Z. Wahrscheinlichkeitstheorie verw. Geb. 19, 225–230 (1971)

Complexity Oscillations in Infinite Binary Sequences

PER MARTIN-LÖF

We shall consider finite and infinite binary sequences obtained by tossing an ideal coin, failure and success being represented by 0 and 1, respectively. Let $s_n = x_1 + x_2 + \cdots + x_n$ be the frequency of successes in the sequence $x_1 x_2 \ldots x_n$. Then, for an arbitrary but fixed n, we know that the deviation of s_n from its expected value $n/2$ is of the order of magnitude $\sqrt{n}$ provided we neglect small probabilities. On the other hand, if we consider the initial segments of one and the same infinite sequence $x_1 x_2 \ldots x_n \ldots$, the law of the iterated logarithm tells us that from time to time the deviation $s_n - n/2$ will be essentially bigger than $\sqrt{n}$, the precise order of magnitude being $\sqrt{n \log \log n}$. In other words, there will be ever recurring moments n when the initial segment $x_1 x_2 \ldots x_n$, considered as an element of the population of all binary sequences of the fixed length n, is highly non random.

According to Martin-Löf 1966, the conditional complexity $K(x_1 x_2 \ldots x_n | n)$ in the sense of Kolmogorov 1965 may be regarded as a universal measure of the randomness of the sequence $x_1 x_2 \ldots x_n$ considered as an element of the population of all binary sequences of length n, and, if we, to be more precise, define the sequence $x_1 x_2 \ldots x_n$ to be random on the level $\varepsilon = 2^{-c}$ if $K(x_1 x_2 \ldots x_n | n) \geqq n - c$, then the proportion of the population made up by the elements that are random on the level ε is greater than $1 - \varepsilon$. We shall show that the phenomenon described in the previous paragraph is general in the sense that it occurs when the randomness of $x_1 x_2 \ldots x_n$ is measured by $K(x_1 x_2 \ldots x_n | n)$ instead of the deviation of s_n from $n/2$, the latter representing just one aspect of the randomness of the sequence $x_1 x_2 \ldots x_n$.

Theorem 1. *Let f be a recursive function such that*

$$\sum_{n=1}^{\infty} 2^{-f(n)} = +\infty .$$

Then, for every binary sequence $x_1 x_2 \ldots x_n \ldots$,

$$K(x_1 x_2 \ldots x_n | n) < n - f(n)$$

for infinitely many n.

Note that, in contrast to the law of the iterated logarithm and related theorems of probability theory, the assertion of Theorem 1 holds for *all* sequences $x_1 x_2 \ldots x_n \ldots$ and not only with probability one.

In an earlier version of this paper (Martin-Löf 1965) the theorem was proved for the unconditional complexity $K(x_1 x_2 \ldots x_n)$ instead of the conditional complexity $K(x_1 x_2 \ldots x_n | n)$. Since $K(x_1 x_2 \ldots x_n | n) \leqq K(x_1 x_2 \ldots x_n) + c$ for some constant c but not vice versa, the earlier form of the theorem is slightly stronger than the present one.

Proof. We first replace f by a slightly more rapidly growing recursive function g such that

$$\sum_{n=1}^{\infty} 2^{-g(n)} = +\infty$$

and

$$g(n) - f(n) \uparrow +\infty \qquad \text{as } n \to \infty.$$

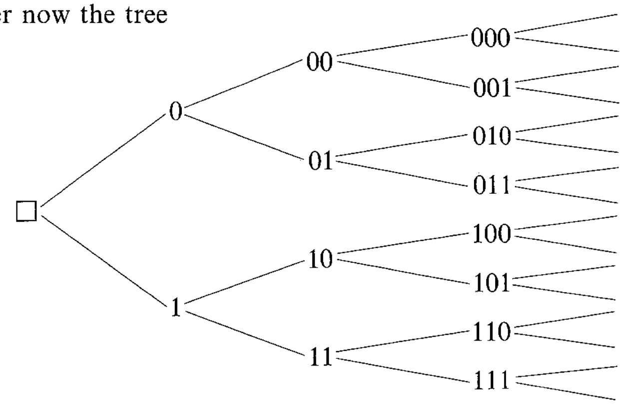
For example, put $n_0 = 0$ and let n_{m+1} be the smallest integer greater than n_m such that

$$\sum_{n_m+1}^{n_{m+1}} 2^{-f(n)} \geqq 2^m, \qquad m = 0, 1, \ldots.$$

We can then define g by putting

$$g(n) = f(n) + m \qquad \text{if } n_m < n \leqq n_{m+1}.$$

Consider now the tree



of all finite binary sequences, those of the same length being ordered as indicated from the top to the bottom with the extra convention that $00\ldots0$ is to follow after $11\ldots1$. For every $n = 0, 1, \ldots$ we shall define a certain set A_n of binary sequences of length n. A_0 is to contain the empty sequence □. Suppose now that

$$A_0, \ldots, A_m \neq \emptyset, \qquad A_{m+1} = \cdots = A_{n-1} = \emptyset$$

have been defined already, and let $x_1 x_2 \ldots x_m$ be the last sequence in A_m. If $g(n) < n$, then A_n is to contain the $2^{n-g(n)} - 1$ sequences of length n that follow immediately after $x_1 x_2 \ldots x_m 11\ldots1$, and, if $g(n) \geqq n$, then A_n is to be empty.

Letting μ denote the coin tossing measure, we have

$$\mu(A_n) = \begin{cases} 2^{-g(n)} - 2^{-n} & \text{if } g(n) < n \\ 0 & \text{if } g(n) \geqq n \end{cases}$$

for $n = 1, 2, \ldots$, so that, under all circumstances,

$$\mu(A_n) \geqq 2^{-g(n)} - 2^{-n}.$$

Consequently,

$$\sum_{n=1}^{\infty} \mu(A_n) = +\infty$$

which forces the sets $A_1, A_2, \ldots, A_n, \ldots$ to circle around the tree of finite binary sequences an infinite number of times. Therefore, if $x_1 x_2 \ldots x_n \ldots$ is a fixed infinite sequence, the initial segment $x_1 x_2 \ldots x_n$ will belong to A_n for infinitely many n.

Let $B(p, n)$ be an algorithm which enumerates A_n as the program p runs through $\square$, 0, 1, 00, 01, ... until A_n is exhausted. When the length of p is $\geqq n - g(n)$ we may let $B(p, n)$ remain undefined. Clearly,

$$K_B(x_1 x_2 \ldots x_n | n) < n - g(n)$$

if and only if $x_1 x_2 \ldots x_n$ belongs to A_n. On the other hand, by the fundamental theorem of Kolmogorov 1965,

$$K(x_1 x_2 \ldots x_n | n) \leqq K_B(x_1 x_2 \ldots x_n | n) + c$$

for some constant c, and g was constructed such that

$$g(n) \geqq f(n) + c$$

if $n > n_c$. Consequently, for every infinite sequence $x_1 x_2 \ldots x_n \ldots$,

$$K(x_1 x_2 \ldots x_n | n) < n - f(n)$$

for infinitely many n as was to be proved.

The construction carried out in the course of the proof is similar to one used by Borel 1919 in connection with a problem of diophantine approximations.

Theorem 2. *Let f be such that*

$$\sum_{n=1}^{\infty} 2^{-f(n)} < +\infty.$$

Then, with probability one,

$$K(x_1 x_2 \ldots x_n | n) \geqq n - f(n)$$

for all but finitely many n.

Proof. The number of sequences of length n for which

$$K(x_1 x_2 \ldots x_n | n) < n - f(n)$$

is less than $2^{n-f(n)}$. Thus, the probability that this inequality is satisfied is less than $2^{-f(n)}$, and the theorem now follows from the lemma of Borel and Cantelli.

Theorem 3. *Let f be a recursive function such that*

$$\sum_{n=1}^{\infty} 2^{-f(n)}$$

is recursively convergent. Then, if $x_1 x_2 \dots x_n \dots$ is random in the sense of Martin-Löf 1966,

$$K(x_1 x_2 \dots x_n | n) \geqq n - f(n)$$

for all but finitely many n.

Proof. That $\sum_{n=1}^{\infty} 2^{-f(n)}$ is recursively convergent means that there is a recursive sequence $n_1, n_2, \dots, n_m, \dots$ such that

$$\sum_{n_m+1}^{\infty} 2^{-f(n)} \leqq 2^{-m}, \qquad m = 1, 2, \dots.$$

Let U_m be the union of all neighbourhoods $x_1 x_2 \dots x_n$ for which $n > n_m$ and $K(x_1 x_2 \dots x_n | n) < n - f(n)$. Since the latter relation is recursively enumerable, $U_1, U_2, \dots, U_m, \dots$ is a recursive sequence of recursively open sets. Furthermore,

$$\mu(U_m) < \sum_{n_m+1}^{\infty} 2^{-f(n)} \leqq 2^{-m}$$

so that $\bigcap_{m=1}^{\infty} U_m$ is a constructive null set in the sense of Martin-Löf 1966 and hence contained in the maximal constructive null set whose elements are precisely the non random sequences.

Let f be a (not necessarily recursive) function such that

$$\sum_{n=1}^{\infty} 2^{-f(n)} < +\infty.$$

Then, the set of all sequences $x_1 x_2 \dots x_n \dots$ such that

$$K(x_1 x_2 \dots x_n | n) \geqq n - f(n)$$

for all but finitely many n is not measurable in the sense of Brouwer 1919, except in the trivial case when $n - f(n)$ is bounded. Suppose namely that it were Brouwer measurable. Its measure in Brouwer's sense would then have to equal one and, in particular, be positive. Hence, it would contain a recursive sequence $e_1 e_2 \dots e_n \dots$. But for a recursive sequence $e_1 e_2 \dots e_n \dots$ there exists a constant c such that

$$K(e_1 e_2 \dots e_n | n) \leqq c$$

for all n. On the other hand, $K(e_1 e_2 \dots e_n | n) \geqq n - f(n)$ for all but finitely many n so that $n - f(n)$ must be bounded.

Theorem 4. *With probability one, there exists a constant c such that*

$$K(x_1 x_2 \dots x_n | n) \geqq n - c$$

for infinitely many n.

Proof. Let A_{cn} denote the set of infinite sequences $x_1 x_2 \dots x_n \dots$ for which $K(x_1 x_2 \dots x_n | n) \geqq n - c$. Then

$$\mu\left(\bigcup_{n=m}^{\infty} A_{cn}\right) \geqq \mu(A_{cm}) > 1 - 2^{-c}$$

so that

$$\mu\left(\bigcap_{m=1}^{\infty}\bigcup_{n=m}^{\infty}A_{cn}\right)\geqq 1-2^{-c}.$$

Consequently,

$$\mu\left(\bigcup_{c=1}^{\infty}\bigcap_{m=1}^{\infty}\bigcup_{n=m}^{\infty}A_{cn}\right)=1$$

as was to be proved.

Theorem 5. *If there exists a constant c such that*

$$K(x_1 x_2 \dots x_n|n)\geqq n-c$$

for infinitely many n, then the sequence $x_1 x_2 \dots x_n \dots$ *is random in the sense of Martin-Löf* 1966.

Proof. Let $m_U(x_1 x_2 \dots x_n)$ denote the critical level of $x_1 x_2 \dots x_n$ with respect to the universal sequential test constructed by Martin-Löf 1966. Since a sequential test is so much more a test without the sequentiality condition, there is a constant c such that

$$m_U(x_1 x_2 \dots x_n)\leqq m(x_1 x_2 \dots x_n)+c$$

where $m(x_1 x_2 \dots x_n)$ denotes the non sequential critical level. On the other hand, $m(x_1 x_2 \dots x_n)$ and $n-K(x_1 x_2 \dots x_n|n)$ differ at most by a constant. Consequently,

$$m_U(x_1 x_2 \dots x_n)\leqq n-K(x_1 x_2 \dots x_n|n)+c$$

for some other constant c so that

$$\lim_{n\to\infty} m_U(x_1 x_2 \dots x_n)\leqq \liminf_{n\to\infty}\left(n-K(x_1 x_2 \dots x_n|n)\right)+c.$$

Thus, if the assumption of the theorem

$$\liminf_{n\to\infty}\left(n-K(x_1 x_2 \dots x_n|n)\right)<+\infty$$

is satisfied, then

$$\lim_{n\to\infty} m_U(x_1 x_2 \dots x_n)<+\infty$$

which means precisely that the sequence $x_1 x_2 \dots x_n \dots$ is random.

Combining Theorem 3 and Theorem 5, we arrive at the following conclusion. If f is a recursive function such that $\sum_{n=1}^{\infty} 2^{-f(n)}$ converges recursively and

$$K(x_1 x_2 \dots x_n|n)\geqq n-c$$

for some constant c and infinitely many n, then

$$K(x_1 x_2 \dots x_n|n)\geqq n-f(n)$$

for all but finitely many n. This result, which shows the relation between the upward and downward oscillations of the complexity, was announced without proof by Martin-Löf, 1965.

References

Borel, É.: Sur la classification des ensembles de mesure nulle. Bull. Soc. math. France **47**, 97–125 (1919).

Brouwer, L. E. J.: Begründung der Mengenlehre unabhängig vom logischen Satz vom ausgeschlossenen Dritten. Zweiter Teil. Verhdl. Nederl. Akad. Wet. Afd. Natuurk. Sect. I, **12**, 7, 3–33 (1919).

Kolmogorov, A. N.: Three approaches to the definition of the notion "amount of information" [Russian]. Probl. Peredači Inform. **1**, 3–11 (1965).

Martin-Löf, P.: On the oscillation of the complexity of infinite binary sequences [Russian]. Unpublished (1965).

– The definition of random sequences. Inform. and Control **9**, 602–619 (1966).

P. Martin-Löf
Barnhusgatan 4
S-111 23 Stockholm
Sweden

(Received March 16, 1970)