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

Invariancia por cambio de base de la aleatoriedad computable y la aleatoriedad con recursos acotados

Tesis presentada para optar al título de
Licenciado en Ciencias de la Computación

Javier Gonzalo Silveira

Director: Santiago Daniel Figueira

Buenos Aires, Abril de 2011

Resumen

Si bien se suele hablar de números reales aleatorios, en realidad la condición de ser aleatorio depende de la *representación* del número y no del número en sí. Por lo tanto, las nociones de aleatoriedad no necesariamente son invariantes para distintas representaciones, por ejemplo, representaciones en distintas bases.

El concepto de aleatoriedad de Martin-Löf intenta capturar la noción intuitiva de aleatoriedad para secuencias infinitas y es hoy en día la noción que mayor aceptación tiene. Puede ser caracterizada mediante funciones especiales llamadas martingalas, y al imponer restricciones de efectividad sobre éstas surgen de forma natural las nociones de *aleatoriedad computable* y *aleatoriedad con recursos acotados*. Se sabe que la aleatoriedad de Martin-Löf es invariante por cambio de base, pero no hay muchos resultados para otras nociones como aleatoriedad computable o aleatoriedad con recursos acotados.

Basándonos en la idea de una correspondencia entre martingalas y funciones continuas de un trabajo en preparación de Brattka, Miller y Nies, construimos una nueva demostración de que la aleatoriedad computable es invariante por cambio de base. Si bien el mencionado trabajo incluye una demostración de este hecho, creemos que nuestra prueba es más simple, intuitiva y corta. Luego usamos y modificamos nuestra propia construcción para probar que aleatoriedad polinomial también es invariante por cambio de base.

Índice

Agradecimientos

Agradezco a mi papá, mi mamá y mis hermanos, por apoyarme en todo momento y estar siempre ahí conmigo. Me siento la persona más afortunada del mundo por tenerlos a ellos como familia.

A Santiago Figueira, por darme la oportunidad de hacer la tesis con el, dedicarme una cantidad de tiempo y de trabajo increíble, estar en todos los detalles y ayudarme en absolutamente todo. También por tratarme siempre con calidez, alegría y con esa humildad infinita que es un ejemplo para cualquiera.

A los jurados Verónica Becher y Rafael Grimson, por tomarse el trabajo de leer y corregir esta tesis.

A mis amigos Eddy y Bruno, por bancarme y ser mi grupo de trabajos prácticos en casi todas las materias. Soportar toda la carrera no hubiera sido lo mismo sin ellos.

A la manada de *Gente de la facu*, compañeros de cursada y amigos en todos estos años: Chapa, Facu, Fer, Giga, Lean, Leo Rodriguez, Leo Spett, Luisito, Martin, Mati, Maxi, Nati, Nelson, Pablito, Palla, Serch, Tara, Vivi y Z. Son un grupo único e increíble.

A todos los docentes y gente copada de la facultad y del Departamento de Computación que hicieron y hacen de la carrera algo muy especial.

A mis queridos amigos de matemática Juli, Leon, Lu, Quimey, Xime y Yanu. Me alegro de haber cursado álgebra a la mañana y así haberlos conocido.

A Cin, Colors, Sobral y Zoppi, el *grupo de élite*, por haber compartido tantos buenos momentos conmigo.

A mis amigos del alma Nico y Facu, por seguir cerca.

A mis compañeros de esa aventura surrealista que fue *Kayxo*, con mención especial a Carnero, siempre apoyando a los "pendejos" para que no dejen la facu.

A Gonzalo Zabala, casi seguro no estaría en esta carrera si no fuera por el.

Por último, un agradecimiento muy especial a Euge, por bancarme, estar al lado mío y ser una luz en mi vida, que cambió completamente para bien desde que la conocí.

1. Introducción

La aleatoriedad es un concepto para el cual, en mayor o menor medida, todos tenemos ciertas nociones intuitivas. Generalmente un objeto al azar o aleatorio se asocia con algo desorganizado, sin patrones, sin regularidades. Trasladando esta intuición sobre aleatoriedad a cadenas de símbolos, por ejemplo de ceros y unos, nadie diría que una cadena en cuyas posiciones pares siempre hay un cero es una cadena verdaderamente aleatoria. Cuando en lugar de hablar de cadenas finitas se pasa a secuencias infinitas de números, los conceptos se empiezan a tornar un poco menos naturales. Aún así, la mayoría de las personas coincidiría en que una secuencia infinita de unos no tiene nada de aleatoria. Tratándose de un concepto abstracto pero a la vez muy presente en la mente humana, no es sorprendente que hayan existido numerosos intentos de capturar y plasmar de manera formal estas nociones intuitivas.

Si bien uno de los primeros intentos en definir el concepto de secuencia aleatoria se remonta a von Mises en 1919 [22], este (y muchos otros trabajos que le siguieron) sufrían de distintos problemas y falencias, como definiciones difusas en algunos casos y resultados que no satisfacían algunas de las leyes fundamentales de la estadística en otros. La definición de aleatoriedad de Martin-Löf en 1966 [11] se mostró mucho más sólida que las anteriores, y actualmente es considerada por gran parte de la comunidad científica como la noción que mejor captura la idea intuitiva de aleatoriedad.

En la teoría de la probabilidad el concepto de martingala (una formalización basada en estrategias de apuestas) fue inventado por Levy, y más tarde fue aplicado por primera vez al estudio de secuencias aleatorias por Ville [21]. Luego fue Schnorr [15] quien trajo las martingalas al primer plano, al usarlas por primera vez en relación al concepto de aleatoriedad algorítmica. Schnorr desarrolló una caracterización alternativa de la aleatoriedad de Martin-Löf basada en martingalas. Su caracterización mediante martingalas dio una forma natural de definir criterios de efectividad sobre la aleatoriedad de secuencias, dando origen a una importante conexión entre las teorías de la aleatoriedad, computabilidad y complejidad.

Cuando se analiza la aleatoriedad de una secuencia infinita, esta secuencia se puede pensar como la representación de un número real. Sin embargo, los números reales son objetos matemáticos que tienen varias representaciones. Dentro de la numeración posicional, la representación decimal es quizás la más común de todas, pero existen otras muy usadas como la binaria o la hexadecimal. En principio, son estas secuencias de símbolos (representaciones) y no los números reales las que tienen la propiedad de ser aleatorias según un criterio u otro. Entonces, la pregunta que surge naturalmente cuando se estudia una noción de aleatoriedad específica es si la aleatoriedad de una representación de un número real implica la aleatoriedad de otras representaciones posibles del mismo número. Esta tesis se centra en esa pregunta aplicada a las nociones de aleatoriedad computable y aleatoriedad con recursos acotados (definidas a partir de martingalas computables y con recursos acotados respectivamente).

Al pensar sobre secuencias aleatorias es intuitivo y razonable sospechar que esta propiedad no puede depender de la base en la que se representa un número, de algo tan mecánico y regular como una transformación de cambio de base. Efectivamente, esta intuición resulta correcta si se usa como criterio la aleatoriedad de Martin-Löf [4, 5, 7, 18, 19]. Sin embargo, si se pasa a usar un criterio de aleatoriedad mucho más débil, se sabe que la normalidad de un número en una base (que todas las posibles cadenas finitas de igual longitud aparecen en la secuencia con igual frecuencia) no implica normalidad en todas las demás bases [14]. Con respecto a otras nociones, se sabe que tanto la aleatoriedad de Schnorr como la de Kurtz son invariantes por cambio de base [19].

Determinar si una noción de aleatoriedad es invariante por cambio de base no suele ser sencillo. Existen varias nociones para las cuales la pregunta está abierta, como por ejemplo aleatoriedad de Kolmogorov-Loveland [12].

Este trabajo se centra en la invariancia por cambio de base para las nociones de aleatoriedad computable y aleatoriedad polinomial. Nos basamos en una conexión entre martingalas y funciones continuas presentada en un trabajo, todavía no publicado, de Brattka, Miller y Nies [3]. Si bien el resultado principal del mismo es una caracterización de Martin-Löf aleatoriedad y la aleatoriedad computable mediante criterios de diferenciabilidad de ciertas funciones, en el camino también se prueba que la aleatoriedad computable es invariante por cambio de base mediante una correspondencia entre martingalas y funciones continuas no decrecientes. Usando esa idea como inspiración, damos una nueva demostración constructiva de la invariancia por cambio de base de la aleatoriedad computable. Creemos que nuestra demostración es más intuitiva, directa y autocontenida que la presentada en [3]. En el camino también generalizamos a cualquier base algunas propiedades interesantes de las martingalas que hasta ahora estaban estudiadas para la base binaria. Por otra parte, la naturaleza constructiva de nuestra nueva demostración provee un buen punto de partida para analizar el comportamiento de las martingalas con recursos acotados respecto a las transformaciones de base. En esta dirección demostramos que la aleatoriedad polinomial también es invariante por cambio de base, lo cual es un resultado nuevo. Este resultado puede extenderse a otras clases de complejidad.

Esta tesis se organiza de la siguiente forma:

En la Sección 2 se introduce notación, algunos conceptos generales, las definiciones relativas a martingalas, sus variaciones y el resto de las definiciones formales que son necesarias para entender las demás secciones.

En la Sección 3 se presentan y demuestran, generalizadas a cualquier base, algunas propiedades de las martingalas que son especialmente importantes para las secciones posteriores. Si bien son resultados conocidos para base 2, aquí se extienden a cualquier base, algo no trivial en algunos casos.

La Sección 4 desarrolla la nueva demostración de invariancia por cambio de base de la aleatoriedad computable. La demostración es constructiva y se basa en la idea de construir una medida a partir de una martingala.

En la Sección 5 se demuestra que la aleatoriedad polinomial es invariante por cambio de base. Se toma como base la demostración de la sección anterior, y se la modifica para lograr una construcción polinomial. Por último, se extiende el resultado a otras clases de complejidad temporal.

Por último, en la Sección 6 se presentan algunas conclusiones generales del trabajo y posibles líneas de investigación para trabajos futuros.

2. Preliminares

2.1. Notación

Se entiende que las *cadenas* son siempre finitas y las *secuencias* infinitas.

El alfabeto $\{0, \ldots, k-1\}$ se denota con k. Entonces k^* representa todas las cadenas finitas formadas con el alfabeto k. Las *cadenas en base k* son los elementos de k^*. Las letras $\sigma, \tau, \rho, \upsilon$ usualmente van a denotar cadenas. Luego se usa la notación estándar:

$\sigma\tau$	para concatenación de σ y τ
σa	para σ seguido del símbolo a
$\sigma \preceq \tau$	para decir que σ es un prefijo de τ
$\lvert\sigma\rvert$	es la longitud de la cadena σ
$\sigma(n)$	para $n \in \mathbb{N}$ es el n-ésimo símbolo de σ
$\emptyset$	la cadena vacía, de longitud cero
$\sigma \upharpoonright_n$	representa la subcadena de σ que contiene sus primeros n símbolos

Con k^ω denotamos el conjunto de todas las secuencias (infinitas) con el alfabeto k. Observar que k^ω es un *espacio de Cantor*. Usualmente se usará Z e Y para secuencias pertenecientes a k^ω. Por $Z \upharpoonright_n$ se entiende la cadena formada por los primeros n símbolos de Z.

Usualmente z e y denotarán números reales. $\mathbb{R}_0^+$ denota los números reales no negativos.

Si $\sigma \in k^*$ y $Z \in k^\omega$ entonces

$$0.Z \text{ representa al número real } \sum_{n=1}^{\infty} Z(n) \cdot k^{-n}$$

$$0.\sigma \text{ representa al número real } 0.Z, \text{ donde } Z = \sigma 00000\ldots$$

Para $\sigma \in k^*$, $[\sigma] = \{Z : \sigma \preceq Z\}$. Esta clase de conjuntos se conoce como *cilindros abiertos básicos* del espacio k^ω. Se define $[D]^\prec$ como $\bigcup_{\sigma \in D}[\sigma]$.

Para $\sigma \in k^*$, $[\sigma]_k$ denota el intervalo real $[0.\sigma, 0.\sigma + k^{-|\sigma|})$. Esta notación es muy usada, por lo que es importante no confundirla con la de los cilindros $[\sigma]$, que representan conjuntos de secuencias en el espacio de Cantor k^ω (en lugar de intervalos reales).

Para la teoría de complejidad se usa la notación estándar. Se considerará en particular la clase de tiempo polinomial determinista:

$$\mathbf{P} = \mathbf{DTIME}(poly) = \bigcup_{k \geq 1} \mathbf{DTIME}(n^k)$$

2.2. Aleatoriedad

Se podría decir que la búsqueda de nociones de aleatoriedad más sólidas tuvo su hito principal en 1966, cuando Martin-Löf [11] definió las secuencias aleatorias como aquellas que satisfacen todos los tests estadísticos razonables. Una muestra de la robustez de este concepto fue la posterior demostración de la existencia de caracterizaciones alternativas en términos de la compresibilidad de cadenas (Levin [8], Schnorr [17] y Chaitin [6]) y en términos de estrategias de apuestas llamadas martingalas (Schnorr [15]), el principal objeto de estudio de esta tesis. Aún así, esta noción de aleatoriedad recibió sus críticas, una de ellas por parte de Schnorr [16], quién argumentaba que era demasiado fuerte como para ser considerada algorítmica. Si bien su crítica no tuvo demasiada aceptación, el enfoque de sus trabajos utilizando martingalas derivó en una forma muy natural a conceptos de aleatoriedad en teorías de complejidad y medidas con recursos acotados.

A continuación se profundiza más sobre las definiciones relativas a martingalas, sus propiedades y sus variaciones.

2.2.1. Martingalas

Las martingalas son el equivalente matemático del concepto intuitivo de una estrategia de apuestas. A modo de ejemplo, supongamos que se tiene una secuencia infinita secreta Z de ceros y unos. El apostador comienza con un capital inicial. La secuencia se revela de a un dígito por vez, y en cada ronda el jugador debe apostar una parte de su capital al dígito que predice que va a salir. Si sale el dígito apostado recibe el doble de lo que apostó, en caso contrario lo pierde. Además, el jugador conoce todo lo que ya salió de la secuencia hasta el momento. El objetivo es ganar capital a lo largo de Z prediciendo el próximo dígito luego de haber visto todos los anteriores. Una estrategia de apuestas ganadora para una secuencia Z es una estrategia que a la larga permite aumentar el capital de forma ilimitada. A continuación, este tipo de estrategias se formalizan matemáticamente con el concepto de martingala.

Definición 2.1. Una *martingala* es una función $M : 2^* \to \mathbb{R}_0^+$ que para todo $\sigma \in 2^*$ satisface

$$M(\sigma 0) + M(\sigma 1) = 2M(\sigma),$$

condición que en la literatura se suele llamar "*fairness condition*" o "*averaging condition*" (condición de equidad o promedio).

Desde el punto de vista de las estrategias de apuestas, $M(\sigma)$ representa el capital que tiene el apostador después de haber visto σ (y apostado en cada paso siguiendo su estrategia). Es claro que en esta formalización la estrategia (cuánto apostar a cada símbolo) no está explícita, sin embargo cada martingala está caracterizada por su *estrategia de apuestas subyacente*. La estrategia es la función que determina, dada una secuencia binaria, qué porcentaje del capital acumulado se debe apostar a que el próximo bit es un 0 (el porcentaje restante es si sale 1). Una *estrategia* es una función $s : 2^* \to [0, 1]$. Dada una martingala M, su *estrategia subyacente* s_M es

$$s_M(\sigma) = \begin{cases} \frac{M(\sigma 0)}{2M(\sigma)} & \text{si } M(\sigma) \neq 0; \\ 0 & \text{si no.} \end{cases}$$

De forma análoga, dada una estrategia s y un real $\alpha > 0$, la martingala M_s con capital inicial α *inducida* por s se define como $M_s(\emptyset) = \alpha$ y para todo $\sigma \in 2^*$

$$M_s(\sigma 0) = 2 \cdot s(\sigma) M_s(\sigma)$$
$$M_s(\sigma 1) = 2 \cdot (1 - s(\sigma)) M_s(\sigma).$$

Como se mencionó anteriormente, es de interés saber si para una secuencia en particular una martingala puede alcanzar una cantidad de capital no acotado mediante apuestas sobre la misma. A continuación se formaliza esta noción de éxito sobre una secuencia.

Definición 2.2. Una *martingala* M tiene éxito en $Z \in 2^\omega$ si

$$\limsup_{n \to \infty} M(Z\restriction_n) = \infty.$$

Intuitivamente, la relación entre aleatoriedad y martingalas radica en el hecho de que si una secuencia es verdaderamente aleatoria, uno no debería ser capaz de predecir su comportamiento y ganar capital con ello.

La familia de funciones martingalas no sólo es útil por formalizar el concepto intuitivo de estrategias de apuestas, sino también por las numerosas propiedades algebraicas que poseen.

Las siguientes propiedades se pueden encontrar en [13, Fact 7.1.7].

Proposición 2.3.

1. *Si $\alpha \in \mathbb{R}^+$ y B y C son martingalas, entonces también lo son αB y $B + C$.*
2. *Si N_i es una martingala para cada $i \in \mathbb{N}$ y $\sum_i N_i(\emptyset) < \infty$ entonces $N = \sum_i N_i$ es una martingala.*
3. *Si B es una martingala y $\upsilon \in 2^*$ entonces $\lambda\sigma.B(\upsilon\sigma)$ es una martingala.*

Para cualquier martingala M se puede construir M' tal que $M'(\emptyset) < 1$ y tenga éxito en las mismas secuencias que M.

2.2.2. Supermartingalas

Es usual trabajar con una noción un poco más amplia que las martingalas, en el sentido de que relaja la *fairness condition*.

Definición 2.4. Una *supermartingala* es una función $S : 2^* \to \mathbb{R}_0^+$ que para todo $\sigma \in 2^*$ satisface

$$S(\sigma 0) + S(\sigma 1) \leq 2S(\sigma).$$

El éxito de S sobre una secuencia $Z \in 2^\omega$ se define igual que para las martingalas. Las supermartingalas muchas veces son convenientes para realizar manipulaciones algebraicas de martingalas con mayor flexibilidad. La siguiente proposición, sencilla de probar [13, Proposition 7.1.6], las hace especialmente útiles:

Proposición 2.5. *Para cada supermartingala S existe una martingala B tal que $B(\emptyset) = S(\emptyset)$ y $B(\sigma) \geq S(\sigma)$ para cada σ.*

Observar que de esta proposición se deduce que si una supermartingala S tiene éxito en una secuencia Z, existe una martingala M que también tiene éxito en Z (ya que M es siempre mayor que S, entonces si S no está acotada para Z, M tampoco).

2.2.3. Martingalas en otras bases

La definición de martingala se puede generalizar a dominios distintos de 2^*. Dada una base $k \geq 2$, el concepto de martingala en base k se puede definir [3] de la siguiente forma:

Definición 2.6. Una *martingala en base k* es una función $M : k^* \to \mathbb{R}_0^+$ que para todo $\sigma \in k^*$ satisface la condición de equidad

$$\sum_{i=0}^{k-1} M(\sigma i) = kM(\sigma).$$

Esta generalización se la puede seguir pensando como una estrategia de apuestas. Un ejemplo sería jugar repetidamente a algún tipo de lotería donde k es el número de resultados posibles. Se conoce una cadena $\sigma \in k^*$, es decir los $|\sigma|$ resultados que ya salieron. Se apuesta entonces una cantidad $q \leq M(\sigma)$ a un resultado en particular, si se acierta se gana $(k-1) \cdot q$, en caso contrario se pierde q. De forma análoga a las martingalas en base 2, aquí $M(\sigma)$ representa el capital que el apostador tiene luego de haber visto σ, es decir, luego de haber hecho $|\sigma|$ apuestas usando su estrategia a medida que se revelaban los símbolos de σ.

Para una martingala en base k, la definición de *éxito* sobre una secuencia $Z \in k^\omega$ es exactamente análoga a la Definición 2.2.

La noción de supermartingala también se puede generalizar a base k de forma análoga.

2.2.4. Martingalas computables

Como las martingalas son funciones en valores reales, y es de interés usarlas en contextos constructivos con requerimientos de efectividad sobre ellas, es necesario introducir alguna noción de computabilidad para funciones reales.

En este trabajo se optó por usar una definición de funciones reales computables bastante intuitiva, equivalente a la presentada por Terwijn [20, Definition 1.5.2], y que a su vez se basa en el trabajo de Lutz sobre teoría de medidas constructivas y con recursos acotados [10].

Definición 2.7. Sea Σ un alfabeto finito y sea $f : \Sigma^* \to \mathbb{R}$. Se dice que f es una *función real computable* si existe una función computable $\tilde{f} : \Sigma^* \times \mathbb{N} \to \mathbb{Q}$ tal que

$$\forall \sigma \in \Sigma^* \text{ y } q \in \mathbb{N}, \quad |\tilde{f}(\sigma, q) - f(\sigma)| < 2^{-q}. \tag{2.7.1}$$

Decimos que $\tilde{f}$ es una *aproximación computable* de f.

En particular, se hablará de que M es una *martingala computable* (o martingala real computable) cuando M sea una función real computable de acuerdo a la definición anterior.

Definición 2.8. Una secuencia $Z \in k^\omega$ es *computablemente aleatoria* si no existe ninguna martingala computable que tenga éxito en Z.

Se sabe que toda secuencia Martin-Löf aleatoria es computablemente aleatoria, pero que su recíproca es falsa [13, Teorema 7.5.7].

2.2.5. Martingalas con recursos acotados

Es posible tomar la definición de aleatoriedad computable y extenderla agregando requerimientos de efectividad con recursos acotados.

Schnorr [15] fue uno de los primeros en hablar de aleatoriedad acotada por recursos basándose en martingalas. Luego Lutz [9] estudió las medidas acotadas por recursos, un concepto estrechamente relacionado con la aleatoriedad y que se basa en la caracterización de las clases de medida-0 mediante martingalas. Si bien estos dos enfoques tienen sus diferencias, en el fondo son casi equivalentes. Ambos-Spies y Mayordomo [1] introducen ambos conceptos para las clases de complejidad temporal, optando por definir una $t(n)$-martingala como aquella que es inducida por una $t(n)$-estrategia s, donde s es una función racional computable no decreciente perteneciente a $\mathbf{DTIME}(t(n))$. Sin embargo, en este trabajo se opta por continuar con la línea de Lutz, trabajando con aproximaciones de martingalas reales (ya adoptada para martingalas computables) y agregando restricciones sobre la efectividad de estas aproximaciones.

Definición 2.9. Sea $f : \Sigma^* \to \mathbb{R}$ una función real computable y $t : \mathbb{N} \to \mathbb{N}$ una función no decreciente computable. Se dice que f es una *funcion real $t(n)$-computable* si existe una aproximación computable $\tilde{f} : \Sigma^* \times \mathbb{N} \to \mathbb{Q}$ que cumple (2.7.1) y $\tilde{f} \in \mathbf{DTIME}(t(n))$.

Se dirá que M es una *$t(n)$-martingala* cuando M sea una función real $t(n)$-computable. También se hablará de *martingalas polinomiales* para referirse a $t(n)$-martingalas con $t(n) \in \mathbf{P}$.

Como es usual, cuando se habla de $t(n)$, el parámetro n se refiere a la longitud de la representación de la entrada en una máquina de Turing. Es necesario aclarar que al representar $(\sigma, q) \in \Sigma^* \times \mathbb{N}$, por convención se asumirá que q se codifica en unario. De esta forma, la entrada (σ, q) tiene longitud $|\sigma| + q$ y no $|\sigma| + |q|$.

Definición 2.10. Una secuencia $Z \in k^\omega$ es *$t(n)$-aleatoria* si no existe ninguna $t(n)$-martingala que tenga éxito en ella.

Se hablará de secuencias *polinomialmente aleatorias* para referirse a secuencias $t(n)$-aleatorias con $t(n) \in \mathbf{P}$.

2.2.6. Martingalas racionales

Como se verá más adelante (Lema 3.1), en el marco de la aleatoriedad computable y la aleatoriedad con recursos acotados es indistinto si se trabaja con martingalas reales o racionales, debido a que existe una correspondencia entre las mismas.

Luego, si bien desde el punto de vista de la teoría clásica de la complejidad lo más razonable sería elegir trabajar con funciones computables racionales, decidimos utilizar martingalas reales para desarrollar y probar la mayoría de los resultados. Principalmente, esta decisión se debió a que uno de los argumentos centrales usados en las demostraciones de invariancia por cambio de base utiliza una correspondencia entre martingalas y medidas en la cual resulta más cómodo y natural trabajar con funciones reales.

Como toda función que toma valores racionales también toma valores reales, las definiciones de aleatoriedad computable y $t(n)$-aleatoriedad se extienden trivialmente para martingalas racionales: la función racional computable es su propia aproximación computable (donde el parámetro del error es sencillamente ignorado, ya que no hay error). De la misma manera, para $t(n)$-aleatoriedad las restricciones temporales se imponen directamente sobre la martingala racional original (en lugar de una aproximación).

Como convención, cuando se hable de martingalas computables y $t(n)$-martingalas se estará haciendo referencia a martingalas reales. En los casos en que se trate de martingalas racionales se aclarará de forma explícita.

2.3. Medidas y espacios topológicos

Existe una equivalencia entre martingalas y medidas en 2^ω que es central para los resultados más importantes de esta tesis. Por completitud, se presentan a continuación algunas nociones y resultados útiles para entender los argumentos principales de teoría de medida que se usan en este trabajo.

Definición 2.11. Un *álgebra de conjuntos* $\mathcal{A}$ es una familia de subconjuntos de un espacio X tal que:

1. X y el conjunto vacío pertenecen a $\mathcal{A}$;
2. si A, $B \in \mathcal{A}$, entonces $A \cap B \in \mathcal{A}$, $A \cup B \in \mathcal{A}$ y $A \backslash B \in \mathcal{A}$.

Definición 2.12. Un álgebra de conjuntos $\mathcal{A}$ se llama *σ-álgebra* si para cualquier secuencia de conjuntos $A_n \in \mathcal{A}$ vale que $\bigcup_{n=1}^{\infty} A_n \in \mathcal{A}$.

Definición 2.13. Sea $\mathcal{B}$ una σ-álgebra. Una función $\mu : \mathcal{B} \to \mathbb{R}_0^+$ se llama *medida* si cumple:

- $\mu(\emptyset) = 0$
- $\mu(E) \geq 0$ para todo $E \in \mathcal{B}$
- μ es σ-aditiva (o numerablemente aditiva): $\mu(\bigcup_i D_i) = \sum_i \mu(D_i)$ para cada familia numerable $(D_i)_{i \in \mathbb{N}}$ de conjuntos disjuntos dos a dos.

Definición 2.14. Las *clases de Borel* son las subclases de 2^ω que se pueden obtener a partir de los cilindros abiertos básicos $[\sigma]$ mediante las operaciones de complemento y uniones numerables.

En otras palabras, son todos los conjuntos que pueden generarse a partir de conjuntos abiertos de E mediante uniones numerables, intersecciones numerables y complementos.

Teorema 2.15. (Teorema de la extensión de Carathéodory [2]) *Sea R un álgebra de conjuntos de un espacio X y $\mu : R \to [0, +\infty]$ una medida sobre R. Existe una medida $\mu' : \sigma(R) \to [0, +\infty]$ tal que μ' es una extensión de μ ($\mu'|_R = \mu$), donde $\sigma(R)$ es la σ-álgebra generada por R (la σ-álgebra más chica que contiene todos los conjuntos de R).*

Un subconjunto de un espacio topológico se dice *clopen* si es abierto y cerrado al mismo tiempo.

La siguiente proposición, que se usará más adelante, es una pieza fundamental de los argumentos necesarios para desarrollar los principales resultados de este trabajo.

Proposición 2.16. *Si $\mu : 2^* \to [0, 1]$ es una medida definida para los cilindros $[\sigma]$ con $\sigma \in 2^*$, entonces se puede extender a los conjuntos de Borel en $[0, 1]$.*

Idea de la demostración. Sea $\mu : 2^* \to [0, 1]$ una medida definida para los cilindros abiertos básicos de la forma $[\sigma]$ con $\sigma \in 2^*$. Tenerla definida sobre estos cilindros en el espacio de Cantor es equivalente a que esté definida sobre el álgebra de conjuntos clopen de este espacio (ya que $C \subseteq 2^\omega$ es clopen si y solo si $C = [F]^\prec$ para un conjunto finito $F \subseteq 2^*$ [13, Proposition 1.8.6]).

A su vez, se puede ver que se cumplen las hipótesis del teorema de Carathéodory, cuya aplicación dice que entonces existe μ', una extensión de la medida μ definida sobre la σ-álgebra generada por los conjuntos clopen del espacio de Cantor. Esto implica que μ' está definida sobre los conjuntos de Borel del espacio de Cantor, ya que justamente estos forman la σ-álgebra más chica que contiene a todos los conjuntos clopen [13, Pág. 70]. Por último, esta medida se puede extender a los conjuntos de Borel en $[0, 1]$ debido a que, desde el punto de vista de la teoría de la medida, 2^ω es isomorfo a $[0, 1]$. □

3. Propiedades extendidas

En esta sección se presentan y analizan algunas propiedades de las martingalas que jugarán un papel importante en el desarrollo de resultados subsiguientes.

3.1. Equivalencia entre martingalas reales y racionales

A continuación se enuncia de manera formal esta equivalencia y también se da una prueba. Si bien la demostración que se presenta es esencialmente una generalización a base k de la prueba de Terwijn [20], se incluye porque es didáctica y ayuda a presentar un panorama más completo del tema.

Lema 3.1. *Para cada martingala computable real L en base k hay una martingala M computable racional en base k que tiene éxito en todas las secuencias en las que L tiene éxito. Más aún, si L es polinomial entonces M también.*

Demostración. La demostración tiene dos partes. Primero se construye una supermartingala S racional computable que tiene éxito en por lo menos las mismas secuencias que L. Luego se transforma S en una martingala M que también es computable y tiene éxito en como mínimo las mismas secuencias que S (y por lo tanto en las mismas secuencias que L).

Primero, por la definición de función real computable, existe $\tilde{L} : k^* \times \mathbb{N} \to \mathbb{Q}^+$, una aproximación de L:

$$\forall q \in \mathbb{N} \quad \forall \sigma \in k^*(|L(\sigma) - \tilde{L}(\sigma, q)| \leq 2^{-q}).$$

Sea $\mathcal{A}$ el conjunto de secuencias sobre las que L tiene éxito. Luego, la supermartinagala S que tiene éxito en cada $Z \in \mathcal{A}$ se define de la siguiente forma:

$$S(\sigma) = \tilde{L}(\sigma, |\sigma|) + 4 \cdot 2^{-|\sigma|}.$$

De esta forma, $L(\sigma) + 3 \cdot 2^{-|\sigma|} \leq S \leq L(\sigma) + 5 \cdot 2^{-|\sigma|}$. Además,

$$\begin{aligned}
\sum_{i=0}^{k-1} S(\sigma i) &\leq \sum_{i=0}^{k-1} (L(\sigma i) + 5 \cdot 2^{-|\sigma i|}) \\
&\leq k(L(\sigma) + 5/2 \cdot 2^{-|\sigma|}) \\
&\leq k(L(\sigma) + 3 \cdot 2^{-|\sigma|}) \\
&\leq kS(\sigma),
\end{aligned}$$

con lo cual S es una supermartingala. Como $S(\sigma) \geq L(\sigma)$, para cada $Z \in \mathcal{A}$, al igual que L, S también tiene éxito en Z.

Segundo, se transforma la supermartingala S en una martingala M. Para esto simplemente se define (inductivamente) $M(\emptyset) = S(\emptyset)$ y

$$\begin{aligned}
M(\sigma i) &= S(\sigma i) \quad \text{para } 1 \leq i \leq k-1 \\
M(\sigma 0) &= kM(\sigma) - \sum_{i=1}^{k-1} M(\sigma i).
\end{aligned}$$

Claramente M es una martingala, además tiene éxito en por lo menos todas las secuencias en las cuales lo tenía S, debido a que para todo σ, $M(\sigma) \geq S(\sigma)$ (esto es sencillo de probar por inducción en $|\sigma|$ usando la condición de equidad que cumple S por ser supermartingala).

Con lo cual M tiene éxito en todas las secuencias de $\mathcal{A}$. Observar también que por la forma en que se construyen, S y M son claramente computables.

Por último, si además L es polinomial, claramente S también. Por otro lado se puede ver que calcular $M(\sigma)$ requiere a lo sumo $O(|\sigma|)$ evaluaciones de S, con lo cual la martingala racional M también es polinomial.

□

3.2. Martingalas con la *savings property*

Una de las dificultades que se presentan al estudiar las nociones de aleatoriedad basadas en martingalas es que las mismas engloban a un conjunto de funciones posibles muy grande y variado. Las escasez de restricciones que existe (por definición) en el comportamiento de las martingalas, agrega complejidad a los intentos de analizar sus propiedades o de utilizar argumentos constructivos. Por esta razón es que son de mucha utilidad aquellas propiedades que permiten identificar clases de equivalencia en el conjunto de las martingalas posibles.

Cuando se estudian las martingalas con especial interés en el conjunto de secuencias sobre el cual tienen éxito, hay una propiedad que resulta especialmente útil y se define a continuación.

Definición 3.2. Decimos que una martingala M en base k tiene la *savings property* si

$$M(\sigma\tau) \geq M(\sigma) - k^2 \tag{3.2.1}$$

para cada cadena σ, $\tau \in k^*$.

Si bien es una propiedad conocida (con una ligera modificación en la desigualdad 3.2.1) para base 2 (se puede ver en [3, Definition 4.3], de dónde tomamos prestado el nombre), su generalización a cualquier base no fue trivial debido a que la versión para cadenas binarias usa algunas propiedades únicas de esa base. Por este motivo, aunque tomamos el mismo nombre y la esencia de la propiedad es la misma, la cota aquí enunciada es ligeramente distinta, por lo que no se trata estrictamente de una generalización. Intuitivamente, lo que la *savings property* dice sobre una martingala es que el capital que la misma puede ir ganando a lo largo de una secuencia no puede crecer demasiado rápido ni caer significativamente una vez que ha crecido. Esta propiedad será de gran utilidad más adelante, ya que el siguiente lema permitirá que ciertos razonamientos sobre estrategias de apuestas se puedan reducir a la clase de martingalas que cumplen la *savings property*.

Lema 3.3. *Para cada martingala computable L en base k hay una martingala computable M en base k con la savings property que tiene éxito en las mismas secuencias que L.*

La siguiente prueba se basa en la demostración de [3, Proposition 4.4], que prueba algo muy parecido para la base $k = 2$, y aquí se la generaliza para una base k arbitraria. Si bien la idea central es parecida, algunos argumentos de [3, Proposition 4.4] sólo funcionan para base 2, con lo cual nuestra generalización a cualquier base requiere algunas modificaciones.

Demostración. El objetivo es construir una nueva martingala en la cual la velocidad de crecimiento está limitada, pero al mismo tiempo las pérdidas están acotadas. Informalmente, y retomando la idea intuitiva de las estrategias de apuestas, lo que se hace es construir una martingala M con dos partes: un pozo de ahorro que acumula capital y que nunca se apuesta (que se llamará G), y una caja para apuestas (denominada E) que es la que se usa para

apostar, pero con un límite sobre su capital de manera que cuando el mismo supera el valor fijado de antemano, transfiere la mayor parte de su valor al pozo de ahorro G. El resultado de hacer esto es que la nueva martingala M sigue siendo exitosa en la mismas secuencias que L, aunque quizás a una velocidad que puede llegar a ser muchísimo menor que la original. Por otro lado, se verá más adelante que las pérdidas que puede llegar a sufrir M son muy acotadas. A continuación se desarrolla esta misma idea de manera formal.

Se puede asumir sin pérdida de generalidad que $L(\sigma) > 0$ para $\sigma \in k^*$ y que $L(\emptyset) < 1$.

Se define $M(\sigma) = G(\sigma) + E(\sigma)$ donde para todo $a \in k$

$$E(\emptyset) = L(\emptyset) \quad \text{y} \quad E(\sigma a) = \begin{cases} \dfrac{L(\sigma a)}{L(\sigma)} E(\sigma)^{\frac{1}{k}}, & \text{si } E(\sigma) > k \\ \\ \dfrac{L(\sigma a)}{L(\sigma)} E(\sigma), & \text{sino} \end{cases}$$

$$G(\emptyset) = 0 \quad \text{y} \quad G(\sigma a) = \begin{cases} G(\sigma) + E(\sigma)^{\frac{k-1}{k}}, & \text{si } E(\sigma) > k \\ \\ G(\sigma), & \text{sino} \end{cases}$$

Observación 3.3.1. *G no decrece: si $\sigma \preceq \tau$ entonces $G(\sigma) \leq G(\tau)$.*

Demostración. Esto se puede formalizar con una simple prueba inductiva, ya que por la definición recursiva de G, es claro que $G(\sigma a)$ es igual a $G(\sigma)$ en un caso, o que es mayor en el otro, ya que $E(\sigma)$ es positivo y $\frac{k-1}{k}$ también (recordar además que $G(\emptyset) = 0$). □

Observación 3.3.2. *Para cualquier cadena σ, $0 \leq E(\sigma) \leq k^2$*

Demostración. $E(\sigma) \geq 0$ ya que se supone eso mismo de $L(\sigma)$ y luego E se define como multiplicación de términos no negativos. Se puede ver entonces que $E(\sigma) \leq k^2$ por inducción en la longitud de σ:

- Caso base $\sigma = \emptyset$: Por definición $E(\emptyset) = L(\emptyset)$, valor que se asume positivo y menor a 1.
- Paso inductivo para $E(\sigma a)$: Se supone por HI que $0 \leq E(\sigma) \leq k^2$. Notar además que $\frac{L(\sigma a)}{L(\sigma)} \leq k$ porque L es una martingala.
  - Si $E(\sigma) > k$, $E(\sigma a) = \frac{L(\sigma a)}{L(\sigma)} E(\sigma)^{\frac{1}{k}} \leq k \cdot k^2 \cdot \frac{1}{k} = k^2$
  - Si $E(\sigma) \leq k$, $E(\sigma a) = \frac{L(\sigma a)}{L(\sigma)} E(\sigma) \leq k \cdot k = k^2$

Esto concluye la demostración de la Observación 3.3.2. □

A continuación se verifica que la construcción M es efectivamente una martingala computable en base k con la *savings property* y que tiene éxito en las mismas secuencias que L.

- ***M* es una martingala en base *k*:**

  Por definición, se tiene:

$$\sum_{i=0}^{k-1} M(\sigma i) = \sum_{i=0}^{k-1} G(\sigma i) + E(\sigma i) \tag{3.3.1}$$

  Por la forma partida en que están definidas E y G lo más fácil es analizar en dos casos:

- Si $E(\sigma) > k$ entonces, tomando (3.3.1) y expandiendo las definiciones de G y E:

$$\begin{aligned}
\sum_{i=0}^{k-1} M(\sigma i) &= \sum_{i=0}^{k-1}(G(\sigma) + E(\sigma)\frac{k-1}{k}) + \frac{L(\sigma i)}{L(\sigma)}E(\sigma)\frac{1}{k} \\
&= k(G(\sigma) + E(\sigma)\frac{k-1}{k}) + E(\sigma)\frac{1}{k}\frac{\sum_{i=0}^{k-1} L(\sigma i)}{L(\sigma)} \\
&= kG(\sigma) + E(\sigma)(k-1+\frac{1}{k}\frac{kL(\sigma)}{L(\sigma)} \\
&= kG(\sigma) + E(\sigma)(k-1+1) \\
&= kM(\sigma)
\end{aligned}$$

- Sino

$$\begin{aligned}
\sum_{i=0}^{k-1} M(\sigma i) &= \sum_{i=0}^{k-1} G(\sigma) + \frac{L(\sigma i)}{L(\sigma)}E(\sigma) \\
&= kG(\sigma) + E(\sigma)\frac{\sum_{i=0}^{k-1} L(\sigma i)}{L(\sigma)} \\
&= kG(\sigma) + E(\sigma)\frac{kL(\sigma)}{L(\sigma)} \\
&= k(G(\sigma) + E(\sigma)) \\
&= kM(\sigma)
\end{aligned}$$

- ***M* es computable:** La definición de $M(\sigma)$ es claramente computable conociendo $L(\sigma)$ porque realiza operaciones básicas como suma, resta, división y recursión primitiva.

- ***M* tiene éxito en las mismas secuencias que *L*:** Veamos que si L tiene éxito en una secuencia entonces M también, y que si L no tiene éxito en una secuencia, M tampoco.

  Sea $S \in k^\omega$ tal que L tiene éxito en S, es decir, $L(S\restriction_n)$ no está acotada.

  Si $\limsup_n L(S\restriction_n) = \infty$ se da que $\limsup_n G(S\restriction_n) = \infty$. Esto se debe a que infinitas veces $E(\sigma) > k$. Esto último vale ya que de no ser así, a partir de cierto q_0, $E(S\restriction_q) \leq k$ para todo $q \geq q_0$, entonces $E(S\restriction_n)$ se comportaría casi igual que $L(S\restriction_n)$ (ya que iría usando siempre $\frac{L(\sigma i)}{L(\sigma)}$), es decir que $E(S\restriction_n)$ es equivalente a $L(S\restriction_n)$ multiplicada por una constante fija, y como $L(S\restriction_n)$ no está acotada, entonces $E(S\restriction_n)$ no podría estarlo, lo cual es absurdo ya que supusimos que solo finitas veces $E(\sigma) > k$. Y cada vez que $E(\sigma) > k$, G aumenta en al menos $k-1$. Como, por Observación 3.3.1, G no decrece en los prefijos de S, entonces $\lim_n G(S\restriction_n) = \infty$.

  Un razonamiento similar se puede hacer al revés, si $\limsup_n M(S\restriction_n) = \infty$, por la Observación 3.3.2 (de que E nunca es mayor a k^2) debe darse que $\limsup_n G(S\restriction_n) = \infty$. Pero eso significa que existen infinitos n tales que $E(S\restriction_n) > k$. Como $E(\sigma)$ es en realidad de la forma $L(\sigma)\frac{1}{k^m}$ (donde m es la cantidad de veces que, para un prefijo $\tau \preceq \sigma$, $E(\tau) > k$), para cualquier m existe al menos un n tal que $E(S\restriction_n) = L(S\restriction_n)\frac{1}{k^m} > k$, lo que implica que $L(S\restriction_n) > k^{m+1}$ y por lo tanto podemos concluir que $L(S\restriction_n)$ no está acotada, es decir, que L tiene éxito en S.

- ***M* cumple la *savings property* en base *k*:** Notar que $E(\sigma) \geq E(\tau) - k^2$ para cualquier σ y τ (ya que para cualquier cadena σ vale $0 \leq E(\sigma) \leq k^2$ por la Observación 3.3.2). Recordar también que $G(\sigma\tau) \geq G(\sigma)$ (Observación 3.3.1). Entonces:

$$M(\sigma\tau) = E(\sigma\tau) + G(\sigma\tau) \quad \geq \quad E(\sigma) - k^2 + G(\sigma) = M(\sigma) - k^2$$

Esto concluye la prueba del Lema 3.3.

□

Lema 3.4. *Si M es una martingala en base k que cumple la savings property, para cualquier cadena $\sigma \in k^*$ vale*

$$M(\sigma) \leq k^3|\sigma| + M(\emptyset).$$

Demostración. Se puede ver por inducción en la longitud de σ. Es trivial que la cota vale para el caso base $\sigma = \emptyset$.

Si $\sigma = \tau a$, por HI $M(\tau) \leq k^3|\tau| + M(\emptyset)$. Por la definición de martingala, usando luego la *savings property* y finalmente la HI:

$$\begin{aligned} M(\tau a) &= kM(\tau) - \sum_{i=0, i\neq a}^{k-1} M(\tau i) \\ &\leq kM(\tau) - (k-1)(M(\tau) - k^2) \\ &= M(\tau) + k^3 - k^2 \\ &\leq M(\tau) + k^3 \\ &\leq k^3(|\tau a|) + M(\emptyset) \end{aligned}$$

□

Lema 3.5. *Para cada martingala polinomial real L en base k hay una martingala real M en base k con la savings property que tiene éxito en por lo menos las mismas secuencias que L y que también es polinomial.*

Demostración. Esta demostración es mucho más sencilla si se trabaja con martingalas racionales, es por eso que aplicando el Lema 3.1, se supondrá que L es una martingala racional polinomial (ya que de no serlo, por el lema existe una equivalente que sí lo es).

No se entrará en los detalles del cálculo de la complejidad, pero informalmente, se puede ver que la martingala M construida en la demostración del Lema 3.3 requiere $O(|\sigma|)$ evaluaciones de la martingala original para computar $M(\sigma)$, y $O(|\sigma|)$ operaciones aritméticas de costo polinomial, con lo cual la nueva martingala es también polinomial (si bien de un grado mayor).

Finalmente, observar que M es de hecho racional, sin embargo eso no es un problema, ya que toda martingala racional polinomial es trivialmente una martingala real polinomial. □

4. Aleatoriedad computable es invariante por cambio de base

En esta sección desarrollamos una demostración constructiva de que la aleatoriedad computable es invariante por cambio de base. Alcanza con probar que si una secuencia no es computablemente aleatoria en una base entonces no lo es en ninguna otra. Es decir, que si una martingala computable M tiene éxito en un número real x representado en una base k, que existe otra martingala computable N en base r que tiene éxito en x representado en base r.

Teorema 4.1. *Sea $Z \in k^\omega$ tal que existe una martingala computable M en base k que tiene éxito en Z. Sea Y la expansión en base r de $0.Z$. Entonces existe una martingala N computable en base r que también tiene éxito en Y.*

Demostración. Podemos suponer sin pérdida de generalidad que $r \neq k$ y que M cumple la *savings property* en base k.

Por otro lado, si $0.Z \in \mathbb{Q}$ entonces $0.Z$ no es computablemente aleatorio en ninguna base, en particular en r y por lo tanto tiene que existir N. Luego, podemos suponer que $0.Z$ es irracional.

Como se mencionó ya en los preliminares sobre notación, a continuación se usará mucho una forma abreviada para ciertos intervalos de números reales:

$$[\sigma]_r := [0.\sigma, 0.\sigma + r^{-|\sigma|}) \quad \text{para } \sigma \in r^*$$

Este tipo de intervalo es justamente el conjunto de números reales representados por cada una de las posibles secuencias infinitas que extienden a una cadena particular en un alfabeto determinado (en este caso la base r). De hecho, una definición equivalente es:

$$[\sigma]_r := \{0.\sigma X \mid X \in r^\omega\} \text{ para } \sigma \in r^*.$$

Sea $\mu'_M : \{[\tau] : \tau \in k^*\} \to \mathbb{R}_0^+$ la siguiente medida

$$\mu'_M[\tau] = M(\tau)k^{-|\tau|} \quad \text{para } \tau \in k^*$$

Aplicando el teorema de Carathéodory (Proposición 2.16) es posible extender μ'_M a los conjuntos de Borel en $[0, 1]$. Es a esta nueva medida, definida sobre $[0, 1]$, a la que llamamos μ_M. Como μ_M es una extensión de μ'_M, en particular tenemos

$$\mu_M[\tau]_k = \mu_M[0.\tau, 0.\tau + k^{-|\tau|}) = M(\tau)k^{-|\tau|} \quad \text{para } \tau \in k^*.$$

Finalmente definimos

$$N(\sigma) = r^{|\sigma|}\mu_M[\sigma]_r = r^{|\sigma|}\mu_M[0.\sigma, 0.\sigma + r^{-|\sigma|}) \quad \text{para } \sigma \in r^* \tag{4.1.1}$$

Notar que esta manera de definir a μ_M no da una forma inmediata de computar esta medida para intervalos que no sean de la forma $[\tau]_r$, sin embargo, como se verá más adelante nada impide usar la σ-aditividad de la misma para calcular la medida de otro tipo de conjuntos.

- ***N* satisface la condición de martingala en base *r*:**

$$\begin{aligned}\sum_{i=0}^{r-1} N(\sigma i) &= \sum_{i=0}^{r-1} r^{|\sigma i|}\mu_M[0.\sigma i, 0.\sigma i + r^{-|\sigma i|}) \\ &= \sum_{i=0}^{r-1} r^{|\sigma|+1}\mu_M[\sigma i]_r \\ &= r^{|\sigma|} r \sum_{i=0}^{r-1} \mu_M[\sigma i]_r \\ &= r^{|\sigma|} r \mu_M[\sigma]_r \\ &= rN(\sigma)\end{aligned}$$

(usando que $\bigcup_{i=0}^{r-1}[\sigma i]_r = [\sigma]_r$ y la aditividad de la medida μ_M)

- ***N* también tiene éxito en *Y*:**

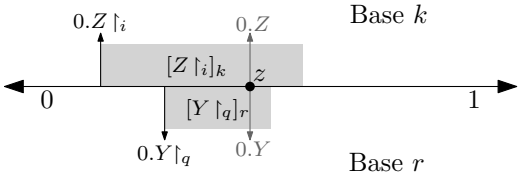
Sea $m \in \mathbb{N}$ dado, a continuación se ve que existe $q \in \mathbb{N}$ tal que $N(Y\restriction_q) \geq m$ (es decir, que N no está acotada sobre Y).

Como M no está acotada para Z, existe $i \in \mathbb{N}$ tal que $M(Z\restriction_i) > m + k^2$. Debido a que además tiene la *savings property* en base k, vale que

$$\forall \tau \in k^* \;\; M(Z\restriction_i \tau) \geq M(Z\restriction_i) - k^2 > m + k^2 - k^2 = m. \tag{4.1.2}$$

También, como $0.Z$ es irracional, tiene que existir $q \in \mathbb{N}$ suficientemente grande tal que:

$$[Y\restriction_q]_r \subset [Z\restriction_i]_k$$



Usando ese q, podemos ver que $N(Y\restriction_q) \geq m$:

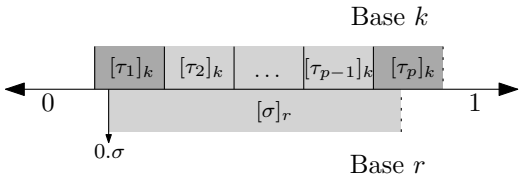
$$\begin{aligned}N(Y\restriction_q) &= r^{|Y\restriction_q|} \cdot \mu_M[Y\restriction_q]_r \\ &= r^q \cdot \lim_{n\to\infty} \sum_{\tau \in A_n^q} \mu_M[\tau]_k && (4.1.3) \\ &= r^q \cdot \lim_{n\to\infty} \sum_{\tau \in A_n^q} M(\tau) k^{-|\tau|} && (4.1.4) \\ &\geq r^q \cdot \lim_{n\to\infty} \sum_{\tau \in A_n^q} m\, k^{-|\tau|} && (4.1.5) \\ &= r^q \cdot m \cdot \lim_{n\to\infty} \sum_{\tau \in A_n^q} k^{-|\tau|} \\ &= r^q \cdot m \cdot r^{-q} = m && (4.1.6)\end{aligned}$$

Donde $A_n^q = \{\tau \in k^* \text{ tales que } |\tau| = n \text{ y } [\tau]_k \subseteq [Y\restriction_q]_r \}$

La igualdad de (4.1.3) usa que μ_M es una medida, lo que permite dividir un intervalo en subintervalos disjuntos y sumar la medida de cada uno de ellos para computar la del intervalo original (gracias a la σ-aditividad). La igualdad de (4.1.4) vale por definición de μ_M. La desigualdad (4.1.5) está garantizada por construcción, ya que $[\tau]_k \subseteq [Y\restriction_q]_r \subset [Z\restriction_i]_k$, con lo cual $\tau \preceq Z\restriction_i$ y por lo tanto vale $M(\tau) > m$ por (4.1.2). Por último, (4.1.6) es verdadero por propiedades elementales de la medida, ya que la sumatoria resultante es equivalente a una aproximación de la medida de Lebesgue en el intervalo $[Y\restriction_q]_r$.

- ***N* es computable:** Al estar N definida como $r^{|\sigma|}\mu_M[\sigma]_r$, alcanza con ver que $\mu_M[\sigma]_r$ es computable. La medida μ_M está definida para cadenas en base k a partir de M, que es computable por hipótesis, lo que la hace computable para esas cadenas. Lo que falta es dar una forma efectiva de computar μ_M para las cadenas en base r, que son las que aparecen en la definición N.

  Lo que se hará es aproximar $\mu_M[\sigma]_r$ subdividiendo y aproximando el intervalo $[\sigma]_r$ con intervalos más pequeños de la forma $[\tau]_k$, para los cuales es posible computar μ_M sin ningún problema (como se trata de una medida, se puede partir el intervalo en subconjuntos disjuntos y sumar luego las medidas de cada uno de estos subintervalos). Entonces, para computar $\mu_M[\sigma]_r$ se aproxima $[\sigma]_r$ con todos los intervalos de la forma $[\tau_i]_k$ de una misma longitud m determinada y que tengan intersección no vacía con $[\sigma]_r$. Si nombramos estos intervalos en orden como $[\tau_1]_k, [\tau_2]_k, \ldots, [\tau_p]_k$, la diferencia entre $[\sigma]_r$ y la unión de todos estos intervalos puede residir únicamente en $[\tau_1]_k$ y $[\tau_p]_k$. Por este motivo, el error que se comete al aproximar μ_M en el intervalo original con la suma de la medida en los $[\tau_i]_k$ es a lo sumo $\mu_M[\tau_1]_k + \mu_M[\tau_p]_k$. Por lo tanto, el error cometido se puede acotar con la elección del tamaño de estos intervalos (cuanto más pequeños, menor el error).



Como μ_M es computable para cadenas en base k existe $\tilde{\mu}_M^k(\tau, q) : k^* \times \mathbb{N} \to \mathbb{Q}$, la función que aproxima $\mu_M[\tau]$ con error menor a 2^{-q}.

A continuación se detalla cómo construir $\tilde{\mu}_M^r(\sigma, q) : r^* \times \mathbb{N} \to \mathbb{Q}^+$. Por simplicidad, usaremos equivalentemente una aproximación de μ_M que recibe un racional positivo ϵ en lugar de un número natural q. Es decir usaremos la función $\tilde{\mu}_M^r(\sigma, \epsilon) : r^* \times \mathbb{Q}^+ \to \mathbb{Q}$ tal que

$$\forall \sigma \in \Sigma^* \text{ y } \epsilon \in \mathbb{Q}^+, \quad |\tilde{f}(\sigma, \epsilon) - f(\sigma)| < \epsilon. \tag{4.1.7}$$

Dado σ y ϵ, lo primero que se hace es elegir la longitud de los τ_i de forma tal que $\mu_M[\tau_i]_k < \frac{\epsilon}{3}$. Como M cumple la *savings property* se puede usar el Lema 3.4.

Si $m = |\tau_i|$, para casi todo m,

$$\mu_M[\tau_i]_k = M(\tau_i)k^{-m} \leq (k^3 m + M(\emptyset))k^{-m} \leq k^{\frac{1}{2}m}k^{-m} = k^{-\frac{1}{2}m} \tag{4.1.8}$$

(usando que $k^3 m + M(\emptyset) \leq k^{\frac{1}{2}m}$).

Usando la desigualdad, es fácil computar un m tal que $\mu_M[\tau_i]_k < \frac{\epsilon}{3}$.

La elección de m determina a su vez los p intervalos $[\tau_1]_k, [\tau_2]_k, \ldots, [\tau_p]_k$ que cubren $[\sigma]_r$ y que se usan para aproximar. Por construcción:

$$|\sum_{i=1}^{p} \mu_M[\tau_i]_k - \mu_M[\sigma]_r| \leq \mu_M[\tau_1]_k + \mu_M[\tau_p]_k \leq \frac{2\epsilon}{3} \tag{4.1.9}$$

Luego, para aproximar $\mu_M[\tau_i]_k$ se usa $\tilde{\mu}_M^k(\tau, \epsilon)$, y para que la suma de los errores en estas aproximaciones no supere $\frac{\epsilon}{3}$, se computa $\tilde{\mu}_M^k(\tau_i, \frac{\epsilon}{3p})$ para cada τ_i, resultando así:

$$|\sum_{i=1}^{p} \mu_M[\tau_i]_k - \sum_{i=1}^{p} \tilde{\mu}_M^k(\tau_i, \frac{\epsilon}{3p})| \leq \sum_{i=1}^{p} |\mu_M[\tau_i]_k - \tilde{\mu}_M^k(\tau_i, \frac{\epsilon}{3p})| \leq \sum_{i=1}^{p} \frac{\epsilon}{3p} = \frac{\epsilon}{3} \tag{4.1.10}$$

Entonces, para $\sigma \in r^*$ se define

$$\tilde{\mu}_M^r(\sigma, \epsilon) := \sum_{i=1}^{p} \tilde{\mu}_M^k(\tau_i, \frac{\epsilon}{3p}), \tag{4.1.11}$$

donde p y los τ_i están determinados por la elección previa de m (longitud de los τ_i) como se describió anteriormente.

Finalmente, comprobamos que el error de esta aproximación se mantiene dentro de los márgenes deseados.

Abriendo los módulos de (4.1.9) y (4.1.10) se obtiene

$$-\frac{2\epsilon}{3} \leq \mu_M[\sigma]_r - \sum_{i=1}^{p} \mu_M[\tau_i]_k \leq \frac{2\epsilon}{3} \quad \text{y}$$

$$-\frac{\epsilon}{3} \leq \sum_{i=1}^{p} \mu_M[\tau_i]_k - \sum_{i=1}^{p} \tilde{\mu}_M^k(\tau_i, \frac{\epsilon}{3p}) \leq \frac{\epsilon}{3}.$$

Sumando las dos ecuaciones anteriores

$$-\epsilon \leq \mu_M[\sigma]_r - \sum_{i=1}^{p} \tilde{\mu}_M^k(\tau_i, \frac{\epsilon}{3p}) \leq \epsilon$$

y finalmente por la definición de $\tilde{\mu}_M^r$ en (4.1.11) se llega a que

$$|\mu_M[\sigma]_r - \tilde{\mu}_M^r(\sigma, \epsilon)| \leq \epsilon.$$

Esto concluye la demostración del Teorema 4.1. □

5. Aleatoriedad polinomial es invariante por cambio de base

La invariancia por cambio de base de la aleatoriedad computable quizás no es un resultado demasiado sorprendente, es algo que incluso puede resultar intuitivo. Sin embargo, se vuelve mucho más difícil responder este tipo de preguntas cuando se trabaja con nociones de aleatoriedad con recursos limitados. Notar que, como se mencionó en la introducción, esta dificultad no es exclusiva de la aleatoriedad computable, ya que existen preguntas semejantes y abiertas para la mayoría de las nociones de aleatoriedad.

Esta sección se ocupa de estudiar qué ocurre con la invariancia por cambio de base cuando se introducen restricciones en la complejidad temporal determinista de las martingalas. En particular, se pone el foco en la aleatoriedad polinomial (definida mediante martingalas polinomiales).

5.1. Martingalas polinomiales

Uno de los principales aportes de la sección anterior es una demostración constructiva y sencilla de la propiedad de invariancia por cambio de base en la aleatoriedad computable. Gracias a esto, las construcciones de esa demostración pueden ser aprovechadas y modificadas para probar otros resultados, como veremos a continuación.

Teorema 5.1. *Sea $Z \in k^\omega$ tal que existe una martingala real polinomial M en base k que tiene éxito en Z. Sea Y la expansión en base r de $0.Z$. Entonces existe una martingala real polinomial N en base r que tiene éxito en Y.*

Demostración. Se toma como base la demostración del Teorema 4.1, y la idea es probar que la martingala N propuesta y definida en (4.1.1) como $r^{|\sigma|}\mu_M[\sigma]_r$, es computable en tiempo polinomial.

En la demostración de que N es computable se definió $\tilde{\mu}^r_M(\sigma, q)$, una función computable que aproxima $\mu_M[\sigma]_r$ con error menor a 2^{-q}. Probando primero que $\tilde{\mu}^r_M$ es computable en tiempo polinomial en función de $|\sigma|$ y q, es luego trivial ver que N también lo es. Con el objetivo de probar lo primero, a continuación se analizan las distintas partes de la construcción de N y sus complejidades temporales.

- **Computar $\boldsymbol{\mu_M[\tau]_k}$**

  La construcción de N propuesta se basa en que computar μ_M para cadenas en base k es, por definición, casi inmediato conociendo a la martingala M. Es fundamental ver entonces que esto se puede seguir haciendo en tiempo polinomial.

  Por hipótesis, M es computable en tiempo polinomial, es decir, existe su aproximación $\tilde{M}(\tau, q) : k^* \times \mathbb{N} \to \mathbb{Q}$ tal que

  $$\forall \tau \in k^* \quad |\tilde{M}(\tau, q) - M(\tau)| < 2^{-q}$$

  y $\tilde{M}$ es computable en tiempo polinomial en función de $|\tau|$ y q.

  Es importante destacar que una de las hipótesis en el Teorema 4.1 es que M tiene la *savings property*. Es gracias al Lema 3.5 que se puede suponer que esta hipótesis sigue valiendo cuando M es una función real polinomial.

  Usando $\tilde{M}$ se puede computar una aproximación de $\mu_M[\tau]_k$ (recordar que estaba definida como $M(\tau)k^{-|\tau|}$) que también sea computable en tiempo polinomial y que llamaremos

$\tilde{\mu}_M^k$:

$$\tilde{\mu}_M^k(\tau, q) := \tilde{M}(\tau, q)k^{-|\tau|}$$

Calcular $k^{-|\tau|}$ y multiplicarlo por el resultado de $\tilde{M}$ tiene costo polinomial. Como $\tilde{M}$ ya tenía complejidad temporal polinomial, $\tilde{\mu}_M^k$ es computable en tiempo polinomial en función de $|\tau|$ y q.

Notar que $|\tilde{\mu}_M^k(\tau, q) - \mu_M(\tau)| < 2^{-q}$ (de hecho, el error absoluto es mucho menor, ya que $k^{-|\tau|}$ es un número muy chico que disminuye el error arrastrado de $\tilde{M}$).

- **Determinar el tamaño de los τ_i**

  Recordar que para aproximar el intervalo $[\sigma]_r$ (en la construcción de $\tilde{\mu}_M^r$) se usan intervalos de la forma $[\tau_i]_k$, donde los τ_i tienen una longitud m que garantiza una cota sobre el error cometido al usar esta aproximación. Dado el error que se desea cometer 2^{-q}, se puede calcular un tamaño mínimo de m usando (4.1.8) y despejando $k^{-\frac{1}{2}m} \leq 2^{-q-1}$, con lo cual surge que con m mayor o igual a $2q+3$, el error cometido en la aproximación será a lo sumo 2^{-q}. Dado q, está claro que calcular m es un cómputo $O(|q|)$ (la suma es lineal en la longitud de la entrada).

- **Computar τ_1 y τ_p**

  Una vez determinado el tamaño de los τ_i, un buen punto de partida para aproximar μ_M en $[\tau_1]_k, \ldots, [\tau_p]_k$ es determinar primero qué cadenas son τ_1 y τ_p. Si bien no es estrictamente necesario, contribuye a la claridad del algoritmo que se propondrá más adelante para calcular $\tilde{\mu}_M^r$.

  Entonces, dado σ y con m ya calculado en función de q, τ_1 es la mayor cadena de longitud m tal que $0.\tau_1 < 0.\sigma$. La misma se puede encontrar con este sencillo procedimiento:

```
τ1 = ∅
Mientras |τ1| < m
   i = 1
   Mientras i < k y 0.τ1 i ≤ 0.σ
        i++
   τ1 ← τ1(i-1)
```

  De forma análoga se puede computar τ_p.

  Analizando la complejidad de este algoritmo se puede observar que el bucle exterior itera m veces y que el bucle interior itera a lo sumo k veces (y k es una de las bases, un número fijo). A su vez, las operaciones dentro de los bucles no son más que una cantidad finita y fija de comparaciones y sumas. En consecuencia, y como m es $O(q)$, todo el algoritmo corre en tiempo polinomial en función de $|\sigma|$ y q.

- **Calcular $\tilde{\mu}_M^r$ eficientemente**

  Teniendo m, τ_1 y τ_p es muy fácil hacer un algoritmo que aproxima

$$\mu_M[0.\tau_1, 0.\tau_p + k^{-m}) \tag{5.1.1}$$

  (equivalente a $\sum_{i=1}^{p} \mu_M[\tau_i]_k$) usando y sumando $\tilde{\mu}_M^k[\tau_i]$ con $1 \leq i \leq p$ de la forma que se planteó al probar la computabilidad de N en (4.1.11). Sin embargo, como la longitud de

cada intervalo $[\tau_i]_k$ es k^{-m}, la cantidad de intervalos necesarios para cubrir un intervalo fijo (en este caso $[\sigma]_r$) crece exponencialmente en función de m (o q, equivalentemente).

Para solucionar esto, a continuación se propone una función recursiva que captura otra forma de computar (5.1.1) pero reduciendo la cantidad de veces que se usa la función μ_M. La idea consiste en aprovechar la naturaleza recursiva de las cadenas para cubrir el intervalo $[0.\tau_1, 0.\tau_p + k^{-m}]$ usando la menor cantidad posible de intervalos de la forma $[\tau]_k$.

Dados $\rho, \upsilon \in k^*$ y $x, y \in k$, con $|\rho| = |\upsilon|$, se define

$$U(\rho x, \upsilon y) = \begin{cases} \displaystyle\sum_{x \leq i < y} \mu_M[\rho i]_k & \text{si } \rho = \upsilon \\ \displaystyle\sum_{x \leq i < k} \mu_M[\rho i]_k + U(\bar{\rho}, \upsilon) + \sum_{0 \leq j < y} \mu_M[\upsilon j]_k & \text{si } \rho \neq \upsilon \end{cases}$$

donde $\bar{\rho}$ es igual a $0.\rho + k^{|\rho|}$ interpretado como cadena (o equivalentemente, $\rho+1$ tomando ρ como un número en base k).

La función recursiva U tiene como argumentos dos cadenas ρx y υy, y calcula $\mu_M[0.\rho x, 0.\upsilon y]$. La idea es computar μ_M sobre intervalos tan grandes como sea posible, lo cual para intervalos de la forma $[\rho]_k$ se traduce en buscar cadenas ρ lo más cortas posibles. En definitiva, se trata de aprovechar que la unión de $[\rho 0]_k, [\rho 1]_k, \ldots, [\rho(k-1)]_k$ es $[\rho]_k$ y usar esto para reducir la cantidad de evaluaciones de μ_M.

En la Figura 5.1 se puede ver un ejemplo de la función U para cadenas en la base $k = 3$. Notar que en este ejemplo fueron necesarias 6 evaluaciones de μ_M, mientras que si se hubiera usado el algoritmo más sencillo inducido por la ecuación (4.1.11) (de sumar todos los intervalos de la forma $[\tau_i]_3$) habrían sido necesarias 18 evaluaciones.

Proposición 5.1.1. $U(\rho x, \upsilon y) = \mu_M[0.\rho x, 0.\upsilon y]$.

Demostración. Es sencillo demostrar esto por inducción en la longitud de ρx. En el caso base $\rho = \upsilon = \lambda$ ($|\rho x| = 1$), por definición

$$U(x, y) = \sum_{x \leq i < y} \mu_M[i]_k = \mu_M[0.x, 0.y]$$

Para el paso inductivo $|\rho x| \geq 2$. Si $\rho = \upsilon$ entonces

$$U(\rho x, \upsilon y) = \sum_{x \leq i < y} \mu_M[\rho i]_k = \mu_M[0.\rho x, 0.\rho y] = \mu_M[0.\rho x, 0.\upsilon y]$$

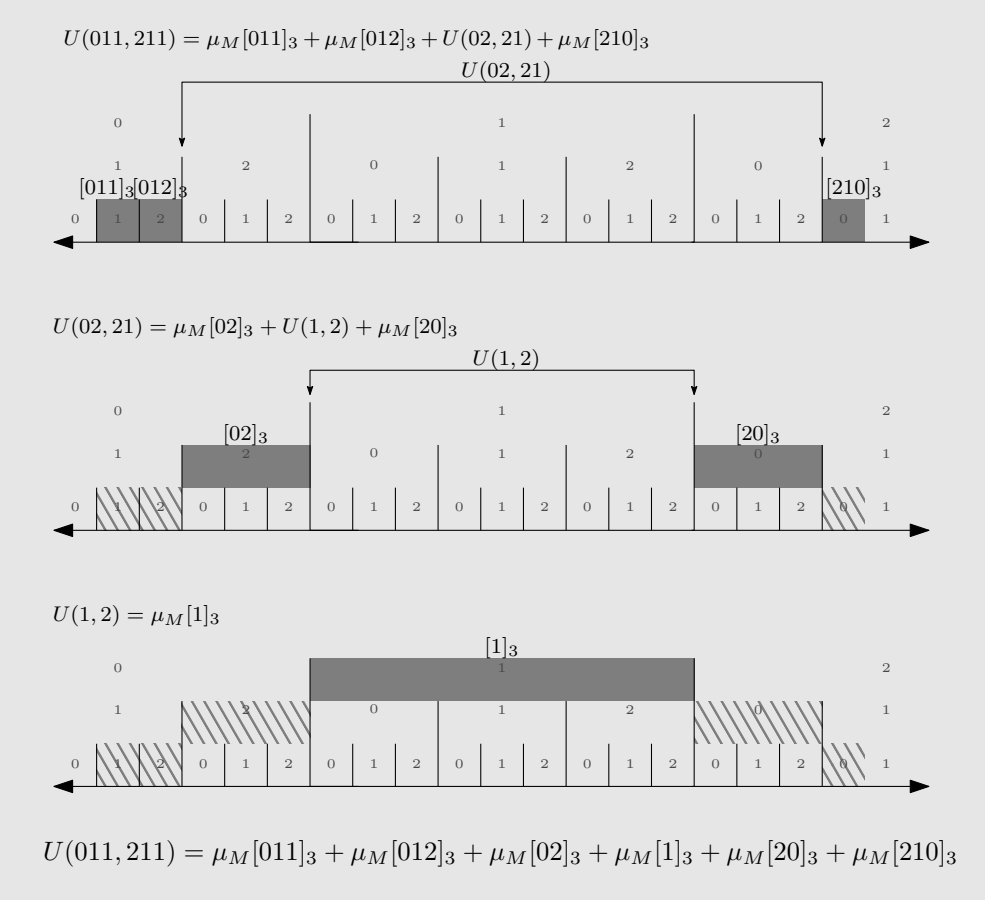
si en cambio $\rho \neq \upsilon$

$$\begin{aligned} U(\rho x, \upsilon y) &= \sum_{x \leq i < k} \mu_M[\rho i]_k + U(\bar{\rho}, \upsilon) + \sum_{0 \leq j < y} \mu_M[\upsilon j]_k \\ &= \mu_M[0.\rho x, 0.\rho + k^{-|\rho|}] + U(\bar{\rho}, \upsilon) + \mu_M[0.\upsilon, 0.\upsilon y] \end{aligned}$$

y como por H.I. $U(\bar{\rho}, \upsilon) = \mu_M[0.\rho + k^{-|\rho|}, 0.\upsilon]$, usando la aditividad de la medida μ_m llegamos a que $U(\rho x, \upsilon y)$ es igual a $\mu_M[0.\rho x, 0.\rho y]$.

□

Figura 5.1: Ejemplo en base 3 de $U(011, 211)$



Lo que nos da la función U es una forma inmediata de dividir al intervalo $[0.\tau_1, 0.\tau_p + k^{-m}]$ en subintervalos de la forma $[\sigma]_k$ sobre los cuales podemos aproximar μ_M usando $\tilde{\mu}_M^k$. Como la longitud de cada τ_i es m por construcción, $U(\tau_1, \tau_p + k^{-m})$ requiere menos de $2 \cdot k \cdot m$ evaluaciones de $\mu_M[\sigma]_k$.

Definimos $\tilde{U}(\tau_1, \tau_p, q)$ igual que U pero usando $\tilde{\mu}_M^k(\sigma, q')$ en lugar de μ_M para obtener una aproximación de U. Como cada $\tilde{\mu}_M^k$ introduce un error, hay que elegir q' de forma tal que la suma de los errores de los $\tilde{\mu}_M^k$ (que son a lo sumo $2 \cdot k \cdot m$) no supere 2^{-q}. Tomando $q' = q + \lceil \log_2(m \cdot k) \rceil + 1$ se garantiza que

$$|U(\tau_1, \tau_p) - \tilde{U}(\tau_1, \tau_p, \epsilon)| < 2^{-q}$$

Analicemos la complejidad de $\tilde{U}$. Realiza $O(m)$ sumas de las $O(m)$ evaluaciones de $\tilde{\mu}_M^k$. Estas evaluaciones son además para un q' fijo que es $O(q)$ y con cadenas de longitud menor o igual a m (que recordemos es también es $O(q)$). Por lo tanto, si $\tilde{\mu}_M^k$ es computable en tiempo polinomial, $\tilde{U}$ también.

Cuando combinamos estas tres cosas (determinar el tamaño m de los τ_i, encontrar a τ_1 y τ_p, y construir $\tilde{U}$), podemos definir:

$$\tilde{\mu}_M^r(\sigma, q) := \tilde{U}(\tau_1, \tau_p, q + 1)$$

con τ_1 y τ_p dados por los pasos detallados previamente con m calculado para un error menor a 2^{-q-1}.

En la ecuación anterior, el $q+1$ como parámetro de $\tilde{U}$ es necesario para contemplar también el error analítico por usar U. Recapitulando sobre los errores presentes en esta aproximación, recordar que aproximar $[\sigma]_r$ con los intervalos $[\tau_i]_k$ siempre conlleva un error, que se mantiene acotado con la elección de la longitud m de los τ_i. Pero a ese error, luego hay que sumarle el proveniente de usar la aproximación $\tilde{U}$ (en lugar de U). Justamente, al computar m y $\tilde{U}$ para error 2^{-q-1}, se puede asegurar que al sumar los errores, $\tilde{\mu}_M^r(\sigma, q)$ aproximará μ_M con el deseado error menor a 2^{-q}.

La complejidad temporal de $\tilde{\mu}_M^r(\sigma, \epsilon)$ es el resultado de sumar las complejidades de las tres partes de su construcción. Pero como ya se analizó, todas son polinomiales en $|\sigma|$ y la cota del error deseado q (y además, usar $q+1$ en lugar de q no afecta la complejidad asintótica). Con lo cual, claramente $\tilde{\mu}_M^r \in \mathbf{P}$.

- **Computar N a partir de $\tilde{\mu}_M^r$**

  Como N es $r^{|\sigma|}\mu_M[\sigma]_r$, computarlo a partir de $\tilde{\mu}_M^r$ consiste en sólo un par de operaciones aritméticas. Sin embargo, hay que tener en cuenta que el factor $r^{|\sigma|}$ amplifica el error contenido en $\tilde{\mu}_M^r$, por lo que si al aproximar N se desea un error total menor a 2^{-q}, $\tilde{\mu}_M^r(\sigma, q)$ debe ser calculado con un q que garantice que, aún con el error aumentando, el mismo se mantendrá dentro de las cotas deseadas. Por este motivo se define

  $$\tilde{N}(\sigma, q) := r^{|\sigma|}\tilde{\mu}_M^r(\sigma, q + C|\sigma|)$$

  donde se incrementa q en $C|\sigma|$ (donde C es la constante fija $\lceil \log_2(r) \rceil$ que sólo depende de la base r), lo cual es suficiente para garantizar el error deseado.

  Como $\tilde{\mu}_M^r$ ya es polinomial y se la está evaluando con un parámetro de error que, si bien modificado, sigue siendo $O(q)$, se puede afirmar que esa evaluación es polinomial en $|\sigma|$ y q. Además, calcular $r^{|\sigma|}$ y multiplicarlo por el resultado de $\tilde{\mu}_M^r$ también tiene costo polinomial. Luego, se puede concluir que la aproximación $\tilde{N}(\sigma, q)$ de $N(\sigma)$ es una función computable polinomial en función de $|\sigma|$ y q, es decir, $\tilde{N} \in \mathbf{P}$.

Esto prueba que la martingala N propuesta en la demostración del Teorema 4.1 es una función real computable en tiempo polinomial, lo cual concluye la demostración del Teorema 5.1. □

5.2. Martingalas racionales polinomiales

Trabajar con martingalas reales fue razonable y práctico para elaborar una demostración que, en esencia, se basa en extender la medida μ'_M del espacio de Cantor a una nueva medida μ_M sobre el intervalo real $[0, 1]$. Observar que aún si la medida original sólo toma valores racionales, potencialmente su extensión μ_M podría tomar valores irracionales, con lo cual no se podría garantizar que la nueva martingala basada en μ_M sea racional.

Sin embargo, la teoría clásica de la complejidad no suele trabajar con funciones reales. Como se pudo ver a lo largo de toda la demostración anterior, trabajar con funciones reales obliga a utilizar aproximaciones y manejar todos los errores inherentes a las mismas. Por todos estos motivos, es deseable tener una formulación del teorema anterior pero para martingalas racionales polinomiales, de forma tal que el resultado sea más autocontenido y no dependa de

la definición de *función real polinomial*. Usando el Lema 3.1 se puede extender el resultado anterior a martingalas racionales polinomiales, como se ve en el siguiente corolario.

Corolario 5.1. *Sea $Z \in k^\omega$ tal que existe una martingala M racional polinomial en base k que tiene éxito en Z. Sea Y la expansión en base r de $0.Z$. Entonces existe una martingala N racional polinomial en base r que tiene éxito en Y.*

Demostración. Primero M se puede pensar como una función real polinomial. Luego se aplica el Teorema 5.1. La martingala real polinomial N resultante es equivalente a otra martingala racional polinomial gracias al Lema 3.5. □

5.3. Δ-aleatoriedad

Se puede aprovechar la noción de $t(n)$-martingalas y extenderla a clases de funciones de la siguiente forma: si Δ es una clase de funciones, una Δ-martingala es una $t(n)$-martingala tal que $t(n) \in \Delta$. Esto permite hablar de Δ-aleatoriedad. Sin ir más lejos, con esta notación se puede decir que el Teorema 5.1 demuestra que la **P**-aleatoriedad es invariante por cambio de base. Surge entonces la siguiente pregunta: ¿se pueden aprovechar las demostraciones hechas para sacar conclusiones sobre otras clases de funciones, además de **P**? La respuesta parece ser afirmativa. Analizando la demostración del Teorema 5.1, se puede ver que la hipótesis sobre la complejidad temporal de la martingala M apenas se usa para el cálculo final de la complejidad de la nueva martingala N. Se puede observar también que la complejidad de la construcción N es básicamente $p(t(n))$, donde $p(n)$ es un polinomio y $t(n)$ es la complejidad de la martingala M. Se usa también como hipótesis que M cumple la *savings property*, con lo cual es también necesario chequear que esta suposición sigue siendo válida para clases de funciones distintas de **P**. Una vez más, los argumentos usados en los Lemas 3.1 y 3.4 son constructivos y de una complejidad polinomial en función de la entrada y la complejidad de la martingala original. Con lo cual, se puede concluir que los resultados del Teorema 5.1 se pueden extender a cualquier clase de Δ-martingalas siempre que la clase Δ sea cerrada para transformaciones polinomiales.

A modo de ejemplo, algunas clases cerradas para transformaciones polinomiales son

$$\mathbf{E} = \mathbf{DTIME}(2^{lin}) = \bigcup_{k\geq 1} \mathbf{DTIME}(2^{kn}),$$
$$\mathbf{E2} = \mathbf{DTIME}(2^{poly}) = \bigcup_{k\geq 1} \mathbf{DTIME}(2^{n^k}) \text{ y}$$
$$\mathbf{P_2} = \bigcup_{k\geq 1} \mathbf{DTIME}(2^{(\log n)^k}).$$

Siguiendo esta lógica, se concluye que **E**-aleatoriedad, **E2**-aleatoriedad y $\mathbf{P_2}$-aleatoriedad son invariantes por cambio de base.

6. Algunas reflexiones y trabajo futuro

Los resultados obtenidos en este trabajo son bastante autocontenidos. Algo interesante para destacar es el rol que terminó cumpliendo la demostración constructiva del Teorema 4.1. Además de su uso para demostrar el teorema, sirvió de base para extender el resultado a martingalas polinomiales y luego para hacer lo mismo con otras clases de martingalas acotadas por recursos. Se podría decir que terminó funcionando como una suerte de demostración canónica aplicable a una amplia gama de clases de martingalas. Fue algo que realmente no estaba previsto y que fue surgiendo a medida que se desarrollaba esta tesis.

Por otro lado, entre las herramientas teóricas que permitieron llegar a los resultados definitivamente destaca el uso de la conexión entre martingalas y medidas definidas en el intervalo $[0, 1]$. Esta conexión no es nueva y de hecho está inspirada en el novedoso trabajo de Brattka, Miller y Nies, que es un excelente ejemplo de la clase de resultados que se pueden llegar a obtener con este tipo de argumentos. Entonces, vale la pena recalcar que se trata de una herramienta potente cuando se analizan propiedades sobre martingalas, ya que en definitiva permite sortear y evitar los problemas inherentes a la naturaleza combinatoria de las representaciones simbólicas y las cadenas discretas, permitiendo otro tipo de razonamientos. Es probable que en el futuro surjan aún muchos más resultados valiosos e interesantes como fruto de este tipo de enfoques.

Es también interesante destacar el valor de propiedades como la *savings property*. Estas constituyen una herramienta muy útil para toda clase de argumentaciones ya que permiten acotar el espacio de funciones sobre el cual es necesario probar resultados y también aportan valiosa información sobre el comportamiento intrínseco de ciertas clases de funciones, como por ejemplo las martingalas exitosas para una secuencia. Descubrir e identificar de forma sistemática este tipo de resultados puede tener mucho interés para el área, con el objetivo de contar con más y mejores herramientas para atacar problemas que continúan abiertos.

Por último, a continuación se enumeran algunas de las cosas que quedaron fuera del alcance de este trabajo, pero que puede ser interesante profundizar a futuro:

- Algo pendiente es calcular con precisión la complejidad temporal asintótica de la nueva martingala polinomial construida en la demostración del Teorema 5.1 (que inevitablemente tendrá que ser expresada en la función de tiempo de la martingala de entrada). También es posible que haya partes de la construcción que puedan ser computadas con algoritmos más eficientes.

- Si bien nunca se da un orden preciso para la nueva martingala polinomial, debido a que en la construcción es necesario evaluar la martingala original una cantidad de veces que depende del error deseado, parecería que inevitablemente la complejidad de la nueva martingala corresponderá a un polinomio con al menos un grado más que la original. Puede ser interesante analizar si existe una forma de construir una martingala polinomial en otra base que como complejidad temporal tenga un polinomio de exactamente el mismo grado que la original. Seguramente la construcción de este trabajo en su forma actual no permita esto, pero de ser posible, es probable que un camino viable sea definiendo de entrada una martingala muy aproximada, quizás incluso una supermartingala, que para una entrada fija, use finitos valores de la martingala original elegidos cuidadosamente para garantizar el éxito en las mismas secuencias.

- La generalización de los resultados a otras clases de funciones es sin lugar a dudas

algo con mucho potencial, y permite en cierta forma aprovechar al máximo toda la información contenida dentro de las demostraciones (que muchas veces dicen más de lo que se deseaba probar). Explorar este camino en más profundidad es sin dudas algo de mucho interés que podría dar lugar a caracterizar las nociones de aleatoriedad basadas en martingalas invariantes por cambio de base de forma mucho más general y completa.

- Como un caso particularmente interesante del punto anterior, es posible que vía la equivalencia entre la aleatoriedad de Martin-Löf y martingalas c.e. se pueda dar una demostración alternativa de que la aleatoriedad de Martin-Löf es invariante por cambio de base.

Referencias

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

[2] Vladimir I. Bogachev. *Measure Theory*, volumen 1. Springer, 2006.

[3] Vasco Brattka, Joseph S. Miller, y André Nies. Randomness and differentiability. `http://dl.dropbox.com/u/370127/papers/RandomnessAnalysis.pdf`, Marzo 2011.

[4] C. Calude y H. Jürgensen. Randomness as an invariant for number representations. En Juliani Karhumäki, Hermann Maurer, y Grzegorz Rozenberg, editores, *Results and Trends in Theoretical Computer Science*, volumen 812 de *Lecture Notes in Computer Science*, páginas 44–66. Springer Berlin / Heidelberg, 1994.

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

[6] Gregory J. Chaitin. A theory of program size formally identical to information theory. *Journal of the ACM*, 22:329–340, 1975.

[7] Peter Hertling, Peter Hertling, Klaus Weihrauch, Klaus Weihrauch, y Theoretische Informatik I. Randomness space. En *Automata, Languages and Programming, Proceedings of the 25th International Colloquium, ICALP 98*, páginas 796–807. Springer-Verlag, 1998.

[8] Leonid A. Levin. Laws of information conservation (non-growth) and aspects of the foundations of probability theory. *Problems of Information Transmission*, 10(3):206–210, 1974.

[9] Jack H. Lutz. Almost everywhere high nonuniform complexity, 1992.

[10] Jack H. Lutz. The quantitative structure of exponential time. En *Complexity theory retrospective II*, páginas 158–175. Springer-Verlag, 1997.

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

[12] André Nies. Computability and randomness: Five questions. `http://www.cs.auckland.ac.nz/~nies/papers/Nies5questions.pdf`, 2010.

[13] André Nies. *Computability and Randomness*. Oxford University Press, USA, 2009.

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

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

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

[17] Claus-Peter Schnorr. Process complexity and effective random tests. *Journal of Computer Systems Science*, 7:376–388, 1973.

[18] Ludwig Staiger. The kolmogorov complexity of real numbers. En Gabriel Ciobanu and Gheorghe Paun, editores, *Fundamentals of Computation Theory*, volumen 1684 de *Lecture Notes in Computer Science*, páginas 827–827. Springer Berlin / Heidelberg, 1999.

[19] Andrés Taraciuk. Nociones de aleatoriedad y transformaciones de cambio de base. Tesis de Licenciatura, Departamento de Computación, FCEyN, UBA, Diciembre 2010.

[20] Sebastiaan Augustinus Terwijn. Computability and measure, Amsterdam, 1998.

[21] Jean Ville. *Étude critique de la concept du collectif*. Gauthier-Villars, 1939.

[22] Richard von Mises. Grundlagen der wahrscheinlichkeitsrechnung. *Mathematische Zeitschrift*, 5:52–99, 1919.