Traducción del alemán al español del artículo "Endliche Automaten und Zufallsfolgen"

Autores: C. P. Schnorr y H. Stimm.
Publicado en *Acta Informatica*, 1:345–359. Springer-Verlag, 1972.

Traducido por Facundo López Bristot

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

Fecha: 9 de diciembre de 2012

La traducción de este artículo fue realizada con la colaboración de Nicolás Rosner, docente del Departamento de Computación de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires, sin la cual no habría sido posible. Pablo Ariel Heiber participó en la revisión técnica.

Esta traducción se realizó en el marco de la Beca de Estímulo a las Vocaciones Científicas de 2011 del Consejo Interuniversitario Nacional de Argentina de Facundo López Bristot, dirigida por Verónica Becher.

Autómatas finitos y secuencias aleatorias*

C. P. Schnorr y H. Stimm

Recibido el 10 de Diciembre de 1971

Summary

We consider the behaviour of finite automata on infinite binary sequences and study the class of random tests which can be carried out by finite automata. We give several equivalent characterizations of those infinite binary sequences which are random relative to finite automata. These characterizations are based on the concepts of selection rules, martingales and invariance properties defined by finite automata.

1. Introducción

Motivados por Kolmogorov y Chaitin, últimamente han tenido lugar varios intentos –entre ellos los de Martin-Löf, Loveland y Schnorr– de definir con precisión la noción de secuencia binaria infinita aleatoria en base a los fundamentos de la teoría algorítmica. En [13] se presenta una caracterización más precisa del concepto intuitivo de test de aleatoriedad efectivo. Los demás enfoques hasta entonces estudiados, que de diversas maneras intentaron aprehender dicha noción, se demuestran equivalentes. El autor provee así una definición de aleatoriedad libre de arbitrariedades formales: una secuencia es aleatoria cuando sobrevive a todo posible test efectivo.

Computar una secuencia aleatoria es necesariamente imposible: no son computables. El problema, importante para la aplicación, de computar secuencias "lo más aleatorias posible", por lo tanto, sólo puede abarcarse en el sentido de su aproximación mediante secuencias computables. Las secuencias computables que resuelven con precisión arbitraria este problema de aproximación se llaman pseudoaleatorias. De una secuencia pseudoaleatoria debe esperarse que satisfaga al menos las leyes más importantes del azar. Cabe conjeturar que los tests algorítmicamente más simples sean aquellos que capturan leyes particularmente importantes. Entre los algoritmos, aquellos que pueden ser representados por autómatas finitos deben ser considerados especialmente fáciles. Surge entonces la pregunta acerca de si existirá alguna clase destacada de leyes del azar que puedan ser puestas a prueba mediante autómatas finitos.

Para responderla, hemos restringido algunos de los enfoques tratados en [13], con miras a caracterizar los tests efectivos, a aquellos producibles por autómatas finitos. A tal efecto consideramos los siguientes conceptos relacionados con el azar:

- el principio de sistema de juego,

*Este trabajo fue realizado en el marco del proyecto de investigación Schn 143/1 del Deutsche Forschungsgemeinschaft.

- el principio de no predictibilidad y
- propiedades invariantes de las secuencias aleatorias.

En cada uno de estos casos, las secuencias llamadas *de Bernoulli* (o también normales, libres de efectos colaterales y *admissible numbers*) resultan ser las que satisfacen la totalidad de los tests producibles por autómatas finitos. Las de Bernoulli, pues, son las secuencias que, según los autómatas finitos, deberían ser consideradas aleatorias.

Nos hemos circunscripto aquí al caso de la distribución normal sobre un conjunto finito; la adaptación a otros espacios probabilísticos con probabilidades arbitrarias queda al alcance de la mano. Los resultados del presente trabajo generalizan los de las investigaciones de Agafonov sobre reglas de selección generadas por autómatas finitos.

2. Secuencias de Bernoulli y estados ergódicos de autómatas finitos

En adelante X es un conjunto finito y X^* (X^∞) es el conjunto de secuencias finitas (infinitas) de elementos de X. $\Lambda \in X^*$ es la secuencia vacía. $|u|$ denota la longitud de $u \in X^*$. Si $u \in X^*$ ($z \in X^\infty$) e $i \in \mathbb{N}$ ($\mathbb{N}$ es el conjunto de enteros no negativos) $u(i)$ ($z(i)$) denota la secuencia inicial de longitud i de u (z). Si $u \in X^*$ e $y \in X^* \cup X^\infty$, $uy \in X^* \cup X^\infty$ denota la concatenación de u e y. De manera natural, esto resulta en el producto $AB \subseteq X^* \cup X^\infty$ de conjuntos $A \subseteq X^*$ y $B \subseteq X^* \cup X^\infty$. Sea $\chi_A : B \to \{0,1\}$ la función característica (función indicadora) del conjunto $A \subseteq B$. $\|A\|$ denota el número de elementos del conjunto A. En adelante $\|X\| = p$. Suponemos $p \geq 2$.

Definición 2.1. *$z \in X^\infty$ es una secuencia de Bernoulli si*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi_{X^*u}(z(i)) = p^{-|u|}$$

para toda $u \in X^*$.

Sea $\mathfrak{B} \subseteq X^\infty$ el conjunto de secuencias de Bernoulli.

Esto quiere decir que la frecuencia relativa con la que u aparece como subsecuencia de z es exactamente la probabilidad de u. Las secuencias de Bernoulli fueron llamadas secuencias normales, *admissible numbers* y libres de efectos colaterales, y fueron presentadas de diversas maneras por, entre otros, Borel, Copeland, Reichenbach y Popper.

Denotemos con $\overline{\mu}$ a la medida de Lebesgue en X^∞ para una distribución uniforme en X. De los principios de la teoría de la probabilidad se sigue que

Corolario 2.2.

$$\overline{\mu}(\mathfrak{B}) = 1.$$

Ahora procederemos a establecer una primera relación entre las secuencias de Bernoulli y los autómatas finitos.

Definición 2.3. *Un autómata finito es una 4-tupla $\mathfrak{A} = (X, S, \delta, s_1)$. X y S, ambos conjuntos finitos, son el alfabeto de entrada y el conjunto de estados, respectivamente. $s_1 \in S$ es el estado inicial. $\delta : X \times S \to S$ es la función de transición.*

Si el autómata lee el símbolo de entrada $x \in X$ en el estado $s \in S$, pasa al estado $\delta(x, s)$. δ se puede extender de manera natural a $\delta^* : X^* \times S \to S$:

$$\begin{aligned} &\delta^*(\Lambda, s) = s_1 \\ &\delta^*(ux, s) = \delta(x, \delta^*(u, s)) \qquad (u \in X^*, x \in X, s \in S). \end{aligned}$$

Probaremos a continuación el Teorema 2.5 que más adelante, a la hora de testear secuencias utilizando autómatas finitos, nos permitirá restringirnos a los fuertemente conexos. A tal efecto son necesarios algunos resultados preliminares.

Sean $\mathfrak{U}$ un autómata finito y $s, t \in S$. t se dice alcanzable desde $s :\Leftrightarrow (\exists u \in X^*) : \delta^*(u, s) = t$.

Notación: $s \to t$. La relación $\to$ es reflexiva y transitiva, y puede restringirse a una relación de equivalencia como sigue:

$$s \leftrightarrow t :\Leftrightarrow s \to t \wedge t \to s.$$

Para un $s \in S$, $\overline{s} \subseteq S$ denota la clase de equivalencia de s respecto de la relación de equivalencia $\leftrightarrow$. Sea $S_{/\leftrightarrow}$ el conjunto de tales clases de equivalencia.

$\mathfrak{U}$ se dice fuertemente conexo cuando S cae en exactamente una clase de equivalencia respecto de $\leftrightarrow$.

En general, $S_{/\leftrightarrow}$ puede ordenarse parcialmente como sigue:

$$\overline{s} > \overline{t} :\Leftrightarrow (\exists u \in \overline{s})(\exists v \in \overline{t}) : u \to v.$$

Por definición de $\leftrightarrow$ vale entonces:

$$\overline{s} > \overline{t} \Leftrightarrow (\forall u \in \overline{s})(\forall v \in \overline{t}) : u \to v.$$

Dado que S es finito, en $S_{/\leftrightarrow}$ existen elementos minimales respecto del orden parcial. Dichos elementos minimales exhiben la siguiente propiedad ergódica:

Corolario 2.4. *Sea $\overline{s} \in S_{/\leftrightarrow}$ minimal. Entonces vale:*

$$(\forall a \in \overline{s})(\forall u \in X^*) : \delta^*(u, a) \in \overline{s}.$$

Demostración. Supóngase la existencia de $a \in \overline{s}$ y $u \in X^*$ tales que $\delta(u, a) \notin \overline{s}$. Asígnese $t := \delta^*(u, a)$. Valen entonces $\overline{t} \neq \overline{s}$ y $\overline{s} > \overline{t}$, contradiciendo la minimalidad de $\overline{s}$. □

Tomando la terminología de la teoría de las cadenas de Markov, llamemos *conjuntos ergódicos* a los elementos minimales de $S_{/\leftrightarrow}$, y *estados ergódicos* a los elementos de esos conjuntos. Será importante en adelante el

Teorema 2.5. *Sea z una secuencia de Bernoulli y $\mathfrak{U}$ un autómata finito. Entonces para cada estado s existe un $n \in \mathbb{N}$ tal que $\delta^*(z(n), s)$ es un estado ergódico.*

La demostración del teorema se basa en el

Lema 2.6. *Para cada autómata finito existe un $u \in X^*$ tal que $\delta^*(u, s)$ es un estado ergódico para todo estado s.*

Demostración. Sea $S = \{s_1, \ldots, s_m\}$ el conjunto de estados del autómata. Probaremos por inducción en i que para cada $i \leq m$ existe un $u^{(i)} \in X^*$ tal que, para todo $j \leq i$, $\delta^*(u^{(i)}, s_j)$ es ergódico.

Caso base. Sea $\bar{t} \in S_{/\leftrightarrow}$ un elemento minimal con $\bar{s}_1 > \bar{t}$. Entonces vale $s_1 \to t$. Elíjase $u^{(1)} \in X^*$ de modo tal que $\delta^*(u^{(1)}, s_1) = t$. Entonces $\delta^*(u^{(1)}, s_1)$ es ergódico.

Paso inductivo. Sea $\bar{t} \in S_{/\leftrightarrow}$ un elemento minimal con $\overline{\delta^*(u^{(i)}, s_{i+1})} > \bar{t}$. Entonces vale $\delta^*(u^{(i)}, s_{i+1}) \to t$. Elíjase $v \in X^*$ de modo que $\delta^*(v, \delta^*(u^{(i)}, s_{i+1})) = t$. Asígnese $u^{(i+1)} := u^{(i)}v$. Entonces vale que $\delta^*(u^{(i+1)}, s_{i+1}) = t$. Como $\bar{t} \in S_{/\leftrightarrow}$ es minimal, $\delta^*(u^{(i+1)}, s_{i+1})$ debe ser ergódico. Más aún, $\delta^*(u^{(i+1)}, s_j)$ con $j \leq i$ también es ergódico, puesto que $\delta^*(u^{(i)}, s_j)$ con $j \leq i$ lo es por hipótesis inductiva, y los estados ergódicos sólo son traducibles en estados ergódicos. □

Teorema 2.5. Sea z una secuencia de Bernoulli y $\mathfrak{U}$ un autómata finito. Satisfaga $u \in X^*$ el lema 2.6. u aparece como subsecuencia de z. Elíjase $n \in \mathbb{N}$ de modo que $z(n) \in X^*u$. Entonces de 2.6 se sigue que $\delta^*(z(n), s)$ es ergódico. □

3. Martingalas producidas por autómatas finitos

Consideraremos juegos (en sentido naif) sobre secuencias $u \in X^*$. El resultado de un juego sobre la secuencia u es un número real no negativo $V(u)$ que denota el capital del jugador tras haber jugado en u. En general, cualquier "estrategia de juego" fijada de antemano (que el jugador respete para toda secuencia $u \in X^*$) induce una función

$$V : X^* \to \mathbb{R}^+,$$

siendo $\mathbb{R}^+$ el conjunto de los números reales no negativos. Se considera que un juego ofrece chances equitativas (respecto de la distribución uniforme) cuando la función V satisface la propiedad de *martingala*

$$V(u) = \frac{1}{p} \sum_{x \in X} V(ux) \qquad (u \in X^*). \tag{M}$$

En tal caso, las chances de ganar y las perder resultan de igual magnitud. En adelante llamaremos martingalas a las funciones que satisfagan la ecuación (M). La construcción de una martingala V puede pensarse de la siguiente manera: el jugador comienza en posesión de un capital inicial $V(\Lambda) \in \mathbb{R}^+$. Tras haber jugado sobre la secuencia $u \in X^*$, elige para cada $x \in X$ una cantidad (el valor de su apuesta) $B_x(u) \in \mathbb{R}^+$ a favor de que el siguiente miembro de la secuencia sea x. La suma de estas apuestas no puede superar el total de su patrimonio en ese instante. En otras palabras, las funciones de apuesta $B_x : X^* \to \mathbb{R}^+$ deben satisfacer la *condición de apuesta*

$$\sum_{x \in X} B_x(u) \leq V(u) \qquad (u \in X^*). \tag{A}$$

El capital actualizado tras una ronda de juego, $V(ux)$, puede entonces deducirse de la *condición de pago*:

$$V(ux) = V(u) + \sum_{y \in X} (p\delta_{x,y} - 1) B_y(u). \tag{P}$$

donde $\delta_{x,y}$ es la función delta de Kronecker. Es decir que ante la aparición de y el jugador gana $(p-1)$ veces lo apostado a favor de y, y pierde el total de sus demás apuestas. Es fácil ver que la condición de pago (P) asegura la propiedad de martingala (M). De la ecuación (A) se sigue que V es no negativa. A la inversa, no es difícil mostrar que toda función $V : X^* \to \mathbb{R}^+$ puede obtenerse mediante funciones de apuesta apropiadas $B_x : X^* \to \mathbb{R}^+$ con la propiedad (A). A continuación explicaremos cuándo una martingala V es producida por un autómata finito $\mathfrak{U} = (X, S, \delta, s_1)$. Lo antedicho debería ser el caso para las funciones tales que el cociente $V(ux)/V(u)$ sólo dependa del estado instantáneo $\delta^*(u, s_1)$ del autómata y del símbolo de entrada x. Interpretaremos dicho cociente, entonces, como la salida del autómata. Formalmente asociaremos con cada autómata $\mathfrak{U} = (X, S, \delta, s_1)$ y función de salida $\lambda : X \times S \to \mathbb{R}^+$ una función $V_{\mathfrak{U}} : X^* \to \mathbb{R}^+$ del siguiente modo:

$$\begin{aligned}
&V_{\mathfrak{U}}(\Lambda) = 1 \\
&V_{\mathfrak{U}}(ux) = V_{\mathfrak{U}}(u)\lambda(x, \delta^*(u, s_1)) \qquad (u \in X^*, x \in X) \\
&(\text{Multiplicación en } \mathbb{R}).
\end{aligned} \tag{3.1}$$

$V_{\mathfrak{U}}$ es una martingala si y sólo si vale:

$$\sum_{x \in X} \lambda(x, s) = p \qquad (s \in S).$$

Las martingalas así obtenidas se dicen producidas por autómatas finitos.

También existe otro modo alternativo de proceder. Sean $\mathfrak{U} = (X, S, \delta, s_1)$ un autómata finito y $\overline{\lambda} : X \times S \to \mathbb{R}^+$ una función de salida. Entonces es posible definir funciones de apuesta $B_x : X^* \to \mathbb{R}^+$ $(x \in X)$ y una función $\overline{V}_{\mathfrak{U}} : X^* \to \mathbb{R}^+$ del siguiente modo:

$$\begin{aligned}
\overline{V}_{\mathfrak{U}}(\Lambda) &= 1 \\
B_x(u) &= \overline{V}_{\mathfrak{U}}(u)\overline{\lambda}(x, \delta^*(u, s_1)) \\
\overline{V}_{\mathfrak{U}}(ux) &\underset{(I)}{=} \overline{V}_{\mathfrak{U}}(u) + \sum_{x \in X} (p\delta_{x,y} - 1) B_y(u) \\
&= \overline{V}_{\mathfrak{U}}(u) \left(1 + \sum_{y \in X} (p\delta_{x,y} - 1)\overline{\lambda}(y, \delta^*(u, s_1)) \right) \qquad (u \in X^*, x \in X).
\end{aligned} \tag{3.2}$$

La condición de apuesta (A) se verifica justamente cuando

$$\sum_{x \in X} \overline{\lambda}(x, s) \leq 1 \qquad (s \in S)$$

vale. En tal caso $\overline{V}_{\mathfrak{U}}$ resulta no negativa y por ende una martingala. Por (3.2), la proporción $B_x(u)/\overline{V}_{\mathfrak{U}}$ del capital $\overline{V}_{\mathfrak{U}}$ que se apuesta a favor de x sólo depende del estado instantáneo $\delta^*(u, s_1)$ y de x. La igualdad (I) de (3.2) es justamente la condición de pago (P). Pero de la última fórmula de (3.2) se sigue que también el cociente $\overline{V}_{\mathfrak{U}}(ux)/\overline{V}_{\mathfrak{U}}(u)$ depende únicamente del estado $\delta^*(u, s_1)$ y de x. Por lo tanto una martingala V definida de acuerdo con (3.2) también puede, mediante una elección adecuada de λ, ser definida de acuerdo con (3.1). Para ello, asígnese por cada $x \in X$ y $s \in S$:

$$\lambda(x, s) := 1 + \sum_{y \in X} (p\delta_{x,y} - 1)\overline{\lambda}(y, s).$$

Por otro lado, sea $V_{\mathfrak{U}}$ la expresada por $\mathfrak{U}$ y la función de salida λ según (3.1). Asígnese $\overline{\lambda}(x, s) := \lambda(x, s)/p$. Mostraremos por inducción que las funciones $B_x, \overline{V}_{\mathfrak{U}}$ según (3.2) satisfacen lo siguiente:

$$\overline{V}_{\mathfrak{U}}(u) = V_{\mathfrak{U}}, \qquad B_x(u) = \frac{1}{p} V_{\mathfrak{U}}(ux) \qquad (u \in X^*, x \in X).$$

Es claro para $u = \Lambda$. En cuanto al paso inductivo,

$$\begin{aligned}
\overline{V}_{\mathfrak{U}}(ux) &= \overline{V}_{\mathfrak{U}}(u) + \sum_{y \in X} (p\delta_{x,y} - 1) B_y(u) \\
&= V_{\mathfrak{U}} + \sum_{y \in X} (p\delta_{x,y} - 1) p^{-1} V_{\mathfrak{U}}(uy) \\
&= V_{\mathfrak{U}}(u) + pp^{-1} V_{\mathfrak{U}}(ux) - p^{-1} \sum_{y \in X} V_{\mathfrak{U}}(uy) \\
&= V_{\mathfrak{U}}(ux).
\end{aligned}$$

Asimismo,

$$\begin{aligned}
B_x(uy) &= \overline{V}_{\mathfrak{U}}(uy)\overline{\lambda}(x, \delta^*(uy, s_1)), && (3.2) \\
&= V_{\mathfrak{U}}(uy) p^{-1} \lambda(x, \delta^*(uy, s_1)) \\
&= p^{-1} V_{\mathfrak{U}}(uyx). && (3.1)
\end{aligned}$$

De lo antedicho obtenemos el

Teorema 3.1. *Las clases de martingalas producidas por un autómata finito de acuerdo con (3.1) y (3.2), respectivamente, coinciden.*

En lo sucesivo usaremos (3.1) para definir martingalas.

4. Caracterización de las secuencias de Bernoulli por medio de martingalas producidas por autómatas finitos

Una martingala producida por un autómata finito representa un *test de aleatoriedad*. Una secuencia $z \in X^\infty$ debería fallar, es decir ser rechazada como no aleatoria por dicho test, cuando $V_{\mathfrak{U}}$ crece arbitrariamente en z, es decir, cuando

$$\limsup_{n \to \infty} V_{\mathfrak{U}}(z(n)) = \infty.$$

El siguiente y primer resultado central de este trabajo muestra que las secuencias de Bernoulli y son fundamentalmente distinguibles del resto de las secuencias desde el punto de vista de las martingalas producidas por autómatas finitos. Son justamente las de Bernoulli las que, en lo que a tales martingalas respecta, se comportan como el ideal de secuencia aleatoria. En adelante usaremos el cuantificador $\forall^\infty n$ para denotar "para todo salvo cantidad finita de n", y el cuantificador $\exists^\infty n$ significará "para infinitos n".

Teorema 4.1. *(a) Sea $z \in X^\infty$ una secuencia de Bernoulli y $V_{\mathfrak{U}} : X^* \to \mathbb{R}^+$ una martingala producida por autómata finito. Entonces necesariamente vale (1) o bien vale (2):*

$$(\forall^\infty n \in \mathbb{N}) : V_{\mathfrak{U}}(z(n)) = V_{\mathfrak{U}}(z(n+1)). \tag{1}$$

Existe un $r \in \mathbb{R}$, con $0 < r < 1$, tal que

$$(\forall^\infty n \in \mathbb{N}) : V_{\mathfrak{U}}(z(n)) \leq r^n. \tag{2}$$

(b) Sea $z \in X^\infty$ una secuencia que no es de Bernoulli. Entonces existen una función $V_{\mathfrak{U}}$ producida por un autómata $\mathfrak{U}$ y un $r > 1$ tales que

$$(\exists^\infty n \in \mathbb{N}) : V_{\mathfrak{U}}(z(n)) > r^n.$$

La parte (a) afirma que para una secuencia de Bernoulli z, el capital $V_{\mathfrak{U}}$ deviene o bien constante o bien exponencialmente decreciente tras una cantidad finita de pasos. Para probarlo mostraremos que el cociente $V_{\mathfrak{U}}(z(n+1))/V_{\mathfrak{U}}(z(n))$ toma los valores $1+\epsilon$ y $1-\epsilon$ con aproximadamente igual frecuencia. Como $(1+\epsilon)(1-\epsilon) = (1-\epsilon^2) < 1$, de ello se sigue la tesis. La parte (b) afirma que, ante el caso de una secuencia que no sea de Bernoulli, una martingala apropiada crecerá asimismo de manera exponencial.

Con miras a la demostración presentamos los siguientes dos lemas.

Lema 4.2. *Sea $\mathfrak{U} = (X, S, \delta, s_1)$ un autómata finito fuertemente conexo, y sean $x \in X$ y $t \in S$ fijos. Entonces existe una $u \in X^*$ tal que*

$$(\forall s \in S)(\exists i < |u|) : \delta^*(u(i), s) = t \wedge u(i+1) = u(i)x.$$

Demostración. Sea $S = \{s_1, \ldots, s_m\}$. Por inducción en j mostramos que para cada $j \leq m$ existe $u^{(j)} \in X^*$ tal que

$$(\forall k < j)(\exists i < |u^{(j)}|) : \delta^*(u^{(j)}(i), s_k) = t \wedge u^j(i+1) = u^j(i)x.$$

Caso base. Elíjase $v \in X^*$ de modo tal que $\delta^*(v, s_1) = t$, y asígnese $u^{(1)} := vx$.

Paso inductivo. Sea $r = \delta^*(u^{(j)}, s_{j+1})$. Elíjase $v \in X^*$ de modo que $\delta^*(v, r) = t$, y asígnese $u^{(j+1)} := u^{(j)}vx$. La tesis se verifica sin más. $\square$

Para la prueba del segundo lema necesitamos algunas definiciones y teoremas de la Teoría de Cadenas de Markov. Las que presentamos aquí han sido tomadas en su totalidad del libro [4] de Kay Lai Chung, "Finite Markov Chains with Stationary Transition Probabilities".

Sea $\mathfrak{U} = (X, S, \delta, s_1)$ un autómata finito con un conjunto de estados fuertemente conexo $S = \{s_1, \ldots, s_m\}$.

Sean $s_q, s_r \in S$ fijadas de antemano. Definimos las magnitudes aleatorias $Z_n : X^\infty \to S$ ($n \in \mathbb{N}$) mediante

$$Z_n(z) := \delta^*(z(n), s_q).$$

Los Z_n conforman una cadena de Markov con distribución inicial

$$(p_i)_{i=1,\ldots,m} = (0, \ldots, 0, 1, 0, \ldots, 0)$$

(1 en la q-ésima posición) y matriz de transición $(p_{ij})_{i,j=1,\ldots,m}$ con

$$p_{ij} := \frac{1}{p}\|\{x \in X : \delta(x, s_i) = s_j\}\|.$$

La matriz de transición en n pasos $\left(p_{ij}^{(n)}\right)$ satisface:

$$\left(p_{ij}^{(n)}\right) = (p_{ij})^n.$$

Se ve fácilmente que S, el conjunto de estados de la cadena de Markov, constituye una clase positivo-recurrente. Gracias a ello, el límite de Cesaro

$$\pi_j := \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} p_{ij}^{(k)}$$

existe independientemente de i ([4], §6 Teorema 4 y su corolario y §5 Teorema 6).

Fijemos $f : S \to \{0, 1\}$ como

$$f(s) := \begin{cases} 1 & \text{si } s = s_r \\ 0 & \text{en caso contrario.} \end{cases}$$

Entonces $f(Z_0) + f(Z_1) + \cdots + f(Z_n)$ mide la cantidad de veces que la cadena de Markov estuvo en el estado s_r en los primeros n pasos. Vale

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=0}^{n} f(Z_k) = \pi_r \qquad \text{con certeza } \overline{\mu}$$

([4], §15 Teorema 2). Por la definición de las variables aleatorias Z_n, puesto que vale para cada $s_q, s_r \in S$, lo anterior equivale a que

$$(\forall s_i, s_j \in S) : \overline{\mu} \left\{ z \in X^\infty : \lim_{n\to\infty} \frac{1}{n} \|\{k \leq n : \delta^*(z(k), s_i) = s_j\}\| = \pi_j \right\} = 1. \tag{4.3}$$

Partiendo de las magnitudes aleatorias $Z_n : X^\infty \to S \times X$ $(n \in \mathbb{N})$ definidas por

$$\overline{Z}_n(z) := (\delta^*(z(n), s_q), z_{n+1})$$

mediante proceder análogo (con igual π_j) se obtiene que

$$\begin{aligned} &(\forall s_i, s_j \in S)(\forall x \in X) : \\ &\overline{\mu} \left\{ z \in X^\infty : \lim_{n\to\infty} \frac{1}{n} \|\{k \leq n : \delta^*(z(k), s_i) = s_j \wedge z_{k+1} = x\}\| = \frac{\pi_j}{p} \right\} = 1. \end{aligned} \tag{4.4}$$

Con la ayuda de estas últimas demostraremos ahora el

Lema 4.5. *Sea $\mathfrak{A} = (X, S, \delta, s_1)$ un autómata finito con conjunto de estados fuertemente conexo $S = \{s_1, \ldots, s_m\}$. Entonces existen números $\pi_j > 0$ $(j = 1, \ldots, m)$ tales que para toda secuencia de Bernoulli z, todo $s_i \in S$ y todo $x \in X$*

$$\pi_j/p = \lim_{n\to\infty} \frac{1}{n} \|\{k \leq n : \delta^*(z(k), s_i) = s_j \wedge z_{k+1} = x\}\|.$$

Resulta visible que los π_j conforman una distribución probabilística en S.

Demostración. Elegiremos π_j $(j = 1, \ldots, m)$ como en (4.4). Por (4.4) vale para cada $\epsilon, \epsilon' > 0$:

$$\begin{aligned} &(\forall^\infty k \in \mathbb{N})(\forall s_i, s_j \in S)(\forall x \in X) : \\ &p^{-k} \left\| \left\{ u \in X^k : \left| \frac{1}{k} \|\{q < k : \delta^*(u(q), s_i) = s_j \wedge u_{q+1} = x\}\| - \pi_j/p \right| < \epsilon \right\} \right\| > 1 - \epsilon'. \end{aligned} \tag{4.6}$$

Asimismo vale para cada secuencia de Bernoulli z, cada $k \in \mathbb{N}$ y cada $\epsilon'' > 0$:

$$(\forall^\infty n \in \mathbb{N})(\forall u \in X^k) : \left| \frac{1}{n} \sum_{q=1}^{n} \chi_{X^* u}(z(kq)) - p^{-k} \right| < \epsilon''. \tag{4.7}$$

Dados $\epsilon, \epsilon' > 0$, elíjase k de la magnitud necesaria para que valga (4.6). Para k y $\epsilon'' > 0$ elíjase entonces n de la magnitud necesaria para satisfacer (4.7). Se sigue entonces inmediatamente que

$$\left| \frac{1}{nk} \|\{q < nk : \delta^*(z(q), s_i) = s_j \wedge z_{q+1} = x\}\| - \pi_j/p \right| < \epsilon + \epsilon' + \epsilon''.$$

Del hecho que esta última relación se satisface para $\epsilon, \epsilon', \epsilon'' > 0$ arbitrarios y con valores de k y n crecientes se sigue la convergencia de (4.5). Del que $\mathfrak{U}$ sea fuertemente conexo se sigue que $\pi_j > 0$. □

Teorema 4.1. (a) Queremos clasificar el comportamiento en el límite de las martingalas producidas por autómatas finitos sobre secuencias de Bernoulli. A continuación mostraremos que no hay pérdida de generalidad en restringirse a los autómatas fuertemente conexos. Dada una secuencia de Bernoulli z como entrada, un autómata finito $\mathfrak{U} = (X, S, \delta, s_1)$ alcanza tras una cantidad finita de pasos, que llamaremos n, un estado ergódico (por el Teorema 2.5). El comportamiento asintótico de una martingala $V_{\mathfrak{U}}$ producida por $\mathfrak{U}$ sobre z es, en caso que $V_{\mathfrak{U}}(z(n)) \neq 0$, por ende el mismo que el de la función $V_{\overline{\mathfrak{U}}}$ sobre la secuencia de Bernoulli $z_{n+1}z_{n+2}z_{n+3}\ldots$. Sea en lo anterior $V_{\overline{\mathfrak{U}}}$ la martingala correspondiente a $V_{\mathfrak{U}}$ que es producida por el autómata fuertemente conexo $\overline{\mathfrak{U}} = (X, \bar{t}, \delta_{/\bar{t}}, t)$, cuyo conjunto de estados coincide con la clase de equivalencia de t, cuya función de transición coincide con δ en $\bar{t}$ y cuyo estado inicial es justamente t.

Sea $V_{\mathfrak{U}}$ una función producida por el autómata fuertemente conexo $\mathfrak{U} = (X, S, \delta, s_1)$ con $S = \{s_1, \ldots, s_m\}$ de acuerdo con (3.1):

$$\begin{aligned} V_{\mathfrak{U}}(ux) &= V_{\mathfrak{U}}(u)\lambda(x, \delta^*(u, s_1)) \\ \sum_{x \in X} \lambda(x, s) &= p \qquad (s \in S). \end{aligned}$$

Distinguiremos dos casos:

$$(\forall s \in S)(\forall x \in X) : \lambda(x, s) = 1. \tag{1}$$

En este caso $V_{\mathfrak{U}}$ es constante. Estas martingalas surgen cuando el jugador apuesta a todos los $x \in X$ por igual.

$$(\exists t \in S)(\exists y \in X) : \lambda(y, t) < 1. \tag{2}$$

Dado un estado $s \in S$, definimos

$$U_s := \prod_{x \in X} \lambda(x, s).$$

Se verifica entonces la siguiente proposición auxiliar

$$\begin{aligned} &0 \leq U_s \leq 1 \\ &U_s = 1 \Leftrightarrow (\forall x \in X) : \lambda(x, s) = 1. \end{aligned} \tag{4.8}$$

Con métodos bien conocidos puede mostrarse entonces que, bajo las condiciones $\sum_{x \in X} \lambda(x, s) = p$ y $\lambda(x, s) \geq 0$, la expresión $\prod_{x \in X} \lambda(x, s)$ alcanza su máximo 1 exactamente cuando $\lambda(x, s) = 1$ para todo $x \in X$.

Del lema 4.5 se sigue, para cada secuencia de Bernoulli z, la relación

$$\lim_{n \to \infty} V_{\mathfrak{U}}(z(n)) \Big/ \left(\prod_{j=1}^{m} U_{s_j}^{\pi_j/p} \right)^n = 1 \ .$$

Por la hipótesis $\lambda(y, t) < 1$ y (4.8):

$$\prod_{j=1}^{m} U_{s_j}^{\pi_j/p} < 1.$$

con lo que existe un $r < 1$ tal que

$$(\forall^\infty n \in \mathbb{N}) : V_{\mathfrak{U}}(z(n)) < r^n.$$

(b) Si $z \in X^\infty$ no es una secuencia de Bernoulli, existen un $u \in X^*$, un $y \in X$ y un $\delta > 0$ tales que

$$\begin{aligned} \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi_{X^*u}(z(i)) &= p^{-|u|} \\ \limsup_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi_{X^*uy}(z(i)) &= p^{-|u|}(p^{-1} + \delta). \end{aligned} \tag{4.9}$$

Definimos una martingala V de tal manera que $V(w(n+1)) > V(w(n))$ si y sólo si $w(n+1) \in X^*uy$. Para cierto número a definir α tal que $-1 < \alpha < 1$ definimos V tal que $V(\Lambda) = 1$ y

$$V(w(n+1)/w(n)) = \begin{cases} 1 & \text{si } w(n) \notin X^*u \\ 1+\alpha & \text{si } w(n+1) \in X^*uy \\ 1-\alpha/(p-1) & \text{en otro caso.} \end{cases}$$

Es sencillo advertir que V es una martingala producida por un autómata finito según (3.1).

Por (4.9) vale para

$$r(\alpha) := (1+\alpha)^{p^{-|u|}(p^{-1}+\delta)}(1-\alpha/(p-1))^{p^{-|u|}(1-p^{-1}-\delta)}$$

la relación

$$\limsup_{n\to\infty} V(z(n))r(\alpha)^{-n} = 1.$$

Para probar nuestra afirmación basta mostrar que α puede elegirse de modo tal que $r(\alpha) > 1$. Como $r(0) = 1$, alcanza para esto la relación

$$\frac{d}{d\alpha} r(\alpha)|_{\alpha=0} > 0.$$

Vale lo siguiente:

$$\begin{aligned} \frac{d}{d\alpha} r(\alpha)|_{\alpha=0} &= p^{-|u|}(p^{-1}+\delta) - p^{|u|}(1-p^{-1}-\delta)/(p-1) \\ &= \delta p^{-|u|+1}/(p-1) > 0, \end{aligned}$$

pues vale $\delta > 0$, q.e.d. □

5. Caracterización de las secuencias de Bernoulli mediante el concepto de la predecibilidad.

En estos párrafos estudiaremos más casos de tests producidos por autómatas finitos para los que, nuevamente, exactamente las de Bernoulli resultan ser aquellas secuencias que se comportan como idealmente aleatorias.

Sea $z \in X^\infty$. Entonces interpretamos la salida $x \in X$ de un autómata finito, tras haber dado como entrada la secuencia inicial $z(i)$, como una predicción del próximo elemento z_{i+1} de la secuencia. El siguiente teorema afirma que la proporción de predicciones acertadas vs. erradas supera $1/p$ cuando la secuencia dada no es de Bernoulli.

Teorema 5.1. *Una secuencia $z \in X^\infty$ no es de Bernoulli cuando y sólo cuando existen un autómata finito $\mathfrak{U} = (X, S, \delta, s_1)$ y una función de salida $\lambda : X \times S \to X$ tales que*

$$\limsup_{n\to\infty} \frac{1}{n} \|\{i \leq n : \lambda(z_i, \delta^*(z(i), s_1)) = z_{i+1}\}\| > \frac{1}{p}.$$

Demostración. **(⇐).** Sean $z \in X^\infty$, $\mathfrak{U} = (X, S, \delta, s_1)$ un autómata finito y $\lambda : X \times S \to X$ una función de salida con

$$\limsup_{n\to\infty} \frac{1}{n} \|\{i \leq n : \lambda(z_i, \delta^*(z(i), s_1)) = z_{i+1}\}\| > \frac{1}{p}.$$

Entonces existen un estado $t \in S$, un $\delta > 0$ y un conjunto infinito $M \subseteq \mathbb{N}$ tales que, para todo $n \in M$,

$$\begin{aligned}&\frac{1}{n}\|\{i \leq n : \delta^*(z(i), s_1) = t \wedge \lambda(z_i, t) = z_{i+1}\}\| \\ >&\frac{1}{p}\frac{1}{n}\|\{i \leq n : \delta^*(z(i), s_1) = t\}\| + \delta.\end{aligned}$$

Para un α a definir con $-1 < \alpha < 1$, definimos las martingalas V con $V(\Lambda) = 1$ mediante

$$V(w(n+1))/V(w(n)) = \begin{cases} 1 & \text{si } \delta^*(w(n)) \neq t \\ 1+\alpha & \text{si } \delta^*(w(n)) = t \text{ y } \lambda(w_n, t) = w_{n+1} \\ 1-\alpha/(p-1) & \text{en otro caso.} \end{cases}$$

Se ve de inmediato que V es una martingala de $\mathfrak{U}$ definida de acuerdo con (3.1). Asignamos

$$a := \limsup_{\substack{n\to\infty \\ n\in M}} \frac{1}{n}\|\{i \leq n : \delta^*(z(i), s_1) = t\}\|$$

y

$$r(\alpha) := (1+\alpha)^{ap^{-1}+\delta}(1-\alpha/(p-1))^{a(1-p^{-1})-\delta}.$$

Entonces vale que

$$\limsup_{n\to\infty} V(z(n))/r(\alpha)^n \geq 1.$$

Como en la demostración de (4.1)(b), basta mostrar que es posible elegir α de modo tal que $r(\alpha) > 1$. Por lo antedicho y en base a (4.1), z no es una secuencia de Bernoulli.

(⇒) Si $z \in X^\infty$ no es una secuencia de Bernoulli, existen $u \in X^*$, $y \in X$ y $\delta > 0$ tales que (4.9). Entonces hay un $t \in X$ y un $\delta' \geq 0$ tales que

$$\begin{aligned}(\exists^\infty n \in \mathbb{N}) : \frac{1}{n}\sum_{i=1}^{n} \chi_{X^*uy}(z(i)) &> p^{-|u|}\left(\frac{1}{p} + \frac{\delta}{2}\right) \\ \wedge \frac{1}{n}\sum_{i=1}^{n} \chi_{X^*ut}(z(i)) &< p^{-|u|}\left(\frac{1}{p} - \delta'\right).\end{aligned} \tag{5.2}$$

Usaremos lo antedicho para construir un autómata $\mathfrak{U} = (X, S, \delta, s_1)$ y una función de salida $\lambda : X \times S \to X$ de tal forma que la proporción de predicciones correctas versus incorrectas supere $1/p$.

Elegimos a tal efecto el autómata $\mathfrak{U} = (X, S, \delta, a_1)$ definido por

$$S := \cup_{i=0}^{|u|} X^i = \{v \in X^* : |v| \leq |u|\}, \qquad s_1 := \Lambda,$$

$$\delta(x, v) := \begin{cases} vx & \text{si } |v| < |u| \\ w & \text{con } vx \in Xw \text{ en caso contrario} \end{cases}$$

y la función de salida $\lambda : X \times S \to X$ con

$$\lambda(x, v) := \begin{cases} t & \text{si } v \neq u \\ y & \text{si } v = u. \end{cases}$$

Distinguimos dos casos:

$$|u| = 0, \text{ es decir } u = \Lambda. \tag{1}$$

En este caso es

$$\begin{aligned} &\limsup_{n\to\infty} \frac{1}{n} \|\{i \le n : \lambda(z_i, \delta^*(z(i), s_1)) = z_{i+1}\}\| \\ &\quad = \limsup_{n\to\infty} \frac{1}{n} \|\{i \le n : z_{i+1} = y\}\| \\ &\quad = 1/p + \delta > 1/p \end{aligned}$$

$$|u| > 0. \tag{2}$$

Entonces vale

$$\begin{aligned} 1/p &= \lim_{n\to\infty} \frac{1}{n} \|\{i \le n : z_{i+1} = t\}\| \\ &= \lim_{n\to\infty} \frac{1}{n} \left(\sum_{i=1}^{n} \sum_{v \in X^{|u|}} \chi_{X^* vt}(z(i)) \right). \end{aligned} \tag{5.3}$$

Por lo tanto el autómata $\mathfrak{U}$ acertaría justamente $1/p$ de las predicciones, en promedio, si siempre devolviese t. Sin embargo, en caso de aparecer u como subsecuencia de z, devolverá y. Por ello y en base a (4.9), (5.2) y (5.3) vale:

$$\begin{aligned} &\limsup_{n\to\infty} \frac{1}{n} \|\{i \le n : \lambda(z_i, \delta^*(z(i), s_1)) = z_{i+1}\}\| \\ &\quad \ge 1/p - p^{-|u|}(1/p - \delta') + p^{-|u|}(1/p + \delta/2) \\ &\quad = 1/p + \delta'\delta/2 > 1/p. \end{aligned}$$

□

6. Propiedades invariantes definidas por autómatas finitos.

Sea $z \in X^\infty$ una secuencia aleatoria. Entonces esperamos que suceda lo siguiente: al seleccionar de cualquier manera posible (diremos: por medio de una *regla de selección*) suficientes elementos para conformar una secuencia infinita, en la misma aparecen todos los elementos de X con igual frecuencia. Esto es, la nueva secuencia cumple la ley fuerte de los grandes números. Consideramos reglas de selección producidas por autómatas finitos en las que la decisión (la selección o no del siguiente elemento de una secuencia) sólo dependa del estado instantáneo de un autómata. Podemos describir esto explícitamente con una función de salida $\lambda : X \times S \to X^*$ que satisfaga las siguientes condiciones adicionales:

$$\begin{aligned} &\text{o bien} \quad (\forall x \in X) : \lambda(x, s) = \Lambda \quad \text{(no selección en } s) \\ &\text{o bien} \quad (\forall x \in X) : \lambda(x, s) = x \quad \text{(selección en } s). \end{aligned} \tag{6.1}$$

Al haber asociado a cada secuencia infinita z (o finita u) la secuencia $\Phi_{\mathfrak{U}}(z)$ (o $\Phi_{\mathfrak{U}}(u)$) resultante de llevar a cabo la selección, obtenemos una función parcial claramente definida $\overline{\phi}_{\mathfrak{U}} : X^\infty \to X^\infty$ (o $\Phi_{\mathfrak{U}} : X^* \to X^*$).

Agafonov demostró que la secuencia seleccionada, para todas las reglas de selección basadas en autómatas finitos, cumple la ley fuerte de los grandes números siempre que la secuencia de entrada sea de Bernoulli y la seleccionada sea infinita. Procederemos a generalizar este concepto eliminando la principal restricción (6.1) sobre las posibles funciones de salida. Sin embargo, es seguro que no cualquier función de salida $\lambda : X \times S \to X^*$ es admisible. En efecto, basta tomar $\lambda(x, s) = y$ ($y \in X$ fijo) para obtener una constante $\overline{\phi}_{\mathfrak{U}}$ que asocia toda secuencia $z \in X^\infty$ con la secuencia $yyy\ldots$; ciertamente esto no satisface la ley fuerte de los grandes números. Mostraremos que alcanza con requerir de $\overline{\phi}_{\mathfrak{U}}$ la propiedad de ser de medida acotada. $\overline{\phi}_{\mathfrak{U}}$ se dice de *medida acotada* cuando existe un $k \in \mathbb{N}\backslash\{0\}$ tal que para todo conjunto medible $M \subseteq X^\infty$:

$$\overline{\mu}(\overline{\phi}_{\mathfrak{U}}^{-1}(M)) \leq k\overline{\mu}(M).$$

Sin duda son de medida acotada todas las funciones $\overline{\phi}_{\mathfrak{U}}$ producidas por reglas de selección (comp. también con Doob); sin embargo, muchas otras funciones cumplen esta propiedad. A modo de ejemplo presentaremos las permutaciones: un autómata lee n elementos, los permuta y los devuelve. El autómata definido como sigue es un ejemplo de lo antedicho:

Sea $\pi : X^n \to X^n$ ($n \in \mathbb{N}$ fijo) una permutación.

Sea $\mathfrak{U} = (X, S, \delta, s_1)$ definida como

$$S := \cup_{i=0}^{n} X^i = \{u \in X^* : |u| \leq n\}, \qquad s_1 := \Lambda,$$
$$\delta(x, v) := \begin{cases} vx & \text{si } |v| < n \\ x & \text{si } |v| = n \end{cases}$$

y la función de salida $\lambda : X \times S \to X^*$ tal que

$$\lambda(x, v) := \begin{cases} \Lambda & \text{si } |v| < n \\ \pi(v) & \text{si } |v| = n. \end{cases}$$

Teorema 6.2. *(a) Si $z \in X^\infty$ es una secuencia de Bernoulli y $\overline{\phi}_{\mathfrak{U}} : X^\infty \to X^\infty$ es una función de medida acotada, producida por el autómata $\mathfrak{U}$ mediante una función de salida $\lambda : X \times S \to X^*$, entonces o bien z no pertenece al dominio de $\overline{\phi}_{\mathfrak{U}}$, o bien $\overline{\phi}_{\mathfrak{U}}(z)$ cumple la ley fuerte de los grandes números:*

$$\lim_{n\to\infty} \frac{1}{n} \|\{i \leq n : (\overline{\phi}_{\mathfrak{U}}(z))_i = x\}\| = 1/p \qquad (x \in X).$$

(b) Si $z \in X^\infty$ no es de Bernoulli, existe una función $\overline{\phi}_{\mathfrak{U}} : X^\infty \to X^\infty$ producida por un autómata finito computablemente monótona y de medida acotada, de modo tal que $\overline{\phi}_{\mathfrak{U}}(z)$ no satisface la ley fuerte de los grandes números.

Así es como las funciones parciales de medida acotada producidas por autómatas finitos representan propiedades invariantes de las secuencias normales.

$\overline{\phi}_{\mathfrak{U}}$ se dice de *medida invariante* cuando para todo $M \subseteq X^\infty$ medible

$$\overline{\mu}(\overline{\phi}_{\mathfrak{U}}^{-1}(M)) = \overline{\mu}(M)$$

y computablemente monótona cuando existe una función total computable $h : \mathbb{N} \to \mathbb{N}$ tal que para todo z del dominio de $\overline{\phi}_{\mathfrak{U}}$ vale

$$n \geq h(i) \Rightarrow |\overline{\phi}_{\mathfrak{U}}(z(n))| \geq i.$$

Demostración. (a) Sea $z \in X^\infty$ una secuencia de Bernoulli perteneciente al dominio de $\overline{\phi}_{\mathfrak{A}}(z)$. Muéstrese como en la demostración del teorema 4.1 que puede ceñirse la prueba a los autómatas fuertemente conexos. Del lema 4.5 se sigue que cada $x \in X$ tiene, en cada posible estado $s \in S$, una frecuencia fija en el límite. En consecuencia, también tiene límite la frecuencia de x en $\overline{\phi}_{\mathfrak{A}}(z)$. Sea K dicho límite. Si $K \neq \frac{1}{p}$, entonces $\overline{\phi}_{\mathfrak{A}}(z)$ no puede ser una secuencia de Bernoulli para ninguna z que lo sea. Es decir, la preimagen de un conjunto de medida 0 contiene al conjunto de las secuencias de Bernoulli, de medida 1. Por lo tanto $\overline{\phi}_{\mathfrak{A}}(z)$ no es acotado por medida, en contradicción con la hipótesis, y se sigue la afirmación.

(b) La recíproca se demuestra sin mayor dificultad (Agafonov [1]). □

Referencias

[1] V. N. Agafonov. Normal sequences and finite automata. *Soviet Math. Dokl.*, 9:324–325, 1968. Traducción inglesa.

[2] K. H. Böhling and K. Indermark. *Endliche Automaten I.* Mannheim: BI, 1969.

[3] G. J. Chaitin. On the length of programs for computing finite binary sequences. *Journal ACM*, 13:547–569, 1966.

[4] K. L. Chung. *Markov chains with stationary transition probabilities.* Berlin–Göttingen–Heidelberg: Springer, 1967.

[5] A. H. Copeland. Admissible numbers in the theory of probability. *Amer. Journ Math.*, 50:535–552, 1928.

[6] J. L. Doob. Note on probability. *Annals of Math.*, 37:363–367, 1936.

[7] G. Hotz and H. Walter. *Automatentheorie und formale Sprachen.* Mannheim: BI, 1969.

[8] A. N. Kolmogorov. Drei zugänge zur definition des begriffs "informationsgehalt". *Probl. peredaci informacii*, 1:3–11, 1965.

[9] D. W. Loveland. A variant of the kolmogorov concept of complexity. *Inform. Control*, 15:510–526, 1969.

[10] P. Martin-Löf. The definition of random sequences. *Inform. Control*, 6:602–619, 1966.

[11] K. Popper. *Logik der forschung: zur erkenntnistheorie der modernen naturwissenschaft*, volume 9 of *Schriften zur wissenschaftlichen Weltauffassung.* Wien: Springer, 1935.

[12] H. Reichenbach. *Wahrscheinlichkeitslehre.* Leiden: Sijthoff, 1935.

[13] C. P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Lecture Notes.* Berlin–Heidelberg–New York: Springer, 1971.