ISSN : 0007 — 4691

BULLETIN MATHÉMATIQUE

DE LA SOCIÉTÉ DES SCIENCES MATHÉMATIQUES
DE LA RÉPUBLIQUE SOCIALISTE DE ROUMANIE

Nouvelle série

TOME 26 (74), nr. 3, 1982

TIRAGE À PART

S. S. M.
BUCUREȘTI, 1982

ON PER MARTIN-LOF RANDOM SEQUENCES*

BY

CRISTIAN CALUDE and ION CHIȚESCU (Bucharest)

Our aim is to argue about the famous concept of random sequence, due to P. Martin-Löf [1]. This is done by producing examples of primitive recursive binary sequences which are random in the sense of P. Martin-Löf, thus violating our intuition.

Let $X = \{0,1\}$ and denote by X^* the free monoid generated by X, i.e. X^* consists of all finite strings $x = x_1x_2\ldots x_m$, where the x_i — s can be 0 or 1 and also the null string λ belongs to X^*.

For every x in X^*, $l(x)$ is the length of x, i.e. $l(x) = m$, in case $x = x_1x_2\ldots x_m$ and $l(\lambda) = 0$. For x and y in X^*, we write $x \subset y$ to denote the fact that x is an initial segment of y (we agree on the fact that $\lambda \subset x$ for every x in X^*). For every x in X^*, we define $x0$ and $x1$ as follows : if $x = x_1x_2\ldots x_m$, then $x0 = x_1x_2\ldots x_m0$ and $x1 = x_1x_2\ldots$ $\ldots x_m1$; if $x = \lambda$, then $x0 = 0$ and $x1 = 1$.

Now X^∞ is the set of all binary sequences, i.e. we can identify X^∞ to the set of all functions $h : N \to X$, where $N = \{0,1,2,\ldots\}$ is the set of natural numbers. Putting $h(i) = x_i$, the elements of X^∞ will be denoted by $\underline{x}$, i,e. $\underline{x} = x_0x_1\ldots x_m\ldots$ For $\underline{x}$ in X^∞ and n in N, $\underline{x}^n$ stands for the initial segment of length n, i.e. $\underline{x}^n = x_0x_1\ldots x_{n-1}$, if $n \geqslant 1$ and $\underline{x}^n = \lambda$, if $n = 0$. So $\underline{x}$ is in X^∞, but $\underline{x}^n$ is in X^*.

For every x in X^*, we define $xX^\infty = \{\underline{y} \in X^\infty / \underline{y}^n = x\}$, in the case when $n = l(x) > 0$; $\lambda X^\infty = X^\infty$. Let $\mathscr{A}$ be the σ-algebra generated by $\mathscr{P} = \{xX^\infty / x \in X^*\}$.

A computable probability distribution is a function $p : X^* \to [0, 1]$ having the following properties :

(i) $p(\lambda) = 1$,

(ii) $p(x) = p(x0) + p(x1)$, for all x in X^*,

(iii) p is computable (i.e. there exists a recursive function $\varphi : X^* \to N$ and a godelization (r_n) of a subset of all recursive reals in [0, 1], such that for every x in X^* we have $p(x) = r_{\varphi(x)}$).

Example 1. Take $p(x) = 2^{-l(x)}$.

---

* Communication presented at the Workshop on Recursion-Theoretic Aspects of Computer Science, Purdue University, May 19—21, 1981.

Example 2. Fix a natural number $i \geqslant 2$ and take $p(\lambda) = 1$ and

$$p(x0) = p(x) \cdot \left(1 - \frac{1}{(l(x)+2)^i}\right),$$

$$p(x1) = p(x) \cdot \frac{1}{(l(x)+2)^i},$$

for all x in X^*.

Example 3. Again fix a natural number $i \geqslant 2$ and take $p(\lambda) = 1$ and for all x in X^*,

$$\left.\begin{aligned} p(x0) &= p(x) \cdot \left(1 - \frac{1}{(l(x)+2)^i}\right), \\ p(x1) &= p(x) \cdot \frac{1}{(l(x)+2)^i}, \end{aligned}\right\} \quad \text{if } l(x) \text{ is even}$$

$$\left.\begin{aligned} p(x0) &= p(x) \cdot \frac{1}{(l(x)+2)^i}, \\ p(x1) &= p(x) \cdot \left(1 - \frac{1}{(l(x)+2)^i}\right) \end{aligned}\right\} \quad \text{if } l(x) \text{ is odd}$$

Let $\pi : \mathscr{A} \to [0,1]$ be the probability induced by p, which is given by the conditions $\pi(xX^\infty) = p(x)$, for every x in X^*. Note that in the case of Example 1 we got the usual product probability.

Fix a computable probability distribution p. *A p-sequential P. Martin-Löf test* (*p-test*) is a set $U \subset N \times X^*$, subject to the following restrictions:

(1) U is recursively enumerable,

(2) For all natural numbers $m, n \geqslant 1$, and for all x, y in X^* we have the implication:

$$(m \geqslant n \text{ and } x \subset y \text{ and } (m, x) \in U) \Rightarrow (n, y) \in U$$

$$\sum_{\substack{(m,x)\in U \\ l(x)=n}} p(x) < 2^{-m}, \tag{3}$$

for all natural numbers $m \geqslant 1$ and n.

Note that in the case of Example 1, condition (3) can be written as follows:

$$\text{card } \{x \in X^* / (m, x), \in U, l(x) = n\} < 2^{n-m}, \tag{3'}$$

for all natural numbers $m \geqslant 1$ and n.

Notice that in the third paragraph of his paper [1] (page 610) P. Martin-Löf works in the particular case of Example 1, and condition (3) is stated in the form

$$\text{card } \{x \in X^* / (m, x) \in U, l(x) = n\} \leqslant 2^{n-m}, \tag{3''}$$

for all natural numbers $m \geqslant 1$ and n. The author explains in the fourth paragraph (page 613) why he changed the inequality into a strict one.

Let U be a p-test. For every natural $m \geqslant 1$ put $U_m = \{x \in X^* / (m, x) \in U\}$. It is obvious that $U_1 \supset U_2 \supset U_3 \ldots$. One can define a (finite) function $m'_U : U_1 \to N$ by $m'_U(x) = \max\{m \in N / (m, x) \in U\}$. Extend m'_U to a function $m_U : X^* \to N$, putting $m_U(x) = m'_U(x)$, in case x is in U_1 and $m(x) = 0$, otherwise. It is obvious that for all x and y we have $0 \leqslant m_U(x) \leqslant l(x)$ and, in case $x \subset y$, $m_U(x) \leqslant m_U(y)$.

P. Martin-Löf [1] asserts that for every computable probability distribution p there exists a *universal p-test*, i.e. a p-test W having the property that for every p-test U there exists a natural number c (depending upon W and U) such that $U_{m+c} \subset W_m$, for all natural number $m \geqslant 1$.

Taking such a W it is seen that the sequence $m_W(\underline{x}^n))_n$ is increasing, for every x in X^∞, therefore $\lim_n m_W(\underline{x}^n)$ exists, being a natural number or being infinite. Moreover, one can prove that in case W' and W'' are two universal p-tests and x is in X^∞, we have the equivalence

$$\lim_n m_{W'}(\underline{x}^n) < \infty \text{ iff } \lim_n m_{W''}(\underline{x}^n) < \infty$$

The last equivalence enables us to call a binary sequence x *p-random* (*in the sense of P. Martin-Löf*) if

$$\lim_n m_{W'}(\underline{x}^n) < \infty$$

for some universal p-test (and hence for all such tests).

An example of *a* p-random sequence (for the function p in Example 1) is given in [3].

In [1] proofs are merely sketched. P. Martin-Löf proves that in the case of the product probability (Example 1) the set of p-random sequences has measure equal to one.

But he also claims there that this nice result holds for every computable probability distribution p. *This assertion seems very unclear to us, and here is our motivation.*

Consider first the Example 2. Put $\underline{0} = 00\ldots0\ldots \in X^\infty$(i.e. the zero sequence). We have $\{0\} = \bigcap_{n=1}^{\infty} A_n$, where $A_1 = 0\ X^\infty$, $A_2 = \infty\ X^\infty$, $A_3 = 000\ X^\infty$, a.s.o. Hence $\pi(\{0\}) = \lim_n \pi(A_n) = \lim_n \prod_{k=0}^{n-1} \left(1 - \frac{1}{(k+2)^i}\right) = \prod_{k=2}^{\infty} \left(1 - \frac{1}{k^i}\right)$, the product being absolutely convergent. In case i = 2 it is seen that $\prod_{k=2}^{\infty} \left(1 - \frac{1}{k^2}\right) = \frac{1}{2}$, therefore $\pi(\{0\}) \geqslant \frac{1}{2}$. Consequently, if P. MARTIN-LÖF's results hold, then for all p as in Example 2, the sequence $\underline{0}$ must be p-random.

One might argue that the probability distributions from Example 2 are too ,,*bad*'', because they produce constant sequences of strictly positive measure. This is not the case for the probability distributions in Example 3. The reader may convince himself that all binary almost constant sequences have measure zero.
(The sequence $\underline{x}_i = x_0x_1\ldots x_m\ldots$ is almost constant provided there exists a natural number n deepending upon $\underline{x}$ such that $x_n = x_{n+1} = \ldots$). This is seen using the divergence of the infinite products

$$\left(1 - \frac{1}{2^i}\right)\left(\frac{1}{3^i}\right)\left(1 - \frac{1}{4^i}\right)\left(\frac{1}{5^i}\right)\ldots$$

and

$$\left(\frac{1}{2^i}\right)\left(1 - \frac{1}{3^i}\right)\left(\frac{1}{4^i}\right)\left(1 - \frac{1}{5^i}\right)\ldots$$

We produce another ,,pathological'' example within the framework of Example 3, namely the primitive recursive binary sequence *alt*=01010101 (i.e. $\underline{alt} = x_0x_1\ldots$ with $x_i = 0$, if i is even and $x_i = 1$, if i is odd). One can see that $\underline{alt} = \bigcap_{n=1}^{\infty} B_n$, where B_1=0X^∞, B_2=01X^∞, B_3=010 X^∞, a.s.o. Consequently, $\pi(\{\underline{alt}\}) = \lim_m \pi(B_m) = \prod_{n=2}^{\infty} \left(1 - \frac{1}{n^i}\right) \geqslant \frac{1}{2}$. So, if P. MARTIN-LÖF's results hold, $\underline{alt}$ mus be p-random for all p in Example 3.

The above examples of ,,*random sequences*'' having extremely low complexity violate our intuitoin.

We conclude with a remark concerning C. P. Schnorr's ideas in his expository paper [2], where he asks for the enlargement of the class of random sequences : ,,*We argue that the rec. null-sets might be a too general class of null-sets*'' (page 198). For the convenience, we remind that C. P. Schnorr states that a binary sequence is p-random iff it is not contained in any recursive p-null set (page 197). Our examples contrast with Schnorr's requirements.

Received 11.II.1982

REFERENCES

1. P. MARTIN-LÖF, *The Definition of Random Sequences, Information and Control* 19 (1966), 602—619.
2. C. P. SCHNORR, *A Survey of the Theory of Random Sequences*, Butts and Hintikka (eds.), *Basic Problems in Methodology and Linguistics*, D. TReidel Publishing Company, Dordrecht-Holland, 1977, 193—211.
3. A. ZVONKIN, L. LEVIN, *The Complexity of Finite Objects and the Development of the Concepts of Information and Randomness by Means of the Theory of Algorithms, Uspehi Mat. Nauk*, XXV, 156 (1970), 85—127, (Russian).