Tesis de Licenciatura

Otra caracterización de reales aleatorios c.e.

Silvana Picchi
sp8i@dc.uba.ar

Directora:
Dra. Verónica Becher

Departamento de Computación
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

9 de diciembre de 2012

Resumen

En este trabajo presentamos una caracterización de la clase de los números reales aleatorios que son aproximables desde abajo, llamados *computablemente enumerables (c.e.)*, a partir del análisis de la estrategia de demostración de aleatoriedad de Chaitin.

Damos condiciones necesarias y suficientes para mostrar que la medida asociada a un conjunto de cadenas binarias es un real aleatorio c.e. Estas condiciones restringen la longitud de las palabras en el conjunto considerado, con respecto a la longitud de los elementos del dominio de una máquina autodelimitante universal de referencia.

Los resultados obtenidos permiten deducir el Teorema de Chaitin-Slaman, que caracteriza a los números reales aleatorios c.e. como las probabilidades de detención de máquinas autodelimitantes universales, usando exclusivamente conceptos de la teoría de funciones recursivas y de la teoría de la información algorítmica.

Abstract

In this work we present a characterization of the class of random real numbers that can be approximated from below, called *computably enumerable (c.e.)*, starting from an analysis of Chaitin's strategy for proving randomness.

We give necessary and sufficient conditions on sets of binary strings in order to show that their associated measure is a random c.e. real. These conditions restrict the length of words in the set under consideration, with respect to the length of elements in the domain of a reference self-delimiting universal machine.

The results obtained allow us to deduce Chaitin-Slaman Theorem, that characterizes random c.e. real numbers as halting probabilities of self-delimiting universal machines, exclusively using concepts from recursive functions and from algorithmic information theories.

Índice General

1 Introducción

¿Cuándo es aleatorio un número real? La noción intuitiva de aleatoriedad remite a la idea de un número "no excepcional", sin ninguna propiedad particular que lo distinga de otros. Sin embargo, la formalización de este concepto no ha sido trivial. Chaitin (1975), Martin-Löf (1966) y Solovay (1975) han presentado distintas definiciones matemáticas de aleatoriedad. En todos los casos, se define aleatoriedad para una secuencia binaria infinita, y luego se extiende la definición a los números reales, mediante la identificación de cada número real con la secuencia binaria infinita correspondiente a su expansión binaria.

La definición de aleatoriedad está basada en la teoría de la computabilidad y surge a partir de dos aproximaciones diferentes. Una de ellas, dada por la teoría algorítmica de la información desarrollada por Chaitin [8], identifica aleatoriedad con incompresibilidad algorítmica. Formaliza la idea de que una secuencia aleatoria debería ser impredecible, debería carecer de estructura o regularidad. Cualquier patrón o regularidad en una cadena puede usarse para comprimir la cadena y dar una descripción algorítmica de menor longitud a partir de la cual puede reconstruirse la cadena. Entonces, una secuencia infinita es aleatoria si sus segmentos iniciales son algorítmicamente incompresibles [8]. La otra aproximación al concepto de aleatoriedad está basada en la teoría de la medida constructiva: la idea fundamental en este caso es que una secuencia aleatoria debería satisfacer todas las propiedades estadísticas de aleatoriedad expresables mediante tests constructivos, es decir, tests generables mediante un procedimiento efectivo. Esta idea fue desarrollada por Martin-Löf [14] y Solovay [18]. Las dos caracterizaciones de aleatoriedad coinciden [10].

De la definición de Martin-Löf surge que casi todo número real es aleatorio: el conjunto de los reales aleatorios es un conjunto de medida 1 [10]. En la interpretación usual de la medida, esto significa que la probabilidad de que un número real sea aleatorio es 1, cuando cada dígito de su expansión binaria se determina mediante un experimento aleatorio independiente. Sin embargo, no es fácil dar un ejemplo natural de un número aleatorio. Chaitin [10] presenta una familia de números que verifican la propiedad de aleatoriedad: las probabilidades de detención de máquinas autodelimitantes universales, conocidas en la literatura como Ω-*numbers*. Los Ω-*numbers*, además de ser aleatorios, tienen la particularidad de ser computablemente enumerables (c.e.), es decir, pueden ser aproximados desde abajo en forma recursiva.

Las máquinas autodelimitantes [8] son máquinas de Turing con la propiedad de que el conjunto de los programas que se detienen en dichas máquinas es un conjunto de cadenas binarias libre de prefijos. Cada cadena se interpreta como un programa para la máquina. Un conjunto libre de prefijos tiene la propiedad de que la medida (en el sentido de Lebesgue) del conjunto

de todas las secuencias infinitas que extienden a cadenas en el conjunto es un número real entre 0 y 1. Este valor, por lo tanto, puede interpretarse como la probabilidad de que una secuencia infinita arbitraria comience con una cadena que pertenece al conjunto. En otras palabras, la medida del conjunto de todas las extensiones infinitas de programas en el dominio de una máquina autodelimitante es la probabilidad de detención de la máquina.

Recientemente, Slaman y Kučera [13], sobre la base del trabajo de Calude et al. [6], demostraron que la propiedad recíproca a la probada por Chaitin también es cierta: todo real aleatorio c.e. es un Ω-*number*. Entonces, este resultado (conocido como el *Teorema de Slaman*) y el de Chaitin constituyen, en conjunto, una caracterización de los números reales aleatorios c.e. como probabilidades de detención de máquinas autodelimitantes universales.

A partir de este fundamental resultado surge la motivación principal para este trabajo: obtener una caracterización más descriptiva de los conjuntos cuya medida asociada es un número real aleatorio c.e. Dicho de otra manera, queremos dar condiciones que muestren más explícitamente cuáles conjuntos de cadenas binarias pueden ser dominios de máquinas autodelimitantes universales.

Comenzamos examinando la estrategia desarrollada por Chaitin [8, 10] para demostrar, dada una máquina autodelimitante universal, que la medida asociada a su dominio es un número real aleatorio y c.e. Una primer cuestión que surge naturalmente es determinar en qué casos es posible aplicar esta estrategia. En otras palabras:

Pregunta 1 *¿Qué condiciones debe verificar un conjunto de cadenas para que su medida asociada pueda probarse aleatoria y c.e. mediante la estrategia de demostración de Chaitin?*

Uno de los resultados del presente trabajo responde a esta pregunta. Establecemos condiciones suficientes sobre conjuntos de cadenas, que surgen del análisis de los requisitos necesarios para garantizar la aplicabilidad de la estrategia de demostración de Chaitin. Estas condiciones se dan a partir de la definición de *Chaitin-reducción*: una reducción 1 a 1 que restringe la longitud de las palabras del conjunto considerado en relación a la longitud de los programas para una máquina autodelimitante universal *fija*, que llamamos U. Damos una demostración generalizada que aplica la estrategia de Chaitin para probar que la medida asociada a un conjunto A tal que el dominio de U es *Chaitin*-reducible a A es un número real aleatorio y c.e.

Una vez que hemos determinado condiciones suficientes para aplicar la demostración canónica de Chaitin, podemos interrogarnos acerca de la necesariedad de dichas condiciones:

Pregunta 2 *¿Todo número real aleatorio y c.e. es la medida de algún conjunto A tal que el dominio de U es* Chaitin*-reducible a A?*

La respuesta a la Pregunta 2 es afirmativa, y es otro de los resultados centrales que presentamos. Combinando los resultados que responden a estas dos primeras preguntas, obtenemos una caracterización de los números reales aleatorios y c.e.

Analizamos luego las vinculaciones entre nuestra definición de *Chaitin*-reducciones y otros resultados ya conocidos en el contexto de la teoría algorítmica de la inforamción. Uno de ellos es la definición de *strong simulation*, dada por Calude et al. [6]. Algunas propiedades de esta relación se usaron para probar resultados intermedios a partir de los cuales Slaman obtuvo su importante resultado. Esto nos lleva a plantearnos:

Pregunta 3 *¿Es posible obtener una caracterización de los reales aleatorios c.e. directamente de la relación de* strong simulation*?*

Nuevamente, la respuesta es sí, e incluimos esta segunda caracterización como parte de este trabajo. A partir de estas dos caracterizaciones, podemos decir que un real aleatorio c.e. es la medida asociada a un conjunto que contiene, para cada programa para la máquina autodelimitante universal U fijada, una cadena de aproximadamente la misma longitud.

Las definiciones de *strong simulation* y *Chaitin*-reducciones son formalmente similares, en el sentido de que ambas relaciones establecen restricciones sobre las longitudes de las palabras en los conjuntos involucrados. Esta similitud nos sugiere, entonces, investigar la existencia de vinculaciones entre ambas:

Pregunta 4 *¿Qué relación hay entre la* Chaitin*-reducción que definimos y la reducción de* strong simulation*?*

En este caso, demostramos que una es inversa de la otra. Más formalmente, dados dos conjuntos A y B, A es *Chaitin*-reducible a B si y sólo si B simula fuertemente a A.

Una última cuestión relacionada con resultados conocidos se refiere al ya mencionado Teorema de Slaman: "todo número real aleatorio c.e. es la probabilidad de detención de una máquina autodelimitante universal". En vistas de las caracterizaciones que presentamos, nos preguntamos:

Pregunta 5 *¿Es posible demostrar el Teorema de Slaman a partir de los resultados obtenidos?*

Sí, efectivamente. Damos dos demostraciones de este Teorema, una basada en *Chaitin*-reducciones y la otra en *strong simulation*. Y hacemos notar que ambas pruebas usan solamente conceptos de la teoría algorítmica de la información. La demostración original, en cambio, se basa en la teoría de la medida constructiva y sigue la definición de aleatoriedad de Martin-Löf, centrándose en la presentación de un test constructivo de aleatoriedad.

Finalmente, en la teoría de funciones recursivas, es usual extender los resultados a niveles arbitrarios en la jerarquía aritmética. Este es también el caso para nuestro trabajo. Lo concluímos, entonces, enunciando una versión de nuestros resultados relativizada a oráculos dentro de la jerarquía aritmética. En particular, las demostraciones de aleatoriedad dadas en [11, 2] y [1] para los reales α y β, respectivamente, son instancias de nuestro resultado relativizado.

El trabajo está organizado como sigue: en la Sección 2 se introduce la notación y conceptos teóricos básicos; en la Sección 3 se presenta la caracterización en base a *Chaitin*-reducciones; la Sección 4 contiene vinculaciones con resultados conocidos; en la Sección 5 se enuncia la versión relativizada de nuestro trabajo y se muestra su aplicación para los casos particulares de los reales α y β; y en la Sección 6 exponemos conclusiones y continuamos con la lista de preguntas aquí iniciada, para incluír cuestiones aún no resueltas referidas a este tema.

2 Preliminares

Comenzamos con algunas definiciones y resultados, tanto para fijar notación como para repasar los conceptos básicos que usamos. Se asumen conocidos los fundamentos de la teoría de funciones recursivas (ver, por ejemplo, los capítulos iniciales de [15, 16, 17]).

2.1 Definiciones básicas

$\mathbb{N}$, $\mathbb{Q}$ y $\mathbb{R}$ denotan los conjuntos de números naturales, racionales y reales, respectivamente. Trabajamos con el alfabeto binario $\Sigma = \{0, 1\}$. Σ^* es el conjunto de todas las *palabras* o *cadenas* (finitas) sobre el alfabeto Σ. Σ^ω es el conjunto de todas las *secuencias* (infinitas) sobre Σ. Σ^∞ es el conjunto de todas las cadenas y secuencias de elementos de Σ, es decir, $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$.

λ es la cadena vacía. Si $w \in \Sigma^*$, $|w|$ indica la longitud de w. Por ejemplo, $|\lambda| = 0$. Si $v, w \in \Sigma^*$, vw denota la concatenación de las palabras v y w. Si $w \in \Sigma^*$ y $\mathbf{x} \in \Sigma^\omega$, $w\mathbf{x}$ es la secuencia infinita formada anteponiendo la cadena w a la secuencia $\mathbf{x}$.

Fijamos el orden $0 < 1$ para los elementos de Σ, y llamamos *orden cuasilexicográfico* al orden generado sobre Σ^*:

$$\lambda < 0 < 1 < 00 < 01 < 10 < 11 < 000 < 001 < 010 < 011...$$

En base a este orden, definimos la biyección recursiva $string : \mathbb{N} \to \Sigma^*$ de la siguiente manera: $string(i) = w$ sii w es la i-ésima cadena en el orden cuasilexicográfico sobre Σ^*.

Decimos que una palabra v es *prefijo* de otra palabra w, y lo notamos $v \preceq w$, si existe $x \in \Sigma^*$ tal que $vx = w$. Escribimos $v \prec w$ si v es un prefijo

propio de w, es decir, si $v \preceq w$ pero $v \neq w$ (o, equivalentemente, si $vx = w$ entonces $x \neq \lambda$). La relación $\preceq$ induce un orden parcial sobre Σ^*.

Si $\mathbf{x} \in \Sigma^\omega$, la notación $\mathbf{x}_i$, con $i \in \mathbb{N}$, representa el segmento inicial de $\mathbf{x}$ de longitud i, es decir, $\mathbf{x}_i \in \Sigma^*$ y $\mathbf{x}_i = w$ sii $|w| = i$ y $w \preceq \mathbf{x}$.

Las secuencias binarias infinitas pueden identificarse con los números reales en el intervalo $[0, 1]$, si se toma cada secuencia como la expansión binaria de un número real. Así, cada real se corresponde con una secuencia en Σ^ω. Los números racionales diádicos, de la forma $k2^{-i}$, para $k, i \in \mathbb{N}$ (y $k \leq 2^i$), se pueden asociar con dos diferentes secuencias: una que termina con infinitos 0's y la otra con infinitos 1's. Cuando se requiera una identificación única, preferimos la asociación con la secuencia terminada con infinitos 1's. En base a esta correspondencia, nos referimos indistintamente a los elementos de $\mathbb{R}$ y a los de Σ^ω.

Sea $\mathbf{C} \subseteq \Sigma^\omega$ un conjunto medible. La *medida de Lebesgue*, como es usual, se indica con $\mu(\mathbf{C})$ y representa la probabilidad de que una secuencia arbitraria pertenezca a $\mathbf{C}$. Si $A \subseteq \Sigma^*$, $A\Sigma^\omega$ denota el conjunto de secuencias que tienen un prefijo en A: $A\Sigma^\omega = \{w\mathbf{x}/w \in A \wedge \mathbf{x} \in \Sigma^\omega\}$. Los conjuntos $A\Sigma^\omega$, con $A \subseteq \Sigma^*$, son los conjuntos abiertos en la topología natural sobre Σ^ω y por lo tanto son medibles. En este caso, decimos que $\mu(A\Sigma^\omega)$ es la *medida asociada a* A. Por ejemplo, si $A = \{w\}$, con $w \in \Sigma^*$, $A\Sigma^\omega = \{w\}\Sigma^\omega$ es el conjunto de todas las secuencias que comienzan con w y la medida asociada a A es $\mu(\{w\}\Sigma^\omega) = 2^{-|w|}$.

Para un conjunto $A \subseteq \Sigma^*$, nos referiremos frecuentemente a la suma $\sum_{w \in A} 2^{-|w|}$. La convergencia de esta suma depende del conjunto A considerado. En los casos en que converja, para simplificar notación, llamamos $m(A)$ al número real igual al valor de dicha suma: $m(A) = \sum_{w \in A} 2^{-|w|}$. En el ejemplo citado, $A = \{w\}$, $m(\{w\}) = 2^{-|w|} = \mu(\{w\}\Sigma^\omega)$.

Un conjunto $A \subset \Sigma^*$ se dice *libre de prefijos* si ninguna extensión propia de elementos del conjunto pertenece al conjunto. Es decir, A es libre de prefijos sii para todo $w, x \in \Sigma^*$, si $w \in A$ y $x \neq \lambda$ entonces $wx \notin A$. Para un conjunto libre de prefijos es posible expresar convenientemente la medida del conjunto de todas las secuencias que son extensiones de cadenas en dicho conjunto: si $A \subset \Sigma^*$ es libre de prefijos, entonces $\sum_{w \in A} 2^{-|w|}$ converge y $\mu(A\Sigma^\omega) = m(A)$. Notemos que, en el ejemplo que dimos, $A = \{w\}$ es libre de prefijos, y por lo tanto debía ser $\mu(\{w\}\Sigma^\omega) = m(\{w\})$. Además, los conjuntos libres de prefijos satisfacen la desigualdad de Kraft [12]: si $A \subset \Sigma^*$ es libre de prefijos, entonces se cumple que $0 \leq \mu(A\Sigma^\omega) = m(A) \leq 1$.

Sean A, B conjuntos y $f : A \to B$ una función. Como es usual, si $a \in A$, escribimos $f(a) \downarrow$ para indicar que f está definida en a, y $f(a) \uparrow$ en caso contrario. El dominio de f es el conjunto $Dom(f) = \{a \in A/f(a) \downarrow\}$, y el rango de f es el conjunto $Rango(f) = \{f(a) \in B/f(a) \downarrow\}$. Si f, g son funciones en números naturales, notamos $f(n) = g(n) + O(1)$ si existe una constante positiva c tal que para todo n, $f(n) \leq g(n) + c$.

2.2 Máquinas de Turing, reducciones y oráculos

Una *máquina de Turing* es una función recursiva parcial $M : \Sigma^* \to \Sigma^*$. El dominio de M se considera una familia de programas y el valor de $M(p)$, si existe, es la salida del programa p. Para representar programas que toman argumentos para realizar su cómputo, fijamos una biyección recursiva $\langle ., . \rangle : \Sigma^* \times \Sigma^* \to \Sigma^*$ y usamos la convención $M(pa_1a_2 \dots a_n) = M(\langle p, \langle a_1, \dots \langle a_{n-1}, a_n \rangle \rangle \dots \rangle)$.

Una máquina de Turing es *universal* si puede simular el comportamiento de cualquier otra máquina de Turing. Es decir, dada una enumeración fija M_i, con $i \geq 0$, de todas las máquinas de Turing, M_U es universal si existe una función recursiva $f : I\!N \times \Sigma^* \to \Sigma^*$, que *codifica* a cada máquina en la enumeración, tal que $M_U(f(i, p)) = M_i(p)$. Por ejemplo, la máquina M_U dada por $M_U(\langle string_i, p \rangle) = M_i(p)$ es una máquina de Turing universal.

El problema clásico de la teoría de la computabilidad, demostrado algorítmicamente insoluble, es el de la detención de una máquina de Turing universal: el conjunto $K = \{x \in \Sigma^* / M_U(\langle x, x \rangle) \downarrow\}$ no es computable. El problema de la detención es un problema representativo de una clase de problemas insolubles y constituye una herramienta clave para la demostración de numerosos resultados de (in)computabilidad.

Presentamos ahora una clase de relaciones entre conjuntos de cadenas llamadas *reducciones*:

Definición 1 *Una relación $\leq_R$ entre subconjuntos de Σ^* es una* reducción *si verifica:*

(Reflexiva) $\forall A \subseteq \Sigma^* (A \leq_R A)$

(Transitiva) $\forall A, B, C \subseteq \Sigma^* (A \leq_R B \wedge B \leq_R C \Rightarrow A \leq_R C)$

Si A y B son conjuntos tales que $A \leq_R B$ decimos que A es *R-reducible* a B o que $\leq_R$ es una *R-reducción* de A en B. A y B son *R-equivalentes*, y lo notamos $A \equiv_R B$, si $A \leq_R B$ y $B \leq_R A$. Y escribimos $A <_R B$ para indicar que $A \leq_R B$ pero $B \not\leq_R A$.

Veamos un ejemplo de este tipo de relaciones: si A, B son conjuntos de cadenas binarias, A es *Turing-reducible* a B ($A \leq_T B$) si el predicado $x \in A$ es recursivo, para cada $x \in \Sigma^*$, cuando se conoce si $w \in B$ ó $w \notin B$ para toda cadena $w \in \Sigma^*$.

Un caso particular de Turing-reducciones que vamos a usar en este trabajo es el siguiente:

Definición 2 *A es* 1-reducible *a B ($A \leq_1 B$) si existe una función 1-1 recursiva f tal que para todo x, $x \in A \Leftrightarrow f(x) \in B$.*

Es fácil ver que tanto $\leq_T$ como $\leq_1$ son reducciones.

El orden parcial $<_T$ da una clasificación de los conjuntos de cadenas binarias de acuerdo a su dificultad desde el punto de vista de la computabilidad: si $A <_T B$, entonces B es "más insoluble" que A. Para el caso de las 1-reducciones, los conjuntos equivalentes bajo esta relación reciben una denominación particular: si $A \equiv_1 B$ se dice que A y B son *recursivamente isomorfos*.

Dada una clase de conjuntos y una reducción $\leq_R$, podemos considerar a algunos de ellos como elementos "destacados" dentro de la clase, con respecto a la reducción $\leq_R$:

Definición 3 *Sea $\mathcal{W}$ una colección de subconjuntos de Σ^* y $\leq_R$ una reducción. Un conjunto $A \in \mathcal{W}$ es* R-completo para $\mathcal{W}$ *si para todo conjunto $B \in \mathcal{W}$, $B \leq_R A$.*

Un conjunto R-completo para $\mathcal{W}$ puede interpretarse como un representante de dicha clase: todos los demás conjuntos en $\mathcal{W}$ son R-reduccibles a él. Un ejemplo de este tipo de conjuntos es el conjunto asociado al problema de la detención, K, que es 1-completo para la clase de los conjuntos c.e.

Ante la existencia de problemas que no tienen solución algorítmica, como el de la detención, es natural preguntarse qué funciones (o conjuntos) se volverían computables si se dispusiera de un procedimiento externo o "caja negra" capaz de decidirlos. Por supuesto, este procedimiento, que llamaremos *oráculo*, no puede darse por medio de un algoritmo. Como respuesta a esta cuestión, surge el concepto de *computabilidad relativa*.

Un *oráculo* X es un subconjunto de Σ^*. Una máquina de Turing con oráculo X es una función $M^X : \Sigma^* \to \Sigma^*$ recursiva parcial dada la función característica de X

$$\mathcal{C}_X(w) = \begin{cases} 1 & \text{si } w \in X \\ 0 & \text{si } w \notin X \end{cases}$$

Es decir, una máquina de Turing con oráculo X es una máquina a la que se le proporciona, externamente, la información para decidir la pertenencia de una cadena arbitraria a X. La máquina puede acceder a esta información durante la ejecución de su cómputo mediante instrucciones especiales de consulta al oráculo. Notemos que las máquinas de Turing sin oráculos son un caso particular de las máquinas con oráculos, donde el oráculo considerado es el conjunto $X = \emptyset$.

La mayoría de los resultados clásicos de computabilidad pueden relativizarse. Una función o un conjunto que pueden computarse en una máquina con oráculo X se dicen X-*recursivos* o *recursivos relativos a* X (y con esta notación, $A \leq_T B$ sii A es B-recursivo). Un conjunto que puede enumerarse en una máquina con oráculo X se dice X-*computablemente enumerable* (X-*c.e.*) o *computablemente enumerable* en X. Para cada X, existen

máquinas universales M_U^X, y podemos relativizar el problema de la detención: $K^X = \{w \in \Sigma^* / M_U^X(\langle w, w \rangle) \downarrow\}$.

El problema de la detención relativizado puede usarse para definir un operador que permite obtener una jerarquía de problemas cada uno de los cuales es "más insoluble" que el precedente:

Definición 4 *Sea $X \subseteq \Sigma^*$.*

1. *El* salto *de X, X', es el conjunto*

$$X' = \{string_i / M_i^X(string(i)) \downarrow, i \in I\!N\}$$

2. *El n-ésimo* salto *de X, $X^{(n)}$, se obtiene iterando el salto n veces:*

$$X^0 = X,\ X^{(n+1)} = (X^{(n)})'$$

Observemos que, con la notación dada por la definición anterior, $K = \emptyset'$ y, en general, $K^{(n)} = \emptyset^{(n+1)}$.

El resultado de aplicar el operador de salto a un conjunto X es un conjunto más difícil que X desde el punto de vista de la computabilidad: si $X \subseteq \Sigma^*$, X' es X-c.e. pero no X-recursivo. Y como X es X'-recursivo, resulta que $X <_T X'$. Así, la aplicación iterada del operador de salto a X genera una familia de conjuntos cuyo grado de insolubilidad es creciente:

$$X <_T X' <_T X'' <_T \ldots <_T X^{(n)} <_T \ldots$$

La noción de computabilidad relativa permite definir otra jerarquía para clasificar problemas insolubles:

Definición 5 (Jerarquía aritmética relativa a X) *Sea $X \subseteq \Sigma^*$.*

1. *(a)* $\Sigma_0^{0,X} = \{A \subseteq \Sigma^* / A$ *es X-recursivo*$\}$
   (b) $\Sigma_{n+1}^{0,X} = \{A \subseteq \Sigma^* / A$ *es B-recursivo para algún* $B \in \Sigma_n^{0,X}\}$
2. $\Pi_n^{0,X} = \{A \subseteq \Sigma^* / \overline{A} \in \Sigma_n^{0,X}\}$
3. $\Delta_n^{0,X} = \Sigma_n^{0,X} \cap \Pi_n^{0,X}$

Cuando $X = \emptyset$, usamos la notación habitual Σ_n^0, Π_n^0 y Δ_n^0, y estas clases se conocen como *jerarquía aritmética*. Por ejemplo, Δ_1^0 es la clase de conjuntos recursivos y Σ_1^0 es la clase de conjuntos c.e.

El siguiente resultado muestra que las clases $\Sigma_n^{0,X}$, $\Pi_n^{0,X}$ y $\Delta_n^{0,X}$ que hemos definido efectivamente forman una jerarquía:

Teorema 6 (Kleene) *Para todo $n \in \mathbb{N}$ y $X \subseteq \Sigma^*$:*

1. $\Delta_n^{0,X} \subset \Sigma_n^{0,X}$, $\Delta_n^{0,X} \subset \Pi_n^{0,X}$
2. $\Sigma_n^{0,X} \subset \Sigma_{n+1}^{0,X}$, $\Pi_n^{0,X} \subset \Pi_{n+1}^{0,X}$
3. $\Sigma_n^{0,X} \cup \Pi_n^{0,X} \subset \Delta_{n+1}^{0,X}$

La jerarquía aritmética y la generada por la iteración del operador de salto están relacionadas:

Teorema 7 (Post) *Para todo $n \in \mathbb{N}$:*

1. $\emptyset^{(n)}$ *es* 1*-completo para* Σ_n^0
2. $\forall A \subseteq \Sigma^*$, $A \in \Sigma_{n+1}^0$ *sii* A *es* $\emptyset^{(n)}$*-c.e.*
3. $\forall A \subseteq \Sigma^*$, $A \in \Delta_{n+1}^0$ *sii* $A \leq_T \emptyset^{(n)}$

Este importante resultado nos dice que $\emptyset^{(n)}$ es un representante para la clase Σ_n^0 con respecto a 1-reducciones. Vamos a usar una notación abreviada para estos oráculos destacados: decimos que un conjunto A es n-c.e. (n-recursivo) si A es $\emptyset^{(n)}$-c.e. ($\emptyset^{(n)}$-recursivo), que una función f es n-recursiva si f es $\emptyset^{(n)}$-recursiva, y que una máquina M^n es una máquina con oráculo $\emptyset^{(n)}$.

2.3 Máquinas autodelimitantes. Complejidad de largo de programa

Chaitin [8] define una versión de máquina de Turing en la cual el espacio de programas es un espacio probabilístico, con todos los símbolos del alfabeto distribuidos uniformemente. Esta condición no permite que haya un blanco al final del programa, ni ninguna otra forma externa de delimitación. Por lo tanto, el programa debe contener dentro de sí mismo la información necesaria para saber dónde termina, de manera que la máquina pueda determinar en qué momento debe detener la lectura de bits del programa. Esto es lo que significa que una computadora sea "autodelimitante".

Los conjuntos libres de prefijos satisfacen la propiedad de decodificación única e instantánea: si $A \subset \Sigma^*$ es un conjunto libre de prefijos y $\mathbf{x} \in \Sigma^\omega$, entonces es posible detectar si existe $w \in A$ tal que $w \preceq \mathbf{x}$, leyendo de izquierda a derecha los símbolos de $\mathbf{x}$ exactamente hasta $|w|$. En este sentido, el comportamiento de una máquina cuyo dominio es un conjunto libre de prefijos se corresponde con el comportamiento de una máquina autodelimitante:

Definición 8 (Chaitin [8]) *Una* máquina autodelimitante *es una función recursiva parcial $C : \Sigma^* \to \Sigma^*$ tal que $Dom(C)$ es un conjunto libre de prefijos.*

Observemos que para una máquina autodelimitante C, $\mu(Dom(C)\Sigma^\omega) = m(Dom(C))$, y entonces $m(Dom(C))$ representa la probabilidad de que C se detenga cuando su entrada se genera en forma aleatoria.

A excepción de la restricción de que su dominio debe ser libre de prefijos, las máquinas autodelimitantes son máquinas de Turing ordinarias, y tienen exactamente el mismo poder computacional. En particular, se mantiene el concepto de máquinas universales: dada una enumeración fija de todas las máquinas autodelimitantes, y llamando C_i a la i-ésima máquina en la enumeración, una máquina autodelimitante U es *universal* si existe una codificación recursiva $f : \mathbb{N} \times \Sigma^* \to \Sigma^*$ tal que $U(f(i,p)) = C_i(p)$ para todo programa p.

Chaitin [8] da una definición alternativa de universalidad:

Definición 9 (Chaitin [8]) *Una máquina autodelimitante U es* universal de Chaitin *si para toda máquina autodelimitante C_i existe una constante $c_i \geq 0$ tal que para todo programa p existe un programa p' que verifica: $U(p') = C_i(p)$, con $|p'| \leq |p| + c_i$.*

En adelante, cuando hablemos de máquinas nos referimos a máquinas autodelimitantes, y cuando hablemos de máquinas universales asumimos que verifican tanto la noción de universalidad clásica como la dada por Chaitin. Además, fijaremos una máquina universal $U : \Sigma^* \to \Sigma^*$, definida por $U(0^i 1p) = C_i(p)$ para todo $p \in \Sigma^*$, que será la máquina de referencia que usaremos en el resto de este trabajo.

La *complejidad algorítmica* o *de largo de programa* [8] en una máquina autodelimitante C es una función $H_C : \Sigma^* \to \mathbb{N}$ que mapea una cadena w en la longitud del programa más corto que produce como salida a w:

$$H_C(w) = \begin{cases} \min\{|p| / C(p) = w\} & \text{si } w \in Rango(C) \\ \infty & \text{en caso contrario} \end{cases}$$

La función H_C no es recursiva. Cuando C es una máquina universal, H_C es total y $H_C(w) \leq |w| + H_C(|w|) + O(1) \leq |w| + 2\log(|w|) + O(1)$, donde $\log(n) = \lceil \log_2(n) \rceil$, para $n \in \mathbb{N}$. Esta cota superior se obtiene considerando un programa que contiene explícitamente la cadena w además de una codificación de su longitud. Para $n \in \mathbb{N}$, la codificación $11b_1b_1b_2b_2 \ldots b_kb_k01$ (donde $1b_1b_2 \ldots b_k$ es la expresión binaria de n sin 0's a la izquierda) permite obtener la cota $H(n) \leq 2\log(n)$ para su complejidad de largo de programa.

Podemos interpretar a la complejidad de w en una máquina C como una medida de la mínima cantidad de información necesaria para obtener w en la máquina C. Es decir, puede pensarse que $H_C(w)$ representa el contenido de información de w.

Una máquina autodelimitante C es *asintóticamente óptima* si y sólo si para cualquier máquina autodelimitante C_i existe una constante c_i tal que

para toda cadena w, $H_C(w) \leq H_{C_i}(w) + c_i$. Las máquinas autodelimitantes universales de Chaitin son asintóticamente óptimas:

Proposición 10 *Si V es una máquina autodelimitante universal de Chaitin, entonces V es asintóticamente óptima.*

DEMOSTRACIÓN. Como V es universal, para toda C existe sim_C tal que para todo p existe p' con $V(p') = C(p)$ y $|p'| \leq |p| + sim_C$. Sea $w \in \Sigma^*$. Si $w \notin Rango(C)$ entonces $H_C(w) = \infty$ y claramente, para cualquier c, $H_V(w) \leq H_C(w) + c$. Si $w \in Rango(C)$, entonces para todo p tal que $C(p) = w$, existe p' tal que $V(p') = w$ y $|p'| \leq |p| + sim_C$. Luego, $H_V(w) \leq H_C(w) + sim_C$, como queríamos. $\otimes$

Para la máquina universal U que fijamos, la constante c_i es igual a $i+1$, ya que se cumple que para toda máquina autodelimitante C_i y para toda cadena w, $H_U(w) \leq H_{C_i}(w) + i + 1$.

Una importante propiedad que verifican las máquinas autodelimitantes asintóticamente óptimas está dada por el siguiente resultado:

Teorema 11 (Teorema de Invarianza, Chaitin [7]) *Sean U_1 y U_2 dos máquinas autodelimitantes asintóticamente óptimas cualesquiera. Existe una constante c tal que para toda cadena w, $|H_{U_1}(w) - H_{U_2}(w)| \leq c$.*

Este resultado expresa que la complejidad de largo de programa de una cadena es, dentro de un término constante, independiente de la máquina autodelimitante asintóticamente óptima elegida. Y en este sentido, la complejidad de largo de programa en máquinas asintóticamente óptimas puede pensarse como una medida absoluta de complejidad.

El dominio de las máquinas autodelimitantes es un conjunto libre de prefijos y, como ya mencionamos, los conjuntos libres de prefijos satisfacen la desigualdad de Kraft. La recíproca no es cierta, pero sí se cumple la versión débil que presentamos a continuación. Consideremos una lista c.e. de pares $(n_i, w_i)_{i \in \mathbb{N}}$, donde $n_i \in \mathbb{N}$ y $w_i \in \Sigma^*$ para todo i. Llamamos a estos pares *requerimientos* y decimos que son *consistentes* si $\sum_{i \in \mathbb{N}} 2^{-n_i} \leq 1$. Una máquina C *satisface* los requerimientos si, para cada requerimiento (n_i, w_i) en la lista, existe exactamente un progama p_i para C tal que $|p_i| = n_i$ y $C(p_i) = w_i$. El resultado que anticipamos garantiza, dada una lista de requerimientos, la existencia de una computadora C que los satisface:

Teorema 12 (Desigualdad de Kraft-Chaitin [10]) *Sea*

$$\mathcal{L} = \{(n_i, w_i) / n_i \in \mathbb{N} \wedge w_i \in \Sigma^* \forall i \in \mathbb{N}\}$$

una lista c.e. de requerimientos consistentes. Existe una máquina autodelimitante C que satisface los requerimientos en $\mathcal{L}$.

La demostración de este Teorema efectivamente muestra la construcción de C a partir de la enumeración de $\mathcal{L}$. Se dice que la máquina C está *determinada* por los requerimientos. En este trabajo vamos a usar una consecuencia de este resultado: dada una lista c.e. de longitudes $(n_i)_{i\in\mathbb{N}}$ tal que $\sum_{i\in\mathbb{N}} 2^{-n_i} \leq 1$, existe un conjunto libre de prefijos que contiene exactamente una palabra w_i para cada n_i en la lista, con $|w_i| = n_i$.

Damos ahora algunas convenciones de notación que usamos. Con $H(w)$ indicamos la complejidad $H_U(w)$ de una cadena w en la máquina universal U de referencia. Como en el caso de las máquinas de Turing, las definiciones de la presente sección se pueden relativizar de manera inmediata. Si $X \subseteq \Sigma^*$, escribimos C^X para indicar una computadora con oráculo X, U^X para la máquina universal de referencia con oráculo X (en particular, fijamos $U^X(0^i1p) = C_i^X(p)$ para todo $p \in \Sigma^*$, donde $(C_i^X)_{i\in\mathbb{N}}$ es una enumeración de todas las máquinas autodelimitantes con oráculo X). Notamos H_{C^X} para la complejidad con respecto a C^X y H^X para la complejidad en U^X. Consideramos el caso particular de los oráculos $\emptyset^{(n)}$ y usamos las convenciones $C^n = C^{\emptyset^{(n)}}$, $U^n = U^{\emptyset^{(n)}}$ y $H^n = H^{\emptyset^{(n)}}$.

Notemos que, como se esperaría, la ayuda de un oráculo puede contribuir a disminuir la complejidad de largo de programa:

Proposición 13 *Para todo $X \subseteq \Sigma^*$ existe una constante c tal que para toda cadena w, $H^{X'}(w) \leq H^X(w) + c$.*

Demostración. Como hemos visto, X es X'-recursivo para todo X. Luego, existe una máquina $C^{X'}$ que se comporta exactamente igual que U^X: cuando no se consulta al oráculo, realiza el cómputo de la misma manera que U^X, y cuando se consulta al oráculo, obtiene la respuesta computando X a partir de X'. Por lo tanto, para toda cadena w, $H_{C^{X'}}(w) = H^X(w)$. Y en consecuencia, como $U^{X'}$ es asintóticamente óptima, $H^{X'}(w) \leq H^X(w) + c$. ⊗

Como veremos más adelante, este resultado, para el caso particular de los oráculos $\emptyset^{(n)}$, permite una clasificación jerárquica de los números reales de acuerdo a la complejidad de largo de programa de los prefijos de la secuencia correspondiente a su expansión binaria.

2.4 Reales computablemente enumerables (c.e.)

Vamos a considerar una clase particular de números reales: los que podemos obtener o aproximar mediante computadoras. Presentamos ahora las definiciones y propiedades para esta clase de números.

Definición 14 *Una secuencia de racionales $(q_i)_{i\in\mathbb{N}}$ es* computable *si existe una función recursiva $f : \mathbb{N} \to \mathbb{Q}$ tal que, para todo n, $f(n) = q_n$.*

Definición 15 *Una secuencia de racionales convergente* $(q_i)_{i\in\mathbb{N}}$ *se dice que* converge computablemente *si existe una función computable* $g : \mathbb{N} \to \mathbb{N}$ *tal que, para todo* j *y para todo* $i \geq g(j)$, $|q - q_i| \leq 2^{-j}$ *(donde* $q = \lim_{n\to\infty} q_n$*).*

Podemos ahora definir:

Definición 16 $\mathbf{r} \in \mathbb{R}$ *es* computable *si existe una secuencia computable de racionales que converge computablemente a* $\mathbf{r}$*.*

Definición 17 $\mathbf{r} \in \mathbb{R}$ *es* computablemente enumerable (c.e.) *si existe una secuencia de racionales computable y creciente que converge a* $\mathbf{r}$*.*

Notemos que, si $\mathbf{x}$ es la secuencia infinita correspondiente a la expansión fraccional de $\mathbf{r}$, entonces $\mathbf{r}$ es computable sii existe una función recursiva $f : \mathbb{N} \to \Sigma^*$ tal que, para todo $n \in \mathbb{N}$, $f(n) = \mathbf{x}_n$, y $\mathbf{r}$ es c.e. sii existe una función recursiva $f : \mathbb{N} \to \Sigma^*$ tal que, para todo $n \in \mathbb{N}$, $f(n) \leq \mathbf{x}_n$ (pero no es decidible si la vale la igualdad o la desigualdad estricta).

Por ejemplo, los racionales, $0.010010001\ldots$, π y e son computables, y las medidas asociadas a conjuntos libres de prefijos c.e. son reales c.e. (en efecto, si A es libre de prefijos c.e. y $\mathbf{r} = m(A) = \sum_{i\in\mathbb{N}} 2^{-|a_i|}$, con $(a_i)_{i\in\mathbb{N}}$ una enumeración recursiva de A, entonces la sucesión de racionales dada por $q_n = \sum_{i=0}^{n} 2^{-|a_i|}$ es computable, creciente y convergente a $\mathbf{r}$, y por lo tanto $\mathbf{r}$ es c.e.).

La complejidad de largo de programa de los prefijos de la secuencia correspondiente a la expansión binaria de un real computable es baja: si $0.\mathbf{r}$ es computable, existe una máquina C tal que $C(n) = \mathbf{r}_n$ y por lo tanto, existe una constante c tal que $H(\mathbf{r}_n) \leq H(n) + c \leq 2\log(n) + c$. En cambio, si $0.\mathbf{r}$ es un real c.e., sabemos que existe una aproximación computable a $0.\mathbf{r}$, pero la convergencia de la aproximación no es computable, con lo cual no es directo hallar una cota para la complejidad de largo de programa de los prefijos de su expansión binaria.

Para comparar el contenido de información entre números reales c.e., Solovay [18] define la relación de *dominación*:

Definición 18 (Solovay [18]) *Un real* $\mathbf{a}$ domina *a un real* $\mathbf{b}$ *si existe una función computable parcial* $f : \mathbb{Q} \to \mathbb{Q}$ *y una constante* $c > 0$ *con la propiedad de que si* p *es un racional menor que* $\mathbf{a}$*, entonces* $f(p)$ *(está definida) y es menor que* $\mathbf{b}$ *y satisface la desigualdad:*

$$c(\mathbf{a} - p) \geq \mathbf{b} - f(p)$$

En este caso escribimos $\mathbf{a} \geq_{dom} \mathbf{b}$ o $\mathbf{b} \leq_{dom} \mathbf{a}$.

Intuitivamente, un real $\mathbf{a}$ domina a un real $\mathbf{b}$ si a partir de una buena aproximación desde abajo para $\mathbf{a}$ es posible obtener efectivamente una buena

aproximación desde abajo para **b**. Para el caso de los reales c.e., que son los que consideramos en este trabajo, la definición anterior puede expresarse de la siguiente manera:

Lema 19 (Calude [5]) *Un real c.e.* **a** *domina a un real c.e.* **b** *sii existen secuencias de racionales* (a_i) *y* (b_i) *computables crecientes (o no decrecientes), y una constante* c *tales que* $\lim_{n\to\infty} a_n = \mathbf{a}$, $\lim_{n\to\infty} b_n = \mathbf{b}$ *y* $c(\mathbf{a} - a_n) \geq \mathbf{b} - b_n$, *para todo* n.

El siguiente resultado vincula la relación de dominación con la complejidad de largo de programa:

Teorema 20 (Solovay [18]) *Sean* $\mathbf{x}, \mathbf{y} \in \Sigma^\omega$ *dos secuencias binarias infinitas tales que tanto* $0.\mathbf{x}$ *como* $0.\mathbf{y}$ *son c.e. y* $0.\mathbf{x} \geq_{dom} 0.\mathbf{y}$. *Entonces* $H(\mathbf{y}_i) \leq H(\mathbf{x}_i) + O(1)$.

Es decir, si $0.\mathbf{x} \geq_{dom} 0.\mathbf{y}$, entonces la complejidad de largo de programa de **y** no puede ser mayor que la de **x**.

Como antes, estas definiciones y resultados pueden relativizarse. Damos la notación que usamos para el caso de los oráculos en la jerarquía aritmética $\emptyset^{(n)}$. Consideramos las secuencias de racionales n-computables y las que convergen n-computablemente, modificando las definiciones 14 y 15 de manera que las funciones involucradas sean n-recursivas en lugar de recursivas, para obtener las definiciones de reales n-computables y n-c.e. De manera similar, la definición de dominación se extiende a n-dominación y escribimos $\mathbf{a} \geq^n_{dom} \mathbf{b}$ si **a** n-domina a **b**. Por último, el Teorema 20 se relativiza para reales n-c.e. y relaciona la n-dominación con H^n, la complejidad de largo de programa en U^n.

Observemos que un real n-c.e. es $(n+1)$-recursivo: si **r** es n-c.e. entonces $\{q \in \mathbb{Q} / q < \mathbf{r}\}$ es n-c.e., y por el Teorema 6, este conjunto es $(n+1)$-recursivo. Luego, dado i, es posible obtener de manera $(n+1)$-recursiva un racional q tal que $q + 2^{-i} \leq \mathbf{r}$. Por lo tanto, de esta manera se obtiene una secuencia de racionales computable creciente y que converge computablemente a **r**.

En este trabajo consideramos racionales y reales en el intervalo $[0, 1]$, representados en base 2. Así, una cadena binaria o una secuencia binaria terminada en infinitos dígitos binarios iguales se puede interpretar como un racional diádico en $[0, 1]$: la cadena $b_1 b_2 \ldots b_n$ se asocia con el racional $\sum_{i=1}^n b_i 2^{-i}$, y las secuencias $b_1 b_2 \ldots b_n 0111\ldots$ y $b_1 b_2 \ldots b_n 1000\ldots$, con $\sum_{i=1}^n b_i 2^{-i} + 2^{-(n+1)}$. Y cualquier otra secuencia binaria infinita se corresponde con un único racional o real en el mismo intervalo: el número asociado a la secuencia $b_1 b_2 \ldots$ es $\sum_{i=0}^\infty b_i 2^{-i}$.

2.5 Aleatoriedad

Chaitin [8] define la noción de aleatoriedad, o falta de estructura, para una secuencia binaria en base a la incompresibilidad algorítmica de sus prefijos. Cualquier estructura o regularidad en una cadena podría usarse para comprimirla mediante un programa de tamaño mucho menor que la produzca como salida. Una secuencia es aleatoria si sus prefijos tienen esencialmente la misma longitud que el programa más corto para generarlos:

Definición 21 (Chaitin [8]) *Una secuencia* $\mathbf{x} \in \Sigma^\omega$ *es* aleatoria *si existe una constante* $c \geq 0$ *tal que para todo* $i \in \mathbb{N}$

$$H(\mathbf{x}_i) > i - c$$

Existe otra versión más fuerte de esta definición, igualmente debida a Chaitin [10], y otras definiciones dadas por Martin- Löf [14] y Solovay [18]. Sin embargo, todas ellas se demuestran equivalentes [10]. Por lo tanto, cuando hablemos de secuencias aleatorias nos referimos a la definición que hemos presentado.

Un número real en $[0, 1]$ es aleatorio si la secuencia correspondiente a su expansión binaria es aleatoria. La definición se da para el alfabeto binario $\Sigma = \{0, 1\}$ pero puede probarse que es invariante para cualquier alfabeto ([4]). Es decir, la propiedad de aleatoriedad es inherente al número y es independiente del sistema que se elija para representarlo.

En [10] se prueba que, con probabilidad 1, un número real es aleatorio. Sin embargo, no es sencillo dar un ejemplo de un número en esta clase. En [8], Chaitin presenta un número que es un ejemplo natural de real aleatorio: Ω, definido como la probabilidad de detención de una máquina autodelimitante universal:

$$\Omega = \sum_{p/U(p)\downarrow} 2^{-|p|}$$

Ω es aleatorio y c.e. La aleatoriedad de Ω surge del hecho de que codifica de manera muy compacta el problema de la detención: dados los primeros n bits de Ω, es posible decidir si $U(p) \downarrow$ para todos los programas p de longitud menor o igual que n.

La demostración de Chaitin, en realidad, está dada para la probabilidad de detención de *cualquier* máquina universal. Vamos a usar la denominación de Solovay:

Definición 22 (Solovay [18]) *Un real* $\mathbf{a}$ *en* $[0, 1]$ *es un* Ω-number *si existe una máquina autodelimitante universal* V *tal que* $\mathbf{a} = m(Dom(V)) = \Omega_V$.

Entonces, el fundamental resultado de Chaitin es el siguiente:

Teorema 23 (Chaitin [8]) *Sea* **a** *un real en* $[0,1]$. *Si* **a** *es un* Ω-number *entonces* **a** *es aleatorio y c.e.*

Los reales aleatorios c.e. son elementos maximales para la relación $\leq_{dom}$:

Lema 24 (Solovay-Calude) *Si* **a** *es aleatorio c.e., entonces* $\mathbf{a} \geq_{dom} \mathbf{b}$ *para todo* **b** *c.e.*

Este resultado, junto con el Teorema 20, nos dice que los reales aleatorios c.e. son los de mayor complejidad de largo de programa dentro de la clase de los números c.e.

Incluímos ahora las versiones relativizadas. La definición de n-aleatoriedad se obtiene considerando la complejidad H^n. Ω^n es la probabilidad de detención de U^n y un Ω^n-*number* es la medida asociada al dominio de una máquina n-universal. El Teorema de Chaitin (Teorema 23) se relativiza para obtener:

Teorema 25 (Chaitin) *Sea* **a** *un real en* $[0,1]$. *Si* **a** *es un* Ω^n-number, *entonces* **a** *es* n*-aleatorio y* n*-c.e.*

Y la relativización del Lema 24 establece la n-dominación de un real n-aleatorio n-c.e. sobre cualquier otro real n-c.e.

Finalmente, veamos que la jerarquía aritmética induce una jerarquía de aleatoriedad:

Proposición 26 *Sea* $\mathbf{r} \in [0,1]$. *Para todo* $n \in \mathbb{N}$, *si* $\mathbf{r}$ *es* $(n+1)$*-aleatorio, entonces* $\mathbf{r}$ *es* n*-aleatorio.*

Demostración. Como $\mathbf{r}$ es $(n+1)$-aleatorio, existe k tal que para todo i, $H^{n+1}(\mathbf{r}_i) > i - k$. Y por la Proposición 13, existe c tal que para toda w, $H^{n+1}(w) \leq H^n(w) + c$. Luego, $i - k < H^{n+1}(\mathbf{r}_i) \leq H^n(\mathbf{r}_i) + c$, es decir, $H^n(\mathbf{r}_i) > i - k - c$. Por lo tanto $\mathbf{r}$ es n-aleatorio. $\otimes$

Y si $\mathbf{r}$ es n-aleatorio n-c.e., entonces $\mathbf{r}$ es $(n+1)$-recursivo, con lo cual la familia dada por los reales n-aleatorios n-c.e., para cada $n \in \mathbb{N}$, forma una jerarquía con respecto al grado de aleatoriedad de los reales en cada nivel n. Un ejemplo lo constituyen las probabilidades de detención de máquinas n-universales, Ω^n: cada uno de ellos es n-aleatorio, n-c.e. y con un grado de aleatoriedad mayor que el precedente en la jerarquía.

3 Caracterización de reales aleatorios c.e.

3.1 Condiciones suficientes de aleatoriedad

Como ya mencionamos, Chaitin [10] demuestra que si V es una máquina autodelimitante universal, entonces $m(Dom(V))$ es aleatorio. Entonces nos preguntamos en qué casos puede aplicarse la demostración canónica de Chaitin para probar que la medida asociada a un conjunto de cadenas es aleatoria. En otras palabras, si A es un conjunto de cadenas, queremos establecer condiciones suficientes sobre A de manera que pueda usarse la estrategia de Chaitin para demostrar que $\mu(A\Sigma^\omega)$ es aleatorio.

Una condición simple que puede pedirse sobre A, y que podría esperarse que fuera suficiente, es que sea recursivamente isomorfo a $Dom(U)$. Sin embargo, la aleatoriedad no es una propiedad recursivamente invariante:

Proposición 27 *Existen conjuntos $A, B \subseteq \Sigma^*$ recursivamente isomorfos tales que $\mu(A\Sigma^\omega)$ es aleatorio y $\mu(B\Sigma^\omega)$ no lo es.*

Demostración. Consideremos $A = Dom(U)$ y $B = \{0^i 1 / U(string_i)\downarrow\}$. En primer lugar, veamos que $A \equiv_1 B$. En efecto, $string_i \in A$ si y sólo si $0^i 1 \in B$, luego las funciones $f, g : \Sigma^* \to \Sigma^*$ definidas como $f(string_i) = 0^i 1$ y $g(0^i 1) = string_i$, ambas recursivas y 1-1, realizan las 1-reducciones correspondientes.

Notemos que ambos son conjuntos libres de prefijos, de manera que los reales $m(A)$ y $m(B)$ coinciden con las medidas de las extensiones infinitas de los respectivos conjuntos. $m(A) = \Omega$ y por lo tanto es aleatorio. ¿Qué ocurre con $m(B)$? $m(B)$ es el número característico del problema de la detención: el $(i+1)$-ésimo bit de $m(B)$ es 1 sii $U(string_i)\downarrow$. Luego, si conocemos todos los programas que se detienen en U entre las primeras n cadenas, podemos determinar el prefijo de longitud $n+1$ de $m(B)$. Supongamos conocida la cantidad $m \leq n$ de dichos programas. Entonces, intercalando la ejecución de $U(w)$ para las n primeras cadenas w, podemos determinar cuáles son las m que terminan. Por lo tanto:

$$\begin{aligned} H(m(B)_{n+1}) &\leq H(n) + H(m) + O(1) \\ &\leq 2\log(n) + 2\log(m) + O(1) \\ &\leq 4\log(n) + O(1) \end{aligned}$$

(la última desigualdad surge de que $m \leq n$).

Es decir, $H(m(B)_{n+1}) \leq 4\log(n) + k$ para alguna constante positiva k. Y, dada k, es posible hallar, para cada $c \geq 0$, un valor de n suficientemente grande de manera que $4\log(n) + k \leq n + 1 - c$, con lo cual $m(B)$ no es aleatorio. $\otimes$

Por lo tanto, la 1-equivalencia entre conjuntos no garantiza la propiedad de aleatoriedad. Entonces, ¿qué condiciones sobre un conjunto A son suficientes para que sea posible demostrar la aleatoriedad de $\mu(A\Sigma^\omega)$ usando la estrategia de Chaitin? Recordemos primero su demostración:

> Demostración del Teorema 23. Sea $\mathbf{a} = \Omega$. Consideremos el siguiente programa para U, que toma como argumento un programa mínimo para Ω_n:
>
> 1. `Computar` Ω_n
> 2. `Enumerar suficientes elementos de` $Dom(U)$, $p_1, \ldots, p_m$ `hasta que` $w_m = \sum_{i=1}^{m} 2^{-|p_i|} > \Omega_n$
> 3. `Sea` $P = \{p_i / 1 \leq i \leq m\}$. `Computar el conjunto` $O = \{U(p)/p \in P\}$
> 4. `Retornar la primer cadena` $z \in \Sigma^*$ `tal que` $z \notin O$
>
> Observemos:
>
> - Se asume que Ω tiene una expansión binaria infinita (es decir, si Ω fuera un racional diádico, elegimos la represenación binaria que termina con infinitos 1's). Esto garantiza que todos sus prefijos pueden ser superados mediante la suma de los aportes de una cantidad finita de elementos de $Dom(U)$.
> - Si p es una cadena tal que $|p| \leq n$, entonces $p \in Dom(U)$ sii $p \in P$. La dirección $\Leftarrow$ es obvia. Para ver $\Rightarrow$, supongamos $p \notin P$. Entonces:
>
> $$\Omega_n + 2^{-|p|} < w_m + 2^{-|p|} < \Omega \leq \Omega_n + 2^{-n}$$
>
> Es decir, $|p| > n$. Luego, en P están *todos* los programas que se detienen U de longitud menor o igual que n y por lo tanto, $O = \{w \in \Sigma^* / H(w) \leq n\}$.
>
> La última observación garantiza que $H(z) > n$. Y como z es la salida del programa dado más arriba, entonces $H(z) \leq H(\Omega_n) + k$ (donde k es la longitud de dicho programa). Por lo tanto, $n < H(z) \leq H(\Omega_n) + k$, es decir, $H(\Omega_n) > n - k$.
>
> $\otimes$

Analicemos ahora la demostración. Llamemos $A = Dom(U)$ y tratemos de extraer las condiciones que se piden sobre A:

1. En primer lugar, se asume que A es libre de prefijos, de manera que $\mu(A\Sigma^\omega) = m(A)$.
2. Además, la prueba pide enumerar el conjunto A, luego debe ocurrir que $A \in \Sigma_1^0$.

3. También se requiere que $\mathbf{a} = \mu(A\Sigma^\omega)$ sea c.e., de manera que conociendo los primeros n bits de la expansión binaria de $\mathbf{a}$, pueda determinarse efectivamente cuándo detener la enumeración de A. Notemos que si A es libre de prefijos y c.e., entonces $\mathbf{a} = m(A)$ y es c.e.

4. Por último, dado $\mathbf{a}_n$, debe ser posible computar el conjunto $O = \{w \in \Sigma^* / H(w) \leq n\}$.

El último requisito puede relajarse: alcanza con pedir que el conjunto $\{w \in \Sigma^* / H(w) \leq n - c\}$, para alguna constante c, pueda obtenerse a partir de $\mathbf{a}_n$. Una manera de cumplir esta última condición es pedir que el dominio de U sea 1-reducible al conjunto A, pero con una restricción sobre las longitudes. Definimos, entonces, el siguiente caso particular de 1-reducciones:

Definición 28 (*Chaitin*-reducción) *Sean $A, B \subseteq \Sigma^*$. Decimos que A es* Chaitin-reducible *a B, y lo escribimos $A \leq_{Ch} B$, si $A \leq_1 B$ via una función f que satisface:*

(Ch1) *$Rango(f)$ restringido a B es recursivo, es decir, $\forall x \in B$ es decidible si $x \in Rango(f)$*

(Ch2) $\exists c \forall w (f(w) \downarrow \Rightarrow |f(w)| \leq |w| + c)$

La relación $\leq_{Ch}$ es efectivamente una reducción:

Proposición 29 *$\leq_{Ch}$ cumple:*

(a) $\forall A \subseteq \Sigma^* (A \leq_{Ch} A)$

(b) $\forall A, B, C \subseteq \Sigma^* (A \leq_{Ch} B \wedge B \leq_{Ch} C \Rightarrow A \leq_{Ch} C)$

Demostración. Para (a), basta ver que $A \leq_{Ch} A$ via la función identidad. Para (b), sea $A \leq_{Ch} B$ via f y $B \leq_{Ch} C$ via g, y definamos $h = g \circ f$. h es recursiva y 1-1 pues f y g lo son. $Rango(f) \subseteq Dom(g)$, luego $\forall x (x \in A$ sii $h(x) \in C)$. $\forall x \in Dom(h) (|h(x)| \leq |g(f(x))| \leq |f(x)| + c \leq |x| + c + d)$. Veamos que $Rango(h)$ restringido a C es recursivo. Si $y \in C$, $y \in Rango(g)$ es decidible pues $Rango(g)$ restringido a C es recursivo. Luego si $y \notin Rango(g)$ entonces $y \notin Rango(h)$. Si $y \in Rango(g)$, entonces existe $x \in B$ tal que $g(x) = y$ y $|x| \geq |y| - c$. Evaluando $g(w)$ para $w/|w| \geq |y| - c$, es posible hallar x (notar que si bien debería considerarse una cantidad *potencialmente infinita* de cadenas, g es una 1-reducción y $y \in Rango(g)$, lo que garantiza la existencia de x tal que $g(x) = y$, con lo cual x puede efectivamente encontrarse luego de una cantidad *finita* de evaluaciones). Y como $x \in B$, es decidible si $x \in Rango(f)$ pues $Rango(f)$ restringido a B es recursivo. Finalmente, si $x \in Rango(f)$ entonces $y \in Rango(h)$ y en caso contrario, $y \notin Rango(h)$. Por lo tanto, $Rango(h)$ restringido a C es recursivo, y h verifica todas las condiciones de una *Chaitin*-reducción, con lo cual $A \leq_{Ch} C$. $\otimes$

Proponemos, entonces, las siguientes condiciones sobre un conjunto A:

(C1) A es libre de prefijos

(C2) $A \in \Sigma_1^0$

(C3) $Dom(U) \leq_{Ch} A$

y probamos que son suficientes para aplicar la estrategia de Chaitin, dando una versión generalizada de su demostración:

Teorema 30 *Si $A \in \Sigma_1^0$ es libre de prefijos y satisface que $Dom(U) \leq_{Ch} A$, entonces $\mathbf{a} = \mu(A\Sigma^\omega)$ es aleatorio y c.e.*

DEMOSTRACIÓN. Como A es libre de prefijos, $\mathbf{a} = m(A) = \sum_{w \in A} 2^{-|w|}$. Además, A es c.e., de manera que fijamos una función $g : \mathbb{N} \to \Sigma^*$ que enumera a A, y llamamos $(a_i)_{i \in \mathbb{N}}$ a la sucesión de racionales dada por $a_j = \sum_{i=0}^{j} 2^{-|g(i)|}$. $(a_i)_{i \in \mathbb{N}}$ es computable, creciente y convergente a $\mathbf{a}$, y por lo tanto $\mathbf{a}$ es c.e.

Consideremos el siguiente programa para U, que recibe como argumento un programa mínimo para computar $\mathbf{a}_i$:

1. Computar $\mathbf{a}_i$ y i
2. Enumerar suficientes elementos de A, $g(0), g(1), \ldots$, hasta que $a_m = \sum_{j=0}^{m} 2^{-|g(j)|} > \mathbf{a}_i$. En el caso de que $\mathbf{a}$ sea un racional diádico, consideramos la representación binaria que termina con infinitos 1's. Esto garantiza que con la contribución de una cantidad finita de elementos de A, puede alcanzarse cualquier segmento inicial de $\mathbf{a}$[1].
3. Usar la función f y la constante k dadas por la *Chaitin*-reducción de $Dom(U)$ a A, para construir el conjunto

$$P = \{p \in Dom(U) / f(p) \in \{g(0) \ldots g(m)\} \wedge |p| \leq i - k\}$$

   La rutina en la Figura 1 da una posible manera de computar P.
4. Computar el conjunto $O = \{U(p) / p \in P\}$
5. Producir como salida la primer cadena z (en el orden cuasilexicográfico sobre Σ^*) tal que $z \notin O$, y detenerse.

En primer lugar, veamos que, si $|p| \leq i - k$, entonces $U(p) \downarrow \Leftrightarrow p \in P$. La dirección $\Leftarrow$ se cumple obviamente. Veamos la otra implicación. Supongamos $p \in Dom(U)$ y $p \notin P$. Entonces:

$$\mathbf{a}_i + 2^{-i} \geq \mathbf{a} > a_m + 2^{-|f(p)|} > \mathbf{a}_i + 2^{-|f(p)|} \geq \mathbf{a}_i + 2^{-|p|-k}$$

[1] La aclaración no es demasiado importante, pues el teorema implica que $\mathbf{a}$ es un número irracional. Los números racionales son computables, de manera que la complejidad de sus prefijos es muy baja.

```
P:=[ ];
for j=0 to m do {
    if g(j) in Rango(f) then {
    /* computable pues g es computable y   */
    /* Rango(f) es recursivo relativo a A  */
        for s=0 to i-k do {
            if f(string(s))=g(j) then {
            /* string(s) es una biyeccion  */
            /* recursiva de N en {0,1}*    */
                P:=add(P,string(s));
                exit for;
            }
        }
    }
}
```

Figura 1: Cómputo de P

Luego, debe ocurrir que $i < |p| + k$, es decir, $|p| > i - k$. Por lo tanto, P contiene exactamente *todos* los programas de longitud $\leq i-k$ que se detienen en U. Luego, $O = \{U(p)/p \in P\} = \{w \in \Sigma^*/H(w) \leq i - k\}$.

Ahora analicemos la complejidad del resultado producido por este programa. Como z es la primer cadena en el orden cuasilexicográfico que no pertenece a O, z no es la salida de ningún programa en P. Entonces, como en P están todos los programas para U de longitud $\leq i-k$, necesariamente z debe ser producida por programas de longitud mayor. Es decir, como $z \notin O$, debe ocurrir que $H(z) > i - k$. Además, z es la salida del programa que dimos más arriba. Si l es la longitud de este programa, entonces una cota superior para la complejidad de z es l más la complejidad del argumento, $H(\mathbf{a}_i)$. Combinando estas dos últimas observaciones obtenemos:

$$i - k < H(z) \leq H(\mathbf{a}_i) + l$$

Es decir, $H(\mathbf{a}_i) > i - c$, con $c = k + l$. Como el prefijo $\mathbf{a}_i$ que se toma como argumento es arbitrario, hemos probado que existe c tal que para todo i, $H(\mathbf{a}_i) > i - c$, con lo cual $\mathbf{a}$ es aleatorio. $\otimes$

El Teorema 30, entonces, da una respuesta a la Pregunta 1: las condiciones C1, C2 y C3 sobre un conjunto $A \subseteq \Sigma^*$ son suficientes para demostrar la aleatoriedad de $\mu(A\Sigma^\omega)$ usando (una generalización de) la estrategia de Chaitin.

3.2 Condiciones necesarias de aleatoriedad

Nos preguntamos, ahora, si las condiciones dadas en la sección anterior son necesarias, es decir, dado un real aleatorio c.e. $\mathbf{a}$, ¿existe siempre un conjunto A que verifica esas condiciones y tal que $\mathbf{a} = \mu(A\Sigma^\omega)$? Vamos a mostrar que la respuesta es afirmativa, construyendo un conjunto de esas características a partir de $\mathbf{a}$.

Analicemos en detalle las condiciones que debe cumplir el conjunto A que queremos construir. La condición C1 pide que sea libre de prefijos. Usamos el Teorema de Kraft-Chaitin, que garantiza la existencia de un conjunto libre de prefijos y c.e. a partir de una lista c.e. de requerimientos consistentes, y centramos la prueba en la construcción de esta lista. La condición C2 es que A sea c.e. En este caso, la propia construcción es una enumeración del conjunto, con lo cual cumplimos este requisito. Por último, la condición C3 exige que $Dom(U) \leq_{Ch} A$, es decir, debemos probar que existe una función f, cuyo rango restringido a A es recursivo, que 1-reduce $Dom(U)$ a A con la restricción de que $\exists c \forall p \in Dom(f)(|f(p)| \leq |p| + c)$. Consideramos una f de la forma $f(p) = \%p$, donde $\%$ es un prefijo tal que *ninguna* otra palabra A comienza con $\%$. Esto garantiza lo siguiente:

1. f es computable
2. f es 1-1
3. $Rango(f)$ es recursivo (luego también lo es $Rango(f)$ restringido a A)
4. para todo $p \in \Sigma^*$ (en particular para $p \in Dom(f)$), $|f(p)| = |p| + |\%|$

El prefijo $\%$ es una palabra fija de longitud c, donde c se determina durante la construcción de manera que $\mathbf{a} > 2^{-c}\Omega$. El conjunto A está formado por $\%Dom(U)$ (todos los programas de U prefijados con $\%$) más las palabras necesarias para completar la medida requerida. De esta manera se satisface el punto (Ch1) de la definición 28, es decir, que $p \in Dom(U)$ sii $f(p) \in A$, y además obtenemos $m(A) = \mathbf{a}$.

Es decir, comenzamos construyendo dos listas de naturales $(y_i)_{i \in \mathbb{N}}$ y $L = \{l^i_j / i, j \in \mathbb{N}\}$, que serán las longitudes de las palabras del conjunto A. Los números y_i garantizan que $Dom(U) \leq_{Ch} A$, y los números l^i_j se usan para completar el conjunto de manera que $\mu(A\Sigma^\omega) = \mathbf{a}$.

La demostración se basa en la propiedad de que un número aleatorio c.e. domina a cualquier otro real c.e. (Lema 24), en particular, a Ω. Usamos la siguiente versión de dicho Lema, que garantiza la relación de dominación para una secuencia particular de racionales convergente a Ω:

Lema 31 *Sea* $\mathbf{a}$ *aleatorio c.e. Existe* $(a_i)_{i \in \mathbb{N}}$ *una secuencia de racionales creciente computable convergente a* $\mathbf{a}$ *y una constante* $c > 0$ *tales que, si* $(p_i)_{i \in \mathbb{N}}$ *es una enumeración de* $Dom(U)$*, entonces para todo* i*,* $c(\mathbf{a} - a_i) \geq \Omega - \sum_{j=1}^{i} 2^{-|p_j|}$.

DEMOSTRACIÓN. Llamemos $w_i = \sum_{j=1}^{i} 2^{-|p_j|}$.

Como $\mathbf{a}$ es aleatorio c.e., por el Lema 24, $\mathbf{a} \geq_{dom} \mathbf{b}$ para todo real c.e. $\mathbf{b}$, en particular, $\mathbf{a} \geq_{dom} \Omega$. Tanto $\mathbf{a}$ como Ω son c.e., luego por el Lema 19 existen secuencias de racionales $(\overline{a}_i)$ y (b_i) computables crecientes y convergentes a $\mathbf{a}$ y a Ω, respectivamente, y una constante $c > 0$ tales que $c(\mathbf{a} - \overline{a}_i) \geq \Omega - b_i$ para todo i.

Definamos la función computable total g como $g(i) = \max\{j / b_j \leq w_i\}$ y $a_i = \overline{a}_{g(i)}$. (a_i) es computable, creciente y convergente a $\mathbf{a}$ y además, para cada i, $c(\mathbf{a} - a_i) = c(\mathbf{a} - \overline{a}_{g(i)}) \geq \Omega - b_{g(i)} \geq \Omega - w_i$, como queríamos.

$\otimes$

Mostramos ahora la construcción de la lista c.e. de las longitudes de las palabras que completan el conjunto A de tal forma que $m(A) = \mathbf{a}$. La lista $L = \{l_i^s / s, i \in I\!N\}$ se construye en etapas s, con $L^s \subseteq L^{s+1}$ y $L = \cup_{s \in I\!N} L^s$, a partir de una secuencia de racionales (a_i) que aproxima al real $\mathbf{a}$. En cada etapa s, definimos $y_s = |p_s| + |\%|$ (donde $(p_i)_{i \in I\!N}$ es una enumeración fija de $Dom(U)$) y completamos la lista de la etapa s, $L^s = \{l_i^s / i \in I\!N\}$, de forma que $\sum_{l \in L^s} 2^{-l} + \sum_{j=0}^{s} 2^{-y_s} \geq a_s$. Es decir, el aporte de las longitudes ya incluidas más el de los primeros s programas en la enumeración de $Dom(U)$ (con el agregado de la longitud del prefijo $\%$) es mayor o igual que la s-ésima aproximación de $\mathbf{a}$, a_s.

Lema 32 *Sea* $\mathbf{a}$ *un real en* $[0, 1]$ *aleatorio c.e. Existe una lista de longitudes* L *c.e. y una constante* $c' > 0$ *tal que para todo* $c \geq c'$ *se cumple que* $l > c$ *para todo* $l \in L$ *y* $\sum_{l \in L} 2^{-l} = \mathbf{a} - 2^{-c}\Omega$.

DEMOSTRACIÓN. Sea $(p_i)_{i \in I\!N}$ una enumeración de $Dom(U)$.

Sea $(a_i)_{i \in I\!N}$ una sucesión de racionales computable creciente y convergente a $\mathbf{a}$ y $c_0 > 0$ una constante tal que $2^{c_0}(\mathbf{a} - a_i) \geq \Omega - \sum_{j=0}^{i} 2^{-|p_j|}$ (existen por el Lema 31).

Sea c_1 tal que $a_0 > 2^{-(|p_0| + c_1)}$.

Definamos $c' = \max\{c_0, c_1\}$ y fijemos $c \geq c'$. Para cada $i \in I\!N$, sea $y_i = |p_i| + c$.

La construcción de L se realiza por etapas s, de tal manera que para cada s, $L^s \subseteq L^{s+1}$. Luego definimos $L = \bigcup_s L^s$.

Etapa $s = 0$: Sea $q_0 = a_0 - 2^{-y_0}$. $q_0 \in \mathcal{Q}$, es decir, es computable, luego existe una lista c.e. de longitudes $\mathcal{L}_0 = \{l_i^0 / i \in I\!N\}$ tal que $l_i^0 > c \forall i \in I\!N$ y $\sum_{i \in I\!N} 2^{-l_i^0} = q_0$. Entonces definimos $L^0 = \mathcal{L}_0$. Observar que $\sum_{l \in L^0} 2^{-l} = a_0 - 2^{-y_0}$.

Etapa $s \geq 1$: Si $a_s \leq \sum_{i=0}^{s} 2^{-y_i} + \sum_{l \in L^{s-1}} 2^{-l}$ entonces $L^s = L^{s-1}$.
Sino, sea $q_s = a_s - (\sum_{i=0}^{s} 2^{-y_i} + \sum_{l \in L^{s-1}} 2^{-l})$. $q_s \in \mathbb{Q}$, luego existe un lista c.e. $\mathcal{L}_s = \{l_i^s / i \in \mathbb{N}\}$ tal que $l_i^s > c$ para todo $i \in \mathbb{N}$ y $\sum_{i \in \mathbb{N}} 2^{-l_i^s} = q_s$. Entonces definimos $L^s = L^{s-1} \cup \mathcal{L}_s$. Observar que en este caso $\sum_{l \in L^s} 2^{-l} = a_s - \sum_{i=0}^{s} 2^{-y_i}$.

Como $(a_i)_{i \in \mathbb{N}}$ es computable el procedimiento anterior da una enumeración recursiva de L, es decir, L es c.e. Además, por construcción, $\forall l \in L$, $l > c$. Por último, veamos que $\sum_{l \in L} 2^{-l} = \mathbf{a} - 2^{-c}\Omega$:

Caso 1. Existen infinitas etapas s con $a_s = \sum_{i=0}^{s} 2^{-y_i} + \sum_{l \in L^s} 2^{-l}$. Entonces

$$\begin{aligned} \sum_{l \in L} 2^{-l} &= \lim_{s \to \infty} \sum_{l \in L^s} 2^{-l} = \lim_{s \to \infty} (a_s - \sum_{i=0}^{s} 2^{-y_i}) \\ &= \lim_{s \to \infty} a_s - \sum_{i=0}^{\infty} 2^{-y_i} = \mathbf{a} - \sum_{i=0}^{\infty} 2^{-y_i} \\ &= \mathbf{a} - \sum_{i=0}^{\infty} 2^{-|p_i|-c} = \mathbf{a} - 2^{-c}\Omega \end{aligned}$$

Caso 2. Para casi todo s, $a_s < \sum_{l \in L^s} 2^{-l} + \sum_{i=0}^{s} 2^{-y_i}$. Sea s_0 la mayor etapa tal que $a_{s_0} = \sum_{l \in L^{s_0}} 2^{-l} + \sum_{i=0}^{s_0} 2^{-y_i}$ (esta etapa existe, al menos $s_0 = 0$ lo cumple). Observemos:

(a) $\forall s > s_0$, $a_s < \sum_{l \in L^s} 2^{-l} + \sum_{i=0}^{s} 2^{-y_i}$, luego por la construcción debe ocurrir que, $\forall s > s_0$, $a_s < \sum_{l \in L^{s-1}} 2^{-l} + \sum_{i=0}^{s} 2^{-y_i}$ y por lo tanto $L^s = L^{s-1}$. Entonces, $\forall s \geq s_0$, $L^s = L^{s+1}$, con lo cual $L = L^{s_0}$.

(b) Como $a_s < \sum_{l \in L^s} 2^{-l} + \sum_{i=0}^{s} 2^{-y_i}$ $\forall s > s_0$, entonces

$$\begin{aligned} \mathbf{a} &= \lim_{s \to \infty} a_s \leq \lim_{s \to \infty} (\sum_{l \in L^s} 2^{-l} + \sum_{i=0}^{s} 2^{-y_i}) \\ &= \sum_{l \in L} 2^{-l} + \sum_{i=0}^{\infty} 2^{-y_i} = \sum_{l \in L} 2^{-l} + 2^{-c}\Omega \end{aligned}$$

Es decir, $\sum_{l \in L} 2^{-l} \geq \mathbf{a} - 2^{-c}\Omega$.

(c) Como $c \geq c_0$, tenemos que

$$\mathbf{a} - a_{s_0} \geq 2^{-c}(\Omega - \sum_{i=0}^{s_0} 2^{-|p_i|}) = 2^{-c} \sum_{i > s_0} 2^{-|p_i|} = \sum_{i > s_0} 2^{-y_i}$$

Luego

$$\mathbf{a} \geq \sum_{i > s_0} 2^{-y_i} + a_{s_0} = \sum_{i > s_0} 2^{-y_i} + \sum_{l \in L^{s_0}} 2^{-l} + \sum_{i=0}^{s_0} 2^{-y_i}$$

$$= \sum_{i=0}^{\infty} 2^{-y_i} + \sum_{l \in L} 2^{-l} = 2^{-c}\Omega + \sum_{l \in L} 2^{-l}$$

Es decir, $\sum_{l \in L} 2^{-l} \leq \mathbf{a} - 2^{-c}\Omega$.

Por lo tanto, también en este caso $\sum_{l \in L} 2^{-l} = \mathbf{a} - 2^{-c}\Omega$.

$\otimes$

Una vez que tenemos la lista L que satisface $\sum_{l \in L} 2{-}l = \mathbf{a} - 2^{-c}\Omega$, queremos usar la desigualdad de Kraft-Chaitin para construir un conjunto libre de prefijos con exactamente una palabra de cada longitud en la lista. Pero es necesario que ninguna palabra comience con el prefijo %, reservado para los elementos de $Dom(U)$. Una manera de hacerlo es dividir L en una cantidad finita de listas L_i, todas enumerables, tales que cada una de ellas aporte a lo sumo 2^{-c}, con $c = |\%|$. Luego, para cada una, obtenemos un conjunto libre de prefijos que comience con una palabra distinta de longitud c (y por lo tanto se requieren, a lo sumo, $2^c - 1$ listas). La unión de estos conjuntos, entonces, resulta libre de prefijos, y la medida asociada al conjunto unión es exactamente $\mathbf{a} - 2^{-c}\Omega$. A continuación presentamos la construcción de las $2^c - 1$ listas L_i a partir de la lista L ya obtenida:

Lema 33 *Sea L una lista de longitudes c.e. y c una constante tales que $l > c \forall l \in L$ y $\sum_{l \in L} 2^{-l} \leq 1 - 2^{-c}$. Existen $2^c - 1$ listas c.e. L_i, $1 \leq i \leq 2^c - 1$, tales que $\sum_{l \in L_i} 2^{-l} \leq 2^{-c}$, $l > c \ \forall l \in L_i$ y $\sum_i \sum_{l \in L_i} 2^{-l} = \sum_{l \in L} 2^{-l}$.*

Demostración. Sea $k = 2^c - 1$ y sea $(l_j)_{j \geq 1}$ una enumeración de L. Construiremos las listas L_i en etapas s, tales que $L_i^s \subseteq L_i^{s+1}$ para todo s, y definimos $L_i = \cup_s L_i^s$.

Etapa $s = 0$: Asignar $L_i^0 = \{l_i\}$ para cada $i = 1 \ldots k$. Observar que, como $l_j > c$ para todo $j \geq 1$, entonces $\sum_{l \in L_i^0} 2^{-l} = 2^{-l_i} < 2^{-c} \forall i = 1 \ldots k$.

Etapa $s \geq 1$: Sea $m = \min\{j / l_j \notin L_i^{s-1} \forall i = 1 \ldots k\}$ y llamemos $\ell = l_m$ (ℓ es el primer elemento aún no asignado en el orden dado por la enumeración de L).

Si existe i, $1 \leq i \leq k$, tal que $(\sum_{l \in L_i^{s-1}} 2^{-l}) + 2^{-\ell} \leq 2^{-c}$ entonces agregar ℓ a L_i^{s-1} para obtener L_i^s, y mantener $L_j^s = L_j^{s-1} \forall j \neq i$.

Si no, observemos que

$$(\sum_{i=1}^{k} \sum_{l \in L_i^{s-1}} 2^{-l}) + 2^{-\ell} < \sum_{l \in L} 2^{-l} \leq 1 - 2^{-c} = (2^c - 1)2^{-c} = k2^{-c}$$

o lo que es lo mismo

$$k2^{-c} - (\sum_{i=1}^{k} \sum_{l \in L_i^{s-1}} 2^{-l}) = \sum_{i=1}^{k} (2^{-c} - \sum_{l \in L_i^{s-1}} 2^{-l}) > 2^{-\ell} \qquad (1)$$

Es decir, entre todas las L_i^{s-1} hay suficiente "espacio" para ℓ.
Llamemos e_i al "espacio disponible" en L_i^{s-1}, es decir, $e_i = 2^{-c} - \sum_{l \in L_i^{s-1}} 2^{-l}$, y sea $M = \max\{l / l \in \cup_{i=1}^{k} L_i^{s-1}\}$. Observemos:

1. Para cada l en algún L_i^{s-1}, existe una constante c_l tal que $l = M - c_l$
2. $M > c$, luego existe c_c tal que $c = M - c_c$
3. $e_i = 2^{-c} - \sum_{l \in L_i^{s-1}} = 2^{-M}(2^{c_c} - \sum_{l \in L_i^{s-1}} 2^{c_l}) = 2^{-M} m_i$

Es decir, para cada i existe $m_i \geq 0$ (y no todos 0) tal que $e_i = m_i 2^{-M}$.
Además, $M > \ell$, ya que, en caso contrario, como existe algún $m_i \geq 1$, el correspondiente e_i es $\geq 2^{-M}$, y, si $M \leq \ell$, entonces $2^{-M} \geq 2^{-\ell}$, con lo cual

$$\sum_{l \in L_i^{s-1}} 2^{-l} + 2^{-\ell} \leq \sum_{l \in L_i^{s-1}} 2^{-l} + 2^{-M} \leq \sum_{l \in L_i^{s-1}} 2^{-l} + e_i \leq 2^{-c}$$

Es decir, ℓ podía haberse agregado a L_i^{s-1}.
Entonces, reescribiendo (1) con la notación anterior:

$$\sum_i e_i = 2^{-M} \sum_i m_i \geq 2^{-\ell}$$

Luego $\sum_i m_i \geq 2^{-\ell} 2^M = 2^{M-\ell}$, que es un entero positivo pues $M > \ell$, con lo cual existe una combinación de t_i tales que $0 \leq t_i \leq m_i$ (no todos 0), y $\sum_i t_i = 2^{M-\ell}$. Entonces cada lista L_i^s se define agregando a L_i^{s-1} la lista $\{l_1, \ldots, l_{t_i} / l_j = M \forall j = 1 \ldots t_i\}$ (es decir, la lista L_i^s se forma agregando t_i veces la longitud M a la lista L_i^{s-1}).
Primero notemos que $\sum_i (t_i 2^{-M}) = 2^{-M} \sum_i t_i = 2^{-M} 2^{M-\ell} = 2^{-\ell}$, como queríamos. Y además, para cada i, $\sum_{l \in L_i^s} 2^{-l} = \sum_{l \in L_i^{s-1}} 2^{-l} + t_i 2^{-M} \leq \sum_{l \in L_i^{s-1}} 2^{-l} + m_i 2^{-M} = \sum_{l \in L_i^{s-1}} 2^{-l} + e_i \leq 2^{-c}$.

Este procedimiento enumera recursivamente las listas L_i a partir de una enumeración de L, y por lo tanto las L_i son c.e. Además, por construcción, para todo i, si $l \in L_i$, $l > c$, y como para cada $l \in L$, se agregan suficientes longitudes a los L_i^s de manera que la suma total se incremente exactamente en 2^{-l}, tenemos que

$$\sum_{i=1}^{2^c - 1} \sum_{l \in L_i} 2^{-l} = \sum_{l \in L} 2^{-l}$$

Para ver que $\sum_{l\in L_i} 2^{-l} \leq 2^{-c}$, razonemos por el absurdo y supongamos que $\sum_{l\in L_i} 2^{-l} > 2^{-c}$. Como $L_i = \cup_s L_i^s$ debe existir alguna etapa s tal que $\sum_{l\in L_i^s} > 2^{-c}$. Pero esto es imposible por la construcción de los L_i^s. Luego $\sum_{l\in L_i} \leq 2^{-c}$.

$\otimes$

Tenemos ahora todas las herramientas necesarias para responder la Pregunta 2. El resultado es el siguiente:

Teorema 34 *Sea* $\mathbf{a}$ *un real en* $[0,1]$ *aleatorio c.e. Existe* $A \in \Sigma_1^0$ *libre de prefijos tal que* $Dom(U) \leq_{Ch} A$ *y* $\mathbf{a} = \mu(A\Sigma^\omega)$.

Demostración.

Sea L la lista de longitudes c.e. y $c' > 0$ la constante dadas por el Lema 32. Este Lema nos garantiza que $\sum_{l\in L} 2^{-l} = \mathbf{a} - 2^{-c}\Omega$ para todo $c \geq c'$. Para poder aplicar el Lema 33, es necesario encontrar una constante c tal que $\mathbf{a} - 2^{-c}\Omega \leq 1 - 2^{-c}$. Observemos que, en particular, es suficiente hallar c tal que $2^c(1-a_0) \geq 1$, con a_0 el primer término de una sucesión computable creciente y convergente a $\mathbf{a}$. En efecto, $\mathbf{a} - 2^{-c}\Omega \leq 1 - 2^{-c}$ sii $2^{-c} - 2^{-c}\Omega \leq 1 - \mathbf{a}$ sii $2^{-c}(1-\Omega) \leq 1 - \mathbf{a}$ sii $1 - \Omega \leq 2^c(1-\mathbf{a})$, y como $1-\Omega < 1$, pues $\Omega > 0$, y $1 - \mathbf{a} > 1 - a_0$, pues $a_0 < \mathbf{a}$, tenemos $1 - \Omega < 1 \leq 2^c(1-a_0) < 2^c(1-\mathbf{a})$ sii $1 \leq 2^c(1-a_0)$, con lo cual si elegimos c de la manera indicada se verifica la desigualdad estricta. Entonces, si c' verifica que $2^{c'}(1-a_0) \geq 1$, tomamos $c = c'$. En caso contrario, incrementamos c' lo suficiente como para cumplir esta desigualdad, es decir, consideramos $c = \min\{k > c'/2^k(1-a_0) \geq 1\}$.

Ahora, $\mathbf{a} - 2^{-c}\Omega \leq 1 - 2^{-c}$ y entonces, por el Lema 33, existen $2^c - 1$ listas $L_1, \ldots, L_{2^c-1}$ c.e. tales que para cada i, si $l \in L_i$ entonces $l > c$ y $\sum_{l\in L_i} 2^{-l} \leq 2^{-c}$, y además $\sum_i \sum_{l\in L_i} 2^{-l} = \sum_{l\in L} 2^{-l}$. Consideremos $L_i' = \{l - c / l \in L_i\}$. $\sum_{l\in L_i'} 2^{-l} = 2^c \sum_{l\in L_i} 2^{-l} \leq 2^c 2^{-c} = 1$. Luego, aplicando la desigualdad de Kraft-Chaitin, tenemos que, para cada i, existe un conjunto A_i' libre de prefijos c.e. tal que $\mu(A_i'\Sigma^\omega) = \sum_{l\in L_i'} 2^{-l}$. Sea $A_i = \{w_i w / w \in A_i'\}$, donde w_i es la i-ésima palabra de longitud c en el orden cuasilexicográfico habitual sobre Σ^*. Claramente, $\mu(A_i\Sigma^\omega) = \sum_{l\in L_i} 2^{-l}$.

Sea $A = (\bigcup_{i=1}^{2^c-1} A_i) \cup \{\%p / p \in Dom(U) \wedge |\%| = c \wedge \% \not\preceq x \forall x \in A_i \forall i\}$. Esto es posible pues hay $2^c - 1$ A_i's y existen 2^c palabras de longitud c.

A es libre de prefijos y c.e. Además,

$$\mu(A\Sigma^\omega) = \sum_{i=1}^{2^c-1} \mu(A_i\Sigma^\omega) + 2^{-c} \sum_{p\in Dom(U)} 2^{-|p|}$$

$$= \sum_{i=1}^{2^c-1} \sum_{l \in L_i} 2^{-l} + 2^{-c}\Omega = \sum_{l \in L} 2^{-l} + 2^{-c}\Omega$$
$$= \mathbf{a} - 2^{-c}\Omega + 2^{-c}\Omega = \mathbf{a}$$

Por último, definamos $f(p) = \%p$ para todo $p \in \Sigma^*$. f es recursiva, 1-1, con rango recursivo (y por lo tanto $Rango(f)$ restringido a A también lo es), y verifica:

i. $\forall p(p \in Dom(U) \Leftrightarrow f(p) \in A)$

ii. $\exists c \forall p(|f(p)| \leq |p| + c)$

lo cual completa la demostración. $\otimes$

De los Teoremas 30 y 34, obtenemos el siguiente corolario, que da una caracterización de los reales en el intervalo $[0, 1]$ que son aleatorios y c.e.:

Corolario 35 *Sea* $\mathbf{a}$ *un real en el intervalo* $[0, 1]$. $\mathbf{a}$ *es aleatorio c.e. sii existe* $A \in \Sigma_1^0$ *libre de prefijos tal que* $\mathbf{a} = \mu(A\Sigma^\omega)$ *y* $Dom(U) \leq_{Ch} A$.

4 Relaciones con resultados existentes

En la sección anterior presentamos una caracterización de reales aleatorios c.e. Recordemos la caracterización conocida para esta clase de números:

> *Un real es aleatorio c.e. si y sólo si es la probabilidad de detención de una máquina autodelimitante universal.*

La implicación de derecha a izquierda fue demostrada por Chaitin [8] (Teorema 23). Slaman y Kučera [13] probaron la otra dirección, a partir del trabajo de Calude, Hertlind, Khoussainov y Wang [6].

Vamos a considerar ahora algunos aspectos referidos a este resultado. En primer lugar, mostramos que es posible obtener otra caracterización directamente a partir de la relación de *strong simulation* [6]. Luego, observamos una similitud formal entre nuestra definición de *Chaitin*-reducciones y la de *strong simulation*, y analizamos, entonces, una relación entre ambas reducciones. Por último, damos otras dos demostraciones del Teorema de Slaman [13], una de ellas basada en la definición de *Chaitin*-reducciones y la otra, en la de *strong simulation*.

4.1 Algunos resultados conocidos

Comenzamos enunciando definiciones y resultados (sin demostraciones) sobre los que vamos a trabajar.

Calude, Hertlind, Khoussainov y Wang [6] consideran una relación entre conjuntos c.e. de cadenas que está estrechamente vinculada con la relación de dominación definida por Solovay (Definición 18)[2]:

Definición 36 (*Strong simulation* [5]) *Sean $A, B \subset \Sigma^*$ conjuntos infinitos c.e. y libres de prefijos. A* simula fuertemente *a B (notación: $B \leq_{ss} A$) si existe una función f recursiva parcial que satisface:*

1. $A = Dom(f)$
2. $B = f(A)$
3. $\forall x \in A(|x| \leq |f(x)| + O(1))$

Notemos que la relación de *strong simulation* es reflexiva y transitiva, es decir, $\leq_{ss}$ es una reducción.

El siguiente resultado muestra la vinculación entre *strong simulation* y dominación:

Lema 37 ([5]) *Si A, B son conjuntos c.e. infinitos y libres de prefijos tales que $B \leq_{ss} A$, entonces $\mu(B\Sigma^\omega) \leq_{dom} \mu(A\Sigma^\omega)$.*

Sin embargo, la recíproca del Lema 37 no es cierta (en [6] se prueba la existencia de dos conjuntos infinitos libres de prefijos c.e. A y B tales que $m(A) = m(B) = 1$ pero $A \not\leq_{ss} B$ y $B \not\leq_{ss} A$). No obstante, sí se cumple la siguiente propiedad más débil:

Teorema 38 ([5]) *Sea $\mathbf{a}$ un real c.e. y B un conjunto infinito libre de prefijos y c.e. Si $\mu(B\Sigma^\omega) \leq_{dom} \mathbf{a}$, entonces existe un conjunto c.e. infinito libre de prefijos $A \subset \Sigma^*$ tal que $\mathbf{a} = \mu(A\Sigma^\omega)$ y $B \leq_{ss} A$.*

El Teorema 38 es muy importante y permitió demostrar resultados intermedios a partir de los cuales Slaman y Kučera obtuvieron la recíproca del Teorema 23, logrando una caracterización de los reales aleatorios c.e.:

Teorema 39 (Teorema de Slaman [13]) *Si $\mathbf{a}$ es un real en $[0, 1]$ aleatorio c.e., entonces $\mathbf{a}$ es un* Ω-number.

4.2 Una caracterización usando *strong simulation*

Nuestra definición de *Chaitin*-reducciones presenta una similitud formal con la de *strong simulation*. Este hecho motivó nuestra Pregunta 3: ¿es posible obtener una caracterización de los reales aleatorios c.e. mediante la relación de *strong simulation*? Como ya dijimos, $\leq_{ss}$ fue usada en resultados intermedios que permitieron demostrar la equivalencia entre la clase de los reales

[2] Usamos las definiciones y resultados de Calude [5].

aleatorios c.e. y la de las probabilidades de detención de máquinas autodelimitantes universales. Queremos ahora obtener una caracterización basada directamente en la relación de *strong simulation*.

El resultado análogo al Teorema 30 es el siguiente:

Teorema 40 *Sea $A \in \Sigma_1^0$ libre de prefijos tal que $Dom(U) \leq_{ss} A$. Entonces $\mathbf{a} = \mu(A\Sigma^\omega)$ es aleatorio y c.e.*

DEMOSTRACIÓN. Aplicando el Lema 37 tenemos que

$$\mathbf{a} \geq_{dom} \mu(Dom(U)\Sigma^\omega) = \Omega$$

Ahora, por el Lema 20, existe k tal que $H(\Omega_i) \leq H(\mathbf{a}_i) + k$. Y como Ω es aleatorio, $\exists d\ \forall i\ H(\Omega_i) > i - d$. Luego

$$H(\mathbf{a}_i) + k \geq H(\Omega_i) > i - d$$

es decir, con $c = d + k$, obtenemos que existe c tal que $H(\mathbf{a}_i) > i - c$ para todo i, y por lo tanto $\mathbf{a}$ es aleatorio.

Por último, $\mathbf{a}$ es c.e. pues $A \in \Sigma_1^0$: la secuencia de racionales $(a_i)_{i \in I\!N}$ dada por $a_n = \sum_{i=0}^{n} 2^{-|g(i)|}$, donde g es una función recursiva que enumera al conjunto A sin repeticiones, es computable, creciente y convergente a $\mathbf{a}$. $\otimes$

Y la contraparte del Teorema 34 usando *strong simulation*:

Teorema 41 *Si $\mathbf{a}$ es aleatorio c.e., existe $A \in \Sigma_1^0$ libre de prefijos con $\mathbf{a} = \mu(A\Sigma^\omega)$ tal que $Dom(U) \leq_{ss} A$.*

DEMOSTRACIÓN. $\mathbf{a}$ y $Dom(U)$ cumplen las hipótesis del Teorema 38: $\mathbf{a}$ es c.e., $Dom(U)$ es libre de prefijos infinito y c.e., y, por el Lema 24, $\mathbf{a} \geq_{dom} \mu(Dom(U)\Sigma^\omega) = \Omega$. Entonces podemos aplicar el Teorema 38 y obtenemos el resultado buscado. $\otimes$

Finalmente, el siguiente corolario de los Teoremas 40 y 41 responde afirmativamente a la Pregunta 3 y da otra caracterización de los reales aleatorios c.e.:

Corolario 42 *Sea $\mathbf{a}$ un real en $[0, 1]$. $\mathbf{a}$ es aleatorio c.e. sii existe $A \in \Sigma_1^0$ libre de prefijos tal que $\mathbf{a} = \mu(A\Sigma^\omega)$ y $Dom(U) \leq_{ss} A$.*

4.3 *Chaitin*-reducciones y *strong simulation*

La relación $\leq_{Ch}$ que definimos es un caso especial de 1-reducción, que agrega una restricción sobre longitudes: si $A \leq_{Ch} B$, entonces para cada palabra w en A existe una palabra z en B cuya longitud es menor o igual que la longitud de w más una constante. Podemos decir que z es "un poco más corta" que w. La relación de *strong simulation* también acota longitudes, pero en el otro sentido: si $A \leq_{ss} B$, para cada w en A existe z en B con longitud mayor o igual que la de w (más constante).

Esta analogía nos llevó a formularnos la Pregunta 4. Los siguientes dos resultados muestran que $\leq_{Ch}$ y $\leq_{ss}$ son relaciones inversas una de la otra:

Proposición 43 *Sean $A, B \subseteq \Sigma^*$ c.e. Si $A \leq_{Ch} B$ entonces $B \leq_{ss} A$.*

Demostración.

Supongamos que A y B son conjuntos c.e. tales que $A \leq_{Ch} B$. Veamos primero que existe $C \subseteq B$ tal que $C \leq_{ss} A$. Como $A \leq_{Ch} B$, existe una función f 1-1 recursiva, cuyo rango restringido a B es recursivo, tal que $\forall x(x \in A$ sii $f(x) \in B)$ y $\exists c \forall x \in Dom(f)(|f(x)| \leq |x|+c)$. Sea $C = Rango(f) \cap B$. Para cada $x \in C$, definimos $g(x) = y$ sii $f(y) = x$. g es función pues f es 1-1 y es recursiva pues f lo es. Además, como $f(x) \in C$ para todo $x \in A$, $Dom(g) = C$ y $g(C) = A$. Por último, como $A \leq_{Ch} B$ via f, en particular $A \leq_{Ch} C$ via la misma f, luego si $x \in A$, $f(x) \in C$ y $|f(x)| \leq |x| + c$. Entonces, si llamamos $y = f(x)$, tenemos $g(y) = x$ y $|y| \leq |g(y)| + c$. Por lo tanto, $C \leq_{ss} A$.

Ahora, para $x \in B \setminus C$, definimos $g(x) = y$ con y (por ejemplo) el primer elemento en una enumeración de A que verifique $|x| \leq |y|+c$ (siempre existe pues A es infinito). De esta manera obtenemos $Dom(g) = B$, $g(B) = A$ y $\exists c \forall x \in B(|x| \leq |g(x)| + c)$. $\otimes$

Proposición 44 *Sean $A, B \subseteq \Sigma^*$ c.e. Si $A \leq_{ss} B$ entonces $B \leq_{Ch} A$.*

Demostración. Supongamos $A \leq_{ss} B$ y veamos que $B \leq_{Ch} A$. Sea f recursiva tal que $Dom(f) = A$, $f(A) = B$ y $\exists c \forall x \in A(|x| \leq |f(x)|+c)$. Queremos ver que existe g 1-1 recursiva parcial con rango recursivo restringido a A, tal que $\forall x(x \in B$ sii $g(x) \in A)$ y $\exists c \forall x \in B(|g(x)| \leq |x| + c)$. Sea h una función recursiva que enumera el conjunto A (sin repeticiones). Para $x \in B$, definimos $g(x) = \min_i\{h(i)/i \in I\!N \wedge f(h(i)) = x\}$, es decir, $g(x)$ es el primer elemento y que aparezca en la enumeración de A tal que $f(y) = x$. g es una función recursiva (pues f lo es), es 1-1 y cumple que $x \in B$ sii $g(x) \in A$. Veamos que $Rango(g)$ restringido a A es recursivo. Para cada $y \in A$ debemos decidir si existe $x \in B$ tal que $y = g(x)$. Para ello, sea $y = h(k)$. Primero calculamos $f(y) = z$ y luego evaluamos $f(h(i))$ para todo

$i < k$. Si existe $i < k$ tal que $f(h(i)) = z$ entonces $y \notin Rango(g)$ y en caso contrario, $y \in Rango(g)$. Luego $Rango(g)$, restringido a A, es decidible. Por último, sea $y \in Dom(g)$ y $x \in A$ tal que $g(y) = x$. Como $x \in A$, $f(x) \in B$ y $|x| \leq |f(x)| + c$. Y como $x \in Rango(g)$, entonces $y = f(x)$ y $|g(y)| \leq |y| + c$.

$\otimes$

4.4 El Teorema de Slaman

Vamos a dar ahora dos demostraciones alternativas del Teorema de Slaman [13] basándonos en los resultados presentados, que solamente usan conceptos de la teoría de funciones recursivas. En contraste, la demostración original de Slaman y Kučera se obtiene a partir de la definición de aleatoriedad de Martin-Löf [14], que surge de la teoría de la medida constructiva, y se centra en tests constructivos de aleatoriedad, conocidos como *tests de Martin-Löf.*

En primer lugar probamos dos resultados análogos: un conjunto A es el dominio de una máquina universal si $Dom(U)$ es reducible a A vía *Chaitin*-reducciones o bien si $Dom(U)$ es reducible a A vía *strong simulation.* A partir de estos resultados podemos obtener como corolario el Teorema de Slaman.

El resultado basado en *Chaitin*-reducciones es el siguiente:

Proposición 45 *Sea $A \in \Sigma_1^0$ libre de prefijos tal que $Dom(U) \leq_{Ch} A$. Entonces A es el dominio de una máquina autodelimitante universal.*

Demostración. Damos el comportamiento de una máquina autodelimitante V con entrada p y mostramos que $A = Dom(V)$ y que V es universal.

Sean f y c la función y la constante dadas por la definición de *Chaitin*-reducciones. La Figura 2 da el comportamiento de la máquina V.

Veamos primero que $A = Dom(V)$:

1. Si $p \notin A$, claramente $V(p) \uparrow$.
2. Si $p \in A$ pueden darse dos casos:
   (a) si $p \notin Rango(f)$ entonces $V(p) = 1$.
   (b) si $p \in Rango(f)$ entonces, como $Dom(U) \leq_{Ch} A$, debe existir $w \in Dom(U)$ tal que $f(w) = p$ con $|p| = |f(w)| \leq |w| + c$. Esto garantiza que el ciclo `(*)` (potencialmente infinito) termina y en ese caso $V(p) = U(w)$.

   Luego, en ambos casos, $V(p) \downarrow$.

Veamos ahora que V es universal:

```
if p in A then {
/* semidecidible pues A es c.e.        */
    if p in Rango(f) then {
    /* decidible pues Rango(f)         */
    /* restringido a A es recursivo    */
        for each w s.t. |p|<=|w|+c do (*)
            if f(w)=p then {
                return U(w);
                exit for;
            }
     }
     else
         return 1;
}
else loop forever;
```

Figura 2: Construcción de V a partir de A, con $Dom(U) \leq_{Ch} A$

1. U es universal en el sentido clásico, es decir, satisface que existe una codificación recursiva h tal que $U(h(i,p)) = C_i(p)$ para toda máquina autodelimitante C_i y para todo p. Como $Dom(U) \leq_{Ch} A = Dom(V)$ vía la función recursiva f, entonces para todo $p \in Dom(U)$, $f(p) \in Dom(V)$ y, por la construcción de V, $V(f(p)) = U(p)$. Luego $f \circ h$ es una codificación recursiva que satisface $V(f(h(i,p))) = U(h(i,p)) = C_i(p)$, con lo cual V es universal en sentido clásico.
2. Además U es universal de Chaitin, es decir, para cada C_i existe una constante sim_i tal que para todo programa p exise un programa p' que cumple $U(p') = C_i(p)$ con $|p'| \leq |p| + sim_i$. Y, como $Dom(U) \leq_{Ch} A = Dom(V)$, para cada $p' \in Dom(U)$ existe $q \in Dom(V)$ tal que $|q| \leq |p'| + c$ y $V(q) = U(p')$. Luego, $V(q) = U(p') = C_i(p)$ con $|q| \leq |p'| + c \leq |p| + sim_i + c$ y por lo tanto V también es universal de Chaitin.

$\otimes$

Y la versión que usa *strong simulation*:

Proposición 46 *Sea $A \in \Sigma_1^0$ libre de prefijos tal que $Dom(U) \leq_{ss} A$. Entonces A es el dominio de una máquina autodelimitante universal.*

Demostración. Describimos el comportamiento de una máquina autodelimitante V y mostramos que $A = Dom(V)$ y que V es universal.

```
if p in A {
/* semidecidible pues A es c.e.    */
    for each w s.t. |w|<=|p|+c do (*)
        if f(w)=p then {
            return U(w);
            exit for;
        }
 }
 else loop forever;
```

Figura 3: Construcción de V a partir de A, con $Dom(U) \leq_{ss} A$

Sean f y c la función y la constante dadas por la definición de *strong simulation*. V con entrada p se comporta como se indica en la Figura 3.

Veamos primero que $A = Dom(V)$. Si $p \notin A$, entonces $V(p) \uparrow$. Si $p \in A$, la relación de *strong simulation* garantiza que existe un programa $w \in Dom(U)$ tal que $f(w) = p$ y $|w| \leq |f(w)| + c = |p| + c$, luego el ciclo `(*)` (finito) siempre encuentra el correspondiente w y en este caso $V(p) = U(w)$, con lo cual $V(p) \downarrow$.

Veamos ahora que V es universal:

1. En primer lugar, U es universal en el sentido clásico, luego existe una codificación recursiva h tal que $U(h(i,p)) = C_i(p)$ para toda máquina autodelimitante C_i y para todo programa p. Y si $Dom(U) \leq_{ss} A = Dom(V)$ vía la función recursiva f, entonces si $p \in Dom(U)$, $f(p) \in Dom(V)$ y por la construcción de V, $V(f(p)) = U(p)$. Luego $f \circ h$ es una codificación recursiva tal que $V(f(h(i,p))) = U(h(i,p)) = C_i(p)$. Es decir, V es universal en el sentido clásico.
2. Además, U es universal de Chaitin: para toda C_i existe una constante sim_i tal que para todo programa p existe otro programa p' que cumple:

   $$U(p') = C_i(p), \text{ con } |p'| \leq |p| + sim_i$$

   Y como $Dom(U) \leq_{ss} A = Dom(V)$, para todo $p' \in Dom(U)$ existe $q \in Dom(V)$ tal que $U(p') = V(q)$ y $|p'| \leq |q| + c$. Y $|q| + c \leq |p| + sim_i$ si y sólo si $|q| \leq |p| + sim_i - c$. Luego, tomando $k_i = sim_i - c$ si $c < sim_i$ o $k_i = 0$ en caso contrario, tenemos que para toda C_i existe k_i tal que $\forall p \, \exists q$ $(V(q) = C_i(p)$ y $|q| \leq |p| + k_i)$. Por lo tanto V es universal de Chaitin.

$\otimes$

Aplicando cada uno de estos resultados, obtenemos otras dos demostraciones del Teorema de Slaman:

Teorema 47 *Si* $\mathbf{a} \in [0,1]$ *es aleatorio c.e. entonces* $\mathbf{a}$ *es un* Ω*-number.*

Demostración 1. Como $\mathbf{a}$ es aleatorio c.e., por el Teorema 34, existe $A \in \Sigma_1^0$ libre de prefijos tal que $\mu(A\Sigma^\omega) = \mathbf{a}$ y $Dom(U) \leq_{Ch} A$. Y por la Proposición 45, A es el dominio de una máquina autodelimitante universal. Luego $\mathbf{a}$ es un Ω-number. $\otimes$

Demostración 2. Como $\mathbf{a}$ es aleatorio c.e., por el Teorema 41, existe $A \in \Sigma_1^0$ libre de prefijos tal que $\mu(A\Sigma^\omega) = \mathbf{a}$ y $Dom(U) \leq_{ss} A$. Y por la Proposición 46, A es el dominio de una máquina autodelimitante universal. Luego $\mathbf{a}$ es un Ω-number. $\otimes$

5 Relativización de resultados

En esta sección enunciamos la versión de los resultados obtenidos relativizada a oráculos en la jerarquía aritmética, y ejemplificamos su aplicación para dos casos particulares.

5.1 Caracterizaciones para reales n-aleatorios n-c.e.

Consideramos ahora las definiciones relativizadas de n-aleatoriedad, de reales n-c.e. y de n-dominación. Las definiciones de *strong simulation* y *Chaitin*-reducciones se mantienen sin cambios. Las demostraciones relativizadas se obtienen reemplazando las funciones y conjuntos recursivos (c.e.) usados por sus correspondientes versiones n-recursivas (n-c.e.).

La caracterización relativizada en base a *Chaitin*-reducciones viene dada por los siguientes resultados:

Teorema 48 *Si* $A \in \Sigma_{n+1}^0$ *es libre de prefijos y satisface que* $Dom(U^n) \leq_{Ch} A$*, entonces* $\mathbf{a} = \mu(A\Sigma^\omega)$ *es* n*-aleatorio y* n*-c.e.*

Teorema 49 *Sea* $\mathbf{a}$ *un real en* $[0,1]$ n*-aleatorio* n*-c.e. Existe* $A \in \Sigma_{n+1}^0$ *libre de prefijos tal que* $Dom(U^n) \leq_{Ch} A$ *y* $\mathbf{a} = \mu(A\Sigma^\omega)$*.*

Para el caso de *strong simulation*, los resultados relativizados son:

Teorema 50 *Sea* $A \in \Sigma_{n+1}^0$ *libre de prefijos tal que* $Dom(U^n) \leq_{ss} A$*. Entonces* $\mathbf{a} = \mu(A\Sigma^\omega)$ *es* n*-aleatorio y* n*-c.e.*

Teorema 51 *Si* $\mathbf{a}$ *es* n*-aleatorio* n*-c.e., existe* $A \in \Sigma_{n+1}^0$ *libre de prefijos con* $\mathbf{a} = \mu(A\Sigma^\omega)$ *tal que* $Dom(U^n) \leq_{ss} A$*.*

La relativización de los resultados que relacionan las reducciones $\leq_{Ch}$ y $\leq_{ss}$ permite obtener:

Proposición 52 *Sean $A, B \subseteq \Sigma^*$ n-c.e. Si $A \leq_{Ch} B$ entonces $B \leq_{ss} A$.*

Proposición 53 *Sean $A, B \subseteq \Sigma^*$ n-c.e. Si $A \leq_{ss} B$ entonces $B \leq_{Ch} A$.*

Y la versión generalizada del Teorema de Slaman:

Teorema 54 *Si $\mathbf{a} \in [0,1]$ es n-aleatorio n-c.e. entonces $\mathbf{a}$ es un Ω^n-number.*

5.2 α, β

Los resultados relativizados pueden usarse para demostrar la aleatoriedad de números cuyo grado de aleatoriedad es mayor que el de Ω. Damos, como ejemplo, dos instancias de aplicación para los reales α [11, 2] y β [1].

En ambos casos, la definición del número está basada en una máquina autodelimitante universal para cómputos infinitos fija U^∞. Las máquinas introducidas por Turing en su artículo de 1936 [19] son en efecto máquinas de cómputo infinito. La formalización de la definición de máquinas de cómputo infinito sigue la línea de trabajo comenzada por Chaitin en [9]. Más detalles sobre este tema pueden verse en [3].

α es la probabilidad de que U^∞ produzca una salida finita. En [11, 2] se prueba que α es 1-aleatorio, es decir, es aleatorio aún contando con un oráculo para el problema de la detención. Por lo tanto, su complejidad es mayor que la de Ω: de hecho, α tiene el mismo grado de aleatoriedad que Ω', la probabilidad de detención de U', una máquina autodelimitante universal para cómputos finitos con oráculo $\emptyset'$. La demostración se basa en el siguiente resultado:

Teorema 55 ([2]) *Existe una cadena $\%$ tal que para todo programa p, $U'(p) \downarrow$ sii existe un conjunto finito libre de prefijos maximal E_p tal que, para todo $x \in E_p$, $U^\infty(\%px)$ produce una salida finita.*

Este resultado puede usarse en combinación con nuestro Teorema 48 para obtener la prueba de la 1-aleatoriedad de α. Sea

$$Fin = \{p \in \Sigma^* / U^\infty(p) \text{ produce una salida finita}\}$$

$Fin \in \Sigma_2^0$ y es libre de prefijos, y lo mismo verifica el conjunto

$$\begin{aligned} N(Fin) = & \\ & \{p \in \Sigma^* / \% \preceq p \wedge \{x / px \in Fin\} \text{ es finito libre de prefijos maximal } \} \\ & \cup \{p \in Fin / \% \not\preceq p\} \end{aligned}$$

Se puede ver que $\mu(Fin\Sigma^\omega) = \mu(N(Fin)\Sigma^\omega) = \alpha$ y que la función f dada por $f(p) = \%p$ para todo $p \in \Sigma^*$ es una *Chaitin*-reducción entre $Dom(U')$ y $N(Fin)$, con lo que podemos aplicar el Teorema 48 para obtener que $\alpha = m(N(Fin))$ es 1-aleatorio.

Una estrategia similar puede usarse para probar la 2-aleatoriedad del real β, definido y demostrado aleatorio en [1]. En este caso se interpreta la salida de una máquina de cómputo infinito como un conjunto de naturales. β es la probabilidad de que U^∞ produzca como salida un conjunto cofinito. El grado de aleatoriedad de β es el de Ω'', la probabilidad de detención de una máquina autodelimitante universal de cómputos finitos con oráculo $\emptyset''$, y en consecuencia la complejidad de β es mayor que la de α (y por supuesto que la de Ω). El resultado que se obtiene en [1] es el siguiente:

Teorema 56 ([1]) *Existe una cadena* $\%$ *tal que para todo programa* p, $U''(p)\downarrow$ *sii, para toda secuencia* $\mathbf{x}$, $U^\infty(p\mathbf{x})$ *es un conjunto cofinito.*

Como antes, definimos

$$Cof = \{p \in \Sigma^* / U^\infty(p\mathbf{x}) \text{ es un conjunto cofinito } \forall \mathbf{x} \in \Sigma^\omega\}$$

y en este caso puede mostrarse que $Cof \in \Sigma^0_3$ y es libre de prefijos, que $\beta = \mu(Cof\ \Sigma^\omega)$ y que $Dom(U'') \leq_{Ch} Cof$, con lo cual, por el Teorema 48, β es 2-aleatorio.

Por último, notemos que el Teorema 54 responde a una pregunta planteada sobre el final de [11]: este resultado nos asegura que α es la probabilidad de detención de una máquina autodelimitante universal con oráculo $\emptyset'$, y β la de una con oráculo para $\emptyset''$.

6 Conclusiones y trabajo futuro

Damos una síntesis de los resultados presentados en este trabajo mediante un teorema de equivalencias, y continuamos la lista de preguntas con cuestiones aún no resueltas.

6.1 Equivalencias

En resumen, hemos demostrado las siguientes equivalencias:

Teorema 57 *Sea* $\mathbf{a}$ *un real en* $[0, 1]$. *Las siguientes afirmaciones son equivalentes:*

1. $\mathbf{a}$ *es n-aleatorio n-c.e.*
2. $\mathbf{a}$ *es la medida asociada a un conjunto libre de prefijos y n-c.e.* A *tal que* $Dom(U^n) \leq_{Ch} A$.

3. **a** *es la medida asociada a un conjunto libre de prefijos y n-c.e. A tal que* $Dom(U^n) \leq_{ss} A$.

4. **a** *es la medida asociada a un conjunto libre de prefijos y n-c.e. A tal que* $A \leq_{Ch} Dom(U^n)$.

5. **a** *es la medida asociada a un conjunto libre de prefijos y n-c.e. A tal que* $A \leq_{ss} Dom(U^n)$.

6. **a** *es un* Ω^n-number.

DEMOSTRACIÓN. $1 \Leftrightarrow 2$ por los Teoremas 48 y 49. $2 \Leftrightarrow 3$ por las Proposiciones 52 y 53. $1 \Leftrightarrow 4$ por los Teoremas 51 y 50. $4 \Leftrightarrow 5$ nuevamente por las Proposiciones 52 y 53. $1 \Rightarrow 6$ por el Teorema 54 y por último $6 \Rightarrow 1$ por el Teorema 25.

$\otimes$

Podemos concluir, entonces, que un real es aleatorio c.e. si y sólo si es la medida asociada a un conjunto que, para cada programa en U, contiene una palabra de aproximadamente la misma longitud. Y este es el "aspecto" de los dominios de máquinas autodelimitantes universales. En otras palabras, tenemos cierto grado de libertad para elegir "nombres" para los objetos, pero esta libertad está acotada en el sentido que no podemos variar su complejidad más allá de un término constante. Esto concuerda, felizmente, con el hecho de que las máquinas autodelimitantes universales son asintóticamente óptimas y con la idea que expresa el Teorema de Invarianza.

6.2 Más preguntas

Finalizamos este trabajo proponiendo nuevos interrogantes relacionados con los resultados que hemos obtenido, y que pueden ser motivo de investigación futura sobre el tema.

En primer término nos planteamos generalizar las propiedades de la relación de *Chaitin*-reducciones:

Pregunta 6 *¿Es posible obtener un resultado similar al Lema 37 para la relación* $\leq_{Ch}$*?*

Las Proposiciones 43 y 44 sugieren que la respuesta es afirmativa. Entonces, el cuestión que surge naturalmente es:

Pregunta 7 *¿Es cierta la recíproca de la versión del Lema 37 para* Chaitin*-reducciones?*

Los resultados mencionados indicarían que no, con lo cual se propone exhibir conjuntos que constituyan un contraejemplo y considerar el siguiente interrogante:

Pregunta 8 *¿Se puede demostrar una versión similar a la recíproca débil dada por el Teorema 38 para $\leq_{Ch}$?*

Como propuesta de trabajo inmediato, nos planteamos obtener los resultados que respondan a estas primeras preguntas.

Hemos mostrado en este trabajo la aleatoriedad de las medidas asociadas a conjuntos a los cuales es posible reducir el dominio de U, ya sea vía *Chaitin*-reducciones o vía *strong simulation*. Una cuestión que puede resultar de interés es obtener un resultado similar aunque más fuerte:

Pregunta 9 *¿Existen conjuntos* equivalentes *a $Dom(U)$, con respecto a $\leq_{Ch}$ o a $\leq_{ss}$, tales que su medida asociada sea un real aleatorio?*

Otra cuestión para analizar se refiere a las demostraciones de aleatoriedad de los reales α y β. En ellas usamos la relativización de nuestra caracterización basada en *Chaitin*-reducciones. ¿Qué ocurre con *strong simulation*? Es decir:

Pregunta 10 *¿Es posible exhibir conjuntos a los cuales se puedan reducir $Dom(U')$ y $Dom(U'')$ vía* strong simulation*, cuyas medidas asociadas sean los reales α y β, respectivamente?*

Por último, todos los resultados que presentamos se restringen a reales c.e., o n-c.e. Otra posible línea de trabajo, entonces, sería investigar versiones más generales de las caracterizaciones que hemos dado:

Pregunta 11 *¿Es posible obtener caracterizaciones de otras clases de reales aleatorios, por ejemplo los que no son c.e. para ningún nivel de la jerarquía aritmética?*

Creemos que una respuesta a esta última cuestión podría ser significativa para profundizar la comprensión del concepto de aleatoriedad.

Bibliografía

[1] V. Becher and G. Chaitin. β. Unpublished manuscript, 2001.

[2] V. Becher, S. Daicz, and G. Chaitin. A highly random number. In C. S. Calude, M. J. Dineen, and S. Sburlan, editors, *Combinatorics, Computability and Logic: Proceedings of the Third Discrete Mathematics and Theoretical Computer Science Conference (DMTCS'01)*, pages 55–68. Springer-Verlag London, 2001.

[3] V. Becher and S. Grigorieff. $\emptyset'$-random reals and outputs of possibly infinite computations. Unpublished manuscript, 2002.

[4] C. S. Calude. *Information and Randomness. An Algorithmic Perspective*. Springer-Verlag, Berlin, 1994.

[5] C. S. Calude. A characterization of c.e. random reals. *Theoretical Computer Science*, 271:3–14, 2002.

[6] C. S. Calude, P. H. Hertlind, B. Khoussainov, and Y. Wang. Recursively enumerable reals and Chaitin Ω-numbers. In *Proceedings of the Symposium on Theoretical Aspects of Computer Science (STACS 98)*, pages 596–606. Springer, Berlin, 1998.

[7] G. J. Chaitin. Information-theoretic limitations of formal systems. *J. ACM*, 21:403–424, 1974.

[8] G. J. Chaitin. A theory of program size formally identical to information theory. *J. Assoc. Comput. Mach.*, 22:329–340, 1975.

[9] G. J. Chaitin. Algorithmic entropy of sets. *Computers & Mathematics with Applications*, 2:233–245, 1976.

[10] G. J. Chaitin. *Algorithmic Information Theory*. Cambridge University Press, 3^{rd} printing (with revisions), 1990.

[11] S. Daicz. Una nueva versión de la probabilidad de detención. Tesis de Licenciatura, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, 2000.

[12] L. G. Kraft. A device for quantizing, grouping and coding amplitude modulated pulses. Master's thesis, Dept. of Electrical Engineering, M.I.T., Cambridge, Massachusets, 1949.

[13] A. Kučera and T. Slaman. Randomness and recursive enumerability. *SIAM J. on Computing*, 31(1):199–211, 2001.

[14] P. Martin-Löf. The definition of random sequences. *Information and Control*, (9):602–619, 1966.

[15] P. G. Oddifreddi. *Classical Recursion Theory*, volume 1. North Holland, Amsterdam, 1989.

[16] H. Rogers Jr. *Theory of Recursive Functions and Effective Computability*. MIT Press, Cambridge, Massachusetts, 1987.

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

[18] R. M. Solovay. Draft of a paper (or series of papers) on Chaitin's work. Unpublished manuscript, IBM Thomas J. Watson Research Center, New York, 1975.

[19] A. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society, 2nd series*, 42:230–265, 1936.