Kybernetika

Ivan Kramosil; Jan Šindelář

Infinite pseudo-random sequences of high algorithmic complexity

Kybernetika, Vol. 20 (1984), No. 6, 429--437

Persistent URL: `http://dml.cz/dmlcz/124602`

KYBERNETIKA — VOLUME 20 (1984), NUMBER 6

INFINITE PSEUDO-RANDOM SEQUENCES OF HIGH ALGORITHMIC COMPLEXITY

IVAN KRAMOSIL, JAN ŠINDELÁŘ

A finite sequence of letters over a finite alphabet is defined as pseudo-random, if its length does not exceed "too much" the length of the shortest program which generates the sequence in question using a fixed universal Turing machine. It has been proved (cf. [3]), that if the condition "not to exceed too much" is specified by "not to differ by more than an additive constant", then pseudo-random sequences possess some important and natural properties of true-random sequences, namely, the relative frequencies of occurrences of letters and blocks of letters tend to the uniform (equiprobable) distribution with the length of the pseudo-random sequence increasing. Here we prove, that these properties are preserved also in the case when the difference between the length n of the sequence and that of the shortest generating program is majorized not by a constant but, more generally, by an $o(n)$-function. This result enables to define an infinite pseudo-random sequence preserving the properties of infinite sequence of finite pseudo-random sequences defined in [3].

1. INTRODUCTION

In this first attempts to build theoretical and methodological foundations of probability and statistics considered and conceived as formalized mathematical theories, von Mises (cf. [1]) relied on the notion of random sequence (collective, in his terms) as the basic stone of all the construction. The weak points of this notion, as defined by von Mises, could be used and have been used in order to demonstrate the advantages of the classical Kolmogorov axiomatic and set-theoretic approach to probability theory. This theory resigned, from its very beginning, to questions concerning the randomness of an individualized sequence of results (of statistical observations or experiments), proclaiming such a question to be illegitimate.

Hence, the problem what it might be a random sequence of results or outputs was not solved, but its importance significantly increased with the application of computers in the domain of probabilistical and statistical computational procedures, e.g. decision or estimation making ones. The need for a simple and rapid enough source of random inputs requested by such procedures gave arise the idea of pseudo-random sequences of numbers, i.e. sequences generated in a strictly deterministic way, using an appropriate computer-aided program, but capable to simulate successfully the true-random inputs (numbers), at least from the point of view of statistical qualities of the obtained results. However, the classical probability theory and mathematical statistics were not able to offer a theoretical background for such a conception of pseudo-randomness, and this is why the greatest part of investigations and applications of pseudo-random numbers has been based on empirical level argumentation and ideas.

Kolmogorov himself (cf. [2]), as well as some other authors (Solomonoff, Martin-Löf, Schnor, Chaitin et al.) have proposed and developed, since 1965, the idea according to which a finite sequence of symbols or letters should be defined as pseudo-random supposing that the shortest program which generates this sequence, using a fixed universal Turing machine, is not "substantially" shorter than the generated sequence itself. This idea will be also our starting point, in what follows, let us describe and investigate it more formally and in more details.

2. LIMIT PROPERTIES OF PSEUDO-RANDOM SEQUENCES

Let $A = \{a_1, a_2, \ldots, a_c\}$, $c \geqq 2$, be a finite set (alphabet) of abstract symbols (letters), let U_A be a fixed universal Turing machine which works over finite sequences (words, strings) of letters from A, let $A^* = \bigcup_{n=0}^{\infty} A^n$ denote the set of all such sequences. Let $p, S, \mathbf{x} \in A^*$, then $U_A(p, S) = \mathbf{x}$ means that if the concatenation $p * S$ is written on the input tape of U_A, and the machine is in its initial state reading the left-most symbol of $p * S$, then U_A terminates, eventually, its work over $p * S$ with $\mathbf{x}$ inscribed on the output tape (which may be identical with the input one).

Definition 1. Let $\mathbf{x}, S \in A^*$, then the algorithmic complexity $K_{U,A}(\mathbf{x}/S)$ of $\mathbf{x}$ under the condition (a priori information) S and with respect to U_A is defined by

(1)
$$K_{U,A}(\mathbf{x}/S) = \min \{l : l \in \mathcal{N}, l = l(p), p \in A^*, U_A(p, S) = \mathbf{x}\}, \quad \min(\emptyset) = \infty,$$

where $\mathcal{N} = \{0, 1, 2, \ldots\}$, and $l(p) = n$ iff $p \in A^n$.

Definition 2. Let $\mathbf{x}$, S and U_A be as above, let $f: \mathcal{N} \to \mathcal{N}$ be a total function. The sequence $\mathbf{x} \in A^*$ is called *f-(pseudo)-random*, if

$$K_{U,A}(\mathbf{x}/\bar{l}(\mathbf{x})) \geqq l(\mathbf{x}) - f(l(\mathbf{x})), \tag{2}$$

where $\bar{l}(\mathbf{x}) \in A^*$ is a sequence expressing and coding the length $l(\mathbf{x})$ of $\mathbf{x}$, if not danger of misunderstanding menaces, we shall write $l(\mathbf{x})$ instead of $\bar{l}(\mathbf{x})$ even in such cases.

There are at most c^i programs of the length i, so at most $\sum_{i=0}^{l(\mathbf{x})-1} c^i = (c-1)^{-1}$.

. $(c^{l(\mathbf{x})} - 1) < c^{l(\mathbf{x})}$ sequences can be generated by a program shorter than $l(\mathbf{x})$, hence, (2) hold for at least one $\mathbf{x}$ from each A^n and Definition 2 is not vacuous neither if $f(n) = 0$ for all $n \in \mathcal{N}$. On the other hand, there exists $c_U \in \mathcal{N}$ such that, for all $\mathbf{x}, S \in A^*$, $\mathrm{K}_{U,A}(\mathbf{x}/S) \leqq l(\mathbf{x}) + c_U$ (there is a program, independent of $\mathbf{x}$ and S, erasing S and leaving $\mathbf{x}$ on the tape unchanged). In what follows, we shall investigate the case of f-random sequences with $f \in o(n)$, i.e., such that $\lim_{n\to\infty} n^{-1} f(n) = 0$; it is a natural and straightforward generalization of T-random sequences (with $f(n) \equiv T$ for all $n \in \mathcal{N}$), investigated in [3] or elsewhere.

Let $\mathbf{x} = x_1 x_2 \dots x_n \in A^n$, set, for each $a \in A$,

$$fr(a, \mathbf{x}) = n^{-1} \operatorname{card} \{i\colon i \in \mathcal{N}^+, i \leqq n, x_i = a\} . \tag{3}$$

Set, for $m \in \mathcal{N}^+$,

$$B(m, \mathbf{x}) = \langle x_1 x_2 \dots x_m \rangle \langle x_{m+1} \dots x_{2m} \rangle \dots \langle x_{(k-1)m+1} \dots x_{km} \rangle \in (A^m)^k \subset \\ \subset (A^m)^* , \tag{4}$$

where $k = \max \{k_1\colon k_1 \in \mathcal{N}, k_1 m \leqq n\}$. Hence, $B(m, \mathbf{x})$ is nothing else than $\mathbf{x}$ taken as a sequence of blocks of letters of the length m, neglecting the tail of $\mathbf{x}$, if n is not divisible by m. For $\alpha \in A^m$, we may immediately extend (3) to define $fr(\alpha, B(m, \mathbf{x}))$, which expresses the relative frequency of occurrences of the block $\alpha \in A^m$ in $\mathbf{x}$, clearly, $\mathbf{x} = B(1, \mathbf{x})$, $B(m, \mathbf{x}) = \Lambda$ (the empty sequence) for $m > n$.

If $\mathbf{x}$ is f-random and $f \in o(n)$, then the relative frequency of occurrences of all letters and blocks of letters in $\mathbf{x}$ tends to the uniform distribution with $l(\mathbf{x})$ increasing, as the following theorem proves. This property is an obligatory one which $\mathbf{x}$ should satisfy to be able to simulate a true-random statistically independent repeated ɹandom sample from the equiprobable distribution over A.

Theorem 1. Let $f\colon \mathcal{N} \to \mathcal{N}$, $f \in o(n)$, be a total function, let $\mathcal{S} = \langle S_1, S_2, \dots \rangle$, $S_i \in A^i$, be a sequence of f-random sequences over A, i.e. for each $n \in \mathcal{N}^+$, $l(S_n) = n$, $K_{U,A}(S_n/n) \geqq n - f(n)$. Then

$$\lim_{n\to\infty} fr(\alpha, B(m, S_n)) = c^{-m}$$

for all $m \in \mathcal{N}^+$ and $\alpha \in A^m$ (recall that $c = \operatorname{card} A$).

Proof. First, let us prove (5) for $m = 1$, i.e., let us prove that $\lim_{n\to\infty} fr(a, S_n) = c^{-1}$ for each $a \in A = \{a_1, a_2, \dots, a_c\}$. Set $r_1^n = fr(a_1, S_n)$, then r_1^n is an infinite sequence of reals belonging to a compact set (the closed unit interval $\langle 0, 1 \rangle$). Hence, there exists a convergent subsequence $r_1^{n(i)}$, $i = 1, 2, \dots$. Set $r_2^i = fr(a_2, S_{n(i)})$ and apply the same argument to obtain a convergent subsequence $r_2^{n(i(k))}$. Set $r_3^k = fr(a_3, S_{n(i(k))})$, and proceed in the same way for all the letters from A. Finally, we obtain a subsequence $\mathcal{S}'$ of $\mathcal{S}$ such that the relative frequences of all letters in $\mathcal{S}'$ converge. Without any loss of generality we may suppose that $\mathcal{S}$ itself possesses this property, set $r_i = \lim_{n\to\infty} fr(a_i, S_n)$ for all $i \leqq c$, i.e. for all $a_i \in A$. The proof of (5) will be complete when proving, that if $r_i \neq c^{-1}$ for at least one $i \leqq c$, than S_n cannot be f-random for infinitely many values on n.

Take an S_n, let n_i, $i \leqq c$, be the numbers of occurrences of a_i in S_n, hence, $\lim_{n\to\infty} n^{-1}n_i = r_i$ and $\sum_{i=1}^{c} n_i = n$. There are

$$(6) \qquad R(n, n_1, n_2, \ldots, n_c) = \frac{n!}{n_1!\, n_2! \ldots n_c!}$$

n-tuples from A^n with the same absolute frequencies of $a_1, a_2, \ldots, a_c$ and these n-tuples can be effectively enumerated. In order to define S_n we need, hence, a number $w \leqq R(n, n_1, \ldots, n_c)$, a word $a_1 a_2 \ldots a_c$ of the length c defining the prescribed order of letters in A and, finally, the numbers $n_1, n_2, \ldots, n_c$. In other words, given $w \leqq \leqq R(n, n_1, \ldots, n_c)$, $a_1 a_2 \ldots a_c$, $n_1, n_2, \ldots, n_c$, a fixed program is able to generate S_n, given n. Using the alphabet A to encode the inputs, we obtain, that

$$(7) \qquad K_{U,A}(S_n/n) \leqq \log_c R(n, n_1, \ldots, n_c) + c + c \log_c n + const\,,$$

hence,

$$(8) \qquad n^{-1} K_{U,A}(S_n/n) \leqq n^{-1} \log_c R(n, n_1, \ldots, n_c) + n^{-1}c + n^{-1}c \log_c n + n^{-1}\, const\,,$$

as

$$(9) \qquad \lim_{n\to\infty} n^{-1}c = \lim_{n\to\infty} n^{-1}c \log n = \lim_{n\to\infty} n^{-1}\, const = 0\,,$$

the proof will be completed when proving that

$$(10) \qquad \lim_{n\to\infty} n^{-1} \log_c R(n, n_1, \ldots, n_c) \leqq \delta < 1\,,$$

supposing that $r_1, r_2, \ldots, r_c \neq \langle c^{-1}, c^{-1}, \ldots, c^{-1} \rangle$, as (2) implies that

$$(11) \qquad \lim_{n\to\infty} n^{-1} K_{U,A}(S_n/n) = 1$$

should hold for f-random sequences S_n.

Let $Q(n) \doteq n!$ in the sense that $\lim_{n\to\infty} Q(n)\,(n!)^{-1} = 1$, then

$$(12) \qquad \lim_{n\to\infty} \frac{\dfrac{Q(n)}{Q(n_1)\cdot\ldots\cdot Q(n_c)}}{\dfrac{n!}{n_1! \ldots n_c!}} = 1\,,$$

supposing that $\lim_{n\to\infty} n_i = \infty$ for all $i \leqq c$. This assumption may be accepted without any loss of generality, as if $n_i \leqq const$ for all $n \in \mathcal{N}$, then $n_i/n \to 0$ and this fact can be used in a shorter description of S_n (shortening by the multiplicative constant

$\log_c(c-1) < 1$, which excludes the possible f-randomness of S_n). Hence,

$$\lim_{n\to\infty} \log_c \frac{\dfrac{Q(n)}{Q(n_1)\cdot\ldots\cdot Q(n_c)}}{\dfrac{n!}{n_1!\ldots n_c!}} = 0\,, \tag{13}$$

$$\lim_{n\to\infty} \left|\log_c \frac{Q(n)}{Q(n_1)\ldots Q(n_c)} - \log_c \frac{n!}{n_1!\ldots n_c!}\right| = 0\,, \tag{14}$$

hence

$$\lim_{n\to\infty} \frac{1}{n} \log_c \frac{Q(n)}{Q(n_1)\ldots Q(n_c)} = \lim_{n\to\infty} \frac{1}{n} \log_c \frac{n!}{n_1!\ldots n_c!}\,. \tag{15}$$

Taking $Q(n) = \sqrt{(2\pi)}\, n^{n+1/2}\, \mathrm{e}^{-n}$(the Stirling approximation), we ibtain

$$\lim_{n\to\infty} \frac{1}{n} \log_c \frac{\sqrt{(2\pi)}\, n^{n+1/2}\, \mathrm{e}^{-n}}{\sqrt{(2\pi)^c}\, (\prod_{j=1}^{c} n_j^{n_j+1/2})\, \mathrm{e}^{-\sum_{j=1}^{c} n_j}} =$$

$$= \lim_{n\to\infty} \left[\frac{1}{n} \log_c \frac{\sqrt{(2\pi)}}{(\sqrt{(2\pi)^c}} + \frac{1}{n} \log_c \left(\frac{n^{n+1/2}}{\prod_{j=1}^{c} n_j^{n+1/2}}\right)\right] =$$

$$= \lim_{n\to\infty} \frac{1}{n} \log_c \frac{n^{n+1/2}}{\prod_{j=1}^{c} n_j^{n_j+1/2}} \leqq \lim_{n\to\infty} \frac{1}{n} \log_c \frac{n^{n+c/2}}{\prod_{j=1}^{c} n_j^{n_j+1/2}} =$$

$$= \lim_{n\to\infty} \frac{1}{n} \log_c \frac{n^{\sum_{j=1}^{c}(n_j+1/2)}}{\prod_{j=1}^{c} n_j^{n_j+1/2}} = -\lim_{n\to\infty} \frac{1}{n} \log_c \left(\prod_{j=1}^{c} \frac{n_j^{n_j+1/2}}{n^{n_j+1/2}}\right) =$$

$$= -\lim_{n\to\infty} \frac{1}{n} \sum_{j=1}^{c} \log_c \left(\frac{n_j}{n}\right)^{n_j+1/2} = -\lim_{n\to\infty} \prod_{j=1}^{c} \left(\frac{n_j + 1/2}{n}\right) \log_c \left(\frac{n_j}{n}\right) =$$

$$= -\sum_{j=1}^{c} \lim_{n\to\infty} \left(\frac{n_j}{n} + \frac{1}{2n}\right) \log_c \left(\lim_{n\to\infty} \frac{n_j}{n}\right) = -\sum_{j=1}^{c} r_j \log_c r_j =$$

$$= -(\log_2 c)^{-1} \sum_{j=1}^{c} r_j \log_2 r_j = \frac{H(r_1, r_2, \ldots, r_c)}{H(c^{-1}, c^{-1}, \ldots, c^{-1})}\,,$$

where $H(r_1, r_2, \ldots, r_c)$, $r_j = \lim_{n\to\infty} n_j n^{-1}$, is the entropy of the probability distribution $\langle r_1, r_2, \ldots, r_c\rangle$. It is a well-known fact that $H(r_1, r_2, \ldots, r_c) \leqq \log_2 c = H(c^{-1}, c^{-1}, \ldots \ldots, c^{-1})$, with equality holding iff $\langle r_1, r_2, \ldots, r_c\rangle = \langle c^{-1}, c^{-1}, \ldots, c^{-1}\rangle$. Hence, $\mathrm{H}(r_1, r_2, \ldots, r_c)\, (H(c^{-1}, \ldots, c^{-1}))^{-1} < 1$ and the assertion is proved for $m = 1$.

Let $m > 1$, let $\tilde{U}_A$ be the universal Turing machine U_A taken as a machine which works over the product alphabet A^m. Hence, for each $p, S, \mathbf{x} \in A^*$ the relation $U_A(p * S) = \mathbf{x}$ is interpreted as $U_{A^m}(B(m, p) * B(m, S)) = B(m, \mathbf{x})$. $\tilde{U}_{A^m}$ is, in general, nondeterministic, hence, $K_{\tilde{U},A^m}(\mathbf{x}/S) \leqq K_{U,A^m}(\mathbf{x}/S)$ for each universal Turing machine which works over $(A^m)^*$ and which extends $\tilde{U}_{A^m}$. Everything what can be effectively done over $(A^m)^*$ can be also performed over A^*, hence, the deterministic extension U_{A^m} of $\tilde{U}_{A^m}$ is universal Turing machine due to the Church thesis. Our theorem will be proved for $m > 1$ supposing that we find a function $g \colon \mathcal{N} \to \mathcal{N}$, $g(n) \in o(n)$, such that

$$(16) \qquad K_{\tilde{U},A^m}(B(m, S_n) \mid n) \geqq l_{A^m}(B(m, S_n)) - g(l_{A^m}(B(S_n))) = \\ = \operatorname{Int}(n/m) - g(\operatorname{Int}(n/m)),$$

where $\operatorname{Int}(a) = \max\{n : n \in \mathcal{N}, n \leqq a\}$, $a \in (-\infty, \infty)$.

To arrive at a contradiction, suppose that

$$(17) \qquad K_{U,A^m}(B(m, S_n) \mid n) < \operatorname{Int}(n/m) - g(\operatorname{Int}(n/m))$$

for infinitely many n's. Then there exists $p \in (A^m)^*$ such that $U_{A^m}(p, n) = B(m, S_n)$ and $l_{A^m}(p) < \operatorname{Int}(n/m) - g(\operatorname{Int}(n/m))$. Let $p_0 \in A^*$ be the tail of S_n when erasing $B(m, S_n)$ (if n is divisible by m, p_0 is empty), let P_0 be a fixed program which joints $B(m, S_n)$ with p_0 to obtain S_n. So $U_A(p * p_0 * P_0 * n) = S_n$ and

$$(18) \qquad K_{U,A}(S_n/n) < l_A(p) + m + l_A(\mathrm{P}_0) = \\ = m l_{A^m}(p) + m + l_A(P_0) < n' - mg(\operatorname{Int}(n/m)) + m + l_A(P_0).$$

Set $f^*(n) = \max\{f(j) : j \leqq n\}$, clearly, $f^*(n) \geqq f(n)$ and $f(n) \in o(n)$ implies $f^*(n) \in o(n)$. Moreover, f^* is non-decreasing. Take

$$(19) \qquad g(n) = m^{-1}(f^*(m(n+1)) + \log_2 n),$$

clearly,

$$(20) \qquad \lim_{n\to\infty} \frac{1}{n}\frac{1}{m}(f^*(m(n+1)) + \log_2 n) = \lim_{n\to\infty} \frac{1}{nm} f^*(m(n+1)) = \\ = \lim_{n\to\infty} \left(\frac{m(n+1)}{mn}\right) \frac{f^*(m(n+1))}{m(n+1)} = 0,$$

as $f^*(n) \in o(n)$. Now, we obtain,

$$mg(\operatorname{Int}(n/m)) - f(n) = f^*(m(\operatorname{Int}(n/m) + 1)) + m \log_2(\operatorname{Int}(n/m)) - f(n) \geqq \\ \geqq f^*(n) + m \log_2(\operatorname{Int}(n/m)) - f(n) \geqq m \log_2(\operatorname{Int}(n/m)) \to \infty \quad \text{for} \quad n \to \infty,$$

as $f^*(n) \geqq f(n)$. Hence, (18) contradicts the supposed f-randomness of S_n and (16) is proved for g given by (19). The proof of Theorem 1 is completed, as (16) implies that $\lim_{n\to\infty} fr(\alpha, B(m, S_n)) = c^{-m}$ when applying the result for $m = 1$ to the case of the alphabet A^m. □

3. INFINITE AND EFFECTIVELY DECIDABLE PSEUDO-RANDOM SEQUENCES

In this section we introduce some consequences to the main theorem presented above; these consequences may be divided into three groups.

(I) In [3], [4], and in the foregoing chapters of this paper, when speaking about limit values of relative frequencies, we always consider an *infinite sequences of finite sequences of* increasing lengths, not a *sequence of finite initial segments of an infinite sequence*. The reason is, that due to the result obtained by Martin-Löf (cf., e.g., [1]), if $f(n) \equiv T \in \mathcal{N}$ for all $n \in \mathcal{N}$, then there is *no* infinite sequence such that all its initial segments were f-random in the sense of Definition 2. More precisely, when $A = \{0, 1\}$ is a binary alphabet, Martin-Löf proved the following statement.

Fact 1. Let $f: \mathcal{N} \to \mathcal{N}$ be a total function, then the two following statements are equivalent:

(a) there exists an infinite sequence $S \in \{0, 1\}^\infty$ such that all its initial segments are f-random in the sense of Definition 2;

(b) $\sum_{i=0}^{\infty} 2^{-f(i)} < \infty$.

Theorem 2. (Corollary to Theorem 1.) Let $A = \{0, 1\}$, then there exists a total function $f: \mathcal{N} \to \mathcal{N}$ such that $f \in o(n)$ and all initial segments of S are f-random, hence, for each $m \in \mathcal{N}^+$, $\alpha \in A^m$, $\lim_{n \to \infty} fr(\alpha, B(m. S_n)) = 2^{-m}$, where S_n is the initial segment of length n.

Proof. Fix an ε, $0 < \varepsilon < 1$, clearly, there exists $m_0(\varepsilon)$ such that $\varepsilon m > 1 + \log_2 m$ for $m > m_0(\varepsilon)$. Hence, for $n > n_0(\varepsilon) = 2^{m_0(\varepsilon)}$,

$$\log_2 (n^\varepsilon) = \varepsilon \log_2 n > 1 + \log_2 \log_2 n = \log_2 (\log_2 n^2), \tag{21}$$

so that $n^\varepsilon > \log_2 n^2$ and $2^{-n^\varepsilon} < n^{-2}$ for $n > n_0(\varepsilon)$. But $\sum_{n=1}^{\infty} n^{-2} < \infty$, hence, $\sum_{n=0}^{\infty} 2^{-n^\varepsilon} < \infty$ as well. Moreover, $n^\varepsilon \in o(n)$ for $0 < \varepsilon < 1$ so that $f(n) = n^\varepsilon$ satisfies the conditions of Theorem 2. □

(II) The weak point of the notion of f-randomness, as defined above, consists in the fact that the algorithmic complexity $K_{U,A}(\mathbf{x}/S)$ is not recursive function of arguments $\mathbf{x}$, S (of their Gödel numbers, more precisely). Hence, no general algorithm exists to decide whether, given $\mathbf{x} \in A^*$ and f, $\mathbf{x}$ is f-random or not, even if f is recusrive (the existence of such algorithm would contradict the unsolvability of the halting problem for Turing machines). However, we may use the way of reasoning as in [4]. Let $\mathcal{O}(n, m)$ be an oracle (external with respect to the universal Turing machine U) which stops the work of U supposing that n steps are performed or more than m boxes are used, not counting the boxes occupied by the input sequence in the initial state. We write, for $\mathbf{x}, S, p \in A^*$, $n, m \in \mathcal{N}$, that $U_A(p, S; \langle n, m\rangle) = \mathbf{x}$, if U_A generates $\mathbf{x}$ from $p * S$ without the oracle's $\mathcal{O}(n, m)$ intervention, i.e. within the time and space limitations given by n and m. *Relative algorithmic complexity* $K^*_{U,A}(\mathbf{x}/S; \langle n,m\rangle)$ is defined by (1) with $U_A(p, S, \langle n, m\rangle)$, *relative* $\langle n, m, f\rangle$*-randomnes* is defined by (2) with $K_{U,A}(\mathbf{x}/l(\mathbf{x}))$ replaced by $K^*_{U,A}(\mathbf{x}/l(\mathbf{x}); \langle n, m\rangle)$.

As can be easily seen, relative $\langle n, m, f\rangle$-randomness is recursively decidable. The shortest program generating $\mathbf{x}$ works within finite time and space limitation, so there are, for each $\mathbf{x} \in A^*$, $a(\mathbf{x}) \in \mathcal{N}$, $b(\mathbf{x}) \in \mathcal{N}$ such that $K_{U,A}(\mathbf{x}/l(\mathbf{x})) = K^*_{U,A} \cdot . (\mathbf{x}/l(\mathbf{x}); \langle a(\mathbf{x}), b(\mathbf{x})\rangle)$. Finally, set for all $n \in \mathcal{N}$, $F(n) = \max\{a(\mathbf{x}): \mathbf{x} \in A^n\}$, $G(n) = = \max\{b(\mathbf{x}): \mathbf{x} \in A^n\}$.

Theorem 3. (Corollary to Theorem 1.) Let f be as in Theorem 1, let $\mathcal{S} = = \langle S_1, S_2, \ldots\rangle$, $S_i \in A^i$, be such that, for each $n \in \mathcal{N}^+$, $K^*_{U,A}(S_n/n; \langle F(n), G(n)\rangle) \geqq \geqq n - f(n)$. Then (5) holds for each $m \in \mathcal{N}$ and $\alpha \in A^m$.

Proof. An immediate consequence of Theorem 1, as $K_{U,A}(S_n/n) = K^*_{U,A}(S_n/n; \langle F(n), G(n)\rangle)$ for all $n \in \mathcal{N}^+$. □

The functions F and G are, of course, not recursive in general. In [4] we have proposed their constructive and recursive approximations (in the sense that Theorem 3 rests to hold) for the particular case when $f(n) \equiv T \in \mathcal{N}$. To obtain such approximations for the more general case of $f(n) \in o(n)$, we had to penetrate in more details into the nature of coding procedures used in information theory in order to keep the length of codes as short as possible. Such an investigation is not possible within the limited extent of this paper, let us postpone it to some other occasion.

(III) Let M be a finite set, $M = \{a_1, \ldots, a_N\}$, let $V \subset M$ be generated by a property which some of elements of M may posses, set $\mu(V, M) = N^{-1} \operatorname{card}(V)$. Let $c = = \operatorname{card}(A) \geqq N$ (using A^m instead of A for m great enough, if necessary), then the letters of an infinite sequence $S \in A^\infty$ can be interpreted as samples from M, neglecting those letters which do not correspond to elements from M (if $N < C$). Denote by $\mu^*(V, n)$ the relative frequency of the occurrences of letters, corresponding to symbols from V in the initial fragment S_n of S, then $\lim_{n\to\infty} \mu^*(V, n) = \mu(V, M)$ supposing that S is f-random for $f(n) \in o(n)$. This assertion is a single consequence of Theorem 1, using the same way of reasoning as in [4] for the case of constant $f(n)$. Moreover, we may apply to f-random sequences also the diagonalization technique in order to take a profit from f-random sequences when estimating the Borel measure of such subsets of a finite interval, which can be expressed as a finite union of intervals. This technique has been developed and studied in [4] for the case when $f(n) \equiv T$ for all $n \in \mathcal{N}$.

(Received March 31, 1984.)

REFERENCES

[1] T. L. Fine: Theories of Probability — An Examination of Foundations. Academic Press, New York—London 1973.

[2] A. N. Kolmogorov: Combinatoric foundations of information theory and probability calculus (in Russian). Uspehi matem. nauk *38* (1983), 4 (232), 27—36.

[3] I. Kramosil: On pseudo-random sequences over finite alphabets. Fundamenta Informaticae (to appear).

[4] I. Kramosil: Recursive classification of pseudo-random sequences. Supplement to Kybernetika *20* (1984), 1—36.

RNDr. Ivan Kramosil, CSc., Jan Šindelář, prom. mat., Ústav teorie informace a automatizace ČSAV (Institute of Information Theory and Automation — Czechoslovak Academy of Sciences), Pod vodárenskou věží 4, 182 08 Praha 8. Czechoslovakia.