Tesis de Licenciatura
Departamento de Computación, FCEyN, UBA

Nociones de aleatoriedad y transformaciones de cambio de base

Andrés Taraciuk
Director: Santiago Figueira

21 de Diciembre de 2010

Resumen

Aunque es razonable pensar que cualquier definición de aleatoriedad debe ser invariante por una transformación sencilla como el cambio de base, no hay muchos trabajos sobre este fenómeno. En los casos conocidos, las demostraciones resultan bastante complicadas. En esta tesis trabajamos con distintas definiciones formales de aleatoriedad para representaciones de los números reales en distintas bases.

Para la definición de aleatoriedad vía martingalas con recursos acotados, probamos que $n \cdot \log^3 n$-aleatoriedad implica normalidad, siguiendo la representación tradicional en base 2. Extendemos este resultado para probar que $n \cdot \log^3 n$-aleatoriedad en base b implica normalidad en base b, para cualquier base $b \geq 2$. Este resultado va en la dirección de encontrar nuevos algoritmos para computar números absolutamente normales.

Estudiamos una demostración de que aleatoriedad de Martin-Löf es invariante por cambio de base presentada por Calude. Detectamos y corregimos errores no triviales que aparecen en esa demostración.

Damos una demostración nueva (a nuestro modo de ver, más directa, sencilla y corta que aquella presentada por Calude), de que Martin-Löf aleatoriedad es invariante por cambio de base, y adaptamos el resultado para las definiciones de aleatoriedad de Schnorr y de Kurtz.

Planteamos una conjetura acerca de la invariancia por cambio de base de $t(n)$-aleatoriedad, y damos un esquema nuevo que podría ser usado para construir números absolutamente normales.

Dedicado a mis viejos

'Run, live to fly, fly to live, do or die
Run, live to fly, fly to live, aces high.'

Índice

1. Agradecimientos

A Santiago Figueira, por haber aceptado ser mi director. Por toda la voluntad que puso para que este trabajo sea una realidad. Por todo el apoyo que me dio a lo largo de la tesis. Por haberme empujado en momentos en los que me costaba seguir. Y por haber hecho todo con la mejor disposición posible.

A Verónica Becher y Sergio Daicz, por ser los jurados de la tesis. Por haberse tomado el trabajo de leerla, corregirla y hacer aportes.

A *los pibes de la facu*, por haber compartido conmigo todos estos años de facultad. Habría sido imposible terminar la carrera sin un buen grupo de amigos de la facultad con quien pasar buenos momentos, o en quienes apoyarme para las materias complicadas. Quiero agradecer especialmente a mis compañeros del grupo de TPs, por haberme bancado en algunos trabajos.

A la mayoría de los docentes que tuve a lo largo de la carrera, por haberme dado una educación académica de primer nivel. Y por haberlo hecho siempre con la mejor voluntad y con humilidad.

A mi familia y al resto de mis amigos, por ser parte de mi vida.

2. Introducción

Esta tesis se centra en el estudio de la representación en distintas bases para números aleatorios, para distintas definiciones de aleatoriedad. Trabajaremos con las siguientes definiciones de aleatoriedad: normalidad, aleatoriedad computable ([15] y [14]), aleatoriedad limitada por recursos([15]), aleatoriedad de Martin-Löf ([11]), aleatoriedad de Schnorr ([15]) y aleatoriedad de Kurtz ([10]).

La noción de normalidad es una definición muy débil de aleatoriedad. Un número es *normal* en una base si todas las posibles cadenas finitas de igual longitud aparecen en él con la misma frecuencia.

Una secuencia es *aleatoria computable* si no es posible encontrar una estrategia ganadora para dicha secuencia. Si la estrategia está limitada por algún tipo de recurso (por ejemplo, temporal o de memoria), se trata de *aleatoriedad limitada por recursos*. Para hablar de límites temporales a las estrategias, diremos que una secuencia es $t(n)$-*aleatoria* si no hay una estrategia ganadora cuyo orden de complejidad temporal pertenezca a $\mathbf{DTIME}(t(n))$ (donde n es el tamaño de la cadena).

Una secuencia es *Martin-Löf aleatoria* si es imposible encontrar un test estadístico razonable que detecte patrones en la secuencia. Más específicamente, si no se puede acotar indefinidamente el conjunto al que posiblemente pertenezca dicha secuencia. El concepto de *Schnorr aleatoriedad* es análogo, pero se restringen los posibles tests a aquellos que tienen medida computable. El concepto de *Kurtz aleatoriedad* es análogo al de Martin-Löf pero se restringen los test a aquellos que tienen finitos elementos.

Tradicionalmente, las definiciones de aleatoriedad siempre se basan en el alfabeto $\{0, 1\}$, o sea, trabajan en base binaria. Se ha hecho poco en relación a generalizar las definiciones para trabajar en una base genérica.

Además, a pesar de que se considera lógico suponer que la mayoría de las definiciones de aleatoriedad son invariantes por cambio de base, no existe mucha bibliografía al respecto donde se pruebe esto para distintas definiciones.

En la sección 4, trabajamos con la noción de normalidad, una definición muy débil de aleatoriedad. En esta dirección, probamos que $n \cdot \log^3 n$-aleatoriedad en base b implica normalidad en base b.

En [8], Calude da una demostración de que Martin-Löf aleatoriedad es invariante por cambio de base. Sin embargo, esa demostración resultó tener errores no menores. En la sección 5, mostramos los errores de dicha demostración, encontramos contraejemplos para los lemas que resultaron falsos, y ajustamos y corregimos la demostración de [8].

En la sección 6, damos una demostración propia de que Martin-Löf aleatoriedad es invariante por cambio de base, pues encontramos una demostración mucho más corta y directa que la de [8] y, a nuestro parecer, sencilla; además, extendemos el resultado para probar que Schnorr y Kurtz aleatoriedad son invariantes por cambio de base.

Por último, en la sección 7 mostramos en qué sentido los resultados de la sección 4 sobre normalidad y aleatoriedad acotada por recursos pueden ayudar para dar un esquema general para la construcción de números absolutamente normales. Enunciamos una conjetura que, de ser verdadera, nos permite encontrar nuevos algoritmos para números absolutamente normales, que podrían ser mejores que los conocidos.

3. Preliminares

3.1. Secuencias, conjuntos, intervalos, números reales

Si σ es una cadena, $\sigma(i)$ es el i-ésimo elemento de σ (el primer elemento de σ es $\sigma(0)$), $\sigma \restriction n$ es la cadena $\sigma(0)\dots\sigma(n-1)$, $|\sigma|$ es la longitud de σ y $\sigma[i..j]$ es la cadena $\sigma(i)\sigma(i+1)\cdots\sigma(j)$. Con λ nos referiremos a la cadena vacía.

Para el número natural n, denotamos con n al conjunto $\{0,\dots,n-1\}$. n^* es el conjunto de todas las cadenas finitas formadas con el alfabeto n. n^l es el conjunto de todas las cadenas finitas de longitud l formadas con el alfabeto n. n^+ es el conjunto de todas las cadenas finitas formadas con el alfabeto n, excluyendo a λ. n^ω es el conjunto de todas las secuencias infinitas formadas con el alfabeto n. Diremos que una cadena de n^*, n^+ o n^ω está escrita en base n.

Dadas una clase $\mathcal{C} \subseteq n^\omega$ y una cadena $\sigma \in n^*$, definimos

$$\sigma\mathcal{C} = \{\sigma Z : Z \in \mathcal{C}\}.$$

Es decir, $\sigma\mathcal{C}$ representa la clase de secuencias que empiezan con σ y siguen con alguna secuencia de $\mathcal{C}$. Por ejemplo, 1012^ω es el conjunto $\mathcal{B} \subseteq 2^\omega$ tal que 101 es el prefijo de toda secuencia en $\mathcal{B}$. Análogamente, dados una clase $\mathcal{C} \subseteq n^\omega$ y un conjunto $A \subseteq n^*$, definimos

$$A\mathcal{C} = \{\sigma Z : \sigma \in A, Z \in \mathcal{C}\}.$$

Es decir, $A\mathcal{C}$ representa la clase de secuencias que empiezan con alguna cadena de A y siguen con alguna secuencia de $\mathcal{C}$.

La *medida uniforme* en base b, μ_b asigna a cada cilindro σb^ω (donde $\sigma \in b^*$) la magnitud $b^{-|\sigma|}$. Para cualquier $A \subseteq b^*$ tenemos $\mu_b(Ab^\omega) \leq \sum_{\sigma\in A} b^{-|\sigma|}$. Si además A es libre de prefijos entonces vale la igualdad.

Los conjuntos co-infinitos de números naturales pueden ser identificados con los reales en $[0,1]$ via su expansión binaria. El conjunto $Z \subseteq \mathbb{N}$ se identifica con el número real

$$0.Z = \sum_{i\in Z} 2^{-i-1}.$$

Al revés, cualquier número real r puede ser escrito como $r = \sum_{i\geq 0} r_i \cdot 2^{-i-1}$, donde $r_i \in \{0,1\}$. Decimos que $0.r_0r_1r_2$ es la expansión binaria de r. Los racionales diádicos (de la forma $z\cdot 2^{-n}$, para algún $z,n \in \mathbb{N}$) tienen dos posibles representaciones binarias: una que termina con infinitos ceros y otra que termina con infinitos unos. Para estos racionales, preferimos la representación con infinitos ceros. Por ejemplo, el racional $1/4$ se escribirá en binario como $0{,}010000\dots$ y no como $0{,}001111\dots$, de modo que representará al conjunto co-infinito $\{1\}$ y no al conjunto co-finito $\{2,3,4,5,\dots\}$.

De esta manera, la medida uniforme en el espacio de Cantor 2^ω se convierte en la medida uniforme de Lebesgue sobre $[0,1]$, denotada μ.

Sea $b \geq 2$ y $Z \in b^\omega$. Definimos $v_b(Z)$ al número real en el intervalo $[0,1]$ representado, en base b, con $0.Z$, es decir,

$$v_b(Z) = \sum_{i\geq 0} Z(i)\cdot b^{-(i+1)}.$$

La definición es análoga para cadenas finitas. Sea $b \geq 2$ y $\sigma \in b^*$,

$$v_b(\sigma) = \sum_{0\leq i<|\sigma|} \sigma(i)\cdot b^{-(i+1)}.$$

Dadas dos cadenas σ e τ, notaremos $\sigma \preceq \tau$ cuando σ es prefijo de τ, o sea, cuando existe ρ tal que $\tau = \sigma\rho$. Diremos que $A \subseteq b^*$ es *libre de prefijos* si

$$\sigma \preceq \tau \Rightarrow \sigma = \tau$$

para todo $\sigma, \tau \in A$.

3.2. Números normales

Una secuencia $Z \in 2^\omega$ satisface la Ley de los grandes números si la frecuencia relativa del 0 coincide con la del 1. En otras palabras,

$$\lim_{n\to\infty} \frac{\sum_{0\le i<n} Z(i)}{n} = \frac{1}{2} \ .$$

Para $\sigma, \tau \in b^*$, $|\sigma| \le |\tau|$, sea $C_\sigma(\tau)$ la cantidad de apariciones de σ en τ, es decir,

$$C_\sigma(\tau) = \#\{j : 0 \le j \le |\tau| - |\sigma| \wedge \tau[j..j + |\sigma| - 1] = \sigma\}.$$

Notar que

$$C_\sigma(\tau) - 1 \le \sum_{0\le i<b} C_{\sigma i}(\tau) \le C_\sigma(\tau) \ . \tag{1}$$

Un número $r = 0.Z$ se dice *simplemente normal en base b* si

$$\lim_{n\to\infty} \frac{C_\sigma(Z \upharpoonright n)}{n} = b^{-1}$$

para todo $\sigma \in \{0, 1, \cdots, b-1\}$. O sea, si todos los caracteres del alfabeto aparecen en el límite con la misma frecuencia.

Es inmediato ver que la noción de normalidad simple no es invariante por cambio de base. Por ejemplo, el número 0,101010... escrito en base 2 es simplemente normal en base 2, pero, en base 4, se representa como 0,22222..., que claramente no es normal en base 4.

El número $r = 0.Z$ (en donde $Z \in b^\omega$ representa la expansión en base b de r) es *normal en base b* si

$$\lim_{n\to\infty} \frac{C_\sigma(Z \upharpoonright n)}{n} = b^{-|\sigma|}$$

para todo $\sigma \in b^*$.

En otras palabras, un número Z es normal en base b si, para toda longitud l, todas las cadenas de longitud l en base b aparecen en el límite con la misma frecuencia en Z. Como hay b^l posibilidades, todas las cadenas de longitud l deben aparecer con frecuencia b^{-l} para que el número sea normal.

Un número se dice *absolutamente normal* si es normal para toda base $b \ge 2$.

Es fácil ver que ningún número racional puede ser normal (pues se repite el período). Por otro lado, está probado en [7] que *casi todos* los números reales son absolutamente normales, o sea, el conjunto de los números que no lo son tiene medida 0. Sin embargo, es muy difícil encontrar explícitamente un número absolutamente normal. Se cree que las constantes irracionales conocidas, como π, e y $\sqrt{2}$, son absolutamente normales, pero no hay prueba de ello [3].

El número de *Champernowne*

$$0{,}1234567891011121314\ldots,$$

escrito en base 10, es normal en base 10 [9].

Hay trabajos recientes [6, p. 7] que enuncian que no se sabe si Champernowne es normal en otras bases. En cuanto al problema más general de que normalidad no es lo mismo que normalidad absoluta, Schmidt [13, Teorema 1B] prueba que si r y s son dos bases tal que $r^m \neq s^n$ para todo m, n, entonces la cantidad de números que son normales en base r pero no simplemente normales en base s (y por lo tanto no normales en base s), es no-numerable. Dicho sea de paso, es un ejemplo de un conjunto no numerable de medida cero, como el ternario de Cantor. La demostración no es nada fácil y excede completamente el alcance de esta tesis.

3.3. Definiciones formales de aleatoriedad

En esta sección damos varias definiciones conocidas de aleatoriedad. Clásicamente, estas definiciones se dan para secuencias binarias, pero todas pueden ser generalizadas a bases arbitrarias.

3.3.1. Aleatoriedad de Martin-Löf

En [11], se define a un *test de Martin-Löf* como una secuencia $(G_m)_{m\in\mathbb{N}}$, $G_m \subseteq 2^*$, uniformemente c.e. tal que $(\forall m)\mu_2(G_m 2^\omega) \leq 2^{-m}$. Una secuencia $Z \in 2^\omega$ se dice que es *Martin-Löf aleatoria* si $Z \notin \bigcap_m G_m 2^\omega$ para todo posible test de Martin-Löf $(G_m)_{m\in\mathbb{N}}$ (se dice que no existe ningún test que tenga éxito en Z).

Un *test de Solovay*, definido en [16], es una secuencia $(G_m)_{m\in\mathbb{N}}$, $G_m \subseteq 2^*$, uniformemente c.e. tal que $\sum_m \mu_2(G_m 2^\omega) < \infty$. Una secuencia $Z \in 2^\omega$ *falla* un test de Solovay si $Z \in G_m 2^\omega$ para infinitos ms. De otra manera, Z *pasa* el test. Está probado que una secuencia Z es Martin-Löf aleatoria sii Z pasa cada posible test de Solovay ([12, Proposición 3.2.19] y [8, Teorema 6.37]).

3.3.2. Aleatoriedad de Schnorr

En [15], Schnorr critica la definición de aleatoriedad de Martin-Löf por ser muy fuerte, y entonces no poder ser considerada algorítmica. Esto se debe a que, en un test de Martin-Löf, $\mu_2(G_m 2^\omega)$ puede no ser computable (aunque sí es aproximable computablemente desde abajo). Un *test de Schnorr* es un test de Martin-Löf con la restricción adicional de que $(\forall m)\mu_2(G_m 2^\omega)$ es un número real computable. Una secuencia $Z \in 2^\omega$ es *Schnorr aleatoria* si $Z \notin \bigcap_m G_m 2^\omega$ para todo posible test de Schnorr $(G_m)_{m\in\mathbb{N}}$.

El conjunto de secuencias binarias que son Martin-Löf aleatorias está incluido en el conjunto de secuencias binarias que son Schnorr aleatorias, y que la inclusión es estricta ([12, p. 128]).

3.3.3. Aleatoriedad de Kurtz

Esta definición de aleatoriedad debilita la definición de Martin-Löf, restringiendo los tests a aquellos en los que cada G_m es un conjunto *finito*.

Un *test de Kurtz* [10], es una secuencia efectiva $(G_m)_{m\in\mathbb{N}}$, $G_m \subseteq 2^*$, de conjuntos finitos tal que $\sum_m \mu_2(G_m 2^\omega) < 2^{-m}$. Una secuencia $Z \in 2^\omega$ se dice que es *Kurtz aleatoria* si $Z \notin \bigcap_m G_m 2^\omega$ para todo posible test de Kurtz $(G_m)_{m\in\mathbb{N}}$.

Si una secuencia es Schnorr aleatoria entonces es Kurtz aleatoria, pero la vuelta no vale ([12, 7.5.11]).

3.3.4. Aleatoriedad Computable

En [15] y [14], se introduce la idea de analizar la aleatoriedad de una secuencia mediante el uso de estrategias ganadoras, llamadas martingalas.

Una *martingala* es una función $d : 2^* \to \mathbb{Q}_{\geq 0}$ tal que:

- $d(\lambda) > 0$
- $(\forall x \in 2^*) d(x0) + d(x1) = 2d(x)$

Una martingala d *tiene éxito* en un conjunto Z si

$$\limsup_{n\to\infty} d(Z \upharpoonright n) = \infty.$$

Esta definición puede entenderse como un juego justo de apuestas sobre una secuencia binaria infinita: El apostador empieza con capital $d(\lambda)$ y, en cada ronda, dependiendo de los resultados anteriores x, apuesta una cierta fracción $\alpha \cdot d(x)$ $(0 \leq \alpha \leq 1)$ de su capital actual $d(x)$ a que sale el evento 0 (y el restante $(1-\alpha)\cdot d(x)$ a que sale 1). El jugador recibe el doble de lo apostado en cada caso (quedándose $2\cdot\alpha\cdot d(x)$ como capital en caso de 0 y $2\cdot(1-\alpha)\cdot d(x)$ como capital en caso de 1).

Una martingala también puede ser caracterizada por su estrategia subyacente. La estrategia es la función que determina, dada una secuencia binaria, qué porcentaje del capital acumulado apostar a que el próximo bit es un 0 (el porcentaje restante es si sale 1). Una *estrategia* es una función $s : 2^* \to \mathbb{Q}_{\geq 0} \cap [0, 1]$.

Entonces, dada una martingala d, *su estrategia subyacente* s_d será:

$$s_d(x) = \begin{cases} \frac{d(x0)}{2d(x)} & \text{si } d(x) \neq 0 \\ 0 & \text{si no} \end{cases}$$

De la misma manera, a partir de una estrategia s, podemos encontrar la *martingala inducida* d_s (siendo $d_s(\lambda)$ cualquier racional positivo):

$$\begin{aligned} d_s(x0) &= 2 \cdot s(x) \cdot d_s(x) \\ d_s(x1) &= 2 \cdot (1 - s(x)) \cdot d_s(x) \end{aligned}$$

Una secuencia binaria es *aleatoria computable* si no existe ninguna martingala que tenga éxito para esa secuencia. Está probado que el conjunto de cadenas Martin-Löf aleatorias está incluido en el conjunto de cadenas aleatorias computables, y que la inclusión es estricta ([12, Teorema 7.5.7]). También está probado que el conjunto de cadenas aleatorias computables está incluido en el conjunto de cadenas Schnorr aleatorias, y que la inclusión es estricta ([12, Proposición 7.3.2 y Teorema 7.5.10]). En otras palabras, el concepto de aleatoriedad computable es más débil que Martin-Löf aleatoriedad, pero más fuerte que Schnorr aleatoriedad.

Se dice que una martingala L *domina multiplicativamente* a otra martingala F cuando existe $c \in \mathbb{N}$ tal que $F(\sigma) \leq c \cdot L(\sigma)$ para cada σ ([12, Definición 7.4.7]).

3.3.5. Aleatoriedad limitada por recursos

A partir de la definición de aleatoriedad con martingalas, es posible modificar el concepto de aleatoriedad en base a los recursos necesarios para computar la martingala. Por ejemplo, imponiendo cotas temporales.

Entonces, es necesario relacionar el concepto de complejidad temporal con el concepto de complejidad de una martingala. Existen diferentes variaciones: Ambos-Spies y Mayordomo en [1, p. 10] consideran a una martingala d una $t(n)$-martingala si d es una martingala inducida a partir de una estrategia s tal que $s \in \mathbf{DTIME}(t(n))$. Por otro lado, Schnorr en [15] define a una martingala d una $t(n)$-martingala si $d \in \mathbf{DTIME}(t(n))$. En esta tesis seguimos esta última convención.

De esta manera, se considera que una secuencia binaria es $t(n)$-*aleatoria* si no existe ninguna $t(n)$-martingala que tenga éxito para esa secuencia.

3.4. Generalización de las definiciones de aleatoriedad a otras bases

Todas las definiciones de aleatoriedad enunciadas tratan sobre secuencias binarias. Asimismo, todas las definiciones pueden generalizarse a otras bases.

3.4.1. Aleatoriedad de Martin-Löf para base b

Dada una base b, un *test de Martin-Löf en base b* es una secuencia $(G_m)_{m\in\mathbb{N}}$, $G_m \subseteq b^*$, uniformemente c.e. tal que $(\forall m)\mu_b(G_m b^\omega) \leq b^{-m}$. Una secuencia $Z \in b^\omega$ se dice que es *Martin-Löf aleatoria en base b* si $Z \notin \bigcap_m G_m b^\omega$ para todo posible test de Martin-Löf $(G_m)_{m\in\mathbb{N}}$ en base b (se dice que no existe ningún test que tenga éxito en Z).

3.4.2. Aleatoriedad de Schnorr para base b

Un *test de Schnorr en base b* es un test de Martin-Löf en base b con la restricción adicional de que $(\forall m)\mu_b(G_m b^\omega)$ es computable. Una secuencia $Z \in b^\omega$ se dice que es *Schnorr aleatoria en base b* si $Z \notin \bigcap_m G_m b^\omega$ para todo posible test de Schnorr $(G_m)_{m\in\mathbb{N}}$ en base b.

3.4.3. Aleatoriedad de Kurtz para base b

Un *test de Kurtz en base b* es una secuencia efectiva $(G_m)_{m\in\mathbb{N}}$, $G_m \subseteq b^*$, de conjuntos finitos tal que $\sum_m \mu_b(G_m b^\omega) < b^{-m}$. Una secuencia $Z \in b^\omega$ se dice que es *Kurtz aleatoria en base b* si $Z \notin \bigcap_m G_m b^\omega$ para todo posible test de Kurtz en base b $(G_m)_{m\in\mathbb{N}}$.

3.4.4. Aleatoriedad computable para base b

El concepto de martingala también puede ser extendido: una *martingala en base b* es una función $d : b^* \to \mathbb{Q}_{\geq 0}$ tal que:

- $d(\lambda) > 0$
- $(\forall x \in b^*) \sum_{0\leq i<b} d(xi) = b \cdot d(x)$

La noción de éxito para una secuencia en base b en una martingala en base b es idéntico al de base 2. Una secuencia Z en base b es *aleatoria computable* si no existe ninguna martingala en base b que tenga éxito en Z.

3.4.5. Aleatoriedad limitada por recursos para base b

La definición es análoga a aquella para $t(n)$-aleatoriedad en base 2.

3.5. Invariancia por cambio de base

Algunos números reales tienen dos posibles representaciones en una base dada. Por ejemplo, en base 2,

$$0{,}01111111\ldots \qquad y \qquad 0{,}10000000\ldots$$

representan el mismo número real escrito en binario (es decir $v_2(011111\ldots) = v_2(100000\ldots)$). En caso de reales con más de una representación en base b, elegiremos aquellas representaciones que tengan una cola de infinitos símbolos $b-1$.

Dada una secuencia Z_p en base p, diremos que la secuencia Z_q es la representación de Z_p en base q si $v_p(Z_p) = v_q(Z_q)$.

La pregunta que nos hacemos es, entonces, si las definiciones formales de aleatoriedad son invariantes por cambio de base. En otras palabras, si es válido que para todo $q, p \geq 2$, si $v_p(Z_p) = v_q(Z_q)$ entonces Z_p es aleatorio en base p sii Z_q es aleatorio en base q (aquí 'aleatorio' denota alguna de las definiciones de aleatoriedad que estudiaremos).

Sean P_1 y P_2 dos propiedades tales que $(\forall Z)P_1(Z) \Rightarrow P_2(Z)$ (por ejemplo, P_1 = ser Martin-Löf aleatorio y P_2 = ser Schnorr aleatorio). Sea T una transformación (por ejemplo, T = cambio de base).

Si P_1 es invariante por T, o sea, $(\forall Z)P_1(Z) \Leftrightarrow P_1(T(Z))$, P_2 no tiene por qué ser invariante por T (ver figura 1).

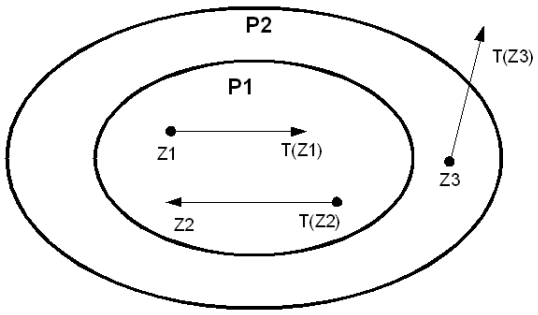

Figura 1: P_1 es invariante en T, pero P_2 no

Por otro lado, que P_2 sea invariante por T tampoco garantiza que P_1 sea invariante por T (ver figura 2).

A partir de esto, si demostramos que Martin-Löf aleatoriedad es invariante por cambio de base, no podemos sacar ninguna conclusión acerca de invariancia por cambio de base para Schnorr aleatoriedad o aleatoriedad computable. Lo mismo sucede con Schnorr aleatoriedad o aleatoriedad computable: demostrar invariancia por cambio de base en alguno de estos conceptos no nos permite concluir nada acerca de invariancia por cambio de base en los otros conceptos.

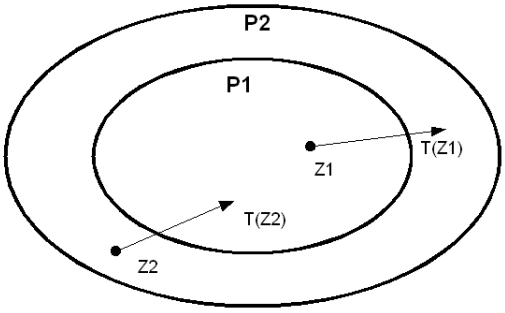

Figura 2: P_2 es invariante en T, pero P_1 no

3.5.1. Dificultad en el cambio de base

A la hora de querer analizar si se conserva aleatoriedad al cambiar de base un número real, surge una gran dificultad: existe un problema de continuidad en la representación. Con esto queremos decir que, por ejemplo, puede ser imposible conocer cuál es el primer dígito de una secuencia en una otra base sin saber toda la secuencia infinita del número en la base inicial.

Por ejemplo, el número 1/2: en base 2, se representa 0.01111.... En base 3, se representa con la secuencia 0.1111....

Entonces, si queremos pasar de base 3 a base 2, en el caso del número 1/2 es necesario conocer toda la secuencia en base 3 para saber el primer dígito en base 2. No es posible, como se podría llegar a suponer, que, a medida que uno conoce más dígitos de la secuencia en base 3, puede ir deduciendo más dígitos de la secuencia en base 2.

Si la secuencia en base 3 empieza con 0.111110, la secuencia en base 2 empezará con 0.0. En cambio, si empieza con 0.111112, la secuencia en base 2 empezará con 0.1. Hasta que no aparezca un caracter distinto de 1, no podemos saber nada del primer caracter en base 2.

Esta dificultad es especialmente grave al analizar el problema de aleatoriedad con martingalas. Esto se debe a que una martingala trata de deducir el próximo dígito en base a todos los anteriores y, al cambiar de base, una cadena finita puede no dar ninguna información.

4. Normalidad y martingalas

En [18, Teorema 5.2.12], Wang demuestra que toda secuencia binaria n^2-aleatoria (o sea, ninguna n^2-martingala tiene éxito con la secuencia) satisface la ley de los grandes números. Dicho de otra manera, en dichas secuencias infinitas el 0 aparece con igual frecuencia que el 1.

En esta sección de la tesis, buscamos ampliar el resultado de [18] para tratar sobre la frecuencia de aparición de toda cadena finita, es decir para tratar sobre normalidad en base 2, y luego para base arbitraria. Nuestro objetivo será, entonces, dada una secuencia que no es normal en base 2, encontrar una n^2-martingala que tenga éxito en dicha secuencia. De esta manera, por contrarrecíproco, demostraremos que toda secuencia n^2-aleatoria es normal en base 2.

Dada una secuencia no normal en base 2, primero daremos una función $F : 2^* \to \mathbb{Q}_{\geq 0}$. Luego, demostraremos que F es una martingala y haremos un análisis de la complejidad temporal de la martingala para asegurarnos que es una n^2-martingala. Y, finalmente, demostrarmos que F tiene éxito en la secuencia, o sea, que la secuencia no es n^2-aleatoria. En la última parte de esta sección, extendemos el resultado para tratar sobre normalidad en cualquier base arbitraria.

Los aportes de esta sección son los siguientes:

Normalidad. Generalizamos el resultado de [18] para analizar no solamente la frecuencia de aparición de 0 y de 1, sino también la frecuencia de aparición de toda cadena finita. Es decir, pasamos de probar la ley de los grandes números a una propiedad mucho más específica como la normalidad en base 2.

Complejidad. Haciendo un análisis más fino de la complejidad de la martingala, logramos probar que $n \cdot \log^3 n$-aleatoriedad implica normalidad en base 2, reduciendo efectivamente la complejidad algorítmica del problema. Dicho de otra manera, si un número no es normal en base 2, es posible construir una $n \cdot \log^3 n$-martingala que tenga éxito para dicho número.

Base. Generalizamos aún más el teorema de [18] para tratar sobre normalidad en cualquier base arbitraria b y no solamente en base 2. Así, para cualquier base b, partiendo de que una secuencia no es normal en una base b, construimos una $n \cdot \log^3 n$-martingala en base b que tiene éxito en dicha cadena.

Claridad. Creemos que nuestra demostración es más completa y clara que la de [18].

Proposición 1. *Para todo* $0 < \delta < 1$,

$$\log(1+\delta) + \log(1-\delta) + \delta(\log(1+\delta) - \log(1-\delta)) > 0.$$

Demostración. Si $\delta = 0$, tenemos

$$\log(1) + \log(1) + 0(\log(1) - \log(1)) = 0.$$

Derivando:

$$\begin{aligned}
(\log(1+\delta) + \log(1-\delta) + \delta(\log(1+\delta) - \log(1-\delta)))' &= \\
\frac{1}{1+\delta} - \frac{1}{1-\delta} + \log(1+\delta) - \log(1-\delta) + \delta(\frac{1}{1+\delta} + \frac{1}{1-\delta}) &= \\
\frac{1}{1+\delta} - \frac{1}{1-\delta} + \log(1+\delta) - \log(1-\delta) + \frac{\delta}{1+\delta} + \frac{\delta}{1-\delta} &= \\
\frac{1-\delta-(1+\delta)+\delta(1-\delta)+\delta(1+\delta)}{(1+\delta)(1-\delta)} + \log(1+\delta) - \log(1-\delta) &= \\
\frac{1-\delta-1-\delta+\delta-\delta^2+\delta+\delta^2)}{(1+\delta)(1-\delta)} + \log(1+\delta) - \log(1-\delta) &= \\
\log(1+\delta) - \log(1-\delta) &> 0
\end{aligned}$$

Lo de arriba es válido para todo $0 < \delta < 1$. Entonces, la función $\log(1+\delta) + \log(1-\delta) + \delta(\log(1+\delta) - \log(1-\delta))$ es creciente para todo $0 < \delta < 1$. Como la función vale 0 cuando $\delta = 0$ y es creciente para $0 < \delta < 1$, entonces la función es > 0 para todo $0 < \delta < 1$. □

4.1. $n \cdot \log^3 n$-aleatoriedad implica normalidad en base 2

Teorema 2. *Si $Z \in 2^\omega$ es $n \cdot \log^3 n$-aleatoria entonces $0.Z$ es normal en base 2.*

Demostración. Supongo $0.Z$ no normal en base 2. Sea $c \in \{0,1\}$ y $\sigma \in 2^*$ tal que σc una cadena de longitud minimal tal que no es cierto

$$\lim_{n\to\infty} \frac{C_{\sigma c}(Z \upharpoonright n)}{n} = 2^{-|\sigma|-1}.$$

Por longitud minimal nos referimos a que, para toda cadena $\tau \in 2^*$, si $|\tau| < |\sigma c|$, entonces sí es cierto que $\lim_{n\to\infty} \frac{C_\tau(Z\upharpoonright n)}{n} = 2^{-|\tau|}$.

Por la elección de σ, tenemos que existe $\epsilon > 0$ tal que una de las siguientes proposiciones es cierta

$$(\exists^\infty n) \qquad \frac{C_{\sigma c}(Z \upharpoonright n)}{n} > 2^{-|\sigma|-1} + \epsilon \tag{2}$$

$$(\exists^\infty n) \qquad \frac{C_{\sigma c}(Z \upharpoonright n)}{n} < 2^{-|\sigma|-1} - 2\epsilon. \tag{3}$$

En el caso (3) tenemos que existen infinitos ns tales que

$$\begin{aligned} 2^{-|\sigma|-1} - 2\epsilon &> \frac{C_{\sigma c}(Z\upharpoonright n)}{n} \\ &\geq \frac{C_\sigma(Z\upharpoonright n) - C_{\sigma\bar{c}}(Z\upharpoonright n) - 1}{n} \quad \text{por (1), página 10.} \end{aligned}$$

Entonces para esos ns tenemos

$$\begin{aligned} \frac{C_{\sigma\bar{c}}(Z \upharpoonright n)}{n} &> \frac{C_\sigma(Z \upharpoonright n) - 1}{n} - 2^{-|\sigma|-1} + 2\epsilon \\ &= \frac{C_\sigma(Z \upharpoonright n) - 1}{n} - 2^{-|\sigma|} + 2^{-|\sigma|-1} + 2\epsilon. \end{aligned}$$

Como σc es de longitud minimal, para n suficientemente grande tenemos $\frac{C_\sigma(Z\upharpoonright n)-1}{n} - 2^{-|\sigma|} > -\epsilon$, de modo que existen infinitos ns tales que

$$\frac{C_{\sigma\bar{c}}(Z \upharpoonright n)}{n} > 2^{-|\sigma|-1} + \epsilon.$$

Entonces, podemos asumir sin pérdida de generalidad que vale (2). Sea $\delta \in \mathbb{Q}^+$, $\delta < 1$, tal que

$$\limsup_{n\to\infty} \frac{C_{\sigma c}(Z \upharpoonright n)}{n} > \frac{1+\delta}{2^{|\sigma|+1}}. \tag{4}$$

Definamos la función $F(\sigma c) : 2^* \to \mathbb{Q}$ de la siguiente manera:

$$\begin{aligned} F(\lambda) &= 1 \\ F(\tau i) &= \begin{cases} F(\tau) & \text{si} \quad |\tau| < |\sigma| \quad \text{o} \quad \tau[|\tau|-|\sigma|..|\tau|-1] \neq \sigma \\ p \cdot F(\tau) & \text{si} \quad |\tau| \geq |\sigma| \quad , \quad \tau[|\tau|-|\sigma|..|\tau|-1] = \sigma \quad \text{y} \quad i = c \\ q \cdot F(\tau) & \text{si} \quad |\tau| \geq |\sigma| \quad , \quad \tau[|\tau|-|\sigma|..|\tau|-1] = \sigma \quad \text{y} \quad i = \bar{c} \end{cases} \end{aligned}$$

donde $p = (1+\delta)$ y $q = 1-\delta$. F es una martingala y es claro que para toda $\tau \in 2^*$,

$$F(\tau) = p^{C_{\sigma c}(\tau)} \cdot q^{C_{\sigma\bar{c}}(\tau)}.$$

Proposición 3. *F es una $n \cdot \log^3 n$-martingala.*

Demostración. Se usará la estructura presentada por Ambos-Spies y Mayordomo en [1, p. 10] para almacenar racionales, y por lo tanto se considerará que la multiplicación de 2 racionales que ocupan m bits se realiza en tiempo $O(m \cdot log^2(m))$, y la suma en tiempo $O(m)$.

Dado $n \in \mathbb{N}$,

$$F(Z \upharpoonright n) = p^{C_{\sigma c}(Z \upharpoonright n)} \cdot q^{C_{\sigma \bar{c}}(Z \upharpoonright n)}. \tag{5}$$

Entonces, tenemos que analizar la complejidad temporal de calcular $p^{C_{\sigma c}(Z \upharpoonright n)} \cdot q^{C_{\sigma \bar{c}}(Z \upharpoonright n)}$.

Sea k la mínima cantidad de bits necesarios para poder representar a p y a q. Está claro que k es un número fijo, pues p y q lo son. Como $C_{\sigma c}(Z \upharpoonright n) \leq n$ y $C_{\sigma \bar{c}}(Z \upharpoonright n) \leq n$, $p^{C_{\sigma c}(Z \upharpoonright n)}$ y $q^{C_{\sigma \bar{c}}(Z \upharpoonright n)}$ pueden representarse ambos con $n \cdot k$ bits. Calcular $C_{\sigma c}(Z \upharpoonright n)$ y $C_{\sigma \bar{c}}(Z \upharpoonright n)$ tiene una complejidad de $O(n)$, pues es encontrar, en cada caso, la cantidad de apariciones de una secuencia de longitud fija en una secuencia de longitud n. Por otro lado, si $t(n,k)$ es la complejidad temporal de elevar a la n un número fijo representado en a lo sumo k bits, se ve claramente que la complejidad de calcular tanto $p^{C_{\sigma c}(Z \upharpoonright n)}$ como $q^{C_{\sigma \bar{c}}(Z \upharpoonright n)}$ es $O(t(n,k)+n)$. De todo esto se deduce que la complejidad de calcular (5) es

$$O(n \cdot k \cdot \log^2(n \cdot k) + t(n,k) + t(n,k) + n + n) \quad = \quad O(n \cdot \log^2 n + t(n,k))$$

Falta entonces analizar $t(n,k)$. Utilizando la técnica de potenciación por cuadrados, para calcular r^n (donde r se representa con k bits), son necesarias $O(\log n)$ multiplicaciones y $O(\log\ n)$ sumas.

La idea básica del algoritmo es calcular r^{2^i} para $0 \leq i \leq \lfloor \log_2 n \rfloor$. Luego, hay que sumar los factores correspondientes. Es directo ver que esto requiere a lo sumo $O(\log\ n)$ multiplicaciones y $O(\log\ n)$ sumas.

r^n ocupa $k \cdot n$ bits. En nuestro cálculo, además, nunca usamos un número que ocupe más de $k \cdot n$ bits. Entonces, el costo de cada multiplicación nunca va a ser mayor que

$$O(n \cdot k \cdot \log^2(n \cdot k)) \quad = \quad O(n \cdot \log^2 n).$$

El costo de cada suma, por su parte, nunca va a ser mayor que

$$O(n \cdot k) \quad = \quad O(n).$$

Entonces, $t(n,k)$ resulta ser el costo de las multiplaciones multiplicado por la cantidad de multiplicaciones, sumado al costo de las sumas multiplicado por la cantidad de sumas.

$$\begin{aligned} t(n,k) &\in O(\log\ n) \cdot O(n \cdot \log^2 n) + O(\log\ n) \cdot O(n) \\ &= O(n \cdot \log^3 n) + O(n \cdot \log\ n) \\ &= O(n \cdot \log^3 n) \end{aligned}$$

Volviendo a la ecuación (5) concluimos que su complejidad temporal es

$$\begin{aligned} O(n \cdot \log^2 n + t(n,k)) &= O(n \cdot \log^2 n + n \cdot \log^3 n) \\ &= O(n \cdot \log^3 n)\ . \end{aligned}$$

□

Proposición 4. *F tiene éxito en Z.*

Demostración. Recordemos que $\log\ p > 0$ y $\log\ q < 0$.

$$\begin{aligned}\log\ F(Z \upharpoonright n) &= C_{\sigma c}(Z \upharpoonright n) \cdot \log\ p + C_{\sigma \bar{c}}(Z \upharpoonright n) \cdot \log\ q \\ &\geq C_{\sigma c}(Z \upharpoonright n) \cdot \log\ p + (C_{\sigma}(Z \upharpoonright n) - C_{\sigma c}(Z \upharpoonright n)) \cdot \log\ q \\ &= C_{\sigma}(Z \upharpoonright n) \cdot \log\ q + C_{\sigma c}(Z \upharpoonright n) \cdot (\log\ p - \log\ q).\end{aligned}$$

Entonces,

$$\frac{\log\ F(Z \upharpoonright n)}{n} \geq \frac{C_{\sigma}(Z \upharpoonright n)}{n} \cdot \log\ q + \frac{C_{\sigma c}(Z \upharpoonright n)}{n} \cdot (\log\ p - \log\ q). \tag{6}$$

Tomando límite superior tenemos

$$\limsup_{n\to\infty} \frac{\log\ F(Z \upharpoonright n)}{n} \geq \limsup_{n\to\infty} \frac{C_{\sigma}(Z \upharpoonright n)}{n} \cdot \log\ q + \frac{C_{\sigma c}(Z \upharpoonright n)}{n} \cdot (\log\ p - \log\ q).$$

Como σc es una cadena de longitud minimal tal que no vale la propiedad de igualdad de frecuencias de aparición de cadenas de misma longitud, sí vale esta propiedad para σ, y entonces

$$\begin{aligned}\limsup_{n\to\infty} \frac{C_{\sigma}(Z \upharpoonright n)}{n} &= \lim_{n\to\infty} \frac{C_{\sigma}(Z \upharpoonright n)}{n} \\ &= 2^{-|\sigma|}.\end{aligned}$$

A partir de esto podemos separar, en la ecuación (6), el límite superior en la suma y que siga valiendo la desigualdad

$$\limsup_{n\to\infty} \frac{\log\ F(Z \upharpoonright n)}{n} \geq 2^{-|\sigma|} \cdot \log\ q + \limsup_{n\to\infty} \frac{C_{\sigma c}(Z \upharpoonright n)}{n} \cdot (\log\ p - \log\ q)$$

Por (4) y la Proposición 1, tenemos

$$\begin{aligned}\limsup_{n\to\infty} \frac{\log\ F(Z \upharpoonright n)}{n} &> 2^{-|\sigma|-1} (\log\ p + \log\ q + \delta(\log\ p - \log\ q)) \\ &= d > 0.\end{aligned}$$

Entonces existen infinitos ns tales que $\frac{\log\ F(Z \upharpoonright n)}{n} > d$, es decir $F(Z \upharpoonright n) > 2^{n \cdot d}$. Esto implica que $\limsup_{n\to\infty} F(Z \upharpoonright n) = \infty$, o sea, F tiene éxito en Z.

□

Esto concluye con la demostración del Teorema 2. □

4.2. Generalización a base arbitraria

Lo que sigue es una generalización de la Proposición 1.

Proposición 5. *Dados $p, q \in \mathbb{Q}_{>0}$, para todo $0 < \delta < q$,*

$$p \cdot \log(1 + \frac{\delta}{p}) + q. \log(1 - \frac{\delta}{q}) + \delta(\log(1 + \frac{\delta}{p}) - \log(1 - \frac{\delta}{q})) > 0.$$

Demostración. Si $\delta = 0$, $p \cdot \log(1) + q.\log(1) + 0(\log(1) - \log(1)) = 0$. Derivando (la variable es δ) obtenemos

$$\begin{aligned}
(p \cdot \log(1+\frac{\delta}{p}) + q.\log(1-\frac{\delta}{q}) + \delta(\log(1+\frac{\delta}{p}) - \log(1-\frac{\delta}{q})))' &= \\
\frac{p}{p}\frac{1}{1+\frac{\delta}{p}} - \frac{q}{q}\frac{1}{1-\frac{\delta}{q}} + \log(1+\frac{\delta}{p}) - \log(1-\frac{\delta}{q}) + \delta(\frac{1}{p}\frac{1}{1+\frac{\delta}{p}} + \frac{1}{q}\frac{1}{1-\frac{\delta}{q}}) &= \\
\frac{1}{1+\frac{\delta}{p}} - \frac{1}{1-\frac{\delta}{q}} + \frac{\delta}{p}\frac{1}{1+\frac{\delta}{p}} + \frac{\delta}{q}\frac{1}{1-\frac{\delta}{q}} + \log(1+\frac{\delta}{p}) - \log(1-\frac{\delta}{q}) &= \\
\frac{1-\frac{\delta}{q} - (1+\frac{\delta}{p}) + \frac{\delta}{p}(1-\frac{\delta}{q}) + \frac{\delta}{q}(1+\frac{\delta}{p})}{(1+\frac{\delta}{p})(1-\frac{\delta}{q})} + \log(1+\frac{\delta}{p}) - \log(1-\frac{\delta}{q}) &= \\
\frac{1-\frac{\delta}{q} - 1 - \frac{\delta}{p} + \frac{\delta}{p} - \frac{\delta^2}{p.q} + \frac{\delta}{q} + \frac{\delta^2}{p.q}}{(1+\frac{\delta}{p})(1-\frac{\delta}{q})} + \log(1+\frac{\delta}{p}) - \log(1-\frac{\delta}{q}) &= \\
\log(1+\frac{\delta}{p}) - \log(1-\frac{\delta}{q}) &> 0.
\end{aligned}$$

Lo de arriba es válido para todo $0 < \delta < q$. Entonces, la función es creciente para todo $0 < \delta < q$. Como la función cuando $\delta = 0$ vale 0 y es creciente para $0 < \delta < q$, entonces la función es > 0 para todo $0 < \delta < q$. □

Teorema 6. *Si $0.Z$ no es normal en base b, entonces existe una $n \cdot \log^3 n$-martingala en base b que tiene éxito en Z.*

Demostración. Sea $c \in \{0, 1, \cdots, b-1\}$ y $\sigma \in b^*$ tal que σc una cadena de longitud minimal tal que no es cierto

$$\lim_{n\to\infty} \frac{C_{\sigma c}(Z \upharpoonright n)}{n} = b^{-|\sigma|-1}.$$

Definimos

$$C_{\sigma \bar{c}}(Z \upharpoonright n) = \sum_{0 \le d < b \wedge d \neq c} C_{\sigma d}(Z \upharpoonright n).$$

Ahora seguimos un razonamiento parecido al utilizado para base 2: Por la elección de σ, tenemos que existe $\epsilon > 0$ tal que una de las siguientes proposiciones es cierta

$$(\exists^\infty n) \qquad \frac{C_{\sigma c}(Z \upharpoonright n)}{n} > b^{-|\sigma|-1} + \epsilon \tag{7}$$

$$(\exists^\infty n) \qquad \frac{C_{\sigma c}(Z \upharpoonright n)}{n} < b^{-|\sigma|-1} - b\epsilon. \tag{8}$$

En el caso (8) tenemos que existen infinitos ns tales que

$$\begin{aligned}
b^{-|\sigma|-1} - b\epsilon &> \frac{C_{\sigma c}(Z \upharpoonright n)}{n} \\
&\ge \frac{C_{\sigma}(Z \upharpoonright n) - C_{\sigma \bar{c}}(Z \upharpoonright n) - 1}{n} \quad \text{por (1), página 10.}
\end{aligned}$$

Entonces para esos ns tenemos

$$\begin{aligned}\frac{C_{\sigma\bar{c}}(Z \upharpoonright n)}{n} &> \frac{C_\sigma(Z \upharpoonright n)-1}{n} - b^{-|\sigma|-1} + b\epsilon \\ &= \frac{C_\sigma(Z \upharpoonright n)-1}{n} - b^{-|\sigma|} + (b-1)b^{-|\sigma|-1} + b\epsilon.\end{aligned}$$

Como σc es de longitud minimal, para n suficientemente grande tenemos

$$\frac{C_\sigma(Z \upharpoonright n)-1}{n} - b^{-|\sigma|} > -\epsilon,$$

de modo que existen infinitos ns tal que

$$\frac{C_{\sigma\bar{c}}(Z \upharpoonright n)}{n} > (b-1)\cdot(b^{-|\sigma|-1}+\epsilon).$$

Como $C_{\sigma\bar{c}}(Z \upharpoonright n)$ es una sumatoria de $b-1$ elementos, existe $d \in \{0,\dots,b-1\}\setminus\{c\}$ tal que existen infinitos ns tal que

$$\frac{C_{\sigma d}(Z \upharpoonright n)}{n} > b^{-|\sigma|-1}+\epsilon.$$

Entonces, podemos asumir sin pérdida de generalidad que vale (7). Sea $\delta \in \mathbb{Q}^+$ tal que

$$\limsup_{n\to\infty} \frac{C_{\sigma c}(Z \upharpoonright n)}{n} > \frac{1+\delta}{b^{|\sigma|+1}}.$$

Definamos la función $F(\sigma c) : b^* \to \mathbb{Q}$ de la siguiente manera:

$$\begin{aligned}F(\lambda) &= 1 \\ F(\tau i) &= \begin{cases} F(\tau) & \text{si} \quad |\tau| < |\sigma| \quad \text{o} \quad \tau[|\tau|-|\sigma|..|\tau|-1] \neq \sigma \\ p\cdot F(\tau) & \text{si} \quad |\tau| \geq |\sigma| \quad , \quad \tau[|\tau|-|\sigma|..|\tau|-1] = \sigma \quad \text{y} \quad i = c \\ q\cdot F(\tau) & \text{si} \quad |\tau| \geq |\sigma| \quad , \quad \tau[|\tau|-|\sigma|..|\tau|-1] = \sigma \quad \text{y} \quad i \neq c \end{cases}\end{aligned}$$

donde $p = (1+\delta)$ y $q = (1-\frac{\delta}{b-1})$. Es claro que para toda $\tau \in b^*$,

$$F(\tau) = p^{C_{\sigma c}(\tau)} \cdot q^{C_{\sigma\bar{c}}(\tau)}.$$

Proposición 7. *F es una martingala en base b.*

Demostración. Si $|\tau| < |\sigma|$ o $\tau[|\tau|-|\sigma|..|\tau|-1] \neq \sigma$,

$$\sum_{0\leq i<b} F(\tau i) = \sum_{0\leq i<b} F(\tau) = b\cdot F(\tau).$$

Si $|\tau| \geq |\sigma|$ y $\tau[|\tau|-|\sigma|..|\tau|-1] = \sigma$,

$$\begin{aligned}\sum_{0\leq i<b} F(\tau i) &= (1+\delta)\cdot F(\tau) + \sum_{0\leq j<b\wedge j\neq c} (1-\frac{\delta}{b-1})\cdot F(\tau) \\ &= (1+\delta)\cdot F(\tau) + (b-1-\delta)\cdot F(\tau) \\ &= b\cdot F(\tau).\end{aligned}$$

□

Proposición 8. *F es una $n \cdot \log^3 n$-martingala.*

Demostración. El caso es análogo para la martingala en base 2. Como $\log_b(x) \in \Theta(\log_2(x))$, el tamaño de entrada y el necesario para almacenar un racional se mantienen, así como los costos de las operaciones.

La única diferencia para base arbitraria es que $C_{\sigma\bar{c}}(Z \upharpoonright n)$ es sumar la cantidad de apariciones de las $b-1$ cadenas σd, donde $d \neq c$. La cantidad de apariciones no puede ser mayor a n, entonces hay que realizar $b-2$ sumas donde cada una cuesta $O(\log(n))$. Como b es fijo, eso tiene un costo de $O(\log(n))$, que es inferior a $O(n)$, el costo de contar la cantidad de apariciones. Entonces la complejidad temporal de sumar las cantidades de apariciones no influye en la complejidad temporal del algoritmo. □

Proposición 9. *F tiene éxito en Z.*

Demostración. Recordemos que $\log\ p > 0$ y $\log\ q < 0$.

$$\begin{aligned}
\log\ F(Z \upharpoonright n) &= C_{\sigma c}(Z \upharpoonright n) \cdot \log\ p + C_{\sigma\bar{c}}(Z \upharpoonright n) \cdot \log\ q \\
&\geq C_{\sigma c}(Z \upharpoonright n) \cdot \log\ p + (C_{\sigma}(Z \upharpoonright n) - C_{\sigma c}(Z \upharpoonright n)) \cdot \log\ q \\
&= C_{\sigma}(Z \upharpoonright n) \cdot \log\ q + C_{\sigma c}(Z \upharpoonright n) \cdot (\log\ p - \log\ q).
\end{aligned}$$

Aplicando límite superior

$$\limsup_{n\to\infty} \frac{\log\ F(Z \upharpoonright n)}{n} \geq \limsup_{n\to\infty} \left(\frac{C_{\sigma}(Z \upharpoonright n)}{n} \cdot \log\ q + \frac{C_{\sigma c}(Z \upharpoonright n)}{n} \cdot (\log\ p - \log\ q)\right).$$

Al igual que en la demostración de la Proposición 4, como σc es la cadena de longitud minimal donde no vale que todas las cadenas de igual longitud aparecen con igual frecuencia, tenemos

$$\begin{aligned}
\limsup_{n\to\infty} \frac{C_{\sigma}(Z \upharpoonright n)}{n} &= \lim_{n\to\infty} \frac{C_{\sigma}(Z \upharpoonright n)}{n} \\
&= b^{-|\sigma|}.
\end{aligned}$$

A partir de esto, podemos dividir el límite superior en la suma y que siga valiendo la igualdad, obteniendo

$$\begin{aligned}
\limsup_{n\to\infty} \frac{\log\ F(Z \upharpoonright n)}{n} &> \frac{1}{b^{|\sigma|}} \cdot \log\ q + \frac{1+\delta}{b^{|\sigma|+1}} \cdot (\log\ p - \log\ q) \\
&= \frac{1}{b^{|\sigma|+1}} \cdot (b \cdot \log\ q + (1+\delta) \cdot (\log\ p - \log\ q)) \\
&= \frac{1}{b^{|\sigma|+1}} \cdot (b \cdot \log\ q + \log\ p - \log\ q + \delta \cdot \log\ p - \delta \cdot \log\ q) \\
&= \frac{1}{b^{|\sigma|+1}} \cdot ((1+\delta) \cdot \log\ p + ((b-1) - \delta) \cdot \log\ q).
\end{aligned}$$

Reemplazando p y q por sus valores tenemos

$$\limsup_{n\to\infty} \frac{\log\ F(Z \upharpoonright n)}{n} =$$
$$\frac{1}{b^{|\sigma|+1}} \cdot (\delta(\log(1+\delta) - \log(1 - \tfrac{\delta}{b-1})) + \log(1+\delta) + (b-1)\log(1 - \tfrac{\delta}{b-1})).$$

Por la Proposición 5 tenemos

$$\limsup_{n\to\infty} \frac{\log\ F(Z \upharpoonright n)}{n} \quad = \quad d > 0.$$

Entonces existen infinitos ns tales que $\frac{\log\ F(Z\upharpoonright n)}{n} > d$, es decir $F(Z \upharpoonright n) > 2^{n\cdot d}$. Esto implica que $\limsup_{n\to\infty} F(Z \upharpoonright n) = \infty$, o sea, F tiene éxito en Z. □

Esto concluye con la demostración del Teorema 6 □

5. Una demostración existente de invariancia para Martin-Löf aleatoriedad

En [8, Cap. 7.2, Teorema 7.18], Calude demuestra que Martin-Löf aleatoriedad es invariante por cambio de base. Para llegar a dicha conclusión, prueba varios lemas y teoremas intermedios. La demostración de [8, Cap. 7.2, Teorema 7.18] se obtiene a partir de combinar dos teoremas. En [8, Cap. 6.4, Teorema 6.58] se demuestra que aleatoriedad de Martin-Löf en una base b implica aleatoriedad de Martin-Löf en cualquier base b^m, para $m \in \mathbb{N}, m > 1$. En [8, Cap. 7.2, Teorema 7.17] se demuestra que aleatoriedad de Martin-Löf en una base $b+1$ implica aleatoriedad de Martin-Löf en la base b. Entonces, para dos bases cualesquiera p y q, si sabemos que una secuencia es Martin-Löf aleatoria en base p, aplicamos [8, Cap. 6.4, Teorema 6.58] para obtener aleatoriedad en p^m, donde m es el menor natural tal que $p^m \geq q$, y luego, aplicamos [8, Cap. 7.2, Teorema 7.17] para ir bajando de base p^m tantas veces como sea necesario hasta llegar a aleatoriedad de Martin-Löf para base q.

Nuestra intención original era utilizar [8, Lema 7.12] para poder demostrar invariancia por cambio de base en aleatoriedad computable. Sin embargo, al empezar a trabajar, encontramos que dicho lema no es correcto. En esta sección de la tesis, entonces, analizaremos los lemas y teoremas que se desprenden a partir de [8, Lema 7.12]. Estos son: [8, Lema 7.12], [8, Lema 7.15] y [8, Teorema 7.17]. Concretamente,

- En la sección 5.1 damos las definiciones tomadas de [8] que usaremos en esta parte de la tesis.
- En la sección 5.2 presentamos un contraejemplo para [8, Lema 7.12].
- El único lema que utiliza a [8, Lema 7.12] es [8, Lema 7.15]. Al analizar este lema, concluimos que tampoco es verdadero. Para probar nuestra afirmación, en la sección 5.3 presentamos un contrajemplo.
- El teorema [8, Teorema 7.17] es el central en el capítulo 7.2. A partir de él, Calude logra demostrar que Martin-Löf aleatoriedad es invariante por cambio de base. Sin embargo, dicho teorema utiliza a [8, Lema 7.15]. En la última parte del capítulo, corregimos a [8, Teorema 7.17] para que siga siendo válido, eliminando su dependencia con [8, Lema 7.15]. En la sección 5.4, además, explicamos con más detalle y con más claridad la demostración de [8, Teorema 7.17], pues nos pareció bastante intrincada.

En la próxima sección de la tesis, daremos una demostración directa de que Martin-Löf aleatoriedad es invariante por cambio de base.

5.1. Definiciones tomadas de [8] que utilizamos en esta sección de la tesis

En esta sección usamos las convenciones de [8]. Por ese motivo, usamos una letra mayúscula para referirnos a una base en particular. Con A_Q nos referimos a $\{0, 1, \cdots, Q-1\}$, con A_Q^* a Q^*, con A_Q^ω a Q^ω, con A_Q^l a Q^l y con A_Q^+ a Q^+. μ_{A_Q} es equivalente a μ_Q, y $\mathbf{rand}(A_Q)$ es el conjunto de todas las secuencias en base Q que son Martin-Löf aleatorias en base Q. $x(n)$, a diferencia de lo definido en la sección 3.1, representará los primeros n carateres de la secuencia x, o sea, será el equivalente a lo que definimos en la sección 3.1 como $x \upharpoonright n$. Por último, recordamos que $v_{Q+1}(w)$ es el número real valor de w en base $Q+1$.

Definimos

$$D_Q = \{w \in A_{Q+1}^+ : v_{Q+1}(w) \leq 1 - Q^{-|w|}\},$$

es decir, D_Q es el conjunto de cadenas finitas en base $Q+1$ que cumplen con la condición enunciada en la definición.

Sea $\Gamma_Q : D_Q \to \{0, 1, ..., Q-1\}^*$ tal que

$$\Gamma_Q(w) = \text{mín}\{z \in A_Q^{|w|} : v_{Q+1}(w) \leq v_Q(z)\}.$$

Si es sabida la base de w, se abrevia $\Gamma_Q(w)$ por $\Gamma(w)$

5.2. Contraejemplo para Lema 7.12

Lema 7.12 de [8]. *Let $u \in D_Q$ and $v \in A_{Q+1}^*$ with $u \preceq v$. Then $v \in D_Q$ and $\Gamma(u) \preceq \Gamma(v)$.*

El lema es inválido. Como contraejemplo, tomemos a las cadenas 1(como u) y 100(como v) en base 3.

Antecedente:

- $1 \in D_2 \Leftrightarrow v_3(1) = 1/3 \leq 1 - 2^{-1} = 1 - 1/2 = 1/2$
- $1 \preceq 100$ trivial.

Sin embargo,

- $\Gamma(1) = \text{mín}\{z \in A_2^1 : v_3(1) \leq v_2(z)\} = 1$
- $\Gamma(100) = \text{mín}\{z \in A_2^3 : v_3(100) \leq v_2(z)\} = 011$

Entonces, $\Gamma(1) = 1 \not\preceq 011 = \Gamma(100)$.

El error se produce cuando en un paso de la demostración se concluye erróneamente que $v_Q(\Gamma(u)) \leq v_Q(\Gamma(v))$. Como se ve en el contraejemplo, $v_2(\Gamma(1)) = v_2(1) = 1/2 \not\leq 3/8 = v_2(011) = v_2(\Gamma(100))$.

5.3. Contraejemplo para Lema 7.15

Lema 7.15 de [8]. *Let $S \subset A_Q^*$. If S is prefix-free, then $\Gamma^{-1}(S)$ is also prefix-free.*

El lema es inválido. Como contraejemplo, tomamos $S = \{1, 011\}$, $Q = 2$.

$\Gamma^{-1}(S) = \{\Gamma^{-1}(1)\} \cup \{\Gamma^{-1}(011)\} \supseteq \{1, 100\}$, pues $\Gamma(1) = 1$ y $\Gamma(100) = 011$ (se usan los mismos ejemplos que para la refutación de [8, Lema 7.12]).

Como se puede apreciar, $\Gamma^{-1}(S)$ no es libre de prefijos. El error surge de suponer verdadero a [8, Lema 7.12], donde se concluye erróneamente que $u \preceq v \Rightarrow \Gamma(u) \preceq \Gamma(v)$

5.4. Ajustes al Teorema 7.17

Teorema 7.17 de [8]. *Let $x \in \textbf{\textit{rand}}(A_{Q+1})$ and $y \in A_Q^\omega$ such that $v_{Q+1}(x) = v_Q(y)$. Then $y \in \textbf{\textit{rand}}(A_Q)$.*

La idea de la demostración es la siguiente. Suponemos que $x \in \mathbf{rand}(A_{Q+1})$. Entonces, ningún test de Solovay en base $Q+1$ tiene éxito en x. A partir de un test de Solovay genérico en base Q, construimos un test de Solovay en base $Q+1$. Como este último no puede tener éxito en x, concluimos que no puede tener éxito en y. Por lo tanto, y es Martin-Löf aleatorio en base Q.

En este teorema, $x \in A_{Q+1}^\omega$, e y es la representación infinita en base Q de x. O sea, $v_Q(y) = v_{Q+1}(x)$.

Incluimos el enunciado de [8, Lema 7.14] porque será usado más adelante en la demostración del teorema: **Lema 7.14 de [8].** *The partial function Γ is surjective and for every string $u \in A_Q^*$ one has: $\#(\Gamma^{-1}(u)) < (\frac{Q+1}{Q})^{|u|} + 1$.*

S y T son aquellos ya definidos en [8]. O sea, $S \subset A_Q^* \times \mathbb{N}_+$ un conjunto c.e. tal que todo S_i es libre de prefijos y $\sum_{j \geq 1} \mu_{A_Q}(S_j A_Q^\omega) < \infty$. $T = \{(x, j) \in A_{Q+1}^* \times \mathbb{N}_+ \ : \ x \in D_Q, \Gamma(x) \in S_j\}$.

Claramente

$$\Gamma^{-1}(S_j)A_{Q+1}^\omega = \bigcup_{w \in S_j} \Gamma^{-1}(w)A_{Q+1}^\omega. \tag{9}$$

$\Gamma^{-1}(w)$ es libre de prefijos pues $(\forall z \in \Gamma^{-1}(w))|z| = |w|$. Entonces, si dos elementos pertenecen a $\Gamma^{-1}(w)$, ambos tienen la misma longitud, por lo que no pueden ser uno prefijo del otro. Entonces,

$$\mu_{A_{Q+1}}(\Gamma^{-1}(w)A_{Q+1}^\omega) = \#\Gamma^{-1}(w) \cdot (Q+1)^{-|w|}$$

Usando [8, Lema 7.14],

$$\begin{aligned} \#\Gamma^{-1}(w) \cdot (Q+1)^{-|w|} &< ((\frac{Q+1}{Q})^{|w|} + 1) \cdot (Q+1)^{-|w|} &(10)\\ &< \frac{2}{Q^{|w|}} \ . &(11)\end{aligned}$$

Entonces, se puede concluir efectivamente que

$$\mu_{A_{Q+1}}(\Gamma^{-1}(w)A^{\omega}_{Q+1}) < \frac{2}{Q^{|w|}} \ . \tag{12}$$

Entonces,

$$\sum_{j\geq 1}\mu_{A_{Q+1}}(\Gamma^{-1}(S_j)A^{\omega}_{Q+1}) = \sum_{j\geq 1}\mu_{A_{Q+1}}(\bigcup_{w\in S_j}\Gamma^{-1}(w)A^{\omega}_{Q+1}).$$

Tal como se expresa en [8], por (9).

Sin embargo, es inválida la igualdad incluida en [8]:

$$\sum_{j\geq 1}\mu_{A_{Q+1}}(\bigcup_{w\in S_j}\Gamma^{-1}(w)A^{\omega}_{Q+1}) = \sum_{j\geq 1}\sum_{w\in S_j}\mu_{A_{Q+1}}(\Gamma^{-1}(w)A^{\omega}_{Q+1}).$$

Para que sea cierta, tiene que ser verdadero [8, Lema 7.15], que se demostró falso. Como $\Gamma^{-1}(S_j)$ puede no ser libre de prefijos, los conjuntos $\Gamma^{-1}(w_1)A^{\omega}_{Q+1}$ y $\Gamma^{-1}(w_2)A^{\omega}_{Q+1}$ (con $w_1 \in S_1$ y $w_2 \in S_2$) pueden no ser disjuntos. Este problema se resuelve fácilmente reemplazando la igualdad por $\leq$, pues siempre es cierto que la suma de medidas de conjuntos es menor o igual a la medida de la unión de dichos conjuntos. Entonces, reemplazamos la igualdad por:

$$\sum_{j\geq 1}\mu_{A_{Q+1}}(\bigcup_{w\in S_j}\Gamma^{-1}(w)A^{\omega}_{Q+1}) \leq \sum_{j\geq 1}\sum_{w\in S_j}\mu_{A_{Q+1}}(\Gamma^{-1}(w)A^{\omega}_{Q+1}).$$

La desigualdad

$$\sum_{j\geq 1}\sum_{w\in S_j}\mu_{A_{Q+1}}(\Gamma^{-1}(w)A^{\omega}_{Q+1}) \leq \sum_{j\geq 1}\sum_{w\in S_j}2Q^{-|w|}$$

es válida por (12).

La igualdad:

$$\sum_{j\geq 1}\sum_{w\in S_j}2Q^{-|w|} = 2\sum_{j\geq 1}\mu_{A_Q}(S_jA^{\omega}_Q)$$

es válida porque, como cada S_j es libre de prefijos, entonces $\bigcup_{w\in S_j} wA^{\omega}_Q$ es una unión de conjuntos disjuntos. Luego, la medida de la unión de conjuntos disjuntos es igual a la suma de medidas de cada conjunto.

De todo lo anterior se concluye que

$$\sum_{j\geq 1}\mu_{A_{Q+1}}(\bigcup_{w\in S_j}\Gamma^{-1}(w)A^{\omega}_{Q+1}) \leq 2\sum_{j\geq 1}\mu_{A_Q}(S_jA^{\omega}_Q).$$

Por otro lado, $2\sum_{j\geq 1}\mu_{A_Q}(S_jA^{\omega}_Q) < \infty$ por definición de S. Entonces,

$$\sum_{j\geq 1}\mu_{A_{Q+1}}(\Gamma^{-1}(S_j)A^{\omega}_{Q+1})$$

converge. Combinando esto con [8, Teorema 6.37], y como x es aleatoria por hipótesis, se deduce que existe un natural N tal que

$$\forall i \in \mathbb{N}, i \geq N, x \notin \Gamma^{-1}(S_i)A^{\omega}_{Q+1} \ . \tag{13}$$

Por [8, Lema 7.6 y Lema 7.16], sea k tal que $\forall n,\ n \geq k,\ x(n) \in D_Q$. Por otro lado, como $\sum_{j\geq 1} \mu_{A_Q}(S_j A_Q^\omega)$ converge, es inmediato que

$$\lim_{m\to\infty} \mu_{A_Q}(S_m A_Q^\omega) = 0,$$

y entonces,

$$\lim_{m\to\infty} \text{mín}\{|w| : w \in S_m\} = \infty.$$

A partir de esto, es posible encontrar un M tal que, $\forall i \geq M$, si $w \in S_i$, entonces $|w| > k$.

Sea $i \geq \text{máx}\{M, N\}$, asumamos que $y \in S_i A_Q^\omega$. Entonces, existe un $n > k$ tal que $y(n) \in S_i$ y $\Gamma(x(n)) = y(n)$. O sea, $\Gamma(x(n)) \in S_i$. Como $|x(n)| = n > k$, resulta que $x(n) \in D_Q$, y entonces podemos aplicar Γ^{-1}. Eso resulta en que para ese $i \geq \text{máx}\{M, N\}$, existe $n > k$ tal que $x(n) \in \Gamma^{-1}(S_i)$. O sea,

$$x \in \Gamma^{-1}(S_i) A_{Q+1}^\omega$$

Pero esto es absurdo, pues contradice (13). El absurdo surge de suponer que existe $i \geq \text{máx}\{M, N\}$ tal que $y \in S_i A_Q^\omega$. Y entonces, se puede concluir que

$$\forall i \geq \text{máx}\{M, N\} : y \notin S_i A_Q^\omega.$$

Como S puede ser cualquier test de Solovay, se deduce que $y \in \mathbf{rand}(A_Q)$.

6. Cambio de base en aleatoriedad de Martin-Löf, Schnorr y Kurtz

En esta sección, damos una demostración directa de que aleatoriedad de Martin-Löf es invariante por cambio de base. Luego, extendemos el resultado para demostrar que aleatoriedad de Schnorr y aleatoriedad de Kurtz son invariantes por cambio de base.

Dado $\sigma \in b^*$, denotamos con $[\sigma]_b$ al intervalo $[v_b(\sigma), v_b(\sigma) + b^{-|\sigma|}]$, de longitud $b^{-|\sigma|}$. Intuitivamente, el conjunto $[\sigma]_b$ contiene a todos los números reales que, escritos en base b, empiezan de la forma $0.\sigma\ldots$.

Para un conjunto $A \subseteq b^*$ definimos

$$[A]_b = \bigcup_{\sigma\in A} [\sigma]_b.$$

Notar que $\mu_b(Ab^\omega) = \mu([A]_b)$.

Teorema 10. *Aleatoriedad de Martin-Löf es invariante por cambio de base.*

Demostración. Sea $Z_b \in b^\omega$ y $Z_q \in q^\omega$ tal que $v_b(Z_b) = v_q(Z_q)$. Probaremos que si existe un test de Martin-Löf en base b $(G_m)_{m\in\mathbb{N}}$ tal que $Z_b \in \bigcap_m G_m b^\omega$ entonces existe un test de Martin-Löf en base q $(H_m)_{m\in\mathbb{N}}$ tal que $Z_q \in \bigcap_m H_m q^\omega$.

Sea $(G_m)_{m\in\mathbb{N}}$, $G_m \subseteq b^*$ una secuencia uniformemente c.e. tal que $Z_b \in \bigcap_m G_m b^\omega$ y $\mu_b(G_m b^\omega) \leq b^{-m}$. Sin pérdida de generalidad, podemos suponer que G_m es libre de prefijos y que

$$\mu_b(G_m b^\omega) \leq b^{-km-1}\ , \tag{14}$$

donde k es el mínimo número natural tal que $b^k \geq q$.

Sea

$$y_{b,q}(n) = \text{mín}\{m \in \mathbb{N} : b^{-n}/2 \geq q^{-m}\} \ .$$

Definimos la función $t_{b,q}$ que traduce cadenas en base b a conjuntos de cadenas en base q de la siguiente manera:

$$\begin{aligned} t_{b,q} &: b^* \to \mathcal{P}(q^*) \\ t_{b,q}(\sigma) &= \{\tau : |\tau| = y_{b,q}(|\sigma|) \wedge [\sigma]_b \cap [\tau]_q \neq \emptyset\} \ . \end{aligned}$$

A modo de ejemplo, dada σ en base 3 tal que $\sigma = 1$. Si deseamos pasar a base 2:

$$\begin{aligned} y_{3,2}(|1|) &= 3 \\ t_{3,2}(1) &= \{010, 011, 100, 101\} \end{aligned}$$

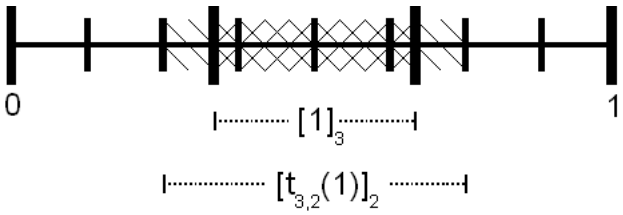

Figura 3: En la recta real, $[1]_3$ y $[t_{3,2}(1)]_2$

Es claro que $t_{b,q}(\sigma)$ tiene cadenas de la misma longitud y por lo tanto es finito. Por un lado, es claro que $[\sigma]_b \subseteq [t_{b,q}(\sigma)]_q$. Por otro, tenemos

$$\begin{aligned} \mu([t_{b,q}(\sigma)]_q \setminus [\sigma]_b) &\leq 2 \cdot q^{-y_{b,q}(|\sigma|)} \\ &\leq b^{-|\sigma|} = \mu_b(\sigma b^\omega), \end{aligned}$$

y por lo tanto

$$\begin{aligned} \mu_q(t_{b,q}(\sigma)q^\omega) &= \mu([t_{b,q}(\sigma)q^\omega]_q) \\ &\leq 2 \cdot \mu_b(\sigma b^\omega). \end{aligned}$$

Definimos $(H_m)_{m\in\mathbb{N}}$, con $H_m \subseteq q^*$, de la siguiente manera:

$$H_m = \bigcup_{\sigma \in G_m} t_{b,q}(\sigma) \ . \tag{15}$$

Hecho 1. *$(H_m)_{m\in\mathbb{N}}$ es un test de Martin-Löf en base q.*

Demostración. Como G_m es uniformemente c.e., y $t_{b,q}(\sigma)$ es computable, entonces H_m es uniformemente c.e..

Además,

$$\begin{array}{lll} \mu_q(H_m q^\omega) \leq & \sum_{\sigma\in G_m} \mu_q(t_{b,q}(\sigma)q^\omega) & \text{por propiedad de la medida} \\ \leq & 2\sum_{\sigma\in G_m} \mu_b(\sigma b^\omega) & \text{pues } \mu_q(t_{b,q}(\sigma)q^\omega) \leq 2 \cdot \mu_b(\sigma b^\omega) \\ = & 2 \cdot \mu_b(G_m b^\omega) & \text{pues } G_m \text{ libre de prefijos} \\ \leq & 2 \cdot b^{-km-1} & \text{por (14)} \\ \leq & (b^k)^{-m} & \text{ya que } 2 \leq b \\ \leq & q^{-m} & \end{array}$$

Por lo tanto, $(H_m)_{m\in\mathbb{N}}$ es un test de Martin-Löf en base q. □

Hecho 2. $Z_q \in \bigcap_m H_m q^\omega$.

Demostración. Es fácil ver que

$$Z_b \in \sigma b^\omega \Leftrightarrow v_b(Z_b) \in [\sigma]_b \ . \tag{16}$$

Como $Z_b \in \bigcap_m G_m b^\omega$, sean σ y n cualesquiera tales que $\sigma \in G_n$ y $Z_b \in \sigma b^\omega$. Entonces, por (16), $v_b(Z_b) \in [\sigma]_b$.

Por lo tanto, por definición de H_m (15), existe τ tal que $\tau \in H_n$ y $v_b(Z_b) = v_q(Z_q) \in [\tau]_q$. Luego, por (16), se puede concluir que $Z_q \in \tau q^\omega$. Como $\tau \in H_n$, se deduce que $Z_q \in H_n q^\omega$.

Dado que el n podía ser cualquier natural, y $Z_b \in \bigcap_m G_m b^\omega$, entonces $Z_q \in \bigcap_m H_m q^\omega$.

Finalmente, Z_q no es Martin-Löf aleatoria en base q. □

Esto concluye la prueba del Teorema 10. □

Teorema 11. *Aleatoriedad de Schnorr es invariante por cambio de base.*

Demostración. Vamos a suponer que Z_b no es Schnorr aleatorio. Entonces, suponemos que existe un test de Martin-Löf en base b $(G_m)_{m\in\mathbb{N}}$ tal que $Z_b \in \bigcap_m G_m b^\omega$ y $\mu_b(G_m b^\omega)$ es computable. Para probar que Z_q no es Schnorr aleatorio, debemos demostrar que existe un test de Martin-Löf en base q $(H_m)_{m\in\mathbb{N}}$ tal que $Z_q \in \bigcap_m H_m q^\omega$ y $\mu_q(H_m q^\omega)$ es computable. Usaremos la construcción utilizada para demostrar que aleatoriedad de Martin-Löf es invariante por cambio de base. Por el Teorema 10 demostrado anteriormente, en base al test en base b $(G_m)_{m\in\mathbb{N}}$ nos construimos un test de Martin-Löf en base q $(H_m)_{m\in\mathbb{N}}$ tal que $Z_q \in \bigcap_m H_m q^\omega$, definido de manera similar al test construido en la demostración para aleatoriedad de Martin-Löf. Debemos probar entonces que $\mu_q(H_m q^\omega)$ es computable. Por simplicidad de notación, nos referiremos a G_m como G, y a H_m como H.

$G = \{\sigma_1, \sigma_2, \sigma_3, ...\}$ es uniformemente c.e. y, como G es libre de prefijos,

$$\mu_b(Gb^\omega) = \sum_i \mu_b(\sigma_i b^\omega) = \sum_i b^{-|\sigma_i|}.$$

Entonces,

$$\lim_{i\to\infty} \mu_b(\bigcup_{j\geq i} \sigma_j b^\omega) = 0. \tag{17}$$

Como $\mu_b(Gb^\omega)$ es computable, existe f computable que acota el error de la aproximación de $\mu_b(Gb^\omega)$ en el siguiente sentido: dado $\varepsilon \in \mathbb{Q}$,

$$\sum_{j\geq f(\varepsilon)} \mu_b(\sigma_j b^\omega) = \mu_b(\bigcup_{j\geq f(\varepsilon)} \sigma_j b^\omega) < \varepsilon. \tag{18}$$

Queremos ver que $\mu_q(Hq^\omega)$ es computable. Para eso, como H es uniformemente c.e. por Teorema 10, y por cómo está definida H en (15), basta con encontrar g computable tal que, dado $\varepsilon \in \mathbb{Q}$:

$$\mu_q(\bigcup_{j\geq g(\varepsilon)} t_{b,q}(\sigma_j) q^\omega) < \varepsilon \ . \tag{19}$$

Ahora bien,

$$\begin{array}{rcll} \mu_q(\bigcup_{j\geq g(\varepsilon)} t_{b,q}(\sigma_j)q^\omega) & \leq & \sum_{j\geq g(\varepsilon)} \mu_q(t_{b,q}(\sigma_j)q^\omega) & \text{por propiedad de la medida} \\ & \leq & 2\sum_{j\geq g(\varepsilon)} \mu_b(\sigma_j b^\omega) & \text{pues } \mu_q(t_{b,q}(\sigma_i)q^\omega) \leq 2\mu_b(\sigma_i b^\omega) \end{array}$$

Si definimos $g(\varepsilon) = f(\varepsilon/2)$:

$$\begin{array}{rcll} \mu_q(\bigcup_{j\geq g(\varepsilon)} t_{b,q}(\sigma_j)q^\omega) & \leq & 2\sum_{j\geq f(\varepsilon/2)} \mu_b(\sigma_j b^\omega) & \\ & < & \varepsilon & \text{por (18)} \end{array}$$

Entonces, con tomar $g(\varepsilon) = f(\varepsilon/2)$ nos alcanza para que valga (19). Además, como f es computable, g es computable.

En conclusión, $\mu(Hq^\omega)$ es computable. Y entonces, Z_q no es Schnorr aleatoria. □

Teorema 12. *Aleatoriedad de Kurtz es invariante por cambio de base.*

Demostración. Seguimos la misma idea que la prueba del Teorema 10 sobre Z_b y Z_q. Si partimos de un test de Kurtz $(G_m)_{m\in\mathbb{N}}$ en base b con la propiedad (14) tal que $Z_p \in \bigcap_m G_m b^\omega$, llegamos a la definición de un test de Kurtz $(H_m)_{m\in\mathbb{N}}$ en base q. Efectivamente, por el Hecho 1, $\mu_q(H_m q^\omega) \leq q^{-m}$. Además como cada G_m es finito, por la definición de H_m en (15), H_m también lo es. Finalmente, por el Hecho 2, tenemos $Z_q \in \bigcap_m H_m q^\omega$. □

7. Un esquema para construir números absolutamente normales

En esta sección mostramos cómo se podrían construir números absolutamente normales siguiendo un método distinto a los utilizados en [4] y [5]. En realidad, el éxito de este esquema dependerá de un resultado esencial, que no pudimos probar en esta tesis (trabajo en esta dirección se encuentra en [17]). Se trata de la siguiente conjetura:

Conjetura 13. *Para alguna función de tiempo $t(n)$, $t(n)$-aleatoriedad es invariante por cambio de base.*

Siguiendo el siguiente razonamiento, se podría concluir que, si Z es $t(n)$-aleatoria (en la definición clásica en base 2), entonces Z es absolutamente normal:

$$\begin{array}{rcll} Z \in 2^\omega \text{ es } t(n)\text{-aleatoria en base 2} & \Rightarrow & \forall b(Z \text{ es } t(n)\text{-aleatoria en base } b) & \text{por (Conj. 13)} \\ & \Rightarrow & \forall b(Z \text{ es normal base } b) & \text{por (Teo. 6)} \\ & \Rightarrow & Z \text{ es absolutamente normal} & \text{por definición} \end{array}$$

Entonces, al construir una secuencia $t(n)$-aleatoria, se estaría garantizando que esa secuencia es absolutamente normal.

Entonces, el problema está en construir una secuencia Z que sea $t(n)$-aleatoria, o sea, que ninguna $t(n)$-martingala tenga éxito en Z. Esto se logra mediante un argumento de diagonalización. Una posibilidad es basarse en [12, Sección 7.4]. En esa sección, se demuestra que es posible encontrar una martingala L universal que domina multiplicativamente a todas las demás martingalas –en el sentido de que para toda martingala F existe una constante c tal que $F(x) \leq c \cdot L(x)$ para todo x.

Habría que hacer una modificación a la construcción presentada en [12] para construir una martingala L que domine multiplicativamente solamente a todas las $t(n)$-martingalas,

pero siendo L una $t'(n)$-martingala, o sea, encontrando una cota temporal para la L deseada. Para eso, primero hay que enumerar todas las $t(n)$-martingalas. Esto se puede hacer con una máquina universal y 'cortando' los cómputos simulados en tiempo $t(n)$. Para detalles sobre la implementación de una máquina universal eficiente, ver [2, Cap. 1.7], para el uso de esta máquina universal en cómputos interrumpidos por cierto tiempo ver por ejemplo [2, Cap. 3.1]. Entonces, si L no tiene éxito en una secuencia Z, como L domina multiplicativamente a todas las $t(n)$-martingalas, ninguna $t(n)$-martingala tendrá éxito en Z, por lo que Z resultará $t(n)$-aleatoria, y por lo tanto absolutamente normal.

A continuación, supongamos que L es nuestra $t'(n)$-martingala que domina multiplicativamente a todas las $t(n)$-martingalas. El siguiente algoritmo, dado $n \in \mathbb{N}$, devuelve $Z(n)$ tal que L no tiene éxito en Z:

Entrada: $n \in \mathbb{N}$; Salida: $Z(n) \in \{0, 1\}$.
$\sigma := \lambda$
Para $i = 0 \cdots n$:
  Si $L(\sigma 0) < L(\sigma 1)$:
    $\sigma := \sigma 0$
  Si no:
    $\sigma := \sigma 1$
Devolver $\sigma(n)$

Es fácil ver que L no tiene éxito en Z.

Analicemos la complejidad del algoritmo. El ciclo principal se ejecuta n veces. En cada iteración del ciclo, se realizan dos llamados a L, se comparan los dos resultados (cada resultado es un racional), y se realizan una asignación. El costo de la asignación es despreciable al lado del costo de las otras operaciones.

El costo de cada llamado a L se puede acotar por $O(t'(n))$. El costo de comparar dos racionales a y b es $O(\log(\text{máx}\{|a|, |b|\}))$. Como el costo de cada llamado a L se puede acotar por $O(t'(n))$, el tamaño de la salida nunca puede ser mayor a $O(t'(n))$. Y, en consecuencia, el costo de cada comparación se puede acotar por $O(\log(O(t'(n)))) = O(\log(t'(n)))$.

En conclusión, si el tamaño de la entrada es $m = \log n$, el costo de todo el algoritmo en función del tamaño de la entrada resulta de

$$2^m \cdot (O(t'(2^m)) + O(\log(t'(2^m)))) = O(2^m \cdot t'(2^m)).$$

Por ejemplo, si se pudiera probar la Conjetura 13 para $t(n) = n^2$ y $t'(n) = n^p$ para un p fijo (o sea, $t'(n)$ tiene complejidad temporal polinomial), entonces tendríamos un algoritmo para computar un número absolutamente normal en tiempo $O(2^{m(p+1)})$, es decir en tiempo simplemente exponencial. Esto representa una mejora significativa con respecto a los tiempos de los algoritmos encontrados en [4] y [5].

Referencias

[1] Klaus Ambos-Spies and Elvira Mayordomo. Resource bounded measure and randomness. In A. Sorbi, editor, *Complexity Logic and Recursion Theory*, pages 1–47. Marcel Dekker, New York NY, 1997.

[2] Sanjeev Arora and Boaz Barak. *Computational Complexity: A Modern Approach*. Cambridge University Press, 2009.

[3] David H. Bailey and Richard E. Crandall. On the random character of fundamental constant expansions. *Experimental Mathematics*, 10(2):175–190, 2001.

[4] Verónica Becher and Santiago Figueira. An example of a computable absolutely normal number. *Theoretical Computer Science*, 270:947–958, 2002.

[5] Verónica Becher, Santiago Figueira, and Rafael Picchi. Turing's unpublished algorithm for normal numbers. *Theoretical Computer Science*, 377(1-3):126–138, 2007.

[6] Adrian Belshaw and Peter Borwein. Strong normality of numbers. 2008. `http://www.cecm.sfu.ca/personal/pborwein/PAPERS/P211.pdf`.

[7] Émile Borel. Les probabilités dénombrables et leurs applications arithmétiques. *Rendiconti del Circolo Matematico di Palermo*, 27:247–271, 1909.

[8] Cristian Calude. *Information and Randomness, an Algorithmic Perspective*. Springer-Verlag, Berlin, 1994.

[9] David G. Champernowne. The construction of decimals in the scale of ten. *Journal of the London Mathematical Society*, 8:254–260, 1933.

[10] Stuart Kurtz. *Randomness and Genericity in the Degrees of Unsolvability*. PhD thesis, University of Illinois at Urbana, 1981.

[11] Per Martin-Löf. The definition of random sequences. *Information and Control*, 9:602–619, 1966.

[12] André Nies. Computability and randomness. To appear in Clarendon Press, Oxford, 2008.

[13] Wolfgang M. Schmidt. On normal numbers. *Pacific Journal of Mathematics*, 10:661–672, 1960.

[14] Claus-Peter Schnorr. A unified approach to the definition of a random sequence. *Mathematical Systems Theory*, 5:246–258, 1971.

[15] Claus-Peter Schnorr. Zufälligkeit und Wahrscheinlichkeit. *Lecture Notes in Mathematics*, 218, 1971.

[16] Robert Solovay. Draft of a paper (or series of papers) on Chaitin's work done for the most part during the period Sept. to Dec. 1974. Unpublished manuscript, IBM Thomas J. Watson Research Center, Yorktown Heights, New York. 215 pp., May 1975.

[17] Joseph S. Miller Vasco Brattka and André Nies. Randomness and differentiability. 2010.

[18] Yongge Wang. *Randomness and Complexity*. PhD thesis, University of Heidelberg, 1996.