subseteq \mathbb{N}^m$ es recursivamente enumerable (r.e.) si es el dominio de alguna función p.r.; si B y B^c son r.e., decimos que B es recursivo.

El Teorema de Post

Sean $B, C \subseteq \mathbb{N}$. Decimos que C es m-reducible a B ($C \leq_m B$) si existe una función recursiva $f : \mathbb{N} \to \mathbb{N}$ tal que $(\forall n)\ (n \in C \Leftrightarrow f(n) \in B)$. Cuando C es m-reducible a B mediante una función inyectiva, decimos que C es 1-reducible a B ($C \leq_1 B$).

Una función $\varphi : \mathbb{N}^m \xrightarrow{o} \mathbb{N}$ es parcial recursiva en $B \subseteq \mathbb{N}$ si φ es computable por una maquina de Turing con *oráculo* para χ_B. Si φ es total, decimos que φ es recursiva en B. En adelante, φ_n^B denota la función p.r. en B cuyo índice es n y por W_n^B su correspondiente dominio. Decimos que C es Turing-reducible a B ($C \leq_T B$) si χ_C es recursiva en B y que C es r.e. en B si $C = W_n^B = \operatorname{dom}\left(\varphi_n^B\right)$, para algún n.

Informalmente, $C \leq_T B$ si existe un algoritmo para decidir si $n \in C$ con la ayuda de un mecanismo externo (oráculo para B) que responde preguntas de la forma "¿m pertenece a B?". Es claro que la relación $B \equiv_T C$, dada por $B \leq_T C \wedge C \leq_T B$, es una equivalencia en $\mathcal{P}(\mathbb{N})$.

Definimos el salto de B por $B' = \mathsf{K}^B = \left\{n \mid \varphi_n^B(n)\downarrow\right\}$. $B^{(n)}$, el n-esimo salto de B, se obtiene iterando el salto n veces (i.e., $B^{(0)} = B$, $B^{(n+1)} = \left(B^{(n)}\right)'$).

Ahora, introducimos la jerarquía aritmética de Kleene, la cual, se basa en la complejidad de los cuantificadores de la definición sintáctica de ciertos conjuntos [So87, 60]. Sea $B \subseteq \mathbb{N}^m$. $B \in \Sigma_0\,(\Pi_0)$ sii B es recursivo. Para $n \geq 1$, $B \in \Sigma_n$ si existe $R \subseteq \mathbb{N}^{m+n}$ recursiva tal que

$$B = \{\overline{x} \in \mathbb{N}^m \mid (\exists y_1)\,(\forall y_2)\,(\exists y_3)\cdots(\mathrm{Q}y_n)\ R\,(\overline{x}, y_1, y_2, \ldots, y_n)\}\,,$$

donde Q es $\exists$ si n es impar y $\forall$ si n es par. Similarmente, $B \in \Pi_n$ si

$$B = \{\overline{x} \in \mathbb{N}^m \mid (\forall y_1)\,(\exists y_2)\,(\forall y_3)\cdots(\mathrm{Q}y_n)\ R\,(\overline{x}, y_1, y_2, \ldots, y_n)\}\,,$$

donde Q es $\exists$ o $\forall$ de acuerdo a que n sea par o impar. Por último, $B \in \Delta_n$, si $B \in \Sigma_n \cap \Pi_n$ y B es aritmético si $B \in \bigcup_n (\Sigma_n \cup \Pi_n)$. Notemos que B es r.e. sii $B \in \Sigma_1$ y que $B \in \Sigma_n$ sii $B^c \in \Pi_n$. B es Σ_n-completo si $B \in \Sigma_n$ y $C \leq_1 B$ para todo $C \in \Sigma_n$. El siguiente resultado es fundamental; para una prueba, ver [So87, 64], [Ro67, 314].

Teorema de Post *Para todo $n \geq 0$:*

(a) $B \in \Sigma_{n+1} \Leftrightarrow B$ *es r.e. en algún conjunto* $\Pi_n \Leftrightarrow B$ *es r.e. en algún conjunto* Σ_n.

(b) $\emptyset^{(n+1)}$ *es* Σ_{n+1}*-completo.*

(c) $B \in \Sigma_{n+1} \Leftrightarrow B$ *es r.e. en* $\emptyset^{(n)}$.

(d) $B \in \Delta_{n+1} \Leftrightarrow B \leq_T \emptyset^{(n)}$.

Corolario 1.2 *Si* $B \leq_T C$ *y* $C \in \Pi_1$, *entonces* $B \in \Delta_2$.

Prueba. Dado que $B \leq_T C$ y $C \equiv_T C^c$, tenemos que $B \leq_T C^c$. Por el teorema de Post, $\emptyset^{(1)}$ es Σ_1-completo. Como $C^c \in \Sigma_1$ (pues $C \in \Pi_1$), $C^c \leq_1 \emptyset^{(1)}$. Así, $B \leq_T C^c$ y $C^c \leq_1 \emptyset^{(1)}$. Por transitividad, $B \leq_1 \emptyset^{(1)}$. De nuevo, por el teorema de Post, $B \in \Delta_2$. □

Ahora, introducimos la *función de pareamiento* estándar $\tau : \mathbb{N}^2 \to \mathbb{N}$ dada por

$$\tau(m,n) = \tfrac{1}{2}(m^2 + 2mn + n^2 + 3m + n), \qquad \text{para todo } m, n \in \mathbb{N}.$$

τ es una biyección cuyas inversas se denotan por $\pi_1(\tau(m,n)) = m$ y $\pi_2(\tau(m,n)) = n$. Es claro que $m, n \leq \tau(m,n)$ y que tanto τ como π_1 y π_2 son funciones recursivas [So87, 16].

Computabilidad en otros dominios

Como es bien sabido, la teoría de la recursión trata con conjuntos y funciones sobre $\mathbb{N}$. Pero, es posible extender las nociones propias de la computabilidad a dominios tan diversos como, por ejemplo, $A^*, \mathbf{2}^*, A^* \times \mathbf{2}^*$, $A^* \times \mathbb{N}^m$ o $\mathbb{Q}$.

Una función $\psi : A^* \overset{o}{\to} A^*$ se dice parcial recursiva (recursiva) si existe $\varphi : \mathbb{N} \overset{o}{\to} \mathbb{N}$ p.r. (recursiva) tal que

$$\psi(w) \simeq \mathsf{string}\left(\varphi\left(\mathsf{string}^{-1}(w)\right)\right), \qquad \text{para todo } w \in A^*.$$

Así, por la *tesis de Church*, $\left\{\mathsf{string} \circ \varphi_n \circ \mathsf{string}^{-1}\right\}_{n\in\mathbb{N}}$ es una enumeración *efectiva* de todas las funciones p.r. de A^* en A^*. Por abuso de lenguaje y notación, cuando resulte conveniente, identificaremos $\varphi_{\mathsf{string}(n)}$ con $\mathsf{string} \circ \varphi_n \circ \mathsf{string}^{-1}$. Análogamente, trataremos las funciones p.r. de $(A^*)^m$ en A^*. De este modo, podemos fijar una enumeración efectiva de todas las funciones p.r.

$$\varphi_e^{(m)} : (A^*)^m \overset{o}{\to} A^*, \quad e \in A^*,$$

que posee propiedades equivalentes a las de la enumeración estándar $\{\varphi_n^{(m)}\}_{n\in\mathbb{N}}$. En particular, enunciamos la versión traducida del *s-m-n* teorema de Kleene para funciones p.r. en A^*.

Teorema 1.3 *Para todo* $m, n \geq 1$, *existe una función total* $s_n^m : (A^*)^{m+1} \to A^*$ *recursiva e*

inyectiva tal que para todo $e \in A^*, \overline{w} = (w_1, \ldots, w_m) \in (A^*)^m$ *se cumple que*

$$\varphi^{(n)}_{s^m_n(e,\overline{w})} \simeq \varphi^{(m+n)}_e (\overline{w}, \cdot).$$

Sea $S \subseteq (A^*)^m$. Diremos que $S \in \Sigma_n$ (Π_n, Δ_n, es aritmético) en A^* sii el correspondiente conjunto

$$\{\overline{n} \in \mathbb{N} \mid (\mathsf{string}(n_1), \ldots, \mathsf{string}(n_m)) \in S\}$$

está en Σ_n (Π_n, Δ_n, es aritmético) en $\mathbb{N}$.

De un modo similar, usando bin (o combinando string y bin) se define computabilidad para funciones y conjuntos en $\mathbf{2}^*$ (o en $A^* \times \mathbf{2}^*$). Sin embargo, no entraremos en la rutina de los detalles requeridos y apelamos a cierta madurez matemática del lector.

Reales y Medidas computables

Fijemos una biyección computable $q : \mathbb{N} \to \mathbb{Q}$ con inversa computable. Una función $\varphi : \mathbb{N}^m \to \mathbb{Q}$ es recursiva si la función $q^{-1} \circ \varphi : \mathbb{N}^m \to \mathbb{N}$ es recursiva. Similarmente, una función $g : A^* \times \mathbb{N} \to \mathbb{Q}$ es recursiva si existe una función $\varphi : \mathbb{N}^2 \to \mathbb{Q}$ recursiva, tal que

$$g(w,k) = \varphi\left(\mathsf{string}^{-1}(w), k\right), \qquad \text{para todo } (w,k) \in A^* \times \mathbb{N}.$$

Un número real α es computable ($\alpha \in \mathbb{R}_c$) si existe una función recursiva $r : \mathbb{N} \to \mathbb{Q}$ tal que

$$|\alpha - r(k)| \leq 2^{-k}, \qquad \text{para todo } k \in \mathbb{N}.$$

Si $r = \varphi_n$, decimos que n es un código de aproximación para el número computable α. Una medida μ en A^ω es computable si existe una función recursiva $g : A^* \times \mathbb{N} \to \mathbb{Q}$ tal que

$$|\mu(\langle w \rangle) - g(w,k)| \leq 2^{-k}, \qquad \text{para todo } (w,k) \in A^* \times \mathbb{N}.$$

Si μ es una medida computable en A^ω, se cumple que $(\forall w \in A^*)$ $(\mu(\langle w \rangle) \in \mathbb{R}_c)$ y que

$$R[\mu] = \{(w,r) \mid \mu(\langle w \rangle) < r\} \qquad \text{y} \qquad L[\mu] = \{(w,r) \mid \mu(\langle w \rangle) > r\}$$

son subconjuntos r.e. de $A^* \times \mathbb{Q}$. Por ejemplo, $(w,r) \in R[\mu] \Leftrightarrow (\exists k)\,(\, g(w,k) + \frac{1}{2^k} < r\,)$.

El siguiente lema será de utilidad más adelante.

Lema 1.4 *Sea $\overline{p} = (p_1, \ldots, p_Q)$ una Q-tupla de reales computables en $[0,1]$ tales que $\sum p_k = 1$. Entonces la medida producto $\mu_{\overline{p}}$ en A^ω es computable.*

Prueba. Definimos una función recursiva $g : A^* \times \mathbb{N} \to \mathbb{Q}$ del siguiente modo. Dado $w = a_{k_1} a_{k_2} \cdots a_{k_m} \in A^*$ (con $a_{k_n} \in A$), tenemos que $\mu_{\overline{p}}(\langle w \rangle) = h_{\overline{p}}(w) = \prod_{n=1}^{m} p_{k_n}$. A partir de las funciones $r_1, \ldots, r_Q : \mathbb{N} \to \mathbb{Q}$ que aproximan a $p_1, \ldots, p_Q \in \mathbb{R}_c$, es posible construir *efectivamente* una función recursiva $g_w : \mathbb{N} \to \mathbb{Q}$ tal que $|\mu(\langle w \rangle) - g_w(k)| \leq 2^{-k}$, para todo $k \in \mathbb{N}$ (ver [Br94, 57]). Luego, tomando $g(w,k) = g_w(k)$, tenemos que $\mu_{\overline{p}}$ es computable. □

1.3 La jerarquía aritmética en A^ω

Desarrollaremos una jerarquía de subconjuntos de A^ω análoga a la jerarquía aritmética de Kleene para $\mathbb{N}$. Para ello, generalizamos el concepto de recursividad a espacios de la forma $A^\omega \times \mathbb{N}^m$ del siguiente modo (ver capítulo 15 en [Ro67]). Sea $k > 0$. Diremos que una función $\psi : A^\omega \times \mathbb{N}^m \xrightarrow{o} \mathbb{N}$ es parcial recursiva si existe un índice e tal que para todo $\mathbf{x} \in A^\omega$:

$$\psi(\mathbf{x}, n_1, \ldots, n_m) \simeq \varphi_e^{\mathbf{x}}(n_1, \ldots, n_m), \qquad \text{para todo } n_1, \ldots, n_m \in \mathbb{N}.$$

Para $k = 0$, diremos que $\psi : A^\omega \xrightarrow{o} \mathbb{N}$ es parcial recursiva si existe e tal que $\psi(\mathbf{x}) \simeq \varphi_e^{\mathbf{x}}(0)$.

En otras palabras, ψ es p.r. si existe una *maquina de Turing $\widehat{M_e}$ con oráculo* tal que para todo $(\mathbf{x}, \overline{n})$ y todo p se cumple que $\psi(\mathbf{x}, \overline{n}) = p$ *sii* cuando $\widehat{M_e}$ tiene la sucesión $\mathbf{x}$ escrita en la cinta de oráculo y se ingresa $\overline{n}$ como entrada, $\widehat{M_e}$ determina una computación que da como salida p.

Ahora, diremos que $\mathcal{R} \subseteq A^\omega \times \mathbb{N}^m$ es una clase $\Sigma_0^0 (= \Pi_0^0)$ si su función característica $\chi_{\mathcal{R}}$ es total recursiva. Las clases Σ_n^0 y Π_n^0 se definen inductivamente. Esto es, $\mathcal{R} \subseteq A^\omega \times \mathbb{N}^m$ es una clase Σ_{n+1}^0 si existe $\mathcal{S} \subseteq A^\omega \times \mathbb{N}^{m+1}$ tal que $\mathcal{S}$ es una clase Π_n^0 y

$$\mathcal{R} = \{(\mathbf{x}, n_1, \ldots, n_m) \mid (\exists n)\ \mathcal{S}(\mathbf{x}, n_1, \ldots, n_m, n)\}.$$

Decimos que $\mathcal{R}$ es una clase Π^0_{n+1} si $\mathcal{R}^c \in \Sigma^0_{n+1}$. Definimos $\Delta^0_n = \Sigma^0_n \cap \Pi^0_n$ y diremos que una relación $\mathcal{R} \subseteq A^\omega \times \mathbb{N}^m$ es aritmética si existe n tal que $\mathcal{R} \in \Sigma^0_n \cup \Pi^0_n$.

Sea $\mathcal{R} \subseteq A^\omega \times \mathbb{N}^m$ una clase Σ^0_0 tal que la maquina de Turing con oráculo $\widehat{M_e}$ computa $\chi_{\mathcal{R}}$. Obviamente, $\widehat{M_e}$ *siempre* para. Notemos que en cualquier caso $\widehat{M_e}$ sólo accesa un número finito k de celdas de la cinta de oráculo durante la computación de $\chi_{\mathcal{R}}(\mathbf{x}, \overline{n})$. Por tanto, si ingresamos el segmento inicial $\mathbf{x}(k)$ como oráculo y la misma entrada $\overline{n}$, tenemos que $\widehat{M_e}$ realiza la misma computación. El anterior análisis motiva la siguiente definición. Decimos que $\widehat{M_e}$ acepta en forma exacta a $(w, \overline{n})$ si al ingresar la cadena $w \in A^*$ como oráculo y $\overline{n} \in \mathbb{N}^m$ como entrada, $\widehat{M_e}$ da como salida 1. Por tanto, podemos asociar a $\mathcal{R}$ el siguiente conjunto *recursivo* de $A^* \times \mathbb{N}^m$:

$$\mathcal{R}_E := \{(w, \overline{n}) \mid \widehat{M_e} \text{ acepta en forma exacta a } (w, \overline{n})\}.$$

Notemos que $(\mathbf{x}, \overline{n}) \in \mathcal{R} \Leftrightarrow (\exists k)\left[(\mathbf{x}(k), \overline{n}) \in \mathcal{R}_E\right]$ y $(w, \overline{n}) \in \mathcal{R}_E \Leftrightarrow (\forall \mathbf{x} \in \langle w \rangle)\left[(\mathbf{x}, \overline{n}) \in \mathcal{R}\right]$.

Lema 1.5 *Sea $\mathcal{K} \subseteq A^\omega$. Entonces los siguientes enunciados son equivalentes*

(a) *$\mathcal{K}$ es una clase Σ^0_0.*

(b) *$\mathcal{K}$ es un conjunto abierto y cerrado* (clopen) *de A^ω.*

(c) *Existen finitas cadenas $w_k \in A^*$ tales que $\mathcal{K} = \bigcup_{k=1}^m \langle w_k \rangle A^\omega$.*

Prueba. (a) $\Rightarrow$ (b) Si $\mathcal{K}$ es una clase Σ^0_0, entonces se tiene que $\mathcal{K} = \bigcup \{\langle w \rangle \mid (w, 0) \in \mathcal{K}_E\}$. Por tanto, $\mathcal{K}$ es abierto. Análogamente, $\mathcal{K}^c \in \Pi^0_0 = \Sigma^0_0$ es abierto. Luego, $\mathcal{K}$ también es cerrado. (b) $\Rightarrow$ (c) Dado que $\mathcal{K}$ es abierto, existe $S \subseteq A^*$ tal que $\mathcal{K} = \bigcup_{w \in S} \langle w \rangle$. Como $\mathcal{K}$ es cerrado y A^ω es compacto, $\mathcal{K}$ también es compacto. Por tanto, existen finitas cadenas $w_k \in S$ tales que $\mathcal{K} = \bigcup_{k=1}^m \langle w_k \rangle$. Por último, (c) $\Rightarrow$ (a) es trivial. $\square$

Proposición 1.6 *Sea $\mathcal{V} \subseteq A^\omega$. Entonces los siguientes enunciados son equivalentes*

(a) *$\mathcal{V}$ es una clase Σ^0_1.*

(b) *Existe $R \subseteq A^*$ tal que R es recursivo y $\mathcal{V} = RA^\omega$.*

(c) *Existe $S \subseteq A^*$ tal que S es r.e. y $\mathcal{V} = SA^\omega$.*

Prueba. (a) $\Rightarrow$ (b) Existe $\mathcal{R} \subseteq A^\omega \times \mathbb{N}$ tal que $\mathcal{R}$ es una clase Σ_0^0 y $\mathcal{V} = \{\mathbf{x} \mid (\exists n)\ (\mathbf{x}, n) \in \mathcal{R}\}$. Por tanto, $\mathbf{x} \in \mathcal{V} \Leftrightarrow (\exists n)(\exists m)((\mathbf{x}(m), n) \in \mathcal{R}_E) \Leftrightarrow (\exists k)(\mathbf{x}(k) \in R)$, donde

$$R = \{w \in A^* \mid \tau(m,n) = |w| \ \wedge\ (w_1 w_2 \cdots w_m, n) \in \mathcal{R}_E\}.$$

(b) $\Rightarrow$ (c) Basta notar que todo conjunto recursivo es r.e..

(c) $\Rightarrow$ (a) Como S es r.e., existe $T \subseteq A^* \times \mathbb{N}$ tal que T es recursivo y $S = \{w \mid (\exists m)((w,m) \in T)\}$. Por tanto, $\mathbf{x} \in \mathcal{V} \Leftrightarrow (\exists n)(\exists m)((\mathbf{x}(n), m) \in T) \Leftrightarrow (\exists k)((\mathbf{x}(\pi_2(k)), \pi_1(k)) \in T)$. Definamos

$$\mathcal{R} = \{(\mathbf{x}, k) \mid (\mathbf{x}(\pi_2(k)), \pi_1(k)) \in T\}.$$

Dado que χ_T es recursiva, $\mathcal{R}$ es una clase Σ_0^0: dado $(\mathbf{x}, k)$, generamos m, n tales que $\tau(m,n) = k$. Mediante el oráculo para $\mathbf{x}$ hallamos $\mathbf{x}(n) = x_1 \cdots x_n$. Luego, computamos $\chi_T(\mathbf{x}(n), m)$. $\square$

Si $S \subseteq A^* \times \mathbb{N}$, la m-ésima sección de S es el conjunto $S_m = \{(w,m) \mid w \in S\}$.

Proposición 1.7 *$\mathcal{G} \subseteq A^\omega$ es una clase Π_2^0 sii existe $S \subseteq A^* \times \mathbb{N}$ r.e. tal que $\mathcal{G} = \bigcap_m S_m A^\omega$.*

Prueba. ($\Rightarrow$) Si $\mathcal{G}$ es una clase Π_2^0, existe una clase $\mathcal{R} \in \Sigma_0^0$ en $A^\omega \times \mathbb{N}^2$ tal que

$$\mathbf{x} \in \mathcal{G} \Leftrightarrow (\forall m)(\exists i)\mathcal{R}(\mathbf{x}, m, i) \Leftrightarrow (\forall m)(\exists i)(\exists k)((\mathbf{x}(k), m, i) \in \mathcal{R}_E).$$

Basta tomar el conjunto r.e. $S = \{(w,m) \mid (\exists n)(n = \tau(i, |w|) \wedge (w, m, i) \in \mathcal{R}_E)\}$.

($\Leftarrow$) Como S es r.e., existe $T \subseteq A^* \times \mathbb{N}^2$ tal que $\mathbf{x} \in \mathcal{G} \Leftrightarrow (\forall m)(\exists k)(\exists i)((\mathbf{x}(k), m, i) \in T)$. Claramente, $\mathcal{R} = \{(\mathbf{x}, m, n) \mid n = \tau(i,k) \wedge (\mathbf{x}(k), m, i) \in T\}$ es una clase Σ_0^0 de $A^\omega \times \mathbb{N}^2$ tal que $\mathbf{x} \in \mathcal{G} \Leftrightarrow (\forall m)(\exists n)\mathcal{R}(\mathbf{x}, m, n)$. Luego, $\mathcal{G} \in \Pi_2^0$. $\square$

Corolario 1.8 *Sean $\mathcal{C}, \mathcal{F} \subseteq A^\omega$.*

(a) *$\mathcal{C}$ es una clase Π_1^0 sii existe $R \subseteq A^*$ recursivo tal que $\mathcal{C} = \{\mathbf{x} \mid (\forall n)\ (\mathbf{x}(n) \in R)\}$.*

(b) *$\mathcal{F}$ es una clase Σ_2^0 sii existe $\{\mathcal{C}_n\}_n$ en A^ω tal que $\mathcal{C}_n \in \Pi_1^0$ y $\mathcal{F} = \bigcup_n \mathcal{C}_n$.*

De forma análoga, se puede definir una jerarquía aritmética para el espacio $A^\omega \times \mathbf{2}^\omega$ y obtener caracterizaciones similares. Por ejemplo, una clase Σ_1^0 en $A^\omega \times \mathbf{2}^\omega$ es un conjunto de la forma $\bigcup_{(u,v)\in T} uA^\omega \times v\mathbf{2}^\omega$, donde T es un subconjunto r.e. de $A^* \times \mathbf{2}^*$.

Capítulo 2

Nociones de Aleatoriedad

2.1 Aleatoriedad y colectivos

En 1919 el físico austríaco Richard von Mises propuso la primera axiomatización de la teoría de la probabilidad basándose en un tipo especial de sucesiones a las que dio el nombre de "*colectivos*" (Kollectives en alemán). Las dos propiedades que caracterizan a los colectivos son, por un lado, la existencia de límites apropiados de ciertas frecuencias relativas dentro de la sucesión (regularidad global) y, por el otro, la invarianza de estos límites bajo la operación de "*selección admisible de lugar*" (irregularidad local). Una selección admisible de lugar es un procedimiento para seleccionar una subsucesión de una sucesión dada $\mathbf{x}$ en forma tal que la decisión de seleccionar un término x_n no depende del valor de x_n.

Ahora introducimos una descripción matemática de los colectivos, inspirada en las intuiciones de von Mises.

Definición 2.1 (von Mises) *Un* colectivo *es una sucesión* $\mathbf{x} \in A^\omega$ *tal que*

(1) *para todo* $B \subseteq A$ *se cumple que* $\Pr(B) := \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \chi_B(x_k)$ *existe, y*

(2) *Si* Φ *es una* selección admisible de lugar, *entonces para todo* $B \subseteq A$

$$\Pr(B) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} \chi_B((\Phi\mathbf{x})_k).$$

La función P definida en (1) se llama la *distribución de probabilidad determinada por el colectivo* $\mathbf{x}$. La condición (2) se denomina el *axioma de aleatoriedad*. Von Mises también la designó como el *principio de exclusión de la estrategia del jugador*. En cuanto a la elusiva noción de selección admisible de lugar, von Mises nunca dio una definición satisfactoria e intentó aclarar su significado apelando a varios ejemplos. Consideremos el caso más sencillo, lanzamiento de monedas; en otras palabras, colectivos en $\mathbf{2}^\omega$:

(a) elija aquellos x_n para los cuales n es primo,

(b) elija aquellos x_n que siguen después de la cadena 00101,

(c) lance una moneda (distinta); elija x_n si en el n-ésimo lanzamiento sale cara.

Es más o menos obvio que todos estos procedimientos de selección son admisibles: el valor de x_n no es usado para determinar si se elige x_n.

Por un tiempo, de 1919 a 1933, la única axiomatización explícita, más o menos rigurosa, de la teoría de la probabilidad hacía uso de los colectivos. Sin embargo, se presentaron varias objeciones a la teoría de von Mises y surgieron dudas concernientes a la existencia de dichos colectivos.

Después de muchos intentos surgió la convicción de que "selección admisible de lugar" debería significar "selección de lugar dada por una ley matemática", como en los dos ejemplos (a) y (b) anteriores. Varios autores llegaron independientemente a una clase de selecciones de lugar que son una generalización del ejemplo (b): las denominadas *selecciones de Bernoulli*. Estas se pueden describir del siguiente modo: sea $\mathbf{x}$ un colectivo; fijemos una cadena w en A^* y elijamos aquellos x_{n+1} tales que w es un segmento final (o sufijo) de $\mathbf{x}(n)$. Notemos que esta selección elige una subsucesión infinita de $\mathbf{x}$ si $\mathbf{x}$ contiene infinitas ocurrencias de w.

Luego, de aquí en adelante, trataremos las selecciones de lugar como funciones parciales $\Phi : A^\omega \xrightarrow{o} A^\omega$ e introducimos la siguiente definición general de selección de lugar que tiene como caso particular las selecciones de Bernoulli.

Definición 2.2 *Sea* $\phi : A^* \to \mathbf{2}$. *Entonces* ϕ *determina una* selección de lugar Φ *en dos pasos*:

(1) $\overline{\Phi} : A^* \to A^*$ *está dada por*

$$\overline{\Phi}(xa) = \begin{cases} \overline{\Phi}(x)\, a, & si\ \phi(x) = 1. \\ \overline{\Phi}(x), & si\ \phi(x) = 0. \end{cases}, \qquad donde\ a \in A.$$

(2) *la función parcial* $\Phi : A^\omega \xrightarrow{o} A^\omega$ *se define por*

(a) $\mathrm{dom}(\Phi) = \{\mathbf{x} \in A^\omega \mid (\forall m)(\exists n \geq m)\ (\ \phi(\mathbf{x}(n)) = 1\ )\}$.

(b) *si* $\mathbf{x} \in \mathrm{dom}(\Phi)$, *entonces* $\Phi(\mathbf{x})$ *es la única sucesión en* $\bigcap_n \overline{\Phi}(\mathbf{x}(n))\, A^\omega$.

Intuitivamente Φ selecciona, mediante ϕ, una subsucesión $\Phi(\mathbf{x})$ de una sucesión $\mathbf{x}$ dada del siguiente modo: si $\phi(\mathbf{x}(n)) = 1$, Φ elige x_{n+1} y si $\phi(\mathbf{x}(n)) = 0$, Φ descarta x_{n+1}. Ahora, es fácil verificar que $\bigcap_n \overline{\Phi}(\mathbf{x}(n)) A^\omega$ tiene a lo sumo un elemento. Por otro lado, si $\mathbf{x} \in \mathrm{dom}(\Phi)$, $\left\{\overline{\Phi}(\mathbf{x}(n)) A^\omega\right\}$ es una sucesión encajada de cerrados no vacíos en A^ω (todo cilindro es clopen). Dado que A^ω es compacto, $\bigcap_n \overline{\Phi}(\mathbf{x}(n)) A^\omega$ *es no vacía.* Por consiguiente, $\Phi(\mathbf{x})$ está bien definida para todo $\mathbf{x} \in \mathrm{dom}(\Phi)$.

Definición 2.3 *Sean $w \in A^*$ y $\phi_w : A^* \to \mathbf{2}$ dada por*

$$\phi_w(u) = \begin{cases} 1, & \textit{si } w \textit{ es un segmento final de } u. \\ 0, & \textit{en caso contrario.} \end{cases}$$

Φ_w *es una* selección de Bernoulli *si se obtiene de ϕ_w al aplicar los dos pasos de la definición* 2.2.

En lo que resta de la sección, nos limitaremos al caso *binario* por comodidad. Sea $p \in [0,1]$, el conjunto $\mathrm{LLN}(p)$ se define por

$$\mathrm{LLN}(p) = \left\{ \mathbf{x} \in \mathbf{2}^\omega \mid \lim_{n\to\infty} \frac{1}{n} \sum\nolimits_{k=1}^{n} x_k = p \right\}.$$

Decimos que $\mathbf{x} \in \mathbf{2}^\omega$ es una sucesión de Bernoulli (con respecto a p) si para toda cadena $w \in \mathbf{2}^* : \mathbf{x} \in \mathrm{dom}(\Phi_w)$ implica que $\Phi_w(\mathbf{x}) \in \mathrm{LLN}(p)$. En el caso particular, $p = \frac{1}{2}$, las sucesiones de Bernoulli se suelen llamar *números normales.*

Aunque von Mises admitió que este tratamiento de los colectivos era matemáticamente aceptable, consideraba que las sucesiones de Bernoulli no eran una formalización satisfactoria de la noción de colectivo. En repetidas ocasiones, él enfatizo que ningún conjunto **fijo** de selecciones de lugar era suficiente para tratar **todos** los problemas de la teoría de la probabilidad. Un resultado más optimista fue obtenido por Abraham Wald en 1936 [vL87a, 39].

Teorema 2.4 (Wald) *Sean $p \in (0,1)$ y $\mathfrak{A}$ un conjunto contable de selecciones de lugar. Entonces el conjunto*

$$C(\mathfrak{A}, p) = \{\mathbf{x} \in \mathbf{2}^\omega \mid (\forall \Phi \in \mathfrak{A})\ (\ \mathbf{x} \in \mathrm{dom}(\Phi) \Rightarrow \Phi(\mathbf{x}) \in \mathrm{LLN}(p)\ )\}$$

tiene la cardinalidad del continuo.

Von Mises estaba satisfecho con el anterior teorema, dado que cualquier aplicación específica de la teoría siempre involucraba una cantidad contable de selecciones de lugar. Aunque la reformulación de Wald solucionó de cierta forma el problema de la consistencia, llevó a una objeción de una naturaleza enteramente diferente, basada en un teorema de Ville. Para cualquier conjunto contable de selecciones de lugar $\{\Phi_n\}$, Ville construyo $\mathbf{x} \in \mathbf{2}^\omega$ tal que

$$\text{(a) } (\forall n)\left(\lim_{m\to\infty} \tfrac{1}{m} \sum_{k=1}^{m} (\Phi_n \mathbf{x})_k = \tfrac{1}{2}\right), \qquad \text{y} \qquad \text{(b) } (\forall m)\left(\tfrac{1}{m} \sum_{k=1}^{m} x_k \geq \tfrac{1}{2}\right).$$

Dicha sucesión $\mathbf{x}$ es un colectivo respecto a los Φ_n, pero parece demasiado regular para ser llamada aleatoria. Formalmente, las sucesiones $\mathbf{x}$ con la propiedad (b) forman un conjunto de medida de Lebesgue cero, dado que Lèvy había probado previamente que

$$\lambda_2 \left\{ \mathbf{x} \in \mathbf{2}^\omega \mid \text{para infinitos } m : \left(\tfrac{1}{2} - \tfrac{1}{m} \sum_{k=1}^{m} x_k\right) > \tfrac{1}{\sqrt{m}} \right\} = 1.$$

La ley de Lèvy es un caso especial de la denominada **ley del logaritmo iterado**.

2.2 Aleatoriedad y estocasticidad

Como consecuencia de las críticas lideradas por Fréchet y Ville en contra del enfoque de von Mises, el problema de definir aleatoriedad se concebía ahora del siguiente modo: una sucesión aleatoria (con respecto a alguna medida de probabilidad) debería satisfacer todas las leyes probabilísticas para dicha medida; en otras palabras, el conjunto de sucesiones aleatorias debería ser la intersección de todas las propiedades de probabilidad uno. Por supuesto, enunciada en esta forma, la exigencia es imposible de satisfacer, dado que la requerida intersección es vacía. Luego, se debe elegir entre las propiedades de probabilidad uno.

En 1966, Martin-Löf propuso una elección canónica para la familia de leyes probabilísticas: la familia de leyes que se pueden probar efectivamente. Una ley probabilística, de acuerdo a la interpretación usual, es un enunciado de la forma "$\mu\{\mathbf{x} \in A^\omega \mid P(\mathbf{x})\} = 1$", donde P es alguna propiedad. Un procedimiento típico para probar dicho enunciado es el siguiente:

Se construye una sucesión $\{\mathcal{V}_n\}$ de abiertos tales que

(a) $\{\mathbf{x} \in A^\omega \mid P(\mathbf{x})\}^c \subseteq \mathcal{V}_n$ para todo n;

(b) cada abierto $\mathcal{V}_n$ es una unión de una sucesión r.e. de cilindros;

(c) $\mu(\mathcal{V}_n) \leq \frac{Q^{-(n+1)}}{Q-1}$ (u otra función recursiva de n que decrezca *adecuadamente* a 0).

La noción de aleatoriedad de Martin-Löf se puede ver como una formalización del procedimiento anterior, el cual se conoce bajo el nombre de "test secuencial recursivo". Este término, acuñado por Martin-Löf, refleja el origen estadístico, más que probabilístico, de estos conjuntos (ver sección 3.5 de [vL87a]).

Definición 2.5 *Sea μ una medida computable en A^ω. Decimos que $\mathcal{N} \subseteq A^\omega$ es un* μ-test secuencial recursivo de Martin-Löf *si existe $V \subseteq A^* \times \mathbb{N}$ r.e. tal que*

(1) $\mathcal{N} = \bigcap_m \mathcal{V}_m$, *donde* $\mathcal{V}_m = V_m A^\omega = \{\mathbf{x} \mid (\exists n)[(\mathbf{x}(n), m) \in V]\}$.

(2) *para todo m :*

$$\mathcal{V}_{m+1} \subseteq \mathcal{V}_m \qquad y \qquad \mu(\mathcal{V}_m) \leq \frac{Q^{-(m+1)}}{Q-1}.$$

(3) *Si $(w, m) \in V$, entonces $|w| > m$.*

En adelante, nos referiremos a los μ-tests secuenciales recursivos de Martin-Löf simplemente como μ-tests secuenciales. Notemos que, por las proposiciones 1.7 y 1.6, $\mathcal{N}$ es una clase Π^0_2 y cada $\mathcal{V}_m$ es una clase Σ^0_1. Por (2), $\mu(\mathcal{N}) = \lim_{m\to\infty} \mu(\mathcal{V}_m) = 0$. Así, $\mathcal{N}$ es lo que se suele conocer como un conjunto de medida cero construible (ver [Li93, 142], [Su03, 40]).

Cuando tomamos $\mu = \lambda_Q$, se tiene que

$$\frac{\#(A^n \cap V_m)}{Q^n} = \sum_{w \in A^n \cap V_m} Q^{-|w|} = \sum_{w \in A^n \cap V_m} \lambda_Q(wA^\omega) \leq \lambda_Q(\mathcal{V}_m) < \frac{Q^{-m}}{Q-1}.$$

Por tanto, en el caso de la medida de Lebesgue λ_Q, la definición 2.5 coincide con la definición de test secuencial de Martin-Löf dada en [Ca02, 109, 158] y [Su03, 29] (ver además el lema 3.1.12 [Su03, 40]).

Cabe mencionar que leyes probabilísticas como la ley del logaritmo iterado ó la ley de los grandes números se pueden probar de hecho construyendo tests secuenciales que cubren los conjuntos de sucesiones que no satisfacen tales leyes (ver [vL87a, 69, 108]).

Ahora introducimos la noción prometida de aleatoriedad.

Definición 2.6 (Martin-Löf) *Sea μ una medida computable en A^ω. Decimos que $\mathbf{x} \in A^\omega$ es* μ-aleatoria *si para todo μ-test secuencial $\mathcal{N}$, se cumple que $\mathbf{x} \notin \mathcal{N}$.*

En otras palabras, si $\mathbf{x} \in \mathcal{N}$, entonces $\mathbf{x}$ *falla* el test o el test *rechaza* la hipótesis de que $\mathbf{x}$ es aleatoria. En caso contrario, $\mathbf{x}$ *pasa* el test. Por tanto, $\mathbf{x}$ es μ-aleatoria, lo que se denotará por $\mathbf{x} \in \mathcal{R}(\mu)$, si $\mathbf{x}$ pasa **cualquier** μ-test secuencial.

Definición 2.7 *Sea μ una medida computable en A^ω. Una función total $\delta : A^\omega \to \mathbb{N} \cup \{\infty\}$ es una* función de deficiencia de aleatoriedad *si existe una función $\gamma : A^* \to \mathbb{N}$ tal que*

(1) *$V[\gamma] := \{(w, m) \mid \gamma(w) > m\}$ es un subconjunto r.e. de $A^* \times \mathbb{N}$.*

(2) *para todo $\mathbf{x} \in A^\omega$ y todo $m \in \mathbb{N}$:*

$$\delta(\mathbf{x}) = \sup_{n \in \mathbb{N}} \gamma(\mathbf{x}(n)) \qquad y \qquad \mu(\{\mathbf{x} \mid \delta(\mathbf{x}) > m\}) \leq \frac{Q^{-(m+1)}}{Q-1}.$$

El siguiente lema muestra la estrecha conexión entre las funciones de deficiencia y los μ-tests.

Lema 2.8 *Si δ es una función de deficiencia de aleatoriedad, entonces*

$$\mathcal{N}_\delta := \{\mathbf{x} \in A^\omega \mid \delta(\mathbf{x}) = \infty\}$$

es un μ-test secuencial. Recíprocamente, si $\mathcal{N}$ es un μ-test secuencial, existe una función de deficiencia de aleatoriedad δ tal que $\mathcal{N} = \mathcal{N}_\delta = \{\mathbf{x} \in A^\omega \mid \delta(\mathbf{x}) = \infty\}$.

Prueba. Si δ es una función de deficiencia de aleatoriedad, basta notar que

$$\mathbf{x} \in \mathcal{N}_\delta \Leftrightarrow (\forall m)(\delta(\mathbf{x}) > m) \Leftrightarrow (\forall m)(\exists n)(\gamma(\mathbf{x}(n)) > m) \Leftrightarrow (\forall m)(\exists n)((\mathbf{x}(n), m) \in V[\gamma]).$$

Ahora, a todo μ-test secuencial $\mathcal{N}$ le podemos asociar su nivel crítico $m_V : A^* \to \mathbb{N}$ dado por

$$m_V(w) = \begin{cases} \max\{m+1 \mid w \in V_m\}, & \text{si } w \in V_0. \\ 0, & \text{en caso contrario.} \end{cases}$$

Dado que $(w, m) \in V$ implica que $|w| > m$, entonces m_V es total y $\{(w, m) \mid m_V(w) > m\} = V$. Por tanto, basta tomar $\delta(\mathbf{x}) = \sup_n m_V(\mathbf{x}(n))$. $\square$

Diremos que un μ-test secuencial es universal si contiene a cualquier otro μ-test secuencial. Para probar la existencia de un μ-test universal, necesitamos el siguiente resultado. Para su prueba, referimos al lector a [Li93, 143]. Como es usual, interpretamos $\infty - c = \infty$.

Proposición 2.9 *Existe una función de deficiencia de aleatoriedad $\delta_0(\cdot|\mu)$ tal que para cada función de deficiencia δ existe una constante $c \geq 0$ tal que para todo $\mathbf{x} \in A^\omega$:*

$$\delta(\mathbf{x}) - c \leq \delta_0(\mathbf{x}|\mu).$$

Ahora, sea $\mathcal{U}$ el μ-test secuencial asociado a $\delta_0(\cdot|\mu)$; esto es, $\mathcal{U} = \{\mathbf{x} \in A^\omega \mid \delta_0(\mathbf{x}|\mu) = \infty\}$. Por el lema 2.8 y la proposición 2.9, es inmediato que

$$\mathcal{U} = \bigcup_{\mathcal{N} \in \mathbf{V}} \mathcal{N},$$

donde $\mathbf{V}$ denota la familia de **todos** los μ-tests secuenciales. Por tanto, $\mathcal{U}$ es un μ-test secuencial universal. Es claro que para todo $\mathbf{x} \in A^\omega$:

$$\mathbf{x} \in \mathcal{R}(\mu) \quad \Leftrightarrow \quad \mathbf{x} \notin \mathcal{U} \quad \Leftrightarrow \quad \delta_0(\mathbf{x}|\mu) < \infty.$$

Por lo cual, $\mathcal{R}(\mu) = A^\omega \setminus \mathcal{U}$ y $\mu(\mathcal{R}(\mu)) = 1$. Así, siempre podemos asociar a toda medida computable μ en A^ω un μ-test secuencial universal $\mathcal{U}$.

2.3 El principio de homogeneidad

Ahora que tenemos dos nociones de aleatoriedad basadas en ideas enteramente distintas, a saber, selecciones de lugar (sección 2.1) y tests estadísticos (sección 2.2), investigaremos las relaciones entre estas dos definiciones. Nuestro principal objetivo será obtener el principio de homogeneidad:

> *Si una sucesión $\mathbf{x} \in A^\omega$ es aleatoria, entonces $\Phi\mathbf{x}$ también es aleatoria para "casi todas" las selecciones de lugar $\Phi : A^\omega \xrightarrow{o} A^\omega$.*

Este principio está inspirado en la siguiente propiedad formulada por von Mises:

Una subsucesión admisiblemente seleccionada de un colectivo es un colectivo, con la misma distribución.

Ahora, para formular este principio de manera que sea susceptible al análisis matemático, debemos dotar el conjunto de selecciones de lugar con cierta medida. Esto se puede lograr si identificamos dicho conjunto con $\mathbf{2}^\omega$ de la siguiente forma.

Definición 2.10 *Sea* $/ : A^\omega \times \mathbf{2}^\omega \xrightarrow{o} A^\omega$ *la función definida por*

$$(\mathbf{x}/\mathbf{y})_n = x_m \quad \textit{sii} \quad m \textit{ es el índice del } n\textit{-ésimo } 1 \textit{ en } \mathbf{y}, \quad \forall \mathbf{x} \in A^\omega, \mathbf{y} \in \mathbf{2}^\omega.$$

La operación / está definida para todo par $(\mathbf{x}, \mathbf{y})$ tales que $\mathbf{y}$ contenga infinitos unos. Sea $\Phi : A^\omega \xrightarrow{o} A^\omega$ una selección de lugar; entonces para todo $\mathbf{x} \in A^\omega$ podemos definir $\mathbf{y} \in \mathbf{2}^\omega$ tal que $\Phi\mathbf{x} = \mathbf{x}/\mathbf{y}$. En efecto, si $\Phi\mathbf{x} = x_{m_1}x_{m_2}\cdots$, donde $m_1 < m_2 < \cdots$, basta definir $\mathbf{y} \in \mathbf{2}^\omega$ por

$$y_i = \begin{cases} 1, & \text{si } i = m_k \text{ para algún } k, \\ 0, & \text{en caso contrario.} \end{cases}$$

Es obvio que $(\mathbf{x}/\mathbf{y})_n = x_{m_n}$. Por tanto, $\Phi\mathbf{x} = \mathbf{x}/\mathbf{y}$. Esta observación nos sugiere que será de utilidad estudiar las selecciones de lugar via la operación /.

Para evitar enunciados extensos en los teoremas, introducimos las siguientes convenciones para el resto de la sección. La expresión "*para todas las medidas* ν *en* $\mathbf{2}^\omega$..." significa "*para todas las medidas de probabilidad* ν *en* $\mathbf{2}^\omega$ tales que $\nu\{\mathbf{y} \in \mathbf{2}^\omega \mid \mathbf{y} \text{ contiene finitos ceros}\} = 0$...". Por $\overline{p}$ denotaremos cualquier vector $(p_1, \ldots, p_Q)$ en $(0,1)^Q$ tal que $\sum_{k=1}^{Q} p_k = 1$ y por $\mu_{\overline{p}}$ la medida producto asociada a la sucesión constante $(\overline{p})_{n=1}^{\infty}$ (ver pág. 3).

En el enfoque de Martin-Löf, se identifican los colectivos con las sucesiones aleatorias; lo cual nos permite enunciar el principio de homogeneidad en los siguientes términos.

Teorema 2.11 (Principio de homogeneidad) *Sean* $\overline{p} = (p_1, \ldots, p_Q)$ *una* Q*-tupla de reales computables en* $(0,1)$, ν *una medida computable en* $\mathbf{2}^\omega$ *y* $\mathcal{R}\left(\mu_{\overline{p}}\right)$ *la noción de aleatoriedad de Martin-Löf asociada a la medida computable* $\mu_{\overline{p}}$. *Entonces*

$$\mathbf{x} \in \mathcal{R}\left(\mu_{\overline{p}}\right) \quad \textit{implica que} \quad \nu\left(\left\{\mathbf{y} \in \mathbf{2}^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{R}\left(\mu_{\overline{p}}\right)\right\}\right) = 1.$$

Cabe observar que el principio de homogeneidad se refiere, no a alguna medida específica, sino a todas las medidas computables (adecuadas) en $\mathbf{2}^\omega$. Esto indica lo extremadamente pequeño que es el conjunto de subsucesiones de una sucesión aleatoria que no son a su vez aleatorias. Notemos que el principio no menciona para nada admisibilidad y posee un caracter puramente cuantitativo. Para probar el teorema 2.11, necesitamos unos resultados preliminares.

Lema 2.12 (Doob) *Sea* $\mathbf{y}$ *una sucesión en* $\mathbf{2}^\omega$ *que contiene infinitos unos. Si* $\mathcal{V}$ *es abierto en* A^ω, *entonces* $\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\}$ *es abierto en* A^ω *y* $\mu_{\overline{p}}(\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\}) = \mu_{\overline{p}}(\mathcal{V})$.

Prueba. Dado que $\mathbf{y}$ contiene infinitos unos, la función $\Phi_{\mathbf{y}} : A^\omega \to A^\omega$, dada por $\Phi_{\mathbf{y}}\mathbf{x} = \mathbf{x}/\mathbf{y}$, es total. Notemos que $\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\} = \{\mathbf{x} \mid \Phi_{\mathbf{y}}\mathbf{x} \in \mathcal{V}\} = \Phi_{\mathbf{y}}^{-1}[\mathcal{V}]$. Supogamos que el enunciado es válido para cualquier cilindro de A^ω y tomemos un abierto arbitrario $\mathcal{V}$ en A^ω. Existe una familia mutuamente disjunta de cilindros $\{\langle w_n\rangle\}_n$ tal que $\mathcal{V} = \bigcup_n \langle w_n\rangle$. Así,

$$\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\} = \Phi_{\mathbf{y}}^{-1}\left[\bigcup_n \langle w_n\rangle\right] = \bigcup_n \Phi_{\mathbf{y}}^{-1}[\langle w_n\rangle].$$

Por tanto, $\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\}$ es abierto en A^ω.
Dado que para todo n : $\mu_{\overline{p}}\left(\Phi_{\mathbf{y}}^{-1}[w_n]\right) = \mu_{\overline{p}}(w_n)$, tenemos que

$$\mu_{\overline{p}}(\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\}) \leq \sum\nolimits_n \mu_{\overline{p}}\left(\Phi_{\mathbf{y}}^{-1}[w_n]\right) = \sum\nolimits_n \mu_{\overline{p}}(w_n) = \mu_{\overline{p}}(\mathcal{V}). \tag{2.1}$$

Por monotonía, $\mu_{\overline{p}}(w_n) = \mu_{\overline{p}}\Phi_{\mathbf{y}}^{-1}[w_n] \leq \mu_{\overline{p}}(\bigcup_n \Phi_{\mathbf{y}}^{-1}[w_n]) = \mu_{\overline{p}}(\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\})$. Luego,

$$\mu_{\overline{p}}(\mathcal{V}) = \sum\nolimits_n \mu_{\overline{p}}(w_n) \leq \mu_{\overline{p}}(\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\}). \tag{2.2}$$

De (2.1) y (2.2), se sigue que lo pedido. Ahora, veamos que el enunciado es válido para cualquier cilindro en A^ω. Sea $w = a_{i_1} \cdots a_{i_n} \in A^*$, donde $a_{i_j} \in A$, para $j = 1, \ldots, n$. Por definición,

$$\mu_{\overline{p}}(wA^\omega) = h_{\overline{p}}(w) = \prod\nolimits_{j=1}^{n} p_{i_j} \in (0,1).$$

Ahora, sean $m_1 < \cdots < m_n$ los índices de los primeros n *unos* en $\mathbf{y}$. Por comodidad, definamos $k_j \in \mathbb{N}$ por $k_1 := m_1 - 1 \quad$ y $\quad k_j := m_j - m_{j-1} - 1, \quad$ para $j = 2, \ldots, n$. Así,
$(\mathbf{x}/\mathbf{y})_1 = x_{m_1} = x_{k_1+1}, \quad (\mathbf{x}/\mathbf{y})_2 = x_{m_2} = x_{m_1+k_2+1}, \quad \cdots \quad (\mathbf{x}/\mathbf{y})_n = x_{m_n} = x_{m_{n-1}+k_n+1}$.

Por tanto,

$$\begin{aligned}\{\mathbf{x}\in A^{\omega}\mid \mathbf{x}/\mathbf{y}\in\langle w\rangle\} &= \{\mathbf{x}\mid(\mathbf{x}/\mathbf{y})(n)=w\}=\{\mathbf{x}\mid x_{m_1}=a_{i_1}\wedge\cdots\wedge x_{m_n}=a_{i_n}\}\\ &= A^{k_1}\{a_{i_1}\}A^{k_2}\{a_{i_2}\}\cdots\{a_{i_{n-1}}\}A^{k_n}\{a_{i_n}\}A^{\omega}\\ &= \bigcup_{u_1\in A^{k_1}}\bigcup_{u_2\in A^{k_2}}\cdots\bigcup_{u_n\in A^{k_n}}u_1a_{i_1}u_2a_{i_2}\cdots a_{i_{n-1}}u_na_{i_n}A^{\omega}.\end{aligned}$$

Como $\{\mathbf{x}\mid \mathbf{x}/\mathbf{y}\in wA^{\omega}\}$ es una unión finita (disjunta) de cilindros, $\{\mathbf{x}\mid \mathbf{x}/\mathbf{y}\in wA^{\omega}\}$ es abierto en A^{ω}. Por la definición de $\mu_{\overline{p}}$ (pág. 3), tenemos que

$$\begin{aligned}\mu_{\overline{p}}(\{\mathbf{x}\mid \mathbf{x}/\mathbf{y}\in\langle w\rangle\}) &= \sum_{u_1\in A^{k_1}}\cdots\sum_{u_n\in A^{k_n}}h_{\overline{p}}(u_1)\cdot p_{i_1}\cdots p_{i_{n-1}}\cdot h_{\overline{p}}(u_n)\cdot p_{i_n}\\ &= (p_{i_1}\cdots p_{i_n})\cdot\sum_{u_1\in A^{k_1}}\cdots\sum_{u_n\in A^{k_n}}h_{\overline{p}}(u_1)\cdots h_{\overline{p}}(u_n)\\ &= \mu_{\overline{p}}(wA^{\omega})\cdot\sum_{u_1\in A^{k_1}}\cdots\sum_{u_2\in A^{k_{n-1}}}h_{\overline{p}}(u_1)\cdots h_{\overline{p}}(u_{n_{-1}})\cdot\sum_{u_n\in A^{k_n}}h(u_n)\\ &= \mu_{\overline{p}}(wA^{\omega})\cdot\sum_{u_1\in A^{k_1}}\cdots\sum_{u_2\in A^{k_{n-1}}}h_{\overline{p}}(u_1)\cdots h_{\overline{p}}(u_{n_{-1}})\cdot\mu_{\overline{p}}\left(A^{k_n}A^{\omega}\right)\\ &= \mu_{\overline{p}}(wA^{\omega})\cdot\sum_{u_1\in A^{k_1}}\cdots\sum_{u_2\in A^{k_{n-1}}}h_{\overline{p}}(u_1)\cdots h_{\overline{p}}(u_{n_{-1}})\cdot 1\\ &\ \ \vdots\\ &= \mu_{\overline{p}}(\langle w\rangle).\qquad\qquad\text{(notemos que } A^{k_n}A^{\omega}=A^{\omega}).\ \square\end{aligned}$$

Lema 2.13 *Para toda medida ν en $\mathbf{2}^{\omega}$ y todo abierto $\mathcal{V}$ en A^{ω} :*

$$\left(\mu_{\overline{p}}\times\nu\right)(\{(\mathbf{x},\mathbf{y})\mid \mathbf{x}/\mathbf{y}\in\mathcal{V}\})=\mu_{\overline{p}}(\mathcal{V}).$$

Prueba. Por el teorema de Fubini, se tiene que

$$\begin{aligned}\left(\mu_{\overline{p}}\times\nu\right)(\{(\mathbf{x},\mathbf{y})\mid \mathbf{x}/\mathbf{y}\in\mathcal{V}\}) &= \int\chi_{\{(\mathbf{x},\mathbf{y})\mid\mathbf{x}/\mathbf{y}\in\mathcal{V}\}}d\left(\mu_{\overline{p}}\times\nu\right)\\ &= \int\int\chi_{\{\mathbf{x}\in A^{\omega}\mid\mathbf{x}/\mathbf{y}\in\mathcal{V}\}}d\mu_{\overline{p}}(\mathbf{x})\,d\nu(\mathbf{y})\\ &= \int\mu_{\overline{p}}(\{\mathbf{x}\in A^{\omega}\mid \mathbf{x}/\mathbf{y}\in\mathcal{V}\})\,d\nu(\mathbf{y}).\end{aligned}\tag{2.3}$$

Dado que $\nu\{\mathbf{y} \in \mathbf{2}^\omega \mid \mathbf{y} \text{ contiene finitos ceros}\} = 0$, en (2.3) basta integrar sobre el conjunto de sucesiones de $\mathbf{2}^\omega$ que contengan infinitos unos. Así, por el lema 2.12, se tiene que

$$\int \mu_{\overline{p}}(\{\mathbf{x} \in A^\omega \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}\})\, d\nu(\mathbf{y}) = \int \mu_{\overline{p}}(\mathcal{V})\, d\nu(\mathbf{y}) = \mu_{\overline{p}}(\mathcal{V}). \tag{2.4}$$

De (2.3) y (2.4), se sigue lo pedido. □

Lema 2.14 *Sea $S \subseteq A \times \mathbb{N}^*$ r.e.. Entonces existe $T \subseteq A^* \times \mathbf{2}^* \times \mathbb{N}$ r.e. tal que para todo m :*

$$\{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}/\mathbf{y} \in S_m A^\omega\} = \bigcup\nolimits_{(u,v)\in T_m} uA^\omega \times v\mathbf{2}^\omega.$$

Prueba. Dado $v \in \mathbf{2}^*$, sea $|v|_1 = \#(\{k \leq |v| \mid v_k = 1\})$ el número de unos en v. Definamos una función $/^* : A^* \times \mathbf{2}^* \to A^*$ del siguiente modo. Dados $u \in A^*, v \in \mathbf{2}^*$: si $|v|_1 \geq 1$ y $|v| \leq |u|$, $u/^*v$ es la única cadena $w \in A^*$ de longitud $|v|_1$ tal que

$$w_k = u_i \quad \text{sii} \quad i \text{ es el índice del } k\text{-ésimo 1 en } v.$$

En caso contrario, $u/^*v = \lambda$. Es claro que $/^*$ es una función total recursiva y para cualquier $w \in A^*$ se tiene que $B_w = \{(u, v) \mid u/^*v = w\}$ es un subconjunto recursivo de $A^* \times \mathbf{2}^*$ tal que

$$\{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}/\mathbf{y} \in \langle w\rangle\} = \bigcup\nolimits_{(u,v)\in B_w} uA^\omega \times v\mathbf{2}^\omega.$$

Sea $T = \{(u, v, m) \mid (u/^*v, m) \in S\}$. Como S es r.e. y $/^*$ es recursiva, T es r.e.. Además,

$$\bigcup\nolimits_{w\in S_m} \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}/\mathbf{y} \in \langle w\rangle\} = \bigcup\nolimits_{w\in S_m} \bigcup\nolimits_{(u,v)\in B_w} \langle u\rangle \times \langle v\rangle = \bigcup\nolimits_{(u,v)\in T_m} \langle u\rangle \times \langle v\rangle,$$

dado que $\bigcup_{w\in S_m} B_w = T_m$. □

Nota. Sean μ, ν medidas computables en A^ω y en $\mathbf{2}^\omega$, respectivamente. En la sección anterior, introducimos los tests secuenciales como subconjuntos de A^ω, pero la definición 2.5 se puede generalizar fácilmente al espacio $A^\omega \times 2^\omega$ y a la medida producto $\mu \times \nu$. En especial, la condición (3) de dicha definición se modifica exigiendo que si $(u, v) \in T_m$, entonces $|u|, |v| > m$, donde T denotaría el subconjunto r.e. de $A^* \times \mathbf{2}^* \times \mathbb{N}$ asociado al $(\mu \times \nu)$-test. Ahora, podemos entonces enunciar la consecuencia más útil de los lemas anteriores.

Lema 2.15 *Sean $\overline{p} = (p_1, \ldots, p_Q)$ una Q-tupla de reales computables en $(0,1)$ y ν una medida computable en $\mathbf{2}^\omega$. Si $\mathcal{N} = \bigcap_m \mathcal{V}_m$ es un $\mu_{\overline{p}}$-test secuencial en A^ω, entonces*

$$\mathcal{T} = \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}/\mathbf{y} \in \mathcal{N}\}$$

es un $\left(\mu_{\overline{p}} \times \nu\right)$-test secuencial.

Prueba. Sea $\mathcal{O}_m := \{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}/\mathbf{y} \in \mathcal{V}_m\}$. Luego,

$$\mathcal{T} = \left\{(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}/\mathbf{y} \in \bigcap\nolimits_m \mathcal{V}_m\right\} = \bigcap\nolimits_m \mathcal{O}_m \qquad \text{y} \qquad \mathcal{O}_{m+1} \subseteq \mathcal{O}_m.$$

Por el lema 2.14, existe $T \subseteq A^* \times \mathbf{2}^* \times \mathbb{N}$ r.e. tal que para todo $m : \mathcal{O}_m = \bigcup_{(u,v)\in T_m} \langle u \rangle \times \langle v \rangle$. Dado que $\mathcal{V}_m$ es abierto en A^ω, por el lema 2.13 se sigue que

$$\left(\mu_{\overline{p}} \times \nu\right)(\mathcal{O}_m) = \mu_{\overline{p}}(\mathcal{V}_m) \leq \frac{Q^{-(m+1)}}{Q-1}.$$

Notemos que, de la prueba del lema 2.14, se puede concluir que si $(u, v, m) \in T$, entonces $|u|, |v| \geq |v|_1 = |w| > m$, donde $w = u/^*v \in V_m$. Podemos concluir que $\mathcal{T}$ es un test secuencial con respecto a $\mu_{\overline{p}} \times \nu$. $\square$

El último paso previo a la demostración del teorema 2.11 requiere de una versión del teorema de Fubini para tests secuenciales recursivos. Para ello modificamos adecuadamente la prueba del teorema 14.2 en [Ox80, 53].

Teorema 2.16 (Fubini) *Sean μ, ν medidas computables en A^ω y en $\mathbf{2}^\omega$, respectivamente. Si $\mathcal{T} \subseteq A^\omega \times \mathbf{2}^\omega$ es un $(\mu \times \nu)$-test secuencial con respecto a $\mu \times \nu$, entonces*

$$\{\mathbf{x} \in A^\omega \mid \nu(\mathcal{T}_\mathbf{x}) > 0\}, \qquad \textit{donde } \mathcal{T}_\mathbf{x} = \{\mathbf{y} \mid (\mathbf{x}, \mathbf{y}) \in \mathcal{T}\},$$

está contenido en un μ-test secuencial.

Prueba. Sea $\mathcal{T} = \bigcap_m \mathcal{O}_m \subseteq A^\omega \times \mathbf{2}^\omega$ un $(\mu \times \nu)$-test secuencial. Luego, existe $T \subseteq A^* \times \mathbf{2}^* \times \mathbb{N}$ r.e. que cumple las condiciones de la definición 2.5. En particular, para todo $m : \mathcal{O}_m = \bigcup_{(u,v)\in T_m} \langle u \rangle \times \langle v \rangle$ y si $(u, v) \in T_m$, entonces $|u|, |v| > m$.

Fijemos m y hagamos $T_{>m} = \{(u,v) \in T_k \mid k > m\}$. Notemos que $T_{>m}$ es un subconjunto r.e. de $A^* \times \mathbf{2}^*$ que se puede escribir en la forma $T_{>m} = \{(u_i, v_i)\}_{i=1}^{\infty}$. Luego,

$$\bigcup\nolimits_{k>m} \mathcal{O}_k = \bigcup\nolimits_{(u,v)\in T_{>m}} \langle u\rangle \times \langle v\rangle = \bigcup\nolimits_{i=1}^{\infty} \langle u_i\rangle \times \langle v_i\rangle .$$

Como para todo i existe $k > m$ tal que $(u_i, v_i) \in T_k$, tenemos que $|u_i|, |v_i| > k > m$.
Ahora, sea $(\mathbf{x}, \mathbf{y}) \in \mathcal{T}$. Como $\mathcal{T} \subseteq \mathcal{O}_k$, para todo $k > m$, existe i_k tal que $(\mathbf{x}, \mathbf{y}) \in \langle u_{i_k}\rangle \times \langle v_{i_k}\rangle$. Así, existen infinitos índices i tales que $(\mathbf{x}, \mathbf{y}) \in \langle u_i\rangle \times \langle v_i\rangle$. Esto es, *la sucesión de básicos* $\{\langle u_i\rangle \times \langle v_i\rangle\}$ *cubre infinitas veces a* $\mathcal{T}$. Definamos $f_n : A^\omega \to [0,\infty)$ por

$$f_0 = 0 \qquad \text{y} \qquad f_n = \sum\nolimits_{i=1}^{n} \nu\left(\langle v_i\rangle\right) \cdot \chi_{\langle u_i\rangle}, \quad \text{para } n \geq 1.$$

Notemos que $\{f_n\}$ es una sucesión *creciente* de funciones escalón y que para todo n :

$$\begin{array}{rcccl}
\displaystyle\int_{A^\omega} f_n \, d\mu & = & \displaystyle\sum\nolimits_{i=1}^{n} \int_{A^\omega} \nu\left(\langle v_i\rangle\right) \cdot \chi_{\langle u_i\rangle} d\mu & = & \displaystyle\sum\nolimits_{i=1}^{n} \mu\left(\langle u_i\rangle\right) \cdot \nu\left(\langle v_i\rangle\right) \\
& \leq & \mu \times \nu\left(\displaystyle\bigcup\nolimits_{k>m} \mathcal{O}_k\right) & \leq & \displaystyle\sum\nolimits_{k>m} (\mu \times \nu)\left(\mathcal{O}_k\right) \\
& \leq & \displaystyle\sum\nolimits_{k>m} \frac{Q^{-(k+1)}}{Q-1} & \leq & \displaystyle\frac{Q^{-(m+1)}}{(Q-1)}.
\end{array}$$

Para $u \in A^*$ fijo, sea $E_u = \{w \mid u \leq_p w\}$. Es obvio que χ_{E_u} es una función recursiva.
Como ν es una medida computable y $\{(u_i, v_i)\}$ es un conjunto r.e. de $A^* \times \mathbf{2}^*$, tenemos que $f_n^*(w) = \sum_{i=1}^{n} \nu\left(\langle v_i\rangle\right) \cdot \chi_{E_{u_i}}(w)$ es una función computable y que $F_> = \{(w,r) \mid f_n^*(w) > r\}$ es un subconjunto r.e. de $A^* \times \mathbb{Q}$. Por tanto,

$$V_m = \{w \mid (\exists n)\ (f_n^*(w) > 1)\}$$

es un subconjunto r.e. de A^* (que depende implícitamente de m). Como $T_{>m+1} \subseteq T_{>m}$, es claro que $V_{m+1} \subseteq V_m$. Si $w \in V_m$, existe n tal que $u_i \leq_p w$, para algún $i \leq n$. Así, $|w| \geq |u_i| > m$. Notemos que $\mathcal{V}_m = V_m A^\omega = \{\mathbf{x} \mid (\exists k)\ (f_k(\mathbf{x}) > 1)\}$.

Afirmamos que $\{\mathbf{x} \mid \nu(\mathcal{T}_{\mathbf{x}}) > 0\} \subseteq \mathcal{V}_m$. En efecto, sea $\mathbf{x} \in A^\omega$ tal que $\nu(\mathcal{T}_{\mathbf{x}}) > 0$. A fortiori, existe $\mathbf{y}_0 \in \mathbf{2}^\omega$ tal que $(\mathbf{x}, \mathbf{y}_0) \in \mathcal{T}$. Luego, existen infinitos índices i tales que $(\mathbf{x}, \mathbf{y}_0) \in \langle u_i\rangle \times \langle v_i\rangle$.

Sea $I_{\mathbf{x}} = \{i \mid (\exists \mathbf{y})\,[(\mathbf{x},\mathbf{y}) \in \langle u_i\rangle \times \langle v_i\rangle]\}$. Así, para cualquier $\mathbf{y} \in \mathcal{T}_{\mathbf{x}}$ existen infinitos índices $i \in I_{\mathbf{x}}$ tales que $(\mathbf{x},\mathbf{y}) \in \langle u_i\rangle \times \langle v_i\rangle$. Esto es, la sucesión de cilindros $\{\langle v_i\rangle\}_{i\in I_{\mathbf{x}}}$ cubre a $\mathcal{T}_{\mathbf{x}}$ infinitas veces. Como $\nu(\mathcal{T}_{\mathbf{x}}) > 0$, la serie $\sum_{i\in I_{\mathbf{x}}} \nu(\langle v_i\rangle)$ debe diverger; pues, en caso contrario, podriamos cubrir $\mathcal{T}_{\mathbf{x}}$ con abiertos de ν-medida arbitrariamente pequeña. Por tanto,

$$\lim_{k\to\infty} f_k(\mathbf{x}) = \lim_{k\to\infty} \sum_{i\leq k, i\in I_{\mathbf{x}}} \nu(\langle v_i\rangle) = \sum_{i\in I_{\mathbf{x}}} \nu(\langle v_i\rangle) = +\infty.$$

Luego, existe k tal que $f_k(\mathbf{x}) > 1$; esto es, $\mathbf{x} \in \mathcal{V}_m$.
Por último, hagamos $\mathcal{G}_n = \{\mathbf{x} \mid (\exists k \leq n)\ (f_k(\mathbf{x}) > 1)\}$. Es claro que $\mathcal{G}_n \subseteq \mathcal{G}_{n+1}$ y $\mathcal{V}_m = \bigcup_n \mathcal{G}_n$. Dado que $k \leq n$ implica $f_k \leq f_n$, tenemos que para todo $\mathbf{x} \in \mathcal{G}_n$ se cumple $1 < f_n(\mathbf{x})$. Así,

$$\mu(\mathcal{G}_n) = \int_{\mathcal{G}_n} 1\, d\mu \leq \int_{\mathcal{G}_n} f_n\, d\mu \leq \int_{A^\omega} f_n\, d\mu \leq \frac{Q^{-(m+1)}}{Q-1}.$$

Por tanto,

$$\mu(\mathcal{V}_m) = \lim_{n\to\infty} \mu(\mathcal{G}_n) \leq \frac{Q^{-(m+1)}}{Q-1}.$$

Por todo lo anterior, podemos concluir que $\mathcal{N} = \bigcap_m \mathcal{V}_m$ es el test secuencial pedido. □

Prueba del principio de homogeneidad. Sea $\mathcal{U}$ un $\mu_{\overline{p}}$-test secuencial universal. Dado que $\left(\mathcal{R}\left(\mu_{\overline{p}}\right)\right)^c = \mathcal{U}$, tenemos que $\left(\mathcal{R}\left(\mu_{\overline{p}}\right)\right)^c$ es un $\mu_{\overline{p}}$-test secuencial. Luego, por el lema 2.15,

$$\mathcal{T} = \left\{(\mathbf{x},\mathbf{y}) \mid \mathbf{x}/\mathbf{y} \notin \mathcal{R}\left(\mu_{\overline{p}}\right)\right\} = \{(\mathbf{x},\mathbf{y}) \mid \mathbf{x}/\mathbf{y} \in \mathcal{U}\}$$

es un $\left(\mu_{\overline{p}} \times \nu\right)$-test secuencial. Así, por el teorema 2.16, existe un $\mu_{\overline{p}}$-test secuencial $\mathcal{N}$ tal que

$$\{\mathbf{x} \in A^\omega \mid \nu(\mathcal{T}_{\mathbf{x}}) > 0\} \subseteq \mathcal{N}.$$

Ahora, si $\mathbf{x}$ es una sucesión aleatoria respecto a $\mu_{\overline{p}}$, se sigue que $\mathbf{x} \notin \mathcal{N}$. Luego, para dicha $\mathbf{x}$:

$$\nu\left(\left\{\mathbf{y} \in \mathbf{2}^\omega \mid \mathbf{x}/\mathbf{y} \notin \mathcal{R}\left(\mu_{\overline{p}}\right)\right\}\right) = \nu\left(\{\mathbf{y} \mid (\mathbf{x},\mathbf{y}) \in \mathcal{T}\}\right) = \nu(\mathcal{T}_{\mathbf{x}}) = 0.$$

Lo cual implica que $\nu\left(\left\{\mathbf{y} \mid \mathbf{x}/\mathbf{y} \in \mathcal{R}\left(\mu_{\overline{p}}\right)\right\}\right) = 1$. □

Mirando restrospectivamente vemos que, al menos en un sentido cuantitativo, las intuiciones de von Mises se pueden salvar: si identificamos provisionalmente los colectivos con las sucesiones aleatorias (en el sentido de Martin-Löf), entonces el conjunto de subsucesiones de un colectivo que no son a su vez colectivos es extremadamente pequeño. Recíprocamente, podemos decir que la definición de Martin-Löf captura al menos algunas de las intenciones de von Mises.

2.4 Complejidad algorítmica

Uno de los desarrollos más importantes estimulado por el intento de von Mises de definir colectivos es la teoría de la complejidad de Kolmogorov, junto con su propuesta de noción de aleatoriedad para cadenas y sucesiones. La intuición detrás de la definición de la complejidad de una cadena finita se puede enunciar de varias formas. Uno podría decir que si una secuencia exhibe una regularidad, se puede escribir como la salida de una regla simple aplicada a una entrada más sencilla. Otra forma de expresar esta idea es decir que una cadena que exhiba una regularidad se puede *codificar* eficientemente, usando la regla para producir la secuencia a partir de su código. Tomando *reglas* como funciones parciales recursivas de A^* en A^*, podemos definir la *complejidad* de una cadena w con respecto a una regla φ como la longitud de la menor entrada p tal que $\varphi(p) = w$. Para poder tener en cuenta todas las posibles reglas, bastará usar una máquina *universal*. Se obtienen diferentes conceptos de complejidad al imponer restricciones adicionales a las funciones. Bosquejamos a continuación la complejidad algorítmica de Kolmogorov, donde no se impone ninguna restricción.

Definimos un computador como una función p.r. $\varphi : A^* \times A^* \xrightarrow{o} A^*$. Esto es, visualizamos un computador como una función p.r. que recibe `programa` + `datos` como entradas y que luego puede imprimir otra cadena como salida.

Definición 2.17 *La* complejidad algorítmica de Kolmogorov $K_\varphi(w)$ *de* w *con respecto al computador* φ *se define por*

$$K_\varphi(w) = \begin{cases} \infty, & \text{si no existe } p \text{ tal que } \varphi(p,\lambda) = w, \\ \min\{|p| : \varphi(p,\lambda) = w\}, & \text{en caso contrario.} \end{cases}$$

En otras palabras, $K_\varphi(w)$ es la longitud del programa p más corto que codifica (sin dato alguno)

el objeto w con respecto al computador φ.

Diremos que un computador ψ es universal, si para todo computador φ, existe una constante c (que depende de ambos computadores) con la siguiente propiedad: si $\varphi(p,d)\downarrow$, entonces existe $q \in A^*$ tal que

$$\psi(q,d) = \varphi(p,d) \qquad \text{y} \qquad |q| \leq |p| + c.$$

Finalmente, fijamos un computador universal ψ y definimos $K(w) = K_\psi(w)$ como la complejidad de Kolmogorov de w.

Kolmogorov desarrolló la noción de complejidad para obtener aproximaciones finitas a los colectivos y propuso definir las sucesiones aleatorias como aquellas que poseen segmentos iniciales de máxima complejidad. Esto es, una sucesión $\mathbf{x} \in A^\omega$ se dice Kolmogorov-irregular (incomprimible) si existe una constante c tal que para todo $n : K(\mathbf{x}(n)) \geq n - c$. Desafortunadamente, Martin-Löf mostró que ninguna sucesión es irregular en este sentido (ver sección 6.1 en [Ca02]). Chaitin y Levin observaron que la idea de irregularidad era consistente si se restringía la clase de algoritmos considerados. Seguiremos la propuesta de Chaitin.

Decimos que un computador $C : A^* \times A^* \xrightarrow{o} A^*$ es un computador de Chaitin si para todo $v \in A^*$ el conjunto $\{u \in A^* \mid C(u,v)\downarrow\}$ es *libre de prefijos* (ver pág. 1); esto es, el dominio de la función p.r. $C_v : A^* \xrightarrow{o} A^*$, dada por $C_v(u) \simeq C(u,v)$, es libre de prefijos. Análogamente, diremos que un computador de Chaitin U es universal, si para todo computador de Chaitin C, existe una constante c (que depende de ambos computadores) tal que si $C(u,v)\downarrow$, entonces existe x tal que $U(x,v) = C(u,v)$ y $|x| \leq |u| + c$.

A partir de la enumeración *efectiva* $\{\varphi_e^{(2)}\}_{e\in A^*}$, es posible construir una función universal $F : (A^*)^3 \xrightarrow{o} A^*$ que simula computadores de Chaitin (ver teorema 2.1.2 en [Su03, 16]); esto es, F es una función p.r. tal que

(a) para todo $e \in A^*$, el computador $F_e : A^* \times A^* \xrightarrow{o} A^*$, dado por $F_e(u,v) \simeq F(e,u,v)$, es un computador de Chaitin; y

(b) si $\varphi_e^{(2)} : A^* \times A^* \xrightarrow{o} A^*$ es un computador de Chaitin, entonces $\varphi_e^{(2)}(u,v) \simeq F(e,u,v)$.

Ahora, por el *s-m-n* teorema, existe una función total recursiva inyectiva $\sigma : A^* \to A^*$ tal que para todo $e \in A^*$:

$$\varphi_{\sigma(e)}^{(2)}(u,v) = F(e,u,v), \qquad \forall u,v \in A^*.$$

Así, obtenemos una enumeración $\{\varphi^{(2)}_{\sigma(e)}\}_{e\in A^*}$ de todos los computadores de Chaitin tal que

$$\text{si } \varphi^{(2)}_e \text{ es un computador de Chaitin, entonces} \quad \varphi^{(2)}_e \simeq \varphi^{(2)}_{\sigma(e)}. \tag{2.5}$$

Además, podemos definir un computador de Chaitin universal U_σ por

$$U_\sigma\left(a_1^i a_2 u, v\right) = \varphi^{(2)}_{\sigma(\mathsf{string}(i))}\left(u, v\right), \qquad \text{donde } i \in \mathbb{N}, a_1, a_2 \in A \text{ y } u, v \in A^*.$$

En adelante, fijaremos un computador universal de Chaitin U estándar (no necesariamente U_σ) para medir, de forma análoga a la complejidad de Kolmogorov, la *complejidad autolimitante*.

Definición 2.18 *La* complejidad de Chaitin *asociada con el computador de Chaitin C es la función parcial $H_C : A^* \xrightarrow{o} \mathbb{N}$ dada por*

$$H_C(w) = \begin{cases} \infty, & \text{si no existe } u \text{ tal que } C(u,\lambda) = w, \\ \min\{|u| \mid C(u,\lambda) = w\}, & \text{en caso contrario.} \end{cases}$$

Cuando $C = U$, escribiremos $H(w) = H_U(w)$.

Ahora, fijemos $v \in A^*$. Dado w, consideremos el computador

$$C(u,v) = \begin{cases} w, & \text{si } u = \lambda, \\ \uparrow, & \text{si } u \neq \lambda. \end{cases}$$

Como U es universal, existe p tal que $U(p,v) = C(\lambda,v) = w$. Por tanto, $U_v : A^* \xrightarrow{o} A^*$ *es sobreyectiva, para todo $v \in A^*$*. Como $\lambda \notin \mathrm{dom}(U_\lambda)$ y U_λ es sobreyectiva, entonces para todo $w \in A^*$ existe al menos un programa $u \neq \lambda$ tal que $U(u,\lambda) = w$. Definimos el programa canónico de w como $w^* = \min\{u \in A^* \mid U(u,\lambda) = w\}$, donde el mínimo se toma de acuerdo al orden lexicográfico de A^*. Es obvio que $H(w) = |w^*|$.

Análogamente al caso de K, tenemos que para todo computador de Chaitin C existe una constante c (que depende efectivamente de C) tal que para todo $w \in A^*$:

$$H(w) \leq H_C(w) + c. \qquad \textbf{(Teorema de Invarianza)}$$

Dado que la complejidad H se definió restringiendo la clase de computadores a aquellos que tengan dominio libre de prefijos, necesitamos algún criterio para decidir si cierta tarea se puede ejecutar mediante un computador de Chaitin. Inicialmente, enunciamos el siguiente análogo de la clásica **desigualdad de Kraft** para computadores de Chaitin.

Lema 2.19 (a) *Si C es un computador de Chaitin, entonces* $\sum_{C_\lambda(u)\downarrow} Q^{-|u|} \leq 1$.

(b) $\sum_{w\in A^*} Q^{-H(w)} \leq 1$.

Prueba. (a) Como $\mathrm{dom}\,(C_\lambda)$ es libre de prefijos, la familia de cilindros $\{\langle u\rangle \mid C_\lambda(u)\downarrow\}$ es mutuamente disjunta. Si consideramos la medida de Lebesgue λ_Q en A^ω, tenemos que

$$\sum_{C_\lambda(u)\downarrow} Q^{-|u|} = \sum_{C_\lambda(u)\downarrow} \lambda_Q(\langle u\rangle) = \lambda_Q\Big(\bigcup_{C_\lambda(u)\downarrow} uA^\omega\Big) \leq 1.$$

(b) Por (a), $\sum_{w\in A^*} Q^{-H(w)} \leq \sum_{U_\lambda(u)\downarrow} Q^{-|u|} \leq 1$. □

El recíproco de la parte (a) del lema 2.19 se conoce como el *Teorema de Kraft-Chaitin* y es una herramienta muy importante para la construcción de computadores de Chaitin. Su prueba, bastante técnica, se puede consultar en [Ca02, 51-59] o [Su03, 78-82].

Teorema de Kraft-Chaitin *Si S es un subconjunto r.e. de $A^*\times\mathbb{N}$ tal que*

$$\sum_{(w,n)\in S} Q^{-n} \leq 1, \qquad \textit{entonces}$$

(a) *podemos construir un computador de Chaitin C tal que para todo $(w,n)\in S$ existe $u\in A^*$ tal que $|u|=n$ y $C(u,\lambda)=w$.*

(b) *existe efectivamente una constante c tal que para todo $(w,n)\in S : H(w)\leq n+c$.*

Finalizamos esta sección con un resultado sencillo.

Lema 2.20 *$\{(w,m) \mid H(w)\leq m\}$ es un subconjunto r.e. de $A^*\times\mathbb{N}$.*

Prueba. Basta notar que

$$H(w)\leq m \Leftrightarrow (\exists n)\,(\exists t)\,[|\mathsf{string}\,(n)|\leq m \ \wedge\ U(\mathsf{string}\,(n),\lambda)=w \text{ en a lo sumo } t \text{ pasos}].$$

□

2.5 Aleatoriedad y complejidad

Los primeros intentos de caracterizar las sucesiones aleatorias en términos de la complejidad de los segmentos iniciales se encontraron con el siguiente obstáculo:

Teorema 2.21 (Martin-Löf) *Si $f : \mathbb{N} \to \mathbb{N}$ es una función recursiva tal que $\sum Q^{-f(n)} = \infty$, entonces para cualquier sucesión $\mathbf{x} \in A^\omega$ y para infinitos valores de n :*

$$K(\mathbf{x}(n)) < n - f(n).$$

Para una prueba, ver [Ca02, 157] o [Li93, 136]. En particular, el teorema se satisface para $f(n) = \lfloor \log_Q n \rfloor$. Por consiguiente, la complejidad de Kolmogorov de cualquier sucesión oscila infinitas veces por debajo de $n - \log_Q n$, esto es, bastante por debajo de su propia longitud. Este callejón sin salida llevó a Martin-Löf a formular su propia noción de aleatoriedad (sección 2.2). Sin embargo, es posible caracterizar la aleatoriedad en términos de la complejidad autolimitante.

Definición 2.22 *Decimos que $\mathbf{x} \in A^\omega$ es* irregular *respecto a μ si*

$$(\exists m)\,(\forall n)\ (\ H\,(\mathbf{x}\,(n)) > -\log_Q\,(\mu\,[\mathbf{x}\,(n)\,A^\omega]) - m\ ).$$

Hemos decidido dar el nombre de sucesiones *irregulares* a las sucesiones que se conocen como *Chaitin-aleatorias*. La ventaja informal de esta terminología es que, hasta el momento, hemos usado la aleatoriedad en un sentido *estocástico*, mientras que la intuición que subyace a la noción de Kolmogorov-Chaitin es de naturaleza *combinatoria*, más que estocástica. Por supuesto, mostraremos que ambas nociones coinciden.

Teorema 2.23 *Sean μ una medida computable en A^ω y $\mathbf{x} \in A^\omega$. Entonces*

$$\mathbf{x} \in \mathcal{R}\,(\mu) \quad \textit{si y sólo si} \quad \mathbf{x} \textit{ es irregular con respecto a } \mu.$$

Prueba. ($\Rightarrow$) Veamos que

$$\mathcal{N} = \left\{\mathbf{x} \in A^\omega \mid (\forall m)\,(\exists n)\ [\ H\,(\mathbf{x}\,(n)) < -\log_Q\,[\mu\,(\mathbf{x}\,(n)\,A^\omega)] - (m+2)\ ]\right\}$$

es un μ-test secuencial. Para ello, definamos $S = \left\{(u,m) \mid H(u) < -\log_Q[\mu(\langle u\rangle)] - (m+2)\right\}$. Notemos que $(u,m) \in S$ sii $\mu(\langle u\rangle) < Q^{-H(u)} \cdot Q^{-(m+2)}$ sii existen $n,k,t \in \mathbb{N}$ tales que

$$U(\mathsf{string}(n),\lambda) = u \text{ en a lo sumo } t \text{ pasos } \wedge\ g(u,k) + 2^{-k} < Q^{-|\mathsf{string}(n)|} \cdot Q^{-(m+2)}$$

(donde $g : A^* \times \mathbb{N} \to \mathbb{Q}$ es una función recursiva tal que $|\mu(\langle w\rangle) - g(w,k)| \leq 2^{-k}$).

Así, tanto S como $V = \{(w,m) \mid (\exists u \leq_p w)(|w| > m \ \wedge\ (u,m) \in S)\}$ son subconjuntos r.e. de $A^* \times \mathbb{N}$. Es claro que $\left\{\mathbf{x} \mid (\exists n)\,[H(\mathbf{x}(n)) < -\log_Q(\mu[\mathbf{x}(n)A^\omega]) - (m+2)]\right\} = V_m A^\omega = \mathcal{V}_m$ y que $\mathcal{V}_{m+1} \subseteq \mathcal{V}_m$. Si $u \leq_p w$, entonces $\langle w\rangle \subseteq \langle u\rangle$. Por tanto, se tiene que

$$\mu(\bigcup\nolimits_{w\in V_m}\langle w\rangle) \leq \mu(\bigcup\nolimits_{u\in S_m}\langle u\rangle) \leq \sum\nolimits_{u\in S_m}\mu(\langle u\rangle) \leq \sum\nolimits_{u\in S_m} Q^{-H(u)}\cdot Q^{-(m+2)}.$$

Por la parte (b) del lema 2.19, se sigue que

$$\mu(\mathcal{V}_m) \leq Q^{-(m+2)}\sum\nolimits_{w\in A^*} Q^{-H(w)} \leq Q^{-(m+2)}\cdot 1 \leq \frac{Q^{-(m+1)}}{Q-1}.$$

Luego, tenemos que $\mathcal{N} = \bigcap_m \mathcal{V}_m$ es un μ-test secuencial. Ahora, si $\mathbf{x} \in \mathcal{R}(\mu)$, entonces $\mathbf{x} \notin \mathcal{N}$. Luego, existe m_0 tal que para todo $n : H(\mathbf{x}(n)) \geq -\log_Q[\mu(\mathbf{x}(n)A^\omega)] - (m_0+2)$. Si tomamos $m = m_0 + 3$, podemos concluir que $\mathbf{x}$ es irregular con respecto a μ.

($\Leftarrow$) Primero, notemos que si $\alpha \in \mathbb{R}_c$, entonces podemos hallar efectivamente un $n \in \mathbb{Z}$ tal que $n \leq \alpha \leq n+2$. Este entero lo denotaremos $\llcorner\alpha\lrcorner$. Ahora, fijemos una constante $c_0 \geq 2$ tal que $\sum_{m=0}^{\infty} Q^{-\frac{m}{2}} \leq Q^{c_0}$. Sea $\mathcal{U} = \bigcap_m \mathcal{U}_m$ un μ-test secuencial universal. Podemos suponer que existe un conjunto r.e. $U \subseteq A^* \times \mathbb{N}$ tal que cada sección U_m es *libre de prefijos* y $\mathcal{U}_m = U_m A^\omega$ (ver lema 3.1.15 en [Su03, 42]). Por tanto, para todo m :

$$\sum\nolimits_{w\in U_m}\mu(\langle w\rangle) = \mu(\bigcup\nolimits_{w\in U_m}\langle w\rangle) = \mu(\mathcal{U}_m) \leq \frac{Q^{-(m+1)}}{Q-1}.$$

Ahora, definimos la función recursiva $\rho : A^* \times \mathbb{N} \to \mathbb{N}$ dada por

$$\rho(w,m) = \llcorner -\log_Q(\mu(\langle w\rangle)) - \tfrac{m}{2} - \log_Q(Q-1) + c_0 + 1\lrcorner.$$

ρ está bien definida, pues, como μ es computable, podemos hallar efectivamente un código de aproximación para $-\log_Q(\mu(\langle w\rangle)) - \frac{m}{2} - \log_Q(Q-1) + c_0 + 1 \in \mathbb{R}_c$. Notemos que

$$\rho(w,m) \leq -\log_Q(\mu(\langle w\rangle)) - \tfrac{m}{2} - \log_Q(Q-1) + c_0 + 1 \leq \rho(w,m) + 2.$$

Como U es r.e. y ρ es recursiva, entonces $S = \{(w, \rho(w,m)) \mid m \in \mathbb{N} \wedge w \in U_m\}$ es un subconjunto r.e. de $A^* \times \mathbb{N}$ tal que

$$\begin{aligned}\sum_{(w,n)\in S} Q^{-n} &= \sum_{m=0}^{\infty} \sum_{w\in U_m} Q^{-\rho(w,m)} \leq Q^{-c_0+1} \cdot (Q-1) \sum_{m=0}^{\infty} Q^{\frac{m}{2}} \cdot \sum_{w\in U_m} \mu(\langle w\rangle) \\ &\leq Q^{-c_0+1} \cdot (Q-1) \sum_{m=0}^{\infty} Q^{\frac{m}{2}} \frac{Q^{-(m+1)}}{Q-1} = Q^{-c_0} \sum_{m=0}^{\infty} Q^{-\frac{m}{2}} \leq 1.\end{aligned}$$

Por el teorema de Kraft-Chaitin, existe una constante c_1 tal que para todo $w \in U_m$:

$$H(w) \leq \rho(w,m) + c_1 \leq -\log_Q(\mu(\langle w\rangle)) - \tfrac{m}{2} + c, \qquad \text{donde } c = c_1 + c_0 + 1 - \log_Q(Q-1).$$

Ahora, si $\mathbf{x} \notin \mathcal{R}(\mu)$, entonces $\mathbf{x} \in \mathcal{U}$. Entonces, $(\forall m)(\exists n)(\, \mathbf{x}(n) \in U_m \,)$. Luego,

$$(\forall m)(\exists n)\ (\ H(\mathbf{x}(n)) \leq -\log_Q(\mu[\mathbf{x}(n)\, A^\omega]) - \tfrac{m}{2} + c\ ).$$

Por tanto, obtenemos la implicación

$$(\exists m)(\forall n)\ (\ H(\mathbf{x}(n)) > -\log_Q(\mu[\mathbf{x}(n)\, A^\omega]) - \tfrac{m}{2} + c\ ) \quad \Rightarrow \quad \mathbf{x} \in \mathcal{R}(\mu).$$

Pero el antecedente es equivalente a $(\exists m)(\forall n)\ (\ H(\mathbf{x}(n)) > -\log_Q(\mu[\mathbf{x}(n)\, A^\omega]) - m\ )$. Así, podemos concluir que si $\mathbf{x}$ es irregular con respecto a μ, entonces $\mathbf{x} \in \mathcal{R}(\mu)$. $\square$

Notemos que para la medida de Lebesgue λ_Q en A^ω, tenemos que $\lambda_Q([\mathbf{x}(n)\, A^\omega]) = Q^{-n}$. Así obtenemos, como caso particular del teorema 2.23, el **teorema de Chaitin-Schnorr**:

$$\mathbf{x} \in \mathcal{R}(\lambda_Q) \quad \text{si y sólo si} \quad (\exists m)\ (\forall n)\ (\ H(\mathbf{x}(n)) > n - m\ )$$

(ver [Ca02, 179] o [Su03, 46]).

Capítulo 3

Incompletez Sintáctica

La teoría algorítmica de la información se ha convertido en un área de estudio bastante popular. Esto se debe en parte a la extendida divulgación de los fámosos resultados de incompletez de Chaitin [Ra98, 585]. De hecho, hay dos resultados enteramente diferentes de Chaitin: el primero se refiere al límite finito de la demostrabilidad de la complejidad (sección 3.2), mientras que el segundo se relaciona con los reales aleatorios, la probabilidad de parada Ω y la insolubilidad del décimo problema de Hilbert (sección 3.4).

El propósito de Chaitin ha sido aplicar ideas propias de la teoría de la información y la teoría de la probabilidad a la teoría de la recursión y a la metamatemática. En particular, ha propuesto *redefinir* el primer teorema de incompletez de Gödel al introducir *grados* de incompletez de los sistemas formales y relacionarlos al "contenido de información" (complejidad algorítmica) de dichas teorías. Además, Chaitin ha afirmado que cree haber demostrado que la aleatoriedad está presente en la matemática pura, de hecho, en ramas elementales de la teoría de números [Ch87, 160].

3.1 Un análisis computacional

El siguiente teorema de Kleene es uno de los resultados más elegantes e importantes en computabilidad. Su prueba es muy corta y sólo apela al *s-m-n* teorema. Recordemos que $\{\varphi_e^{(m)}\}_{e\in A^*}$ denota la enumeración efectiva (estándar) de todas las funciones p.r. $\varphi^{(m)} : (A^*)^m \xrightarrow{o} A^*$.

Teorema de Recursión *Sean $m \geq 1$ y $f : A^* \to A^*$ una función recursiva. Entonces existe $e \in A^*$ (llamado* punto fijo *de f) tal que*

$$\varphi_e^{(m)} \simeq \varphi_{f(e)}^{(m)}.$$

Prueba. Aplicando el *s-m-n* teorema, a la función p.r. $g : A^* \times (A^*)^m \xrightarrow{o} A^*$, dada por

$$g(u, \overline{w}) = \begin{cases} \varphi^{(m)}_{\varphi_u(u)}(\overline{w}), & \text{si } \varphi_u(u) \downarrow, \\ \uparrow, & \text{en caso contrario;} \end{cases}$$

obtenemos una función recursiva $d : A^* \to A^*$ tal que $\varphi^{(m)}_{d(u)} \simeq g(u, \cdot)$ para todo $u \in A^*$. Ahora, dada f, elijamos un índice v tal que $\varphi_v = f \circ d$. Afirmamos que $e = d(v)$ es un punto fijo para f. En efecto, como f y d son funciones totales, φ_v es una función total; por tanto, $\varphi_v(v) \downarrow$ y

$$\varphi^{(m)}_{d(v)}(\overline{w}) = g(v, \overline{w}) = \varphi^{(m)}_{\varphi_v(v)}(\overline{w}), \qquad \forall \overline{w} \in (A^*)^m.$$

Como $\varphi_v(v) = (f \circ d)(v) = f(d(v)) = f(e)$, tenemos que

$$\varphi^{(m)}_e \simeq \varphi^{(m)}_{d(v)} \simeq \varphi^{(m)}_{\varphi_v(v)} = \varphi^{(m)}_{f(e)}. \quad \square$$

Por conveniencia, fijaremos una biyección computable $\langle \cdot \rangle : A^* \times \mathbb{N} \to A^*$. Luego, por el lema 2.20, tenemos que $\{\langle w, m \rangle \mid H(w) \leq m\}$ es un conjunto Σ_1 (r.e.) de A^*, mientras que $\{\langle w, m \rangle \mid H(w) > m\}$ es un conjunto Π_1 de A^*. De hecho, podemos probar que dicho conjunto satisface una propiedad más fuerte.

Definición 3.1 (a) $S \subseteq A^*$ *es* inmune *si* S *es infinito y no contiene subconjuntos r.e. infinitos.*

(b) $S \subseteq A^*$ *es* efectivamente inmune *si existe una función recursiva* $\gamma : A^* \to \mathbb{N}$ *tal que para todo* $e \in A^*$ *si* $W_e \subseteq S$, *entonces* $\#(W_e) \leq \gamma(e)$.

Mediante una aplicación ingeniosa del teorema de recursión, obtenemos un resultado que jugará un papel fundamental en las pruebas de la siguiente sección.

Teorema 3.2 *Existe una constante* d *tal que si*

$$W_e \subseteq \{\langle w, m \rangle \mid (w, m) \in A^* \times \mathbb{N} \wedge H(w) > m\},$$

entonces para todo $\langle w, m \rangle \in W_e : m \leq H(e) + d$.

Prueba. Sea U_σ el computador de Chaitin universal definido en la sección 2.4 (pág. 26). Notemos que para todo $w \in A^* : H_{U_\sigma}(w) \leq H^{(2)}_{\varphi_{\sigma(\mathsf{string}(i))}}(w)+i+1$. Por el teorema de invarianza, existe una constante c tal que

$$H(w) \leq H_{U_\sigma}(w) + c \leq H^{(2)}_{\varphi_{\sigma(\mathsf{string}(i))}}(w) + i + (c+1), \qquad \forall i \in \mathbb{N}, \forall w \in A^*. \tag{3.1}$$

Ahora, si U es el computador de Chaitin universal que hemos fijado, definamos un computador de Chaitin C que opera sobre entradas de la forma $(a_1^n a_2 u, v)$ de acuerdo al siguiente procedimiento:

1. `compute` $U(u,v)$;
2. `si` $U(u,v)\downarrow$, `haga` $e := U(u,v)$;
3. `genere el conjunto` W_e `hasta hallar un` $\langle w, m\rangle$ `tal que`
$$m > |u| + n + (c+1);$$
4. `imprima` w.

Ahora, definamos una función p.r. $G : (A^*)^3 \xrightarrow{o} A^*$ como $G(\mathsf{string}(n), u, v) \simeq C(a_1^n a_2 u, v)$. Por el *s-m-n* teorema, existe una función recursiva inyectiva $f : A^* \to A^*$ tal que

$$\varphi^{(2)}_{f(\mathsf{string}(n))}(u,v) \simeq G(\mathsf{string}(n), u, v).$$

Por el teorema de recursión, existe $n \in \mathbb{N}$ tal que $\mathsf{string}(n)$ es un punto fijo de f; esto es,

$$\varphi^{(2)}_{\mathsf{string}(n)}(u,v) \simeq \varphi^{(2)}_{f(\mathsf{string}(n))}(u,v) \simeq C(a_1^n a_2 u, v), \qquad \forall u, v \in A^*.$$

Luego, $\varphi^{(2)}_{\mathsf{string}(n)}$ es un computador de Chaitin. Por (2.5) en la página 26, tenemos que

$$\varphi^{(2)}_{\sigma(\mathsf{string}(n))}(u,v) \simeq \varphi^{(2)}_{\mathsf{string}(n)}(u,v) \simeq C(a_1^n a_2 u, v), \qquad \forall u, v \in A^*. \tag{3.2}$$

Ahora, sea $e \in A^*$ tal que $W_e \subseteq \{\langle w, m\rangle \mid H(w) > m\}$. Como U_λ es una función sobreyectiva, existe u tal que $U(u,\lambda) = e$. Afirmamos que $\varphi^{(2)}_{\sigma(\mathsf{string}(n))}(u,\lambda)\uparrow$.
En efecto, si $\varphi^{(2)}_{\sigma(\mathsf{string}(n))}(u,\lambda)\downarrow$, sea $w = \varphi^{(2)}_{\sigma(\mathsf{string}(n))}(u,\lambda)$. Por (3.2), se sigue que

$$\varphi^{(2)}_{\sigma(\mathsf{string}(n))}(u,\lambda) = w = C(a_1^n a_2 u, \lambda).$$

Luego, por el paso 3 del procedimiento que define a C, existe $m \in \mathbb{N}$ tal que

$$\langle w, m\rangle \in W_e \qquad \text{y} \qquad H(w) > m > |u| + n + (c+1).$$

Pero, por (3.1), se tiene que

$$H(w) \leq H^{(2)}_{\varphi_{\sigma(\mathsf{string}(n))}}(w) + n + (c+1) \leq |u| + n + (c+1), \qquad \text{absurdo.}$$

Por tanto, si $U(u, \lambda) = e$, entonces, por el paso 3 en el procedimiento anterior, se sigue que para todo $\langle w, m\rangle \in W_e : m \leq |u| + n + (c+1)$. En particular, si tomamos $u = e^*$, tenemos que

$$m \leq H(e) + n + (c+1),$$

Así, $d = n + c + 1$ es la constante buscada. □

Notemos que la constante d está definida a partir de cierto n fijo (dado por el teorema de recursión) y de cierta constante c (dada por el teorema de invarianza). Por tanto, si tuviesemos códigos apropiados para los computadores que aparecen en la prueba del teorema 3.2, podemos determinar *efectivamente* la constante d.

Por el corolario 3.25 en [Ca02, 46], se tiene que

$$\#\{w \in A^n \mid H(w) > n - m\} > Q^n\left(1 - Q^{-m+1}/(Q-1)\right).$$

Por tanto, para m fijo y para n lo suficientemente grande, siempre existe $w \in A^n$ tal que $H(w) > n - m$. Este hecho contrasta con el siguiente corolario.

Corolario 3.3 *Sea $g : \mathbb{N} \to \mathbb{N}$ una función recursiva tal que $\lim_{n\to\infty} g(n) = \infty$.*
Si $S_g = \{w \in A^* \mid H(w) > g(|w|)\}$ es infinito, entonces S_g es inmune.

Prueba. Primero, definamos un computador $\psi : A^* \times A^* \xrightarrow{o} A^*$ del siguiente modo. Dada una entrada (e, u), ψ primero halla el único $(w, m) \in A^* \times \mathbb{N}$ tal que $\langle w, m\rangle = u$. Luego, ψ computa $\varphi_e(w)$. Si $\varphi_e(w) \downarrow$, entonces computa $g(|w|)$. Si $m = g(|w|)$, entonces ψ para e imprime a_2. En caso contrario, ψ entra en un *loop*.
Por el *s-m-n* teorema, existe $s : A^* \to A^*$ recursiva tal que $\varphi_{s(e)}(u) \simeq \psi(e, u), \forall e, u \in A^*$.

Notemos que si $W_e \subseteq S_g$, entonces

$$W_{s(e)} = \{\langle w, m\rangle \mid \varphi_e(w) \downarrow \ \wedge m = g(|w|)\} \subseteq \{\langle w, m\rangle \mid H(w) > m\}.$$

Así, por el teorema 3.2 aplicado a $W_{s(e)}$, existe una constante d tal que para todo $w \in W_e$:

$$g(|w|) \leq H(s(e)) + d.$$

Dado que $\lim_{n\to\infty} g(n) = \infty$, se sigue que W_e es finito. Por tanto, S_g es inmune. □

Presentamos un estimativo para la complejidad autolimitante que nos será de útil.

Lema 3.4 *Existe* (*efectivamente*) *una constante* c *tal que para todo* $w \in A^*$:

$$H(w) \leq |w| + 2\lg|w| + c.$$

Prueba. Recordemos que $D_A = \{d(w) \mid w \in A^*\}$ es un conjunto libre de prefijos (pág. 2). Luego, consideremos el computador de Chaitin $C(d(w), \lambda) = w$. Dado que $|d(w)| = |w| + 2\lg|w| + 1$, basta aplicar el teorema de invarianza. □

Corolario 3.5 *Sea* $g : \mathbb{N} \to \mathbb{N}$ *una función recursiva que* converge recursivamente a ∞ (*i.e.*, *existe una función* $r : \mathbb{N} \to \mathbb{N}$ *creciente recursiva tal que si* $n \geq r(k)$, *entonces* $g(n) > k$).
Si S_g *es infinito*, *entonces* S_g *es efectivamente inmune*.

Prueba. En el contexto de la prueba del corolario 3.3, si $w \in W_e \subseteq S_g$, entonces

$$g(|w|) \leq H(s(e)) + d \leq |s(e)| + 2\lg|s(e)| + c + d = k_e.$$

Por hipótesis, si $|w| \geq r(k_e)$, entonces $g(|w|) > k_e$. Por tanto, si $w \in W_e$, entonces $|w| < r(k_e)$. Luego,

$$\#(W_e) \leq \frac{Q^{r(k_e)} - 1}{Q - 1} < Q^{r(k_e)}.$$

Tomando $\gamma(e) = Q^{r(k_e)}$, obtenemos que S_g es efectivamente inmune. □

De los anteriores corolarios, podemos concluir que el conjunto r.e. $\{\langle w, m\rangle \mid H(w) \leq m\}$ no es recursivo (de hecho, es *simple*) y que la complejidad de Chaitin $H : A^* \to \mathbb{N}$ no es recursiva.

3.2 Incompletez y complejidad algorítmica

El teorema de incompletez de Chaitin es posiblemente uno de los resultados más famosos y popularizados de la lógica en las últimas tres décadas. Afirma que para toda teoría formal F existe una constante c tal que F no prueba ninguna sentencia de la forma "$H(w) > \mathsf{c}$", aún cuando hay infinitas cadenas $w \in A^*$ para las cuales esto es verdadero. En esta sección, desarrollamos una prueba del teorema de Chaitin basándonos en el teorema 3.2.

Por una teoría formal F entendemos un conjunto de sentencias en algún lenguaje de primer orden $\mathcal{L}_{\mathsf{F}}$. Las sentencias de $\mathcal{L}_{\mathsf{F}}$ que sean consecuencias lógicas de F son los teoremas de F; $\mathrm{Th}(\mathsf{F})$ denota el conjunto de teoremas de F y escribimos $\mathsf{F} \vdash \phi$ para $\phi \in \mathrm{Th}(\mathsf{F})$.

Supondremos que $\mathcal{L}_{\mathsf{F}}$ contiene al *lenguaje de la aritmética* $\mathcal{L}_{\mathbb{N}} = \{+, \cdot, 0, s\}$ y que las nociones sintácticas de $\mathcal{L}_{\mathsf{F}}$ y F se pueden codificar (gödelizar) mediante cadenas de A^*. En particular, si ϕ es una sentencia en $\mathcal{L}_{\mathsf{F}}$, el código de ϕ se denota por $\ulcorner \phi \urcorner \in A^*$. El predicado de prueba de F, que expresa que u codifica una prueba de la sentencia con codigo v, se abrevia por $\mathrm{Prf}_{\mathsf{F}}(u, v)$. Así, el predicado de demostrabilidad $\mathrm{Prov}_{\mathsf{F}}(v)$ se define como $(\exists u \in A^*)\, \mathrm{Prf}_{\mathsf{F}}(u, v)$.

En lo que sigue, F siempre denotará una teoría formal tal que

(a) F es *recursivamente enumerable*; i.e., el conjunto $\ulcorner \mathrm{Th}(\mathsf{F}) \urcorner := \{\ulcorner \phi \urcorner \mid \mathsf{F} \vdash \phi\}$ es r.e.

(b) F es "*suficientemente rica*"; i.e. F contiene la aritmética Q de Robinson.

(c) F es *sólida*; i.e., sus teoremas (o al menos los de la forma "$H(w) > c$") son verdaderos en el modelo estándar $\mathbb{N}$.

La condición (c) se puede expresar formalmente mediante el principio de reflexión:

$$\mathsf{ZFC} \vdash [\mathrm{Prov}_{\mathsf{F}}(\ulcorner H(w) > c \urcorner) \Rightarrow (H(w) > c)].$$

Teorema 3.6 (Chaitin) *Sea* F *una teoría formal. Entonces existe una constante* d, *independiente de* F, *tal que si* $e \in A^*$ *cumple que* $W_e = \ulcorner \mathrm{Th}(\mathsf{F}) \urcorner$, *entonces para todo* $w \in A^*$:

$$\mathsf{F} \nvdash H(w) > H(e) + \mathsf{d}.$$

Prueba. Sea ψ el computador que dado $(e,u) \in A^* \times A^*$ ejecuta el siguiente procedimiento:

1. `halle` $(w,m) \in A^* \times \mathbb{N}$ `tal que` $\langle w,m\rangle = u$;
2. `haga` $v := \ulcorner H(w) > m \urcorner$;
3. `compute` $\varphi_e(v)$;
4. `si` $\varphi_e(v)\downarrow$, `entonces imprima` a_2.

Por el *s-m-n* teorema, existe una función total recursiva $s : A^* \to A^*$ tal que

$$\varphi_{s(e)}(u) \simeq \psi(e,u), \qquad \forall e,u \in A^*.$$

Por tanto, si $W_e = \ulcorner \mathrm{Th}(\mathsf{F}) \urcorner$, entonces $W_{s(e)} = \{\langle w,m\rangle \mid \mathsf{F} \vdash H(w) > m\}$. Como F es una teoría sólida, tenemos que

$$W_{s(e)} \subseteq \{\langle w,m\rangle \mid H(w) > m\}.$$

Por el teorema 3.2 aplicado a $W_{s(e)}$, existe una constante d tal que si $\mathsf{F} \vdash H(w) > m$,

$$m \leq H(s(e)) + d. \tag{3.3}$$

Ahora, tomemos el computador de Chaitin $C(u,\lambda) = s(U(u,\lambda))$. Sea e^* el programa canónico para e. Notemos que $s(e) = s(U(e^*,\lambda)) = C(e^*,\lambda)$. Por tanto, $H_C(s(e)) \leq |e^*| = H(e)$. Aplicando el teorema de invarianza, obtenemos (efectivamente) una constante c tal que

$$H(s(e)) \leq H_C(s(e)) + c \leq H(e) + c. \tag{3.4}$$

De (3.3) y (3.4), se sigue que $m \leq H(e) + (c+d)$. Así, basta tomar $\mathsf{d} = c + d$. □

Siguiendo a van Lambalgen [vL89, 1393], llamaremos a la menor constante natural c tal que para todo $w \in A^*$, la teoría formal F **no** prueba ningúna sentencia de la forma "$H(w) > \mathsf{c}$", la constante característica de la teoría formal F y la denotaremos por $\mathsf{c_F}$. Notemos que, por el teorema 3.6, si $W_e = \ulcorner \mathrm{Th}(\mathsf{F}) \urcorner$, entonces $\mathsf{c_F} \leq H(e) + \mathsf{d}$.

Usando el conjunto libre de prefijos $D_A = \{d(w) \mid w \in A^*\}$, podemos obtener una cota para la constante característica que no involucra índices de la teoría formal. Razonaremos con la *aritmética de Peano de primer orden* PA [Ro67, 97], pero el argumento se puede aplicar a otros sistemas formales [Ca02, 322].

Teorema 3.7 *Existe una constante* c *tal que para todo* $w \in A^* : \mathsf{PA} \nvdash H(w) > \mathsf{c}$.

Prueba. Fijemos una enumeración de las pruebas de PA. Consideremos el computador de Chaitin $C(d(u), \lambda) = w$ sii

w es el x en la primera prueba en PA de un enunciado de la forma "$\varphi_u^{(2)}(d(u), \lambda) \neq x$".

Sea $v \in A^*$ tal que $\varphi_v^{(2)} = C$. Afirmamos que $C(d(v), \lambda) \uparrow$. En caso contrario, si $C(d(v), \lambda) = w$, entonces $\mathsf{PA} \vdash \varphi_v^{(2)}(d(v), \lambda) \neq w$, absurdo. Se sigue que $\mathsf{PA} + \{C(d(v), \lambda) = w\}$ es consistente, para todo $w \in A^*$. Porque de no ser así, $\mathsf{PA} \vdash \varphi_v^{(2)}(d(v), \lambda) \neq w \quad \text{y} \quad C(d(v), \lambda) \downarrow$.
Por el teorema de invarianza, existe c tal que $H(w) \leq H_C(w) + c$. Así, si $C(d(v), \lambda) = w$, entonces tendríamos que $H(w) \leq |d(v)| + c = |v| + 2\lg|v| + c$.
Sea $\mathsf{c} = |v| + 2\lg|v| + c$. Dado que para todo w, $\mathsf{PA} + \{C(d(v), \lambda) = w\}$ es consistente, entonces $\mathsf{PA} + \{H(w) \leq \mathsf{c}\}$ también es consistente para todo w. Luego, PA no prueba ningúna sentencia de la forma "$H(w) > \mathsf{c}$". □

Ahora, definimos la complejidad (o el contenido de información) de una teoría formal F por

$$H(\mathsf{F}) = \min\{H(e) \mid W_e = \ulcorner \mathrm{Th}(\mathsf{F}) \urcorner\}.$$

Supongamos que tomamos alguna cota superior recursiva $f(\mathsf{F})$ para la complejidad de F, entonces **no** es posible determinar recursivamente una cadena $w(\mathsf{F})$ tal que $H(w(\mathsf{F})) > f(\mathsf{F}) \geq \mathsf{c}_\mathsf{F}$ [vL87b, 1394]. La siguiente proposición es una formalización del comentario anterior. Cabe observar que dada $f : A^* \to \mathbb{N}$ recursiva, se puede construir otra g recursiva que satisface la condición (a) de la proposición y además $g(e) \geq f(e)$ para todo $e \in A^*$.

Proposición 3.8 Sea $f : A^* \to \mathbb{N}$ una función recursiva tal que

(a) *para todo* $u, v \in A^*$ *con* $|u| < |v|$ *se tiene que* $f(u) \leq f(v)$;

(b) *si* $W_e = \ulcorner \mathrm{Th}(\mathsf{F}) \urcorner$, *entonces* $H(e) + \mathsf{d} \leq f(e)$, *donde* d *es la constante del teorema* 3.2.

Entonces **no** *existe una función recursiva* $\gamma : A^* \to A^*$ *tal que si* $W_e = \ulcorner \mathrm{Th}(\mathsf{F}) \urcorner$, *entonces*

$$\mathsf{c}_\mathsf{F} \leq f(e) < H(\gamma(e)).$$

Prueba. Razonemos por el absurdo. Definamos recursivamente una sucesión de teorías formales del siguiente modo: sea $\mathsf{F}_0 := \mathsf{PA}$ y $e_0 \in A^*$ tal que $W_{e_0} = \ulcorner \mathrm{Th}(\mathsf{PA}) \urcorner$. Para $n \in \mathbb{N}$:

$$\mathsf{F}_{n+1} := \mathsf{F}_n + \{H(\gamma(e_n)) > f(e_n)\}, \qquad \text{donde } W_{e_n} = \ulcorner \mathrm{Th}(\mathsf{F}_n) \urcorner.$$

Sin perdida de generalidad, podemos suponer que $|e_n| < |e_{n+1}|$. Notemos que $\mathsf{F}_{n+1} \vdash H(\gamma(e_n)) > \mathsf{c}_{\mathsf{F}_n}$. Por tanto, $\mathsf{c}_{\mathsf{F}_n} < \mathsf{c}_{\mathsf{F}_{n+1}}$ y $\lim_{n\to\infty} \mathsf{c}_{\mathsf{F}_n} = \infty$. Como $f(e_n) \geq \mathsf{c}_{\mathsf{F}_n}$, se sigue que $\lim_{n\to\infty} f(e_n) = \infty$. Ahora, por el lema 3.4, existe una constante c tal que para todo n :

$$f(e_n) < H(\gamma(e_n)) \leq |\gamma(e_n)| + 2\lg|\gamma(e_n)| + c.$$

Por tanto, $f(e_n) - c < |\gamma(e_n)| + 2\lg|\gamma(e_n)|$ y $\lim_{n\to\infty} |\gamma(e_n)| = \infty$. Luego, $\{\gamma(e_n) \mid n \in \mathbb{N}\}$ es un subconjunto de A^* infinito y r.e..

Ahora sea $g : \mathbb{N} \to \mathbb{N}$ la función que, para un l dado, ejecuta el siguiente procedimiento:

1. `halle el menor` m `tal que` $l + 2\lg(l) + c \leq f(e_m)$;
2. `genere` $\gamma(e_0), \gamma(e_1), \ldots, \gamma(e_m)$;
3. `halle el menor` k $(0 \leq k \leq m)$ `tal que` $l = |\gamma(e_k)|$ `y haga` $g(l) = f(e_k)$;
4. `si el` k `del paso 3 no existe, haga` $g(l) = f(e_m)$.

Es claro que g es una función recursiva. Notemos que los k del paso 3 son distintos y como $\lim_{n\to\infty} f(e_n) = \infty$, se tiene que $\lim_{l\to\infty} g(l) = \infty$. Por la condición (a), tenemos que $H(\gamma(e_n)) > f(e_n) \geq g(|\gamma(e_n)|)$. Por tanto,

$$\{\gamma(e_n) \mid n \in \mathbb{N}\} \subseteq S_g = \{w \mid H(w) > g(|w|)\}.$$

Luego, S_g no sería inmune. Por el corolario 3.3, S_g sería finito, absurdo. □

Ahora, mostraremos que, en general, la constante característica c_F no es aproximadamente igual a la complejidad $H(e)$, donde e es algún índice tal que $W_e = \ulcorner \mathsf{Th}(\mathsf{F}) \urcorner$. Aquí, entendemos por "aproximadamente igual" que la diferencia entre las dos cantidades este acotada.

Entendemos por la aritmética elemental el conjunto de sentencias del lenguaje de la aritmética $\mathcal{L}_\mathbb{N} = \{+, \cdot, 0, s\}$ que son válidas en el módelo estándar de los números naturales. Denotamos por $\mathsf{ZF}/\mathcal{L}_\mathbb{N}$ el fragmento aritmético de ZF; esto es, el conjunto de sentencias de la aritmética

elemental que son demostrables en ZF al interpretar relativamente $\mathcal{L}_{\mathbb{N}}$ mediante la fórmula $n \in \omega$, la constante 0 con el conjunto vacío, el símbolo funcional unario s con la operación sucesor $n^+ = n \cup \{n\}$ y $+, \cdot$ con la suma y el producto ordinal [Kr68, 119]. Informalmente, $\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}$ es la colección de todas las sentencias de la aritmética elemental que son demostrables por todos los medios matemáticos conocidos y aceptados [Ro67, 321].

Una teoría formal S es una extensión de otra teoría formal F si $\mathsf{F} \subseteq \mathrm{Th}(\mathsf{S})$. Es claro que $\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}$ es una extensión propia de PA. Decimos que S es una extensión finita de F si existe un conjunto finito de sentencias G tal que $\mathrm{Th}(\mathsf{S}) = \mathrm{Th}(\mathsf{F} + \mathsf{G})$.

El siguiente lema es un caso particular del teorema 11 en [Kr68, 121].

Lema 3.9 *Ninguna extensión consistente de* $\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}$ *es una extensión finita de* PA.

Dado que $\ulcorner \mathrm{Th}(\mathsf{ZF}) \urcorner$ es r.e. y que podemos decidir efectivamente si una sentencia de ZF es una sentencia (relativa) del lenguaje de la aritmética, tenemos que $\ulcorner \mathrm{Th}(\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}) \urcorner$ es r.e.
Como $\ulcorner \mathrm{Th}(\mathsf{PA}) \urcorner$ también es r.e., por el teorema 3.6, existen constantes características c_{PA} y c_{ZF} para PA y $\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}$, respectivamente (¡no sabemos si $\mathsf{c}_{\mathsf{PA}} < \mathsf{c}_{\mathsf{ZF}}$!).
Supongamos que $\ulcorner \mathrm{Th}(\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}) \urcorner = \{\ulcorner \phi_n \urcorner\}_{n=1}^{\infty}$ y definamos una sucesión infinita de teorías r.e. por

$$\mathsf{F}_0 = \mathsf{PA} \qquad \text{y} \qquad \mathsf{F}_n = \mathsf{PA} + \{\phi_1, \ldots, \phi_n\}, \quad \text{para } n \geq 1.$$

Por el lema previo, $\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}$ no es una extensión finita de PA. Por tanto, $\{\mathsf{F}_n\}$ es una sucesión de teorías numéricas (eventualmente cada vez más fuertes) que yacen entre PA y $\mathsf{ZF}/\mathcal{L}_{\mathbb{N}}$. Es claro que hay una cantidad *finita* de constantes entre c_{PA} y c_{ZF}. Por tanto, tenemos que *infinitas* de las teorías F_n tienen la *misma* constante característica c y tienen que probar el *mismo* conjunto de sentencias de la forma "$H(w) > m$". Por otro lado, sea e_n un índice, *elegido de acuerdo a un esquema fijado de antemano*, tal que $W_{e_n} = \ulcorner \mathsf{Th}(\mathsf{F}_n) \urcorner$ (por ejemplo, se podría tomar e_n tal que $H(e_n) = H(\mathsf{F}_n)$). Notemos que, a medida que n crece, la teoría F_n es eventualmente una extensión propia de las teorías $\mathsf{F}_k, k < n$, que le preceden. Por tanto, $\{e_n \mid n \in \mathbb{N}\}$ es un subconjunto infinito de A^*. Así, $\lim_{n\to\infty} H(e_n) = \infty$. De este modo, las constantes características de los F_n no son aproximadamente iguales a las complejidades $H(e_n)$ relacionadas con estas teorías.

3.3 El teorema de la Base

Decimos que $T \subseteq A^*$ es un árbol si $(\forall u, v \in A^*)$ $(u \leq_p v \wedge v \in T \Rightarrow u \in T)$. Un árbol T es un ω-árbol si para todo $n \in \mathbb{N} : A^n \cap T \neq \emptyset$. Dado un árbol T, denotamos por

$$[T] = \{\mathbf{x} \in A^\omega \mid (\forall n)\ (\mathbf{x}\,(n) \in T)\}$$

el conjunto de trayectorias (ramas) infinitas de T. El siguiente principio combinatorio, debido a D. König, relaciona las nociones previas y su prueba requiere el axioma de elección.

Lema de König. *Si T es un ω-árbol, entonces $[T] \neq \emptyset$.*

Podemos caracterizar las clases Π^0_1 de A^ω en términos de árboles. Un árbol T es recursivo si $T \in \Sigma_0$; esto es, la relación $w \in T$ es recursiva.

Lema 3.10 *$\mathcal{C}$ es una clase Π^0_1 no vacía de A^ω sii existe un árbol recursivo T tal que $\mathcal{C} = [T]$.*

Prueba. Si $\mathcal{C} \in \Pi^0_1$, por el corolario 1.8 (a), existe $R \subseteq A^*$ recursivo tal que

$$\mathcal{C} = \{\mathbf{x} \mid (\forall n)\ (\mathbf{x}\,(n) \in R)\}.$$

Ahora, definamos

$$T = \{v \in A^* \mid (\forall u \leq_p v)\ (u \in R)\}.$$

Como R es recursivo, y dado que toda cadena tiene finitos prefijos, es claro que T es un árbol recursivo. Si $\mathbf{x} \in \mathcal{C}$, entonces para todo n y todo $k \leq n$ se cumple que $\mathbf{x}\,(k) \in R$ y, por tanto, $\mathbf{x} \in [T]$. Como $T \subseteq R$, se sigue que

$$[T] \subseteq \{\mathbf{x} \mid (\forall n)\ (\mathbf{x}\,(n) \in R)\} = \mathcal{C}.$$

Por el corolario 1.8 (a), la otra implicación es obvia. □

El siguiente resultado es una versión débil del *teorema de la base* de Jockusch-Soare [So87, 109]. Decimos que $\mathbf{x} \in A^\omega$ es Δ^0_2-definible si para todo $a \in A : \{n \in \mathbb{N} \mid x_n = a\}$ es un subconjunto Δ_2 de $\mathbb{N}$ [Li93, 221].

Teorema 3.11 *Si $\mathcal{C}$ es una clase Π^0_1 no vacía de A^ω, entonces $\mathcal{C}$ tiene un elemento Δ^0_2-definible.*

Prueba. Por el lema 3.10, existe un árbol recursivo $T \subseteq A^*$ tal que $\mathcal{C} = [T]$.
Diremos que $n \in \mathbb{N}$ (ó $w = \mathsf{string}\,(n)$) es $\mathsf{admisible}$ sii

$$(\forall m > |w|)\ (\exists v \in T)\ (\ m = |v| \ \wedge\ w \leq_p v\ ).$$

Como T es recursivo, es claro que $\mathrm{Ad}\,(T) = \{n \mid n \text{ es admisible}\}$ es un conjunto Π_1 de $\mathbb{N}$. Notemos que, por el lema de König,

$$w \text{ es admisible} \quad \text{sii} \quad (\exists \mathbf{x} \in [T])\ (w <_p \mathbf{x})\,.$$

Dado que $[T] = \mathcal{C} \neq \emptyset$, podemos concluir que $\{w \mid w \text{ es admisible}\} \cap A^m \neq \emptyset$, para todo m. Ahora, la *rama infinita del extremo izquierdo* del árbol T se puede construir recursivamente en el conjunto $\mathrm{Ad}\,(T)$. En efecto, sea $\mathbf{r} : \mathbb{N}^+ \to A$ la sucesión dada por la siguiente recursión:

$$r_1 = \min\left\{a \in A \mid \mathsf{string}^{-1}\,(a) \in \mathrm{Ad}\,(T)\right\}$$

y suponiendo que se han definido $r_1, \ldots, r_n$, hacemos

$$r_{n+1} = \min\left\{a \in A \mid \mathsf{string}^{-1}\,(r_1 r_2 \cdots r_n a) \in \mathrm{Ad}\,(T)\right\},$$

donde los mínimos se toman de acuerdo al orden de A. Es claro, por la definición dada, que

$$R_a = \{n \in \mathbb{N} \mid r_n = a\} \leq_T \mathrm{Ad}\,(T)\,, \qquad \text{para cada } a \in A.$$

Como $\mathrm{Ad}\,(T) \in \Pi_1$, por el teorema de Post (corolario 1.2) tenemos que $R_a \in \Delta_2$. Por tanto, la sucesión $\mathbf{r} = r_1 r_2 \cdots \in [T] = \mathcal{C}$ es Δ^0_2-definible. $\square$

3.4 Aleatoriedad e Incompletez

En [Ch87], Chaitin ofrece una especie de "forma extrema" del primer teorema de incompletez al mostrar que en la matemática, no sólo se presenta la incompletez, sino también la aleatoriedad. Para explicar esta idea, debemos introducir una de las construcciones fundamentales de Chaitin: la probabilidad de parada Ω de un computador de Chaitin universal U :

$$\Omega := \sum\nolimits_{U(u,\lambda)\downarrow} Q^{-|u|}.$$

Debido a la desigualdad de Kraft (lema 2.19 (a)), Ω es un número real bien definido.

Intuitivamente, Ω representa la probabilidad de que un computador de Chaitin universal U se detenga, si el programa $u \in A^*$ se "toma al azar" y no se ingresan datos adicionales. Es importante observar que Ω depende del computador universal U que se halla fijado. Así, lo que tenemos realmente es una familia de números que poseen propiedades muy interesantes. Entre ellas, cabe resaltar que al expandir Ω en base Q se obtiene una sucesión *aleatoria* respecto a la medida de Lebesgue λ_Q (ver teorema 4.3.2 en [Su03, 69]). Como consecuencia de esto, Ω es un número real *aleatorio*, *no computable*, *trascendente* y *Borel normal en cualquier base* [Su03].

Otro de los grandes logros de Chaitin es haber obtenido una conexión de Ω con la teoría de números. Por razones técnicas, Chaitin trabajó con ecuaciones Diofantinas exponenciales; esto es, ecuaciones que se construyen con adición, multiplicación y exponenciación de variables enteras no negativas a partir de coeficientes enteros, y se restringió al alfabeto binario $\mathbf{2} = \{0, 1\}$.

Teorema 3.12 (Chaitin) *Existe una ecuación Diofantina exponencial*

$$P(n, x_1, x_2, \ldots, x_m) = 0 \tag{3.5}$$

tal que para todo n :

el n*-ésimo bit de* Ω *es* 1 *sii la ecuación* $P(n, \overline{x}) = 0$ *tiene* **infinitas** *soluciones.*

Para una prueba, ver [Su03, 73]. Mediante el teorema de Matiyasevič-Jones y un interpretador de LISP, Chaitin ha construído efectivamente la ecuación (3.5). El resultado es una

ecuación enorme cuya escritura requiere por lo menos 200 páginas [Ch87, 142].

Daremos otra versión del teorema de Chaitin, basándonos en el teorema de la base (teorema 3.11) y en la siguiente observación, debida originalmente a Schnorr.

Proposición 3.13 *Para toda medida computable μ en A^ω $\mathcal{R}(\mu)$ tiene elementos Δ_2^0-definibles.*

Prueba. Sea $\mathcal{U}$ un μ-test secuencial universal. Como $(\mathcal{R}(\mu))^c = \mathcal{U}$ es una clase Π_2^0, tenemos que $\mathcal{R}(\mu)$ es una clase Σ_2^0 de A^ω. Por el corolario 1.8 (b), existe una sucesión $\{\mathcal{C}_n\}$ de clases Π_1^0 en A^ω tal que

$$\mathcal{R}(\mu) = \bigcup\nolimits_n \mathcal{C}_n.$$

Como $\mathcal{R}(\mu) \neq \emptyset$ (de hecho, $\mu(\mathcal{R}(\mu)) = 1$), existe k tal que $\mathcal{C}_k \neq \emptyset$. Por el teorema 3.11, podemos concluir que existen sucesiones Δ_2^0-definibles pertenecientes a $\mathcal{R}(\mu)$. □

Cabe observar que la expansión en base 2 de la versión binaria de Ω es una sucesión Δ_2^0-definible [Ca02, 284, 304].

Para obtener el teorema de Chaitin, consideramos la medida de Lebesgue λ_2 en $\mathbf{2}^\omega$ y, por la proposición 3.13, tomamos una sucesión $\mathbf{x} \in \mathcal{R}(\lambda_2)$ que sea Δ_2^0-definible. A fortiori, $\{n \in \mathbb{N} \mid x_n = 1\}$ es un conjunto Π_2. Por tanto, existe una relación r.e. $R \subseteq \mathbb{N}^2$ tal que

$$x_n = 1 \quad \text{si y sólo si} \quad (\forall m)\ R(n,m).$$

Por el Teorema de Matiyasevič-Jones, *todo conjunto r.e. tiene una representación Diofantina exponencial univaluada* (ver [Jo84], [Ma93]). Esto es, existe una ecuación Diofantina exponencial

$$P(n, m, k_1, \ldots, k_r) = 0$$

que tiene una *única* solución $\overline{k}$ si $R(n,m)$ y *no* tiene soluciones si $\neg R(n,m)$. Por tanto,

$$[\text{ el } n\text{-ésimo bit de } \mathbf{x} \text{ es } 1\ ] \quad \text{sii} \quad (\forall m)\,(\ P\left(n, m, \overline{k}\right) = 0 \text{ tiene solución }).$$

Dado que $\mathbf{x}$ es aleatoria respecto a λ_2, podríamos decir que el hecho de que la ecuación $P\left(n, m, \overline{k}\right) = 0$ tenga o no solución (para todo m) oscila de una manera completamente impredecible a medida que n varía.

Conclusiones

Después de un estudio comparativo de las nociones clásicas de aleatoriedad a la luz de los artículos [vL87b] y [vL89] de van Lambalgen y del texto de Calude [Ca02], así como nuestro trabajo previo [Su03], expresaremos nuestro punto de vista respecto a los resultados obtenidos.

1. Reiteradamente, van Lambalgen ha expresado serias dudas acerca de la conveniencia de restringir el concepto de *regla* a la de *función computable* y del uso de la teoría de la recursión en la definición de sucesión aleatoria. Como hemos visto, las nociones de Martin-Löf y Kolmogorov-Chaitin se desarrollan a partir de nociones propias de la computabilidad formalizando intuiciones diferentes. Ahora, el teorema 2.23 muestra que estas dos nociones coinciden para cualquier medida computable mientras que el principio de homogeneidad afirma que la noción de Martin-Löf se preserva bajo cierto tipo de selecciones de lugar. Por tanto, en nuestra opinión, ambos teoremas dan *robustez* a las definiciones clásicas y una mayor *sólidez* al uso de la computabilidad en el estudio de la aleatoriedad, siendo uno de sus atractivos el que sean aplicables a cualquier medida computable. Esto contrasta con el trabajo en [Ca02] o [Su03], donde el uso de la teoría de la medida en A^ω se reducía a la medida de Lebesgue.

De otro lado, otra contribución importante del trabajo de van Lambalgen tiene que ver con su propuesta de un tratamiento axiomático para la noción de aleatoriedad. Él propone que las intuiciones usuales que se involucran en la definición de aleatoriedad, a saber, *irregularidad*, *complejidad*, *independencia*, se traten como *primitivas* y se adicionen axiomas [vL90, 1146] que intenten capturar las intuiciones detrás del concepto de aleatoriedad. Como resultado de esto, ha concluído que la adición de estos axiomas a la teoría ZF implica la negación del axioma de elección (corolario 2.5 en [vL92, 1287]). Aun más, parece ser que el axioma de extensionalidad es incompatible con su formalización de la noción de aleatoriedad (ver [vL92, §3]). El aspecto positivo de esta propuesta, a más de lograr formalizar de manera coherente los colectivos de von Mises, es que abre un nuevo frente para tratar de abordar la noción de aleatoriedad, utilizando las herramientas de la lógica y específicamente la teoría de modelos y la teoría de conjuntos (los modelos booleanos, el forcing, etc.).

2. En [vL89, 1394], van Lambalgen presenta varias críticas a la interpretación *oficial* del teorema de incompletez de Chaitin (teorema 3.6). Según esta interpretación, el resultado afirma que una teoría formal no puede probar que un objeto específico tenga complejidad mayor que la complejidad (contenido de información) de la teoría (ver también [Su03, 65]). Para ello, la noción de *constante característica*, así como la proposición 3.8 y el razonamiento que sigue al lema 3.9, muestran que la complejidad de la teoría no juega ningún papel relevante en el tipo de cota para los enunciados de la forma "$H(w) > c$" que la teoría prueba (para un análisis más detallado consultar [Ra98]). Consideramos que la crítica de van Lambalgen a este respecto es acertada, en el sentido de que la mención que hace Chaitin de "la entropía de un sistema axiomático" y "el contenido de información de una teoría", no parecen tener mucha relevancia con el fenómeno de incompletez que se puede evidenciar en dicha teoría [vL89, $1390-1391$]. De otro lado, se podría argumentar en defensa de Chaitin, que él sólo está promoviendo algunos de sus resultados a la vez que adelanta una propuesta para consideración de los estudiosos. A continuación reproducimos uno de los apartes en los que se basa van Lambalgen para enunciar sus críticas (las cursivas son nuestras):

> Godel's original proof constructed a paradoxical assertion that is true but not provable within the usual formalization of number theory. In contrast *I would like to measure* the power of a set of axioms and rules of inference. *I would like to be able to say* that if one has ten pounds of axioms and a twenty-pound theorem, then the theorem cannot be derived from the axioms. [...] To be more specific, I will apply the viewpoint of thermodynamics and statistical mechanics to Godel´s theorem, and will use such concepts as probability, randomness, and information to study the incompleteness phenomenon and *to attempt to evaluate* how widespread it is [Ch90].

Por último, cabe observar que en [Su03, 64], desarrollamos otra prueba del teorema 3.6 de Chaitin apelando a una noción de complejidad de una teoría que proponemos y que, en este trabajo, introducimos con mayor sencillez (ver pág. 38). Queda a gusto personal qué tipo de método es preferible para probar dicho teorema [Ra98, 575].

3. En [vL89, 1396], van Lambalgen enjuicia de una forma muy fuerte y hasta hóstil el célebre teorema de Chaitin sobre las conexiones entre Ω y las ecuaciones Diofantinas (Caos en la Aritmética). Además, afirma que la construcción efectiva y explícita de la ecuación Diofantina exponencial es un intento de Chaitin de otorgarle importancia a un resultado que van Lambalgen cree falto de profundidad. Para contradecir las opiniones de Chaitin, van Lambalgen nos propone el uso de lo que él denomina "*general nonsense*" ("*tonterías conocidas*") tales como la jerarquía aritmética en A^{ω}, la existencia de un test secuencial universal de Martin-Löf, el teorema de Post, cierta versión del teorema de la base de Jockusch-Soare y el teorema de Matiyasevič-Jones para derivar el teorema de Chaitin. Curiosamente, el resultado de van Lambalgen [vL89, 1397] es una versión diferente (de hecho, más débil) del teorema clásico de Chaitin sobre Ω. Es por esto que consideramos que la crítica de van Lambalgen es un tanto infundada, y quizá de caracter personal, pues los teoremas que usa en la prueba distan de ser triviales (por ejemplo, el teorema de Matiyasevič-Jones relacionado con la insolubilidad del Décimo problema de Hilbert). Como ocurre con muchos teoremas clásicos de las matemáticas, a medida que se profundiza en el área aparecen pruebas distintas, quizá mas cortas o que usan métodos muy diferentes, pero esto en ningún momento significa que dichos teoremas sean triviales o carezcan de profundidad. Para ilustrar lo anterior basta considerar el denominado teorema fundamental del álgebra (Gauss, Argand, 1806) o el famoso teorema del número primo (Hadamard y Vallée Poussin, 1896), para citar solo dos ejemplos ilustres. Un aspecto en el cual sí nos parece factible una discusión es el significado fundacional que se le puede asignar a los teoremas de incompletez de Chaitin. Algo parecido a la discusión, todavía activa, que generaron los teoremas de incompletez de Gödel. Pero obviamente esa es una polémica que pertenece a los fundamentos de la matemática (o la filosofía de la matemática).

4. Como resumen final pensamos que tanto el trabajo clásico de Kolmogorov, Chaitin, Schnorr, Martin-Löf, etc., junto con los aportes de van Lambalgen, se complementan de manera positiva. Como hemos visto se han obtenido generalizaciones y pruebas diferentes para algunos resultados. Además, las últimas propuestas de van Lambalgen han mostrado que algunos aspectos de la aleatoriedad nos pueden llevar a cuestionar la matemática clásica. Obviamente estos avances servirán tanto de guía como de estímulo para investigaciones posteriores.

Bibliografía

[Ba95] Bartle, R. *The Elements of Integration and Lebesgue Measure*. New York: John Wiley & Sons, 1995.

[Br94] Bridges, D. S. *Computability*. Berlin: Springer-Verlag, 1994.

[Ca02] Calude, C. *Information and Randomness - An Algorithmic Perspective*. Berlin: Springer-Verlag, 2002.

[Ch87] Chaitin, G. *Algorithmic Information Theory*. Cambridge: Cambrigde U. P., 1987.

[Ch90] Chaitin, G. *Information, Randomness and Incompleteness. Papers on Algorithmic Information Theory*. Singapore: World Scientific, 1990.

[Ha74] Halmos, P. *Measure Theory*. New York: Springer-Verlag, 1974.

[Jo84] Jones, J. y Matiyasevič, Y. *Register machine proof of the theorem on exponential diophantine representation of the enumerable sets*. J. Symbolic Logic **49** (1984), 818-829.

[Li93] Li, M y Vitányi, P.M. *An Introduction to Kolmogorov Complexity and its Applications*. Berlin: Springer-Verlag, 1993.

[Kr68] Kreisel, G. y Levy, A. *Reflection principles and their use for establishing the complexity of axiomatic systems*. Zeitschrift für Mathematische Logik und Grundlagen der Mathematik. vol. **14** (1968), 97-142.

[Ma93] Matiyasevič, Y. *Hilbert's Tenth Problem.* Cambridge: MIT Press, 1993.

[Ox80] Oxtoby, J. *Measure and Category*. New York: Springer-Verlag, 1980.

[Ra98] Raatikainen, P. *On Interpreting Chaitin's Incompleteness Theorem*. Journal of Philosophical Logic. **27** (1998) 569-586.

[Ra00] Raatikainen, P. *Algorithmic Information Theory and Undecidability*. Synthese. **123** (2000) 217-225.

[Ro67] Rogers, H. *Theory of Recursive Functions and Effective Computability*. New York: McGraw-Hill, 1967.

[Ry88] Royden, H.L. *Real Analysis*. Upper Saddle River: Prentice-Hall, 1988.

[So87] Soare, R. *Recursively Enumerable Sets and Degrees*. Berlin: Springer-Verlag, 1987.

[Su03] Suárez, J. *El Número Omega. Información, Incompletez y Aleatoriedad*. Tesis de Pregrado. Medellín: Universidad de Antioquia, 2003.

[vL87a] van Lambalgen, M. *Random sequences*. Ph.D. Thesis. Amsterdam: University of Amsterdam, 1987.

[vL87b] van Lambalgen, M. *Von Mises' definition of random sequence reconsidered* . J. Symbolic Logic **52** (1987), 725-755.

[vL89] van Lambalgen, M. *Algorithmic Information Theory*. J. Symbolic Logic **54** (1989), 1389-1400.

[vL90] van Lambalgen, M. *The Axiomatization of Randomness*. J. Symbolic Logic **55** (1990), 1143-1167.

[vL92] van Lambalgen, M. *Independence, Randomness and the Axiom of Choice*. J. Symbolic Logic **57** (1992), 1274-11304.

[Vo02] Volchan, S. *What is a random sequence?* AMM **109** (2002) 46-63.