$$
\text { PE } 4582 / 23.198 \% \text {, thiril }
$$

# INDEPENDENT AND IDENTICALLY DISTRIBUTED PSEUDO-RANDOM SAMPLES 

IVAN KRAMOSIL

The most simple algorithm used in order to transform a statistically independent identically distributed random sequence with equiprobable distribution into sequence with some given non-equiprobable distribution is proved to be applicable also in the case of pseudo-random sequences of high algorithmic complexity. The result enables to present a definition of i.i.d. pseudo-random sequences based immediately on the notion of algorithmic complexity.

## 1. INTRODUCTION

Consider an infinite, statistically independent and identically distributed (i.i.d.) sequence $X=X_{1}, X_{2}, \ldots$ of random variables, defined on a probability space $\langle\Omega, \mathscr{S}, P\rangle$ and taking their values in a finite set $\mathscr{A}=\left\{a_{1}, a_{2}, \ldots, a_{r}\right\}$. Set, for $i=$ $=1,2, \ldots, r$,

$$
\begin{equation*}
p_{i}=P\left(\left\{\omega: \omega \in \Omega, X_{1}(\omega)=a_{i}\right\}\right) \tag{1}
\end{equation*}
$$

then $p=\left\langle p_{1}, p_{2}, \ldots, p_{r}\right\rangle$ is the probability distribution of $X$ (corresponding to $X$ ). Realizations of i.i.d. random sequences with a given probability distribution play an important role in some stochastic computational decision making or simulation methods.
Let $\left\langle p_{1}, p_{2}, \ldots, p_{r}\right\rangle$ be a probability distribution over $\mathscr{A}$ and let $Y=Y_{1}, Y_{2}, \ldots$ be another i.i.d. sequence of random variables taking $\langle\Omega, \mathscr{S}, P\rangle$ into $\mathscr{B}=\left\{b_{1}, b_{2}, \ldots\right.$ $\left.\ldots, b_{m}\right\}$ such that $P\left(\left\{\omega: \omega \in \Omega, Y_{1}(\omega)=b_{j}\right\}\right)=m^{-1}$ for each $j \leqq m$. If there are $n_{1}, n_{2}, \ldots, n_{r} \in \mathscr{N}=\{0,1,2, \ldots\}$ such that $\sum_{i=1}^{r} n_{i}=m$ and $p_{i}=n_{i} / m, i=1,2, \ldots, r$, then a realization $Y_{1}(\omega), Y_{2}(\omega), \ldots$ of $Y$ can be transformed into a realization of i.i.d. $X$ with probability distribution $\left\langle p_{1}, p_{2}, \ldots, p_{r}\right\rangle$, setting simply $X_{i}(\omega)=a_{j}$ iff $Y_{i}(\omega)=b_{k}$ and $\sum_{s=0}^{j-1} n_{s}<k \leqq \sum_{s=0}^{j} n_{s}, n_{0}=0$. 260/ 88/n

The infinite sequences of elements from $\mathscr{B}$, the initial segments of which are combinatorially complicated enough lest to be generated by programs substantially shorter than their lengths, are known to be good simulations of realizations of i.i.d. random sequences with equiprobable distribution. The aim of this paper is to investigate whether, in which sense and in which measure, the sequences obtained from such pseudo-random sequences over $\mathscr{B}$ by the factorization transformation can simulate i.i.d. sequences over $\mathscr{A}$ with probability distribution $\left\langle p_{1}, p_{2}, \ldots, p_{r}\right\rangle$.

## 2. PSEUDO-RANDOM SEQUENCES AND FACTORIZATION

The sets $\mathscr{B}=\left\{b_{1}, \ldots, b_{m}\right\}$ and $\mathscr{A}=\left\{a_{1}, a_{2}, \ldots, a_{r}\right\}$ will be taken as non-empty sets of abstract elements with $m>r \geqq 2$. By $\mathscr{B}^{\infty}\left(\mathscr{B}^{*}\right.$, resp.) the set of all infinite (finite, resp.) sequences (strings, words) of elements from $\mathscr{B}$ will be denoted, similarly for $\mathscr{A}^{\infty}$ and $\mathscr{A}^{*} . \mathscr{B}^{*}=\bigcup_{n=0}^{\infty} \mathscr{B}^{n}$, where $\mathscr{B}^{0}=\{\Lambda\}$ and $\Lambda$ is the empty sequence.

Let $U(\mathscr{B})(U(\mathscr{A})$, resp. ) be a fixed universal Turing machine over the alphabet $\mathscr{B}(\mathscr{A}$, resp.); the reader is supposed to be familiar with this notion which is defined in [1], [7] or elsewhere. For $p, S, x \in \mathscr{B}^{*}, U(\mathscr{B})(p, S)=x$ means: having written the concatenation $p * S$ on the input tape of $U(\mathscr{B})$ and having initialized it, $U(\mathscr{B})$ eventually terminates its work with $x$ written on the output tape. The algorithmic complexity $K_{U(\mathscr{B})}(x \mid S)$ of $x$ given $S$ and w.r.t. to $U(\mathscr{B})$ is defined by

$$
\begin{equation*}
K_{U(\mathscr{B})}(x \mid S)=\min \left\{n:\left(\exists p \in B^{n}\right)(U(\mathscr{B})(p, S)=x)\right\} \tag{2}
\end{equation*}
$$

The set over which the minimalization is taken is always non-empty. In fact, there exists $c=c(U(\mathscr{B})) \in \mathscr{N}$ such that, for all $x, S \in \mathscr{B}^{*}, K_{U(\mathscr{B})}(x \mid S) \leqq l(x)+c$, where $l(x)=n$ iff $x \in \mathscr{B}^{n}$. As a more detailed introduction into the notion of algorithmic complexity and its properties, in the extend sufficient for our further reasonings, can serve [8] or [2], Chapter 5.

An infinite sequence $x=x_{1}, x_{2}, \ldots \in \mathscr{B}^{\infty}$ is called absolutely random, if there exists a total function $f: \mathscr{N} \rightarrow \mathscr{N}, f \in o(n)$ (i.e., $\lim _{n \rightarrow \infty} f(n) n^{-1}=0$ ), such that, for all $n$,

$$
\begin{equation*}
K_{U(\mathscr{B})}\left(x_{1}, \ldots, x_{n} \mid n\right) \geqq n-f(n) \tag{3}
\end{equation*}
$$

An immediate generalization of Martin-Löf result ([6], cf. also [2]), shows that absolutely random sequences exist iff, roughly speaking, $\sum_{i=0}^{\infty} r^{-f(i)}<\infty$ and if it is the case, then "almost all" infinite sequences (in the sense of product measure generated by equiprobable distribution on $\mathscr{B}$ ) satisfy (3).

Given $x \in \mathscr{B}^{\infty} \cup \mathscr{B}^{*}$ and $n_{1}, n_{2}, \ldots, n_{r} \in \mathscr{N}$ such that $\sum_{i=1}^{r} n_{i}=m$, we shall denote by $w\left(x, n_{1}, \ldots, n_{r}\right)$, or simply by $w(x)$, the sequence $y \in \mathscr{A}^{\infty} \cup \mathscr{A}^{*}$ defined by the
factorization algorithm described above (i.e., $l(y)=l(x), y_{i}=a_{j}$ iff $x_{i}=b_{k}$ and $\left.\sum_{s=0}^{j-1} n_{s}<k \leqq \sum_{s=0}^{j} n_{s}, n_{0}=0\right)$.

For $x \in \mathscr{B}^{\infty}$, which is absolutely random, the relative frequencies of occurrences of particular letters or blocks of letters tend to equiprobable distribution. In symbols, if $B(k, x)=\left\langle x_{1}, \ldots, x_{k}\right\rangle,\left\langle x_{k+1}, \ldots, x_{2 k}\right\rangle, \ldots \in\left(\mathscr{B}^{k}\right)^{\infty}$, if $B(k, x)[n]$ denotes the initial segment of length $n$ (w.r. to $\mathscr{B}^{k}$ ) of $B(k, x)$ and if $f r(z, b)$ denotes the relative frequency of occurrences of $b$ in $z \in \mathscr{B}^{*}$, then for each $k \in \mathscr{N}^{+}$and each $\alpha \in \mathscr{B}^{k}$,

$$
\begin{equation*}
\left.\lim _{n \rightarrow \infty} f r_{( }^{\prime} \boldsymbol{B}(k, x)[n], \alpha\right)=m^{-k} . \tag{4}
\end{equation*}
$$

Hence, if $x$ is absolutely random, then for each $j \leqq r$,

$$
\begin{equation*}
\lim _{n \rightarrow \infty} f r\left(w(x)[n], a_{j}\right)=n_{j} / m=p_{j}, \tag{5}
\end{equation*}
$$

as follows immediately from the factorization algorithm ((4) is proved in [3] or [5]). Of course, $w(x)$ need not be absolutely random sequence w.r. to $\mathscr{A}$ and, in fact, it is not, supposing that $\left\langle p_{1}, \ldots, p_{r}\right\rangle \neq\left\langle r^{-1}, r^{-1}, \ldots, r^{-1}\right\rangle$, as the following construction proves.
Let $y \in \mathscr{A}^{*}$, denote by $n_{j}(y)$ the total number of occurrences of $a_{j}$ in $y$, so that $\sum_{j=1}^{r} n_{j}(y)=l(y)$. Let $Q(y) \subset \mathscr{A}^{l(y)}$ be the set of all $l(y)$-tuples with the same numbers of occurrences of particular letters as in $y$, let $k(y)$ be the order number of $y$ according to the lexicographical ordering generated in $Q(y)$ by the simple ordering $a_{1}<a_{2}<\ldots$ $\ldots<a_{r}$ of $\mathscr{A}$. Finally, by $\tilde{p} \in \mathscr{A}^{*}$ denote the shortest program with this property: for each $y \in \mathscr{A}^{*}$, and for a fixed encoding of $(r+1)$-tuples in the form of concatenation,

$$
\begin{equation*}
U(\mathscr{A})\left(\tilde{p} * n_{1}(y) * n_{2}(y) * \ldots * n_{r}(y) * k(y), l(y)\right)=y \tag{6}
\end{equation*}
$$

(the concatenation in (6) will be denoted by $P_{0}(y)$ ). As proved in [5], if $\left\langle p_{1}(y), \ldots\right.$ $\left.\ldots, p_{r}(y)\right\rangle=\left\langle n_{1}(y)(l(y))^{-1}, \ldots, n_{r}(y)(l(y))^{-1}\right\rangle \neq\left\langle r^{-1}, r^{-1}, \ldots, r^{-1}\right\rangle$, then there exists $c<1$ and $\left.g: \mathscr{N} \rightarrow \mathcal{N}, g \in o_{( }^{\prime} n\right)$, such that $l\left(P_{0}(y)\right) \leqq c \cdot l(y)+g(l(y))$. In fact, we may take $c=H_{r}\left(p_{1}(y), \ldots, p_{r}(y)\right)=-\sum_{j=1}^{r} p_{j}(y) \log _{r} p_{j}(y)$.

Hence, if $x$ is an absolutely random sequence from $\mathscr{B}^{\infty}$, but $\left\langle n_{1}, n_{2}, \ldots, n_{r}\right\rangle \neq$ $\neq\langle m / r, m / r, \ldots, m / r\rangle$, then $w\left(x, n_{1}, \ldots, n_{r}\right) \in \mathscr{A}^{\infty}$ is not absolutely random as each $w(x)[n]$ can be generated by "substantially shorter" program $P_{0}(w(x)[n])$ for $n$ large enough. We may ask, whether $w(x)[n]$ can be generated by a still shorter program. The answer is negative, as the following theorem shows.

Theorem 1. Let $\mathscr{A}=\left\{a_{1}, \ldots, a_{r}\right\}, \mathscr{B}=\left\{b_{1}, \ldots, b_{m}\right\}, m>r \geqq 2$, let $U(\mathscr{A}), U(\mathscr{B})$ be fixed universal Turing machines over $\mathscr{A}$ and $\mathscr{B}$, let $x \in \mathscr{B}{ }^{\infty}$ be absolutely random,
let $n_{1}, n_{2}, \ldots, n_{r} \in \mathscr{N}, \sum_{i=1}^{r} n_{i}=m$. Then there exists a total function $g: \mathscr{N} \rightarrow \mathscr{N}$, $\left.g(n) \in o_{( }^{( } n\right)$, such that for all $n \in \mathscr{N}$,
(7) $\quad l\left(P_{0}\left(w\left(x, n_{1}, n_{2}, \ldots, n_{r}\right)[n]\right)\right)-K_{U(\alpha)}\left(w\left(x, n_{1}, n_{2}, \ldots, n_{r}\right)[n] \mid n\right) \leqq g(n)$.

Proof. Let $x=x_{1}, x_{2}, \ldots \in \mathscr{B}^{\infty}$ be absolutely random, so that $K_{U(\mathscr{B})}(x[n] \mid n) \geqq$ $\geqq n-f(n)$ for a function $f(n) \in o(n)$. Let $y=y_{1}, y_{2}, \ldots=w(x) \in \mathscr{A}^{\infty}$ and suppose, in order to arrive at a contradiction, that there exists $\gamma<1$ such that, for infinitely many $n$ s,

$$
\begin{equation*}
\left.K_{U(\Omega)}(y[n] \mid n) \leqq \gamma \cdot l\left(P_{0}\left(w_{1}^{\prime} x, n_{1}, \ldots, n_{r}\right)[n]\right)\right) . \tag{8}
\end{equation*}
$$

A computation yields that the assertion of Theorem 1 will be proved if we arrive at a contradiction supposing that there exists $\beta<1$ such that, for infinitely many $n$ 's,

$$
\begin{equation*}
K_{U(\mathbb{N})}(y[n] \mid n) \leqq \beta H_{r}\left(p_{1}, \ldots, p_{r}\right) n, \tag{9}
\end{equation*}
$$

where $p_{i}=n_{i} / m, i \leqq r$.
Given $x$ and $n_{1}, \ldots, n_{r}, w\left(x, n_{1}, \ldots, n_{r}\right)$ is defined uniquely, but not vice versa. Or, having at our disposal $y=y_{1}, y_{2}, \ldots$ with, say, $y_{j}=a_{i}$, we need still a number $v_{j} \leqq n_{i}$ to know, which $b_{k}$ was transformed into $a_{i}$ to be able to reconstruct $x_{j}$. Hence, we need a sequence $v=v_{1}, v_{2}, \ldots$ of numbers, where $0<v_{i} \leqq n_{i}^{*}$ for $i=$ $=1,2, \ldots$ and $n_{i}^{*}=n_{j}$ iff $y_{i}=a_{j}$, namely, we need $y[n]$ and $v[n]$ in order to generate $x[n]$.

Given $y[n]$ the $n$-tuple $v[n]$ of numbers can be enumerated by a number $\alpha(n)$, $\alpha(n) \leqq \prod_{i=1}^{n} n_{i}^{*}$, so that $\log _{r}(\alpha(n)) \leqq \sum_{i=1}^{n} \log _{r} n_{i}^{*}$. The relative frequences of occurrences of each $b_{i}$ in $x$ tend to $\mathrm{m}^{-1}$, so that the relative frequency of cases when $n_{i}^{*}=n_{j}$ will tend to $n_{j} / m$, or, written precisely, will be $\left(n_{j} / m\right)+g(n)$, where $g(n) . n \leqq$ const. Hence

$$
\begin{gather*}
\text { 0) } \begin{array}{c}
\sum_{i=1}^{n} \log _{r} n_{i}^{*} \leqq \sum_{j=1}^{r} n \frac{n_{j}}{m} \log _{r} n_{j}+\text { const }=n \sum_{j=1}^{r} \frac{n_{j}}{m} \log _{r} n_{j}+\text { const }= \\
=n\left[\sum_{j=1}^{r} \frac{n_{j}}{m} \log _{r} n_{j}-\log _{r} m+\log _{r} m\right]+\text { const }= \\
=n\left[\sum_{j=1}^{r} \frac{n_{j}}{m} \log _{r} \frac{n_{j}}{m}+\log _{r} m\right]+\text { const }=n \log _{r} m-n H_{r}\left(p_{1}, \ldots, p_{r}\right)+\text { const },
\end{array} \tag{10}
\end{gather*}
$$

where $p_{i}=n_{i} \mid m$. Combining with the assumptions above we obtain

$$
\begin{gather*}
K_{U(, \infty)}(x[n] \mid n) \leqq K_{U(s))}(y[n] \mid n)+K_{U(s)}(v[n] \mid n)+\text { const }_{1} \leqq  \tag{11}\\
\leqq \beta H_{r}\left(p_{1}, \ldots, p_{r}\right) n+n \log _{r} m-n H_{r}\left(p_{1}, \ldots, p_{r}\right)+\text { const }_{2}= \\
=n \log _{r} m \cdot \gamma+\text { const }_{2},
\end{gather*}
$$

where

$$
\begin{equation*}
\gamma=1-(1-\beta) H_{r}\left(p_{1}, \ldots, p_{r}\right)\left(\log _{r} m\right)^{-1}<1 \tag{12}
\end{equation*}
$$

so that $K_{U(\mathbb{B})}(x[n] \mid n) \leqq n \cdot \gamma^{\prime}$ for $\gamma^{\prime}<1$ and infinitely many $n$ 's, but this contradicts the supposed absolute randomness of $x$.

## 3. PSEUDO-RANDOM INDEPENDENT IDENTICALLY DISTRIBUTED SEQUENCES

Theorem 1 immediately invokes the two following definitions.
Definition 1. A sequence $y \in \mathscr{A}^{\infty}$ is strictly pseudo-random independent and identically distributed sequence (strictly PIID-sequence) with probability distribution $\left\langle p_{1}, p_{2}, \ldots, p_{r}\right\rangle$, if there are $n_{1}, \ldots, n_{r} \in \mathscr{N}$ such that $n_{i} / m=p_{i}, i=1,2, \ldots, r$, $m=\sum_{i=1}^{r} n_{i}$, if there is $\mathscr{B}=\left\{b_{1}, b_{2}, \ldots, b_{m}\right\}$ and if there is $x \in \mathscr{B}^{\infty}$ such that $x$ is absolutely random and $y=w\left(x, n_{1}, \ldots, n_{r}\right)$.

Definition 2. A sequence $y \in \mathscr{A}^{\infty}$ is PIID-sequence, if there exists a total function $g: \mathscr{N} \rightarrow \mathcal{N}, g \in o(n)$, such that for all $n \in \mathscr{N}$,

$$
\begin{equation*}
l\left(P_{0}(y[n])\right)-K_{U(\cdot n)}(y[n] \mid n) \leqq g(n) \tag{13}
\end{equation*}
$$

As immediately follows from Theorem 1, each strictly PIID-sequence is a PIIDsequence, but the inverse implication does not hold, as will be proved below.

Theorem 2. Let $x=x_{1}, x_{2}, \ldots, \in \mathscr{A}^{\infty}$ be a PIID-sequence, then for each $a_{j} \in \mathscr{A}$, $\lim _{n \rightarrow \infty} f r\left(a_{j}, x[n]\right)=\operatorname{pr}\left(a_{j}\right)$ exists and $\sum_{j=1}^{r} \operatorname{pr}\left(a_{j}\right)=1$.

Proof. Suppose, in order to arrive at a contradiction, that $f r\left(a_{j}, x[n]\right)$ oscillates for some $j \leqq r$. Then there exist $\varepsilon>0$ and an infinite sequence $\bar{n}_{1}<\bar{n}_{2}<\ldots$ such that $\left|f r\left(a_{j}, x\left[\bar{n}_{i}\right]\right)-\operatorname{fr}\left(a_{j}, x\left[\bar{n}_{i+1}\right]\right)\right|>\varepsilon$. Set $n=\bar{n}_{i}, m=\bar{n}_{i+l}$ for some $i, l$, and consider a program $P_{1}$ which, joined with $(r+1)$-tuples $\left\langle n_{1}, n_{2}, \ldots, n_{r}, k_{1}\right\rangle$, $\left\langle m_{1}, m_{2}, \ldots, m_{r}, k_{2}\right\rangle$ of integers, calls the program $P_{0}$ and generates the $k_{1}$ th sequence of length $\sum_{s=1}^{r} n_{s}$ with $n_{i}$ occurrences of $a_{i}$, i.e., the $k_{1}$ th sequence from $Q\left(n_{1}, \ldots, n_{r}\right)=Q\left(a_{1}^{n_{1}} \ldots a_{r}^{n_{r}}\right)$, then generates the $k_{2}$ th sequence from $Q\left(m_{1}, m_{2}, \ldots\right.$ $\ldots, m_{r}$ ) and joins them in this order. If $n_{i}\left(m_{i}\right.$, resp.) is the frequency of $a_{i}$ in $x[n]$ (in $\left\langle x_{n+1}, \ldots, x_{m}\right\rangle$, resp.) and if $k_{1}\left(k_{2}\right.$, resp.) is the order number of $x[n]\left(\left\langle x_{n+1}, \ldots\right.\right.$ $\left.\ldots, x_{m}\right\rangle$, resp.) in $Q\left(n_{1}, n_{2}, \ldots, n_{r}\right)$ (in $Q\left(m_{1}, m_{2}, \ldots, m_{r}\right)$, resp.), then $P_{1}(x[m])=$ $=P_{1} *\left\langle n_{1}, \ldots, n_{r}, k_{1}\right\rangle *\left\langle m_{1}, \ldots, m_{r}, k_{2}\right\rangle$ generates $x[m]$. Clearly,
(14) $\quad l\left(P_{1}(x[m])\right) \leqq{ }^{\ulcorner } \log _{r}\left\|Q\left(n_{1}, \ldots, n_{r}\right)\right\|^{\top}+{ }^{\top} \log _{r}\left\|Q\left(m_{1}, \ldots, m_{r}\right)\right\|^{\top}+$ $+\sum_{i=1}^{r}{ }^{r} \log _{r} n_{i}{ }^{\top}+\sum_{i=1}^{r}{ }^{r} \log _{r} m_{i}{ }^{\top}+l\left(P_{1}\right)$.
es can be easily seen,

$$
\begin{equation*}
\sum_{i=1}^{r}\left\ulcorner\log _{r} n_{i}\right\rceil+\sum_{i=1}^{r}\left\ulcorner\log _{r} m_{i}^{\top}+l\left(P_{1}\right) \in o_{( }^{\prime}(m)\right. \tag{15}
\end{equation*}
$$

and the assumption that $x$ is a PIID-sequence yields that

$$
\begin{equation*}
\left|l\left(P_{1}(x[m])\right)-m H_{r}\left(p_{1}, \ldots, p_{r}\right)\right| \in o(m) \tag{16}
\end{equation*}
$$

where $p_{i}=\left(n_{i}+m_{i}\right) / m$. The only we have to prove is that there exists $c_{0}(\varepsilon)<$ $<H_{r}\left(p_{1}, \ldots, p_{r}\right)$ such that

$$
\begin{equation*}
\log _{r}\left\|Q\left(n_{1}, \ldots, n_{r}\right)\right\|+\log _{r}\left\|Q\left(m_{1}, \ldots, m_{r}\right)\right\| \leqq c_{0}(\varepsilon) m \tag{17}
\end{equation*}
$$

where $\|\cdot\|$ denotes the cardinality. But, as proved in [5],

$$
\begin{equation*}
\log _{r}\left\|Q\left(n_{1}, \ldots, n_{r}\right)\right\|=n H_{r}\left(q_{1}, \ldots, q_{r}\right)+f_{1}(n) \tag{18}
\end{equation*}
$$

$$
\begin{equation*}
\log _{r}\left\|\dot{Q}\left(m_{1}, \ldots, m_{r}\right)\right\|=(m-n) H_{r}\left(s_{1}, \ldots, s_{r}\right)+f_{2}(m-n) \tag{19}
\end{equation*}
$$

where $q_{i}=n_{i} / n, s_{i}=m_{i} /(m-n), i \leqq r$, and $f_{1}(n), f_{2}(n) \in o(n)$. So we must prove that
(20) $\quad n H_{r}\left(q_{1}, \ldots, q_{r}\right)+(m-n) H_{r}\left(s_{1}, \ldots, s_{r}\right) \leqq c_{0}(\varepsilon) m H_{r}\left(p_{1}, \ldots, p_{r}\right)$.

As $\left\langle q_{1}, \ldots, q_{r}\right\rangle \neq\left\langle s_{1}, \ldots, s_{r}\right\rangle$ (recall that $\left|q_{j}-s_{j}\right|>\varepsilon>0$ ), and because of the fact that, for $\alpha=n / m, \beta=(m-n) / m$,

$$
\begin{gather*}
\left.\alpha q_{i}+\beta s_{i}=(n \mid m)\left(n_{1} / n\right)+((m-n) \mid n)\left(m_{i}\right)(m-n)\right)=  \tag{21}\\
=\left(n_{i}+m_{i}\right) / n=p_{i},
\end{gather*}
$$

(20) follows from the well-known assertion of classical information theory according to which

$$
\begin{equation*}
\frac{\alpha H_{r}\left(q_{1}, \ldots, q_{r}\right)+\beta H_{r}\left(s_{1}, \ldots, s_{r}\right)}{H_{r}\left(p_{1}, \ldots, p_{r}\right)}<1 \tag{22}
\end{equation*}
$$

so that the left hand side in (22) can be taken as $c_{0}(\varepsilon) . \sum_{j=1}^{r} f r\left(a_{j}, x[n]\right)=1$ for each $n \in \mathscr{N}$, hence, $\sum_{j=1}^{r} p r\left(a_{j}\right)=1$ as well.

Given $\alpha=\left\langle x_{1}, \ldots, x_{n}\right\rangle \in \mathscr{A}^{*}$ and $n_{1}, n_{2}, \ldots, n_{r} \in \mathscr{N}$, we may define the product probability $\underset{r}{\underset{p r}{\sim}}\left(n_{1}, \ldots, n_{r}, \alpha\right)$ of $\alpha$, setting $\tilde{p r}\left(n_{1}, \ldots, n_{r}, \alpha\right)=\prod_{j=1}^{n} \pi\left(x_{i}\right)$, where $\pi\left(x_{i}\right)=$ $=p_{j}=n_{j} \mid \sum_{k=1}^{r} n_{k}$ iff $x_{i}=a_{j}$. Hence, $\tilde{p r}\left(n_{1}, \ldots, n_{r}, \alpha\right)$ is the probability of $\alpha$ supposing that each $x_{j}, j \leqq n$, is sampled independently from the probability distribution $\left\langle p_{1}, \ldots, p_{r}\right\rangle$. The assertion of Theorem 2 can be, in the case of strictly PIID-sequences, generalized from particular letters to finite blocks of letters, as the next assertion proves.

Theorem 3. If $y \in \mathscr{A}^{\infty}$ is a strictly PIID-sequence such that $y=w\left(x, n_{1}, n_{2}, \ldots, n_{r}\right)$ for an absolutely random $x, x \in \mathscr{B}^{\infty},\|\mathscr{B}\|=\sum_{j=1}^{r} n_{j}$, then for each $k \in \mathscr{N}^{+}$and each
$\alpha \in \mathscr{A}^{k}$ $\alpha \in \mathscr{A}^{k}$,

$$
\begin{equation*}
\lim _{n \rightarrow \infty} f r(\alpha, B(k, y)[n])=\tilde{p r}\left(n_{1}, \ldots, n_{r}, \alpha\right) \tag{23}
\end{equation*}
$$

Proof. Let $x=x_{1}, x_{2}, \ldots \in \mathscr{B}^{\infty}$ be an absolutely random sequence over an alphabet $\mathscr{B}=\left\{b_{1}, \ldots, b_{m}\right\}$, let $n_{1}, n_{2}, \ldots, n_{r} \in \mathscr{N}$, let $\sum_{j=1}^{r} n_{j}=m$, let $w\left(x, n_{1}, n_{2}, \ldots\right.$ $\left.\ldots, n_{r}\right)=y=y_{1}, y_{2}, \ldots \in \mathscr{A}^{\infty}$. For $k, n \in \mathscr{N}^{+}$take the $n$th element of $B(k, y)$, i.e. the $k$-tuple $\bar{y}=\left\langle y_{(n-1) k+1}, y_{(n-1) k+2}, \ldots, y_{n k}\right\rangle \in \mathscr{A}^{k}$. Its inverse image under the mapping $w$, i.e. the set

$$
\begin{equation*}
C=\left\{\left\langle v_{1}, v_{2}, \ldots, v_{k}\right\rangle: w\left(\left\langle v_{1}, \ldots, v_{k}\right\rangle\right)=\bar{y}\right\} \tag{24}
\end{equation*}
$$

is a product subset of $\mathscr{B}^{k}$ such that the projection of $C$ to its $j$ th coordinate has $n_{i}$ elements iff $y_{(n-1) k+j}=a_{i}$. Hence, $\|C\|=\prod_{j=1}^{r} n_{j}^{c_{j}}$, where $c_{j}$ is the absolute frequency of $a_{j}$ in $\bar{y}$, the total cardinality of $\mathscr{B}^{k}$ is $m^{k}$, so that the relative frequency of elements from $C$ in $\mathscr{B}^{k}$ is $\prod_{j=1}^{r}\left(n_{j} / m\right)^{c_{j}}$, but this is nothing else than $\prod_{i=1}^{k} \pi\left(y_{(n-1) k+1}\right)=\tilde{p r}\left(n_{1}, \ldots\right.$ $\left.\ldots, n_{r}, \bar{y}\right)$. As $x$ is absolutely random, the same holds for $B(k, x)$, so that the relative frequency of each $k$-tuple from $\mathscr{B}^{k}$ in $B(k, x)$ tends to $m^{-k}$. Consequently, the relative frequency of $\bar{y}$ in $B(k, y)$ tends to $\widetilde{p r}\left(n_{1}, \ldots, n_{r}, \bar{y}\right)$.

## 4. PROPERTIES OF PIID-SEQUENCES

A PIID-sequence $y \in \mathscr{A}^{\infty}$ is called rational, if for each $j \leqq r$ the value $\lim _{n \rightarrow \infty} f_{r}(a, y[n])$ is a rational number. Theorem 3 can be extended to rational $\stackrel{n \rightarrow \infty}{ }$ PIID-sequences, as the next assertion proves.

Theorem 4. Each rational PIID-sequence $y=y_{1}, y_{2}, \ldots \in \mathscr{A}^{\infty}$ is a strictly PIIDsequence, i.e., there exist a set $\mathscr{B}=\left\{b_{1}, \ldots, b_{m}\right\}$ and positive integers $n_{1}, n_{2}, \ldots, n_{r}$ such that $\sum_{i=1}^{r} n_{i}=m$ and $y=w\left(x, n_{1}, n_{2}, \ldots, n_{r}\right)$ for an absolutely random $x \in \mathscr{B}^{\infty}$.

Proof. As proved in Theorem 2, the values $p_{j}=\lim _{n \rightarrow \infty} f r\left(a_{j}, y[n]\right), j \leqq r$, exist and are rational, due to the assumptions. Hence, there exist $n_{1}, \ldots, n_{r} \in \mathscr{N}$ such that $n_{j} / m=p_{j}, j \leqq r$, where $m=\sum_{j=1}^{r} n_{j}$.

Let $\mathscr{B}=\left\{b_{1}, b_{2}, \ldots, b_{m}\right\}$ be a set, let $A_{1}, A_{2}, \ldots \subset \mathscr{B}$ be non-empty subsets of $\mathscr{B}$ such that $\left\|A_{i}\right\|=n_{i}^{*}$ (hence, $n_{i}^{*} \leqq m$ for all $i \in \mathcal{N}$, the connection with $n_{i}^{*}$ 's intro-
duced above will be seen later), let $S^{\prime} \in A_{0}^{\infty}, A_{0} \subset B$, be an infinite sequence. First, we prove: if $f(n) \in o(n)$ is a total function such that $\sum_{k=1}^{\infty} m^{-f(k)}<\infty$, then there exists an infinite sequence $S \in X_{i=1}^{\infty} A_{i}$ such that, for each $n \in \mathscr{N}$,

$$
\begin{equation*}
K_{U(\mathscr{B})}\left(S[n] \mid S^{\prime}[n]\right)>\log _{m}\left(\prod_{i=1}^{n} n_{i}^{*}\right)-f(n) \tag{25}
\end{equation*}
$$

When proving (25) we use some ideas from the proof of Theorem 6, Chapter 5 in [2]. Take $f(n) \in o(n)$ satisfying the conditions (e.g. $f(n)=c \log _{m} n, c>1$ ), and set

$$
\begin{equation*}
D_{n}=\left\{S: S \in X_{i=1}^{\infty} A_{i}, K_{U(g) 3}\left(S[n] \mid S^{\prime}[n]\right)>\log _{m}\left(\prod_{i=1}^{n} n_{i}^{*}\right)-f(n)\right\} \tag{26}
\end{equation*}
$$

We have to prove that there exists $K \in N$ such that $\bigcap_{n}^{\infty} D_{n} \neq \emptyset$ (replacing $f(n)$ by $f(n)+$ const we may always suppose that $\left.\bigcap_{n=1}^{K-1} D_{n}=\bigcap_{n=1}^{\substack{K-1}} A_{n}\right)$. Let $\mathscr{F}_{0} \subset \mathscr{P}\left(\mathscr{B}^{\infty}\right)$ be the minimal $\sigma$-field of subsets of $\mathscr{B}^{\infty}$ generated by elementary cylinders, let $P^{\sim}$ be the probability measure defined on $\mathscr{F}_{0} \cap X_{i=1}^{\infty} A_{i}$ as the unique extension of the function $P^{\sim}$ ascribing to each cylinder $V\left(x_{1}, \ldots, x_{n}\right) \subset X_{i=1}^{\infty} A_{i}$ the value $\prod_{i=1}^{n}\left(n_{i}^{*}\right)^{-1}$. $D_{n}$ is a union of cylinders of the length $n$ and its complement w.r. to $\underset{i=1}{\underset{i=1}{\infty} A_{i} \text { contains }}$ at most

$$
\begin{equation*}
\sum_{i=0}^{L} m^{i}=\left(m^{L+1}-1\right)(m-1)^{-1}<m^{L+1}=\left(\prod_{i=1}^{n} n_{i}^{*}\right) m^{1-f(n)} \tag{27}
\end{equation*}
$$

cylinders of the length $n$, where $L=\log _{m}\left(\prod_{i=1}^{n} n_{i}^{*}\right)-f(n)$. Or, programs which generate $S[n]$ using $U(\mathscr{B})$ and $S^{\prime}[n]$ are sequences from $\mathscr{B}$ and different $S[n]$ 's need different programs. The $P^{\sim}$-probability of each $S[n]$ is $\prod_{i=1}^{n}\left(n_{i}^{*}\right)^{-1}$, hence,

$$
\begin{equation*}
P^{\sim}\left({\left.\underset{i=1}{\infty} A_{i}-C_{n}\right)<m^{1-f(n)}, ~}_{\text {in }}\right. \tag{28}
\end{equation*}
$$

so that

$$
\sum_{i=0}^{\infty} P^{\sim}\left(X_{i=1}^{\infty} A_{i}-D_{n}\right)<\infty
$$

hence, for some $K, P^{\sim}\left(\bigcap_{n=K}^{\infty} D_{n}\right)>0$ and $\bigcap_{n=K}^{\infty} D_{n} \neq \emptyset$.
Now, let $y=y_{1}, y_{2}, \ldots \in \mathscr{A}^{\infty}$ be a rational PIID-sequence, then each sequence $v \in X_{i=1}^{\infty} A_{i}$, where $\left\|A_{i}\right\|=n_{i}^{*}=n$ iff $y_{i}=a_{j}$, defines uniquely a sequence $x \in \mathscr{B}^{\infty}$ such that $y=w\left(x, n_{1}, \ldots, n_{r}\right)$. Hence, there is a fixed program $p_{1}$ which, given $n, n_{1}, \ldots$
$\ldots, n_{r}, y[n]$ and $v[n]$, computes $x[n]$, another fixed program $p_{2}$ computes the concatenation $y[n] * v[n]$ given $n, n_{1}, \ldots, n_{r}$ and $x[n]$. So

$$
\begin{equation*}
\left|K_{U(())}\left(x[n] \mid n, n_{1}, \ldots, n_{r}\right)-K_{U(刃)}\left(y[n] * v[n] \mid n, n_{1}, \ldots, n_{r}\right)\right|<\text { const } \tag{29}
\end{equation*}
$$

(different pairs $\langle y[n], v[n]\rangle$ yield different $x[n]$, so $y[n]$ and $v[n]$ can be effectively computed from $x[n], n, n_{1}, \ldots, n_{r}$ ). We may embed $\mathscr{A}$ into $\mathscr{B}$ by identifying, say, each $a_{j}$ with the first $b_{k}$ to which $a_{j}$ corresponds by factorization. So we may take, due to (25), such a $v \in X_{i=1}^{\infty} A_{i}$ that for all $n \in \mathscr{N}$,

$$
\begin{equation*}
K_{U(g)}(v[n] \mid y[n])>\log _{m}\left(\prod_{i=1}^{n} n_{i}^{*}\right)-f(n), \tag{30}
\end{equation*}
$$

where $f(n)$ is an appropriate $o(n)$-function.
Let $q_{1}$ be the shortest program which generates $y[n]$ (in fact, $q_{1}$ is $P_{0}(y[n])$ up to $g(n)$ where $g(n)$ is an $\left.o_{( }^{\prime} n\right)$-function with respect to which $y$ is a PIID-sequence). So $q_{1}$ can be taken as the $r$-adic number of $y[n]$ in the set of all $n$-tuples which are possible initial segments of a PIID-sequence with respect to the given $g(n)$, $n, n_{1}, \ldots, n_{r}$. Let $q_{2}$ be the shortest program which generates $v[n]$ given $y[n], n_{1}, \ldots$ $\ldots, n_{r}$, again, $q_{2}$ can be taken as the $m$-adic number of the $2 n$-tuple $y[n] * v[n]$ in the set of all $2 n$-tuples such that $y[n]$ is given and $v[n] \in{\underset{X}{i=1}}_{n}^{X} A_{i}$. Different $y[n] *$ $* v[n]$ 's yield different $x[n]$ 's, different $\left\langle q_{1}, q_{2}\right\rangle$ 's yield different $y[n] * v[n]$ 's, hence, the shortest program for $x[n]$ cannot be shorter than $l\left(q_{1} * q_{2}\right)=l\left(q_{1}\right)+$ $+l\left(q_{2}\right)$ (up to an $o(n)$-function). However, the same argumentation as used in the proof of Theorem 1 shows, that $q_{1} * q_{2}$ cannot be encoded, in $\mathscr{B}$, by a sequence shorter than $n-f^{\prime}(n)$, if (30) holds, for an appropriate $f^{\prime}(n) \in o(n)$. Combining this result with (29) we obtain that $x$ is absolutely random and the theorem is proved.

As the limit probabilities of frequences of letters in strictly PIID-sequences correspond to ratios of $n_{i}$ and finite cardinality $m$ of the basic alphabet $\mathscr{B}$, only rational PIID-sequences can be obtained by factorization of absolutely random sequences from $\mathscr{B}^{\infty}$. Let $\left\langle p_{1}, \ldots, p_{r}\right\rangle$ be any probability distribution including those with irrational $p_{i}$ 's, let $C_{p}$ be the set of all sequences from $\mathscr{A}^{\infty}$ which are PIID-sequences with limit values of relative frequencies of letters corresponding to $\left\langle p_{1}, \ldots, p_{r}\right\rangle$, let $\widetilde{p} r\left(p_{1}, \ldots, p_{r}, \cdot\right)$ be the probability measure defined in the same way as $\widetilde{p} r\left(n_{1}, \ldots\right.$ $\left.\ldots, n_{r}, \cdot\right)$, but with $n_{i} / m$ replaced by $p_{i}$. The well-known assertion of information theory and coding theory then enables to prove that $\widetilde{p r}\left(p_{1}, \ldots, p_{r}, C_{p}\right)=1$, hence, the set $C_{p}$ is non-empty so that there exist non-rational and, consequently, nonstrictly PIID sequences.

The following theorems shows that even a slight weakening of the notion of PIIDsequence admits also sequences not satisfying the limit assertion (23) of Theorem 3 for relative frequencies of blocks of letters. Let $c<1$ be given, a sequence $y \in \mathscr{A}^{\infty}$
is called a $c$-PIID-sequence, if for all $n \in \mathscr{N}$

$$
\begin{equation*}
K_{U(\alpha)}(x[n] \mid n) \geqq c \cdot l\left(P_{0}(y[n])\right) \tag{31}
\end{equation*}
$$

Theorem 5. For each $\mathscr{A}=\left\{a_{1}, a_{2}, \ldots, a_{r}\right\}, r \geqq 2$, each probability distribution $\left\langle p_{1}, \ldots, p_{r}\right\rangle$, each $c<1$ and each $\varepsilon>0$ there exist $\left\langle p_{1}^{*}, \ldots, p_{r}^{*}\right\rangle$ and a $c$-PIIDsequence $x=x_{1}, x_{2}, \ldots, \in \mathscr{A}^{\infty}$ such that
(i) $p_{i}^{*}>0, i \leqq r, \sum_{i=1}^{r} p_{i}^{*}=1$,
(ii) $\max \left\{\left|p_{i}-p_{i}^{*}\right|: i \leqq r\right\}<\varepsilon$,
(iii) $\lim _{n \rightarrow \infty} f r(a, x[n])=p_{j}^{*}, j \leqq r$,
(iv) there exist $k \in \mathcal{N}^{+}$and $\alpha \in \mathscr{A}^{k}$ such that $\operatorname{fr}(\alpha, B(k, x)[n])=0$ for all $n \in \mathscr{N}$ (i.e., $\alpha$ does not occur in $B(k, x)$ ).

Proof. Evidently, given a probability distribution $\left\langle p_{1}, \ldots, p_{r}\right\rangle$ and $\varepsilon>0$, there always exist positive integers $n_{1}, \ldots, n_{r} \in \mathscr{N}^{+}$such that, for $m=\sum_{i=1}^{r} n_{i}$, $\max \left\{\mid p_{i}-\right.$ $\left.-\left(n_{i} / m\right) \mid: i \leqq r\right\}<\varepsilon$, set $p_{i}^{*}=n_{i} / m$. Consider the sets $\mathscr{B}_{k}=Q\left(k n_{1}, \ldots, k n_{r}\right)$, $k \in \mathscr{N}^{+}$, of all $k m$-tuples with $k n_{i}$ occurrences of $a_{i}$ for all $i \leqq r$. Let $y=y_{1}, y_{2}, \ldots$ $\ldots \in \mathscr{B}_{k}^{\infty}$ be an absolutely random sequence over the new alphabet $\mathscr{\mathscr { B }}_{k}$, let $z=z_{1}, z_{2}, \ldots$ $\ldots$ be the sequence $y$ taken as a sequence over the original alphabet $\mathscr{A}$. So $B(k m, z)=$ $=y$, and each $B(k m, z)(n)=y_{n}$ contains at least $k$ occurrences of each $a_{j}$ (all $n_{i}$ are positive). Hence, if e.g. $\alpha \in \bigcup_{j=1}^{r}\left(\mathscr{A}-\left\{a_{j}\right\}\right)^{k m}$, then $B(k m, z) \neq \alpha$, so that $f r(\alpha, B(k m, z)[n])=0$ for all $n \in \mathcal{N}$. Clearly, $\operatorname{fr}\left(a_{j}, y_{n}\right)=\operatorname{fr}\left(a_{j},\left\langle z_{(n-1) k m+1}, \ldots\right.\right.$ $\left.\left.\ldots, z_{n k m}\right\rangle\right)=n_{i} / m=p_{i}^{*}$ due to the definition of $y_{n}$ as a sequence from $Q\left(k n_{1}, \ldots, k n_{r}\right)$, so that (iii) holds. The only we have to prove is that for each $c<1$ there exist $k \in \mathscr{N}^{+}$ such that $z=z(k)$ is a $c$-PIID-sequence.

The sequence $y \in \mathscr{B}_{n}^{\infty \infty}$ is absolutely random, so that for each $\tilde{n}$ and an $o(n)$-function $f(n)$,

$$
\begin{equation*}
K_{U\left(3_{k}\right)}(y[\tilde{n}] \mid \tilde{n}) \geqq \tilde{n}-f(\tilde{n}) \tag{32}
\end{equation*}
$$

with respect to the alphabet $\mathscr{\mathscr { O }}_{k}$. If $q \in \mathscr{\mathscr { B }}_{k}^{*}$ is the shortest program such that $U\left(\mathscr{B}_{k}\right)(q, \tilde{n})=y[\tilde{n}]$ and $l_{\mathscr{S H}_{k}}(q)=\tilde{n}-f(\tilde{n})$, then $q$ cannot be encoded in the original alphabet $\mathscr{A}$ by a sequence shorter than

$$
\begin{equation*}
(\tilde{n}-f(\tilde{n}))\left(\log _{r}\left\|B_{k}\right\|+g_{1}(\tilde{n})\right)+g_{2}(\tilde{n}) \tag{33}
\end{equation*}
$$

for appropriate $g_{1}(n), g_{2}(n) \in o(n)$. But

$$
\begin{equation*}
\log _{r}\left\|B_{k}\right\|=\log _{r}\left\|Q\left(k n_{1}, \ldots, k n_{r}\right)\right\|=m k H_{r}\left(p_{1}^{*}, \ldots, p_{r}^{*}\right)-h(m k) \tag{34}
\end{equation*}
$$

$h(n) \in o(n)$, so that, given $c<1$, we may choose $\mathrm{k} \in \mathscr{N}^{+}$such that $q$ cannot be encoded in $\mathscr{\mathscr { F }}_{k}$ by a sequence shorter than $c^{\prime}(\tilde{n}-f(\tilde{n})) H_{r}\left(p_{1}^{*}, \ldots, p_{r}^{*}\right)$ for a $c^{\prime}<1$, but $c^{\prime}>c$. Given $n \in \mathcal{N}$, the algorithmic complexity of $z[n]$ may differ from the algorithmic complexity of $z\left[n^{\prime}\right]$, where $n^{\prime} \geqq n$ is the smallest integer divisible by $k m$,
at most, by a value independent of $n\left(z_{n+1}, z_{n+2}, \ldots, z_{n}\right.$, are joined to $z[n]$ and $n^{\prime}-n<k m$ ). But $z\left[n^{\prime}\right]=y\left[n^{\prime \prime}\right]$ for $n^{\prime \prime}=n^{\prime} \mid k m$. Combining these results we obtain that $z(k)$ is a $c^{\prime}$-PIID-sequence, hence, it is also a $c$-PIID-sequence as $c^{\prime}>c$. The theorem is proved.

## 5. CONCLUSIVE REMARKS

The model explained in this paper is of purely mathematical nature and forms a theoretical background and limitation for models more close to practical use. The theoretical ineffectiveness of the present model goes in two directions:
(1) The notions of absolute random sequence and PIID-sequence are of asymptotic nature, as they are defined up to an $o(n)$-function. Hence, each finite sequence can be an initial segment of an absolute random or PIID-sequence and no definite conclusions about the absolute randomness or PIID-property of infinite sequences can be taken on the grounds of their initial segments. On the other hand, such an asymptotic conception makes the definitions independent of a particular choose of the universal Turing machine $U$ (algorithmic complexities defined w.r. to two universal Turing machines $U_{1}, U_{2}$ differ only by an additive constant which depends only on $U_{1}, U_{2}$, and such a difference is irrelevant from the point of view, how the classes of absolute random sequences and PIID-sequences are defined). The asymptotic feature of this conception may be eliminated by giving a fixed universal Turing machine $U$ and a fixed $o(n)$-function $f: \mathcal{N} \rightarrow \mathcal{N}$, but even in this case it would be interesting to know, which properties of the defined notions are independent of the chosen parameters and it is just what we tried to investigate here. From a point of view the asymptotic notions defined here can be seen as analogies of those statements of classical probability theory which are asymptotically valid "almost surely" or "with the probability one", but it would deserve a more detailed consideration to find how far this analogy goes. Some philosophical remarks concerning the classical "almost surely" valid statements can be found in [2], Chapter 4.
(2) Even with $U$ and $f$ fixed the notions still remain to be ineffective because of the fact that they are defined through an effectively non-computable function $K_{U}(x \mid S)$. This difficulty can be partially eliminated when replacing $U$ by a less efficient computational device (by a partial recursive function, formally said) $\Psi$ such that $K_{Y}(x \mid S)$ is computable. An intuitively reasonable example of this approach consists in taking into considerations only such programs $p$ which compute, given $S$, the desired sequence $x$ within a priori given time and space limitations (in non-trivial cases these limitations may depend on $x$ through, say, $l(x)$, cf. [4]).

On the other hand, the twofold idealization (or abstraction) connected with the model presented here enables to pick out the basic methodological feature of this model which can be easily extended to algorithmical-complexity-based models of more complicated notions of classical probability (e.g. Markov chains). Defining a notion
conceived, as it is the rule in classical probability theory, as a property of a generator which produces random outputs, we must always suppose that this property is projected, somehow, into the combinatorial properties of the output sequence (in the opposite case this property would be of purely metaphysical nature with no possibility to test it on the ground of the observed outputs). Now, the combinatorial (algo-rithmic-complexity based) alternative of the notion in question can be defined by the set of infinite output sequences for which the corresponding combinatorial property represents the shortest way how to define them (the only combinatorial property binding the realizations of classical i.i.d. sequences is the asymptotic stability of relative frequences of particular letters and it is just the property from which the definition of PIID-sequences takes profit). Again, a more detailed formulation and investigation of this methodological principle would deserve some effort.

## ACKNOWLEDGEMENT

The author thanks to Jan Šindelăr for valuable remarks and comments which much improved the final version of this paper.
(Received September 30, 1985.)

## REFERENCES

[1] M. Davis: Computability and Unsolvability. McGraw-Hill New York 1958.
[2] T. L. Fine: Theories of Probability - An Examination of Foundations. Academic Press, New York-London 1973.
[3] I. Kramosil: Monte-Carlo methods from the point of view of algorithmic complexity. In: Trans. 9th Prague Conf. on Inform. Theory, Statist. Dec. Functions and Random Processes, pp. 39-51. Academia, Prague 1983.
[4] I. Kramosil: Recursive classification of pseudo-random sequences. Kybernetika 20 (1984), supplement, pp. 1-34.
[5] I. Kramosil and J. Šindelăr: Infinite sequences of high algorithmic complexity. Kybernetika 20 (1984), 6, 459-466.
[6] P. Martin-Löf: The definition of random sequences. Inform. and Control 9 (1966), 602-619.
[7] H. Rogers, Jr.: Theory of Recursive Functions and Effective Computability. McGraw-Hill, New York 1967.
[8] C.-P. Schnorr: Zufälligkeit und Wahrscheinlichkeit. (Lecture Notes in Mathematics 218.) Springer-Verlag, Berlin-Heidelberg-New York 1971.

RNDr. Ivan Kramosil, CSc., Ústav teorie informace a automatizace ČSAV (Institute of Information Theory and Automation - Czechoslovak Academy of Sciences), Pod vodàrenskou věži 4, 18208 Praha 8. Czechoslovakia.

