

## Información y Azar Aleatoriedad

**Notación.** Usamos  $\mathcal{A}$  para denotar un alfabeto arbitrario (conjunto finito de símbolos).  $\mathcal{A}^*$  es el conjunto de palabras finitas sobre  $\mathcal{A}$  y  $\mathcal{A}^\omega$  el conjunto de palabras infinitas. También las llamamos secuencias finitas e infinitas, respectivamente. Para  $w \in \mathcal{A}^*$ ,  $|w|$  es la longitud de  $w$ .  $\lambda$  es la palabra vacía,  $|\lambda| = 0$ . Si  $w \in \mathcal{A}^*$  o  $w \in \mathcal{A}^\omega$  numeramos las posiciones de  $w$  desde la posición 1. Con  $w[i]$  denotamos el símbolo de  $w$  en la posición  $i$ , y con  $w[i..j]$  denotamos la subpalabra de  $w$  entre las posiciones  $i$  y  $j$  inclusive, donde  $1 \leq i \leq j$ , y en caso de que  $w \in \mathcal{A}^*$ ,  $j \leq |w|$ . Dada  $w \in \mathcal{A}^*$  escribimos  $w\mathcal{A}^\omega$  para denotar el conjunto de secuencias infinitas que empiezan con  $w$ , formalmente,  $w\mathcal{A}^\omega = \{v \in \mathcal{A}^\omega \mid v[1..|w|] = w\}$ .  $\mathcal{A}^*a^\omega$  es el conjunto de secuencias infinitas tales que a partir de una posición en adelante contienen exclusivamente al símbolo  $a \in \mathcal{A}$ .

Escribimos  $\mathbf{2}$  (notar que está en **negrita**) para el alfabeto  $\{0, 1\}$ ,  $\mathbf{2}^*$  para las palabras finitas de 0s y 1s y  $\mathbf{2}^\omega$  para las infinitas. Asumimos la biyección entre los elementos de  $\mathbf{2}^\omega$  y los conjuntos de números naturales, a través de la función característica de conjuntos: para cada  $A \subseteq \mathbb{N}$  y para cada  $n \in \mathbb{N}$ ,  $n \in A$  si y solo si  $\chi_A(n) = 1$ . También ponemos en relación uno a uno a los elementos de  $\mathbf{2}^\omega$  con los números reales, según su expansión binaria. Recordemos que los racionales admiten dos representaciones, una terminada y una cola infinita de 0s, la otra en una cola infinita de 1s. Optamos por la primera representación, y asumimos la biyección entre las secuencias de  $\mathbf{2}^\omega$  que no terminan con 1s y los números reales del intervalo  $(0, 1)$ ,  $r = \sum_{i \geq 1} w[i] 2^{-i}$ . Dadas estas identificaciones, hablamos indistintamente de conjuntos de naturales, de números reales y de elementos de  $\mathbf{2}^\omega$  obviando el problema de las secuencias terminadas en 1s. En general si  $\mathcal{A} = \{0, \dots, (b-1)\}$ , consideramos las secuencias  $\mathcal{A}^\omega \setminus (\mathcal{A}^*1^\omega \cup \mathcal{A}^*2^\omega \cup \dots \cup \mathcal{A}^*(b-1)^\omega)$ .

Recordemos que un conjunto  $A \subseteq \mathcal{A}^*$  (o  $A \subseteq \mathbb{N}$ ) es *computablemente enumerable*, abreviado como *c.e.*, si existe una función  $f$  parcialmente computable tal que  $A = \text{dominio}(f)$ . Equivalentemente,  $A$  es *c.e.* si existe una función total  $g : \mathbb{N} \rightarrow \mathcal{A}^*$  tal que  $A = \text{imagen}(g)$ ; y una enumeración computable de  $A$  está dada por  $g(1), g(2), \dots$ . Si  $A$  es *c.e.* y su complemento  $\mathcal{A}^* \setminus A$  también, entonces  $A$  es *computable* (sus elementos pueden ser enumerados en un orden computable).

Fijamos  $(C_i)_{i \in \mathbb{N}}$  una enumeración de todas las computadoras libres de prefijos. Fijamos  $U : \mathbf{2}^* \rightarrow \mathbf{2}^*$  la computadora universal, óptima y libre de prefijos tal que para toda  $p \in \mathbf{2}^*$ ,  $U(0^i 1 p) = C_i(p)$  o ambas  $U(0^i 1 p) \uparrow$  y  $C_i(p) \uparrow$ .

## 4. Conjuntos, secuencias y reales: computables y c.e.

### Definición.

1.  $r \in \mathbb{R}$  es *left c.e.* si y solamente si existe una sucesión computable y no decreciente de racionales cuyo límite es  $r$ . En símbolos,  $r$  es *left c.e.* si existe  $(q_i)_{i \in \mathbb{N}}$ ,  $q_i \in \mathbb{Q}$  tal que  $q_i \leq q_{i+1}$  y  $\lim_{i \rightarrow \infty} q_i = r$ . Usamos indistintamente los términos *left c.e.*, *computablemente enumerable desde la izquierda* y *algorítmicamente aproximable desde abajo*.
2.  $r \in \mathbb{R}$  es *right c.e.* si y solamente si existe una sucesión computable no creciente de racionales cuyo límite es  $r$ . En símbolos,  $r$  es *right c.e.* si existe  $(q_i)_{i \in \mathbb{N}}$ ,  $q_i \in \mathbb{Q}$  tal que  $q_i \geq q_{i+1}$  y  $\lim_{i \rightarrow \infty} q_i = r$ . Usamos indistintamente los términos *right c.e.*, *computablemente enumerable desde la derecha* y *algorítmicamente aproximable desde arriba*.
3.  $r \in \mathbb{R}$  es *computable* si y solamente si dado  $n \in \mathbb{N}$  podemos computar  $q \in \mathbb{Q}$  tal que  $|r - q| < 2^{-n}$ .

**Ejercicio 4.1.** Sea  $r \in \mathbb{R}$ . Demostrar

1.  $r$  *left c.e.* y *right c.e.* si y solamente si  $r$  es *computable*.
2. Si  $r$  es *computable* entonces  $\{q \in \mathbb{Q} : q < r\}$  es *computable*.
3.  $r$  es *diferencia de dos números left c.e.* si y solamente si existe una sucesión computable de racionales  $(q_i)_{i \in \mathbb{N}}$  tal que  $r = \lim_{i \rightarrow \infty} q_i$  y  $\sum_{i \geq 1} |q_{i+1} - q_i| < \infty$ .

**Ejercicio 4.2.** Determinar Verdadero o Falso y justificar.

1. Si  $A \subseteq \mathbf{2}^*$  es computable y libre de prefijos entonces  $\sum_{a \in A} 2^{-|a|}$  es computable.
2. Si  $A \subseteq \mathbb{N}$  es c.e. entonces, visto como numero real,  $\chi_A$  es left c.e.
3. Si  $r \in \mathbb{R}$  es left c.e. entonces existe  $A \subseteq \mathbb{N}$  tal que  $\chi(A) = r$  en base 2. (Ayuda: usar  $H$ )

**Ejercicio 4.3.** Sea  $M$  una computadora libre de prefijos, y  $\text{time}(p)$  la cantidad de pasos del cómputo  $M(p) \downarrow$ . Sea  $\text{string} : \mathbb{N}_0 \rightarrow \mathbf{2}^*$  la biyección de palabras en  $\mathbf{2}^*$  con su posición en el orden lexicográfico. Demostrar que  $\Gamma = \sum_{i:U(\text{string}(i)) \downarrow} 2^{-i} / \text{time}(\text{string}(i))$  es computable.

**Definición.** Definimos  $\Omega \in \mathbb{R}$  y  $\text{halt}, \beta \in \mathbf{2}^\omega$  tales que

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

$$\text{halt}(i) = 1 \text{ si y solamente si } C_i(\lambda) \downarrow$$

$$\beta(i) = \begin{cases} 0 & \text{, si el } i\text{-ésimo símbolo arrojado por } C_i(\lambda) \text{ es } 1, \text{ o } C_i(\lambda) \text{ no arroja un } i\text{-ésimo símbolo.} \\ 1 & \text{, si el } i\text{-ésimo símbolo arrojado por } C_i(\lambda) \text{ es } 0 \end{cases}$$

**Ejercicio 4.4.** Sea el conjunto  $L \subseteq \mathbf{2}^*$  que contiene prefijos de  $\Omega$  como elementos de  $\mathbf{2}^*$ ,  $L = \{\Omega[1..i] \mid i \geq 1\} \cup \{(1 - \Omega)[i..i] \mid i \geq 1\}$ . ¿Es  $L$  computable?

**Ejercicio 4.5.** ¿Es posible dar un algoritmo para aproximar  $\beta$  desde arriba?

**Ejercicio 4.6.** (difícil). Sea  $A = \{p \in \text{words} \mid U(p) \downarrow \vee U(p) \uparrow \text{ pero imprime finitos símbolos}\}$  Sea  $r = \sum_{p \in A} 2^{-|p|}$ . Demostrar  $r$  no es left c.e. Ayuda: usar Lema de Shoenfield.

## 5. Aleatoriedad por complejidad $H$ de segmentos iniciales

**Definición.**  $w \in \mathcal{A}^\omega$  es aleatoria si, y solamente si,  $\exists c \forall n H(w[1..n]) \geq n - c$ .

**Ejercicio 5.1.** Demostrar que si  $w \in \mathcal{A}^\omega$  es computable, entonces  $\exists c \forall n H(w[1..n]) \leq H(n) + c$ .

**Ejercicio 5.2.** Determinar en cada uno de los siguientes casos si la secuencia  $w \in \mathbf{2}^\omega$  es aleatoria y en caso de que no lo sea dar una cota superior de la complejidad  $H$  de sus prefijos.

1. Sea  $w$  la secuencia que se obtiene “intercalando” 0 entre los bits de  $\Omega$ ,  $w = b_1 0 b_2 0 b_3 0 \dots$  ( $\Omega$  diluida).
2. Sea  $w$  la secuencia que se obtiene “pegando” los prefijos de  $\Omega$ ,  $w = b_1 b_1 b_2 b_1 b_2 b_3 b_1 b_2 b_3 b_4 \dots$
3. Sea  $w$  la secuencia que se obtiene “intercalando” los bits de  $\Omega$  con los de  $(1 - \Omega)$ ,  $w = b_1 c_1 b_2 c_2 b_3 c_3 \dots$
4. Sea  $w$  la secuencia que se obtiene “intercalando” los bits de  $\Omega$  con los de  $\text{halt}$ ,  $w = b_1 a_1 b_2 a_2 b_3 a_3 \dots$
5. Sea  $w$  la secuencia  $\beta$  de Turing.

**Ejercicio 5.3.** Sea  $M$  una computadora libre de prefijos y óptima. Demostrar que

1. para todo conjunto  $A \subseteq \mathbf{2}^*$  c.e. infinito,  $\sum_{p: M(p) \in A} 2^{-|p|}$  es left c.e. y aleatorio.
2.  $\sum_{s \in \{0,1\}^*} 2^{-H_M(s)}$  es left c.e. y aleatorio.

**Ejercicio 5.4.**

- a) Demostrar que para todo  $k \geq 0$  la secuencia  $w = 1^k \Omega$  es aleatoria.
- b) Demostrar que  $(1 - \Omega)$  es aleatoria.

**Ejercicio 5.5.** Demostrar que, para cada palabra  $s \in \mathbf{2}^*$ , la probabilidad de que un programa arbitrario de  $U$  arroje  $s$ ,  $P(s) = \sum_{p:U(p)=s} 2^{-|p|}$ , es aleatoria. Ayuda: Usar que hay una computadora  $C$  tal que para todo  $p$ ,  $C(p) = s$  si y solo si  $U(p) \downarrow$ .  $U$  puede simular  $C$ ,  $U(0^c 1p) = C(p)$ , para un  $c$ . Escribir  $P(s) = r + 2^{-c-1} \Omega$ , para un real c.e.  $r$  y una constance  $c$  apropiada.

## 6. Tests de Martin Löf

**Definición.** Un test de Martin Löf es una sucesión  $(\mathcal{V}_i)_{i \in \mathbb{N}}$  computablemente enumerable de manera uniforme de conjuntos  $\mathcal{V}_i \subseteq \mathbf{2}^\omega$  tal que, para todo  $i \in \mathbb{N}$ ,  $\mathcal{V}_i = \bigcup_{s \in S_i} s\mathbf{2}^\omega$  con  $S_i \subseteq \mathbf{2}^*$  c.e. (es decir,  $\mathcal{V}_i$  es un abierto computable en  $\mathbf{2}^\omega$ ), y la medida de Lebesgue  $\mu(\mathcal{V}_i) \leq 2^{-i}$ .

Una secuencia  $w \in \mathbf{2}^\omega$  no es aleatoria si existe un test de Martin Löf  $(\mathcal{V}_i)_{i \in \mathbb{N}}$  tal que  $w = \bigcap_{i \geq 1} \mathcal{V}_i$  (y decimos que  $w$  no es aleatoria porque  $w$  no pasa este test).

Para un test de Martin Löf  $(\mathcal{V}_i)_{i \in \mathbb{N}}$  dado, llamamos *cobertura* del test al conjunto  $\bigcap_{i \geq 1} \mathcal{V}_i$ . Un conjunto  $\mathcal{Y} \subseteq \mathbf{2}^\omega$  es cubierto por el test si  $\mathcal{Y}$  está incluido en la cobertura del test.

**Ejercicio 6.1.** Calcular la medida de Lebesgue los siguientes conjuntos de  $\mathbf{2}^\omega$ .

$$\mathcal{V} = \{1010010001 \dots\} \text{ (conjunto con una única secuencia)}$$

$$\mathcal{V} = \{1010, 101\}\mathbf{2}^\omega$$

$$\mathcal{V} = \{10100, 10101\}\mathbf{2}^\omega$$

$$\mathcal{V} = \{p \in \mathbf{2}^* : U(p) \downarrow\}\mathbf{2}^\omega.$$

$$\mathcal{V} = \bigcap_{k \geq 1} s1^k\mathbf{2}^\omega, \text{ para } s \in \mathbf{2}^* \text{ fija.}$$

**Ejercicio 6.2.** Determinar Verdadero o Falso y justificar

1. No existe ningún test de Martin Löf que cubra un abierto de  $\mathbf{2}^\omega$ .
2. Sea  $\mathcal{Y} \subseteq \mathbf{2}^\omega$ . No existe ningún test de Martin Löf que cubra al conjunto  $\mathcal{Y} \cup \mathcal{Y}^I$ , donde  $\mathcal{Y}^I = \bigcup_{w \in \mathcal{Y}} \{v \in \mathbf{2}^\omega \mid v(i) = 1 - w(i), \text{ para todo } i \geq 1\}$ .

**Ejercicio 6.3.** Sea  $c \in \mathbb{N}$  fijo, y sea, para todo  $k \geq 1$ ,  $\mathcal{V}_{k+c} = \{s \in \mathbf{2}^* \mid H(s) - |s| \leq -k\}\mathbf{2}^\omega$ . Probar que para un  $c$  conveniente  $(\mathcal{V}_{k+c})_{k \geq 1}$  es un test de Martin-Löf.

Ayuda:  $\mu$  es subaditiva: para  $X \subseteq \mathbf{2}^*$ ,  $\mu(X\mathbf{2}^\omega) \leq \sum_{n \geq 0} (X \cap \mathcal{A}^n)\mathbf{2}^\omega$ .

Y usar  $\#\{s \in \{0,1\}^n \mid H(s) \leq n - k\} \leq 2^{n-k-H(n)+c}$  (ejercicio de la practica 3).

**Ejercicio 6.4.** Dar un test de Martin Löf  $(\mathcal{V}_i)_{i \geq 1}$  tal que  $\mathbf{2}^*0^\omega \subseteq \bigcap_{i \geq 1} \mathcal{V}_i$ .

**Ejercicio 6.5.** Sea  $w \in \mathbf{2}^\omega$  una secuencia computable dada, sea  $\hat{\Omega}$  la secuencia que se obtiene de diluir  $\Omega$  intercalando 00 entre cada dos bits, y sean  $\text{halt}$  y  $\beta$  definidas más arriba. Dar un test de Martin-Löf  $(\mathcal{V}_i)_{i \in \mathbb{N}}$  tal que las cuatro  $w, \text{halt}, \beta, \hat{\Omega} \in \bigcap_{i \geq 1} \mathcal{V}_i$ ,

**Ejercicio 6.6.** Dar un test de Martin-Löf que cubra al conjunto de números reales entre 0 y 1 cuya expansión decimal en base 10 no contienen 7s ni 8s.

Ayuda: Ver apunte en la página de la materia.

**Ejercicio 6.7.** Sea  $f : \mathbb{N} \rightarrow \mathbb{N}$  computable total y uno a uno. Demostrar que si  $w \in \mathbf{2}^\omega$  es aleatoria entonces  $v = v[0]v[1]v[2] \dots$  tal que  $v[f(i)] = 1$  si y solo si  $w[i] = 1$ , también es aleatoria.

Ayuda: Dividir en dos implicaciones. Probar el contrarrecíproco de cada una. Suponer que  $w$  no es aleatorio y mostrar que  $v$  tampoco. Para eso, asumir un test de Martin Löf para  $w$ , y transformarlo en otro para  $v$ .

**Ejercicio 6.8.** Sean  $u, v \in \mathbb{R}$  left c.e. tales que  $r = u + v < 1$ . Demostrar que si  $u$  o  $v$  son aleatorios entonces  $r$  es aleatorio.

Ayuda: Probar el contrarrecíproco. Suponer que  $r$  no es aleatorio y mostrar que  $u$  no es aleatorio. Para eso, asumir un test de Martin Löf para  $r$ , y obtener otro para  $u$ .

## 7. Martingalas

Dada una sucesión  $(x_n)_{n \geq 1}$ ,  $\limsup_{n \rightarrow \infty} x_n = \inf_{n \geq 0} \sup_{m \geq n} x_m = \inf\{\sup\{x_m \mid m \geq n\} \mid n \geq 0\}$ .

**Definición.** Una *martingala* es una función computable  $d : \mathbf{2}^* \rightarrow \mathbb{R}^+$  tal que para toda palabra  $s \in \mathbf{2}^*$ ,  $d(s) = (d(s0) + d(s1))/2$ . Una martingala  $d$  tiene *éxito* sobre una secuencia  $w \in \mathbf{2}^\omega$  si  $\limsup_{n \rightarrow \infty} d(w[1..n]) = \infty$ . El conjunto de secuencias sobre las que  $d$  tiene éxito es

$$S[d] = \{w \in \mathbf{2}^\omega \mid d \text{ tiene éxito sobre } w\}$$

**Ejercicio 7.1.** Dar en cada caso una martingala  $d$  tal que  $S[d]$  contiene al conjunto  $\mathcal{Y} \subseteq \mathbf{2}^\omega$

1.  $\mathcal{Y} = \{101010101010\dots, 01010101010101\dots\}$  (dos secuencias).

Ayuda: Teorema 6 del apunte de martingalas.

2.  $\mathcal{Y} = \mathbf{2}^*1^\omega$ .

**Ejercicio 7.2.** Sea  $d$  la martingala que apuesta la mitad de lo disponible al 0 y la mitad al 1. Dar el conjunto  $S[d]$ .

**Ejercicio 7.3.** Sea  $w \in \mathcal{A}^\omega$ . Demostrar que la siguiente martingala  $d$  tiene éxito sobre  $w$  y solamente sobre  $w$ ,  $\frac{d((w[1..n])0)}{2d(w[1..n])} = 1 - w(n)$ .

**Ejercicio 7.4.** Sea  $A \subseteq \mathbb{N}$  un conjunto infinito, y sea  $\chi_A \in \mathbf{2}^\omega$  la secuencia de la función característica de  $A$ . Sea  $d : \mathbf{2}^* \rightarrow \mathbb{R}^+$  la siguiente martingala

$$\frac{d(\chi_A[1..n]0)}{2d(\chi_A[1..n])} = \begin{cases} 0 & , \text{ si } \chi_A[n] = 1 \\ \frac{1}{2} & , \text{ en caso contrario} \end{cases}$$

Demostrar que  $d$  tiene éxito sobre  $\chi_B$  para todo conjunto  $B \supseteq A$ .

**Ejercicio 7.5.** Dar una condición para que una martingala tenga éxito sobre toda secuencia  $w \in \mathcal{A}^\omega$  cuya frecuencia asintótica de 0s sea mayor que la de 1s. Es decir, queremos asegurar el éxito de las martingalas sobre cada una de las secuencias de

$$\left\{ w \in \mathbf{2}^\omega \mid \lim_{n \rightarrow \infty} \frac{\#0s \text{ en } w[1..n]}{n} > 1/2 \right\}$$

Ayuda: Si  $z$  es la fracción apostada al 0, y  $u$  es la apostada al 1, dar una condición sobre  $\frac{1+z-u}{1-z+u}$ .

## Referencias

- [1] Gregory Chaitin, A theory of program size formally identical to information theory, *Journal of the ACM* 22, 329-340, 1975.
- [2] Martin-Lf, Per. The definition of random sequences. *Information and Control* 9, 602-619, 1966.
- [3] Rod Downey, Denis Hirschfeldt. *Algorithmic Randomness and Complexity*, Springer, 2010.
- [4] Andre Nies. *Computability and Randomness*, Oxford University Press, 2009.