A Unified Approach to the Definition of Random Sequences

by

C. P. SCHNORR

Institut für Angewandte Mathematik
Universität Saarbrücken, West Germany

ABSTRACT

Using the concept of test functions, we develop a general framework within which many recent approaches to the definition of random sequences can be described. Using this concept we give some definitions of random sequences that are narrower than those proposed in the literature. We formulate an objection to some of these concepts of randomness. Using the notion of effective test function, we formulate a thesis on the "true" concept of randomness.

1. The Concept of Test Function. Let X^∞ $[X^*]$ be the set of all infinite [finite] binary sequences. $\Lambda \in X^*$ denotes the empty sequence. $|x|$ denotes the length of $x \in X^*$. The concatenation of sequences x and y is described as the product xy. This in an obvious way defines a product $AB \subset X^* \cup X^\infty$ of sets $A \subset X^*$ and $B \subset X^* \cup X^\infty$. For a sequence $x \in X^* \cup X^\infty$ we denote by $x(n)$ the initial segment of length n ($x(n) = x$ if $|x| < n$). The map φ: $2^{X^*} \to 2^{X^\infty}$ is defined by $\varphi(A) = AX^\infty$ ($A \subset X^*$). Throughout the paper μ will be the product measure on X^∞ relative to the probability $\frac{1}{2}$ for 1 and 0.

Let us first explain the intuitive idea of random sequences, which will be discussed here. An infinite sequence is considered a random sequence if it withstands all constructive stochasticity tests. Our main assumption is that any stochasticity test can be expressed by a function F: $X^* \to R$, where $F(x)$ indicates the extent to which the sequence x is susceptible to the stochasticity test F (R is the set of all reals). It seems natural to think that $F(x)$ is high when x is susceptible to the test and low otherwise. However, this is not inevitable. Let us give some examples.

Consider a function V: $X^* \to R^+$ that indicates the capital of a gambler when playing on binary sequences (R^+ is the set of all non-negative reals). $V(x)$ denotes the capital after the $|x|$st trial when the sequence of the gambling system has the initial segment x. In a fair gambling system the player's gain has to satisfy the relation $V(x) = 2^{-1}(V(x1) + V(x0))$. It is natural to think that $\limsup_n V(z(n)) < \infty$ if z is a random sequence. Consequently high values $V(z(n))$ mean that the sequences $z(n)$ are susceptible to test V. Gambling systems of this kind were introduced by J. Ville [15]. Ville proved that for every function V: $X^* \to R^+$ satisfying $V(x) = 2^{-1}$ $(V(x0)+V(x1))$ the set $\{z \in X^\infty | \limsup_n V(z(n)) = \infty\}$ is a null set.

To give another example, we define a set $U \subset N \times X^*$ to be a sequential test if $U_i =_{\text{def}} \{x \in X^* | (i, x) \in U\}$ satisfies

(1) $U_i = U_i X^*$;
(2) $U_{i+1} \subset U_i$;
(3) $\mu\varphi(U_i) \leq 2^{-i}$.

Then for every null set $\mathfrak{N} \subset X^\infty$ there is a sequential test U such that $\mathfrak{N} \subset \bigcap_{i \in N} \varphi(U_i)$. Relative to the sequential test U the critical level function m_U: $X^* \to N$ is defined by $m_U(x) = \max \{m | x \in U_m\}$. Consequently z withstands the sequential test U if and only if

$$\limsup_n m_U(z(n)) < \infty.$$

Hence m_U reflects our intuition of a test function. A sequential test U is called recursive if $U \subset N \times X^*$ is recursively enumerable (r.e.). These tests were introduced by Martin-Löf [6]. A sequence $z \in X^\infty$ is random in the sense of Martin-Löf if $z \notin \bigcap_{i \in N} \varphi(U_i)$ for every recursive sequential test.

In order to generalize the above mentioned examples, we define a function F: $X^* \to R$ to be a constructive test if F satisfies the following properties, which will be stated in an informal way.

(T1) F has to be constructive, i.e., F is to be given by algorithms.
(T2) There is a rule which assigns to F a null set $\mathfrak{N}_F \subset X^\infty$, the set of infinite sequences which do not withstand the test F. Whether $z \in \mathfrak{N}_F$ has to depend only on the sequence $(F(z(n)) | n \in N)$.

The different definitions of random sequences we shall discuss here are merely distinguished by specifying the above mentioned axioms more precisely. We shall essentially consider two different rules according to (T2), namely:

(a) $$\mathfrak{N}_F = \{z \in X^\infty | \limsup_n F(z(n)) = \infty\},$$

(b) $$\mathfrak{N}_F = \{z \in X^\infty | \liminf_n F(z(n)) = \infty\}.$$

Because of (T1) the set of test functions of any fixed concept of test functions can be enumerated. This implies that relative to any concept of test functions satisfying the above mentioned axioms the following theorem is true.

THEOREM 1.1. *The set of random sequences has measure 1.*

Given a fixed concept of test functions, a test F is called *universal* if $\mathfrak{N}_F \supset \mathfrak{N}_{F_i}$ for any other test F_i.

2. Martin-Löf Random Sequences Described by Martingales. Let Q be the set of all rational numbers.

Definition 2.1. A (total) function F: $X^* \to R$ is called weakly computable if there is a recursive function g: $N \times X^* \to Q$ such that

$$g(i, x) \leq g(i+1, x) \qquad (i \in N, x \in X^*)$$

$$\lim_i g(i, x) = F(x) \qquad (x \in X^*).$$

A function F: $X^* \to R$ is computable in the usual sense if F and $-F$ are weakly computable.

A function F: $X^* \to R$ is said to have the martingale property relative to the probabilities $\frac{1}{2}$ for 0 and 1 if it satisfies the condition

$$(2.2) \qquad F(x) = \tfrac{1}{2}F(x0)+\tfrac{1}{2}F(x1) \qquad (x \in X^*).$$

These functions are called martingales. In the actual case this means that the extent to which x withstands the test F is the weighted average of the extent to which $x0$ and $x1$ withstand the same test.

The following lemma was proved by J. Ville [15].

LEMMA 2.3. *If F: $X^* \to R^+$ satisfies (2.2), then the set $\mathfrak{N} = \{z \in X^\infty \mid \limsup_n F(z(n)) = \infty\}$ is a null set.*

Proof. We define for $k \in N$:

$$F_k = \{x \in X^* \mid F(x) > k\}$$
$$\bar{F}_k = \{x \in F_k \mid x \notin F_k XX^*\}.$$

This implies $\bar{F}_k \cap \bar{F}_k XX^* = \varnothing$. $\bar{F}_k$ consists of all those sequences in F_k which have no initial segment in F_k. We have $\mu\varphi(F_k) = \mu\varphi(\bar{F}_k) = \sum_{x \in \bar{F}_k} 2^{-|x|}$. It follows from (2.2) that

$$F(\Lambda) \geq \sum_{x \in \bar{F}_k} F(x)2^{-|x|} \geq k \sum_{x \in \bar{F}_k} 2^{-|x|} \geq k\mu\varphi(F_k).$$

Consequently,

$$(2.4) \qquad \mu\varphi(F_k) \leq F(\Lambda)k^{-1}$$

Since $\mathfrak{N} \subset \bigcap_{k \in N} \varphi(F_k)$, this proves that $\mathfrak{N}$ is a null set.

We are now able to present our first example of a concept of a test function.

Definition 2.5. A total function F: $X^* \to R^+$ is a (1)-test if it is weakly computable and satisfies (2.2). The set of infinite sequences which do not withstand the (1)-test F is defined to be

$$\mathfrak{N}_F = \{z \in X^\infty \mid \limsup_n F(z(n)) = \infty\}.$$

Definition (2.5) is justified by the following theorem.

THEOREM 2.6. *An infinite sequence withstands all (1)-tests if and only if it is random in the sense of Martin-Löf.*

First we will prove a lemma.

LEMMA 2.7. *For every r.e. set $A \subset X^*$ one can effectively construct a recursive set $B \subset X^*$ such that $AX^* = BX^*$ and $B \cap BXX^* = \varnothing$, i.e. B is prefix-free.*

Proof. Let A be given by a recursive function h: $N \to X^* \cup \{|\}$ such that $A = h(N) \cap X^*$. (The symbol $|$ has to be used if A is empty.) We denote $A_n = \bigcup_{i \leq n} h(i) \cap X^*$. $r(n)$ is to be the maximal length of sequences in A_n, $r(n) = 0$ if $A_n = \varnothing$. The indicator function I_B: $X^* \to \{0, 1\}$ of the set B is defined as follows: $I_B(x) = 0$ for all $x \in X^*$ such that $|x| \neq r(n)+n$ for all $n \in N$. $I_B(x)$ with $|x| = r(n)+n$ is defined recursively. For $|x| = r(0)$:

$$I_B(x) = \begin{cases} 1 & x = h(0) \\ 0 & \text{otherwise,} \end{cases}$$

and for $|x| = r(n)+n,\ n \geq 1$:

$$I_B(x) = \begin{cases} 1 & x \in h(n)X^* - A_{n-1}X^* \\ 0 & \text{otherwise.} \end{cases}$$

The construction implies that B is prefix-free. In addition we have $A_nX^* = (B \cap \{x| \ |x| \leq r(n)+n\})X^*$. Hence $AX^* = BX^*$, as desired.

In the following proof of (2.6) we shall assume that a recursive sequential test U is given by an r.e. set $V \subset N \times X^*$ such that $V_i \cap V_iXX^* = \varnothing$ and $V_iX^* = U_i$ $(i \in N)$.

Proof of (2.6). (1) Let a recursive sequential test U be given an r.e. set $V \subset N \times X^*$ as above. We define the (1)-test F: $X^* \to R^+$ as follows:

$$F(x) = \sum_{i \in N} i \Bigg(\sum_{xy \in V_i} 2^{-|y|} + \sum_{\substack{x(n) \in V_i \\ n < |x|}} 1 \Bigg)$$

It is easy to verify that F satisfies the relation (2.2). One has only to consider the contributions to $F(x)$, $F(x0)$, $F(x1)$ which result from $y \in V_i$. Since V_i is prefix-free, we have $F(\Lambda) = \sum_{i \in N} \mu\varphi(V_i)$. Therefore $F(\Lambda)$ is bounded. Hence F is a function F: $X^* \to R^+$. From the definition of F it follows immediately that F is weakly computable. Let us suppose now that $z \in \varphi(V_i)$. Hence there is an n such that $z(n) \in V_i$. This implies $F(z(n)) \geq i$. It follows that $\bigcap_{i \in N} \varphi(V_i) \subset \mathfrak{R}_F$.

(2) Let z be random in the sense of Martin-Löf and let F: $X^* \to R^+$ be a (1)-test. Choose $k > F(\Lambda)$ and define $V \subset N \times X^*$ as follows:

$$V_i = \{x \in X^* | F(x) > 2^i k\}.$$

Since F is weakly computable, V is r.e. Because of (2.4) we have $\mu\varphi(V_i) \leq 2^{-i}$. Hence a recursive sequential test U can be defined by $U_i = V_iX^*$. From $z \notin \bigcap_{i \in N} \varphi(U_i)$ it follows that z withstands the test F.

Perhaps it is interesting to note that the existence of a universal (1)-test follows from a simple argument. Let $(F_i | i \in N)$ be a recursive enumeration of all (1)-tests with $F_i(\Lambda) \leq 1$. Hence $F = \sum_{i \in N} 2^{-i} F_i$ is a universal (1)-test.

It should be noted that we can use lim inf as well as lim sup in the definition of $\mathfrak{R}_F$ for a (1)-test F.

LEMMA 2.8. *Let F be a universal (1)-test. Then the following equivalence holds for all $z \in X^\infty$:*

$$\liminf_n F(z(n)) = \infty \Leftrightarrow \limsup_n F(z(n)) = \infty.$$

Proof. Let $U \subset N \times X^*$ be a universal recursive sequential test that is given by a r.e. set $V \subset N \times X^*$ as in part (1) of the proof of (2.6). Consider the (1)-test

F as defined in part (1) of the proof of (2.6). It will suffice to show that $z \in \bigcap_{i \in N} \varphi(V_i)$ implies $\lim_n F(z(n)) = \infty$.

Suppose $z \in \bigcap_{i \in N} \varphi(V_i)$. Then to $i \in N$ there exists $n \in N$ such that $z(n) \in V_i$. This implies $F(z(m)) \geq i$ for all $m \geq n$. Since this holds for every $i \in N$, (2.8) is proved.

3. An Objection to Randomness in the Sense of Martin-Löf. The algorithmic structure of a (1)-test F is not symmetrical. There is no reason why a martingale F should be weakly computable and $-F$ should not be so. Taking this into consideration we make the following definition.

Definition 3.1. A function F: $X^* \to R^+$ is a (2)-test if it satisfies (2.2) and if $-F$ is weakly computable. The set of sequences that do not withstand the test F is defined to be

$$\mathfrak{N}_F = \{z \in X^\infty \mid \limsup_n F(z(n)) = \infty\}.$$

We consider the question whether (1)-randomness is equivalent to (2)-randomness. There seems to be an objection to either of these concepts of randomness because this is not true.

THEOREM 3.2. *There exist sequences which are (2)-random and which are not (1)-random.*

We will first prove a lemma.

LEMMA 3.3. *Let F be a (2)-test and $a > 0$ a rational number. Then there exists a recursive $z \in X^\infty$ such that $F(z(n)) < F(\Lambda)+a$ $(n \in N)$. This means that $z \notin \mathfrak{N}_F$.*

Proof. Let the (2)-test F be given by a recursive g: $N \times X^* \to Q$ such that $g(i, x) \geq g(i+1, x)$ and $\lim \sup_n g(i, x) = F(x)$. Let b be rational with $F(\Lambda) - a/2 < b < F(\Lambda)$. The sequence z will be constructed recursively as follows. Assume that $z(n)$ has been constructed such that

$$F(z(n)) \leq b + a \sum_{j=0}^{n} 2^{-j-1} \qquad (i \leq n).$$

(Note that this assumption is trivial for $n = 0$.) Consequently, there exists an $x \in X$ with

$$F(z(n)x) \leq b + a \sum_{j=0}^{n} 2^{-j-1}.$$

Hence we can effectively determine i and x such that

$$g(i, z(n)x) \leq b + a \sum_{j=0}^{n+1} 2^{-j-1}.$$

Define $z(n+1) = z(n)x$. From the construction it follows that

$$F(z(n)) \leq b + a \leq F(\Lambda) + a \qquad (n \in N).$$

Proof of (3.2). Let $(F_i | i \in N)$ be an enumeration of all (2)-tests with $F_i(\Lambda) \leq 1$.

It will suffice to define a sequence z which is not (1)-random and satisfies $\limsup_n F_i(z(n)) < \infty$ for all $i \in N$.

Let F be a universal (1)-test, i.e. $X^\infty - \mathfrak{N}_F$ consists precisely of all (1)-random sequences. $z \in X^\infty$ will be defined inductively. Assume that $z(n_k)$ with $n_k \in N$ is already defined such that $F(z(n_k)) \geq k$, and that

$$\sum_{i=0}^{k} 2^{-n_i-i}F_i(z(j)) \leq \sum_{i=0}^{k} 2^{-i+1} \qquad (j \leq n_k).$$

(Note that the induction hypothesis is trivial for $k = 0$, $n_0 = 0$ and $F_0(\Lambda) \leq 1$.)

To perform the induction step, we consider F_{k+1}. We obviously have $2^{-n_k-k}F_{k+1}(z(n_k)) \leq 2^{-k}$. This follows from $F_{k+1}(\Lambda) \leq 1$ and the martingale property. Consequently there is a recursive $y \in X^\infty$ such that $y(n_k) = z(n_k)$ satisfying for every $n_{k+1} \geq n_k$ the relation

$$\sum_{i=0}^{k+1} 2^{-n_i-i}F_i(y(j)) \leq \sum_{i=0}^{k+1} 2^{-i+1} \qquad (j \in N).$$

This essentially follows from the construction used in the proof of (3.3).

Since y is recursive there is a $n_{k+1} > n_k$ such that $F(y(n_{k+1})) > k+1$. Define $z(n_{k+1}) = y(n_{k+1})$.

The definition of z implies that $z \in \mathfrak{N}_F$. On the other hand we have

$$\limsup_j \sum_{i=0}^{\infty} 2^{-n_i-i}F_i(z(j)) \leq 4 \qquad (i \in N).$$

Consequently $z \notin \mathfrak{N}_{F_i}$ $(i \in N)$.

We remark that it is not difficult to prove that every (1)-random sequence is also (2)-random. (1)-randomness is a narrower concept of random sequences than (2)-randomness. It seems surprising that for a martingale F it is important whether we choose F or $-F$ to be weakly computable.

Now we aim at developing a concept of randomness based on martingales whose algorithmic structure is symmetrical.

Definition 3.4. A martingale $F: X^* \to R^+$ is a (3)-test if there is a recursive function $g: N \times X^* \to Q$ such that $\lim_i g(i, x) = F(x)$ $(x \in X^*)$. The set of sequences that do not withstand a (3)-test F is defined to be

$$\mathfrak{N}_F = \{z \in X^\infty \mid \lim_n F(z(n)) = \infty\}.$$

We will prove that (3)-randomness is considerably narrower than (1)-randomness. Obviously every (1)-test is also a (3)-test. Therefore every (3)-random sequence is a (1)-random sequence. To prove that the converse does not hold, we consider the Kleene hierarchy of sets.

The Kleene hierarchy of predicates classifies the "arithmetical" sets in classes Σ_n, Π_n $(n = 0, 1, \cdots)$ defined as follows. Σ_n is the class of all sets A of the form $A = \{a \mid (Q_1x_1)\ (Q_2x_2)\cdots(Q_nx_n)P(a, x_nx_2, \cdots, x_n)\}$, where P is a recursive predicate, the Q_{2k+1} are existential quantifiers and the Q_{2k} are universal quantifiers. Π_n is the class of all sets as above, except that the Q_{2k+1}

are universal quantifiers and the Q_{2k} are existential quantifiers. The following facts are known (see Davis [17]).

(1) $\Sigma_0 = \Pi_0 = \Sigma_1 \cap \Pi_1$ is the collection of all recursive sets.
(2) $A \in \Sigma_n \Leftrightarrow A^c \in \Pi_n$ (A^c is the complement of A.)
(3) $\Sigma_n \cup \Pi_n \subset \Sigma_{n+1} \cap \Pi_{n+1}$ for all $n \geq 0$ and containment is proper for $n > 0$.
(4) $A \in \Sigma_{n+1} \Leftrightarrow A$ is recursively enumerable relative to a set $B \in \Pi_n$.
(5) $A \in \Sigma_{n+1} \cap \Pi_{n+1} \Leftrightarrow A$ is a recursive relative to a set $B \in \Pi_n$.

The class $\Pi_n \cap \Sigma_n$ is usually denoted by Δ_n. A sequence $z \in X^\infty$ is to be in Σ_n $[\Pi_n]$ if $\{n | z_n = 1\}$ is in Σ_n $[\Pi_n]$.

LEMMA 3.5. *There exist sequences in Δ_2 which are (1)-random.*

Proof. Let F: $X^* \to R^+$ be a universal (1)-test that is given by a recursive function g: $N \times X^* \to Q$. We suppose that $F(\Lambda) < 1$. Then the following predicate P: $X^* \to \{0, 1\}$ is in Π_1: $P(x) = 1 \Leftrightarrow \forall_{i \in N} g(i, x) < 1$. Given P one can construct $z \in X^\infty$ recursively as follows: $z_{i+1} = 1 \Leftrightarrow P(z(i)1) = 1$. Hence it follows from the above property (5) that z is in Δ_2. The construction implies that $z \notin \mathfrak{N}_F$.

To complete the proof of our assertion that (3)-randomness is considerably narrower than (1)-randomness, we establish the following theorem.

THEOREM 3.6. *There do not exist sequences in $\Sigma_2 \cup \Pi_2$ which are (3)-random.*

Proof. (I) Let z be a sequence in Σ_2. According to the definition this means that $\{n | z_n = 1\}$ is in Σ_2. Then there exists a recursive predicate P: $N^3 \to \{0, 1\}$ such that, for all $n \in N$, $z_n = 1 \Leftrightarrow \exists_{j \in N} \forall_{i \in N} P(j, i, n) = 1$. We define a (3)-test F satisfying $z \in \mathfrak{N}_F$ by specifying a recursive function g: $N \times X^* \to Q$. We denote

$$f(i, n) = \{j | \forall_{r \leq i} P(j, r, n) = 1; j \leq i\}.$$

The finite set $f(i, x)$ can be effectively determined. Then we compute $g(i, x)$ recursively as follows: $g(i, \Lambda) = 1$ $(i \in N)$. If $(f(i, n) \neq \varnothing \wedge y_n = 1) \vee (f(i, n) = \varnothing \wedge y_n = 0)$ we define $g(i, y(n)) = 2g(i, y(n-1))$ $(y \in X^\infty)$. If $(f(i, n) \neq \varnothing \wedge y_n = 0) \vee (f(i, n) = \varnothing \wedge y_n = 1)$ we define $g(i, y(n)) = 0$ $(y \in X^\infty)$. This implies that

$$\lim_i g(i, y(n)) = \begin{cases} 2 \lim_i g(i, y(n-1)) & z_n = y_n. \\ 0 & z_n \neq y_n. \end{cases}$$

Hence F is a (3)-test and it follows that

$$F(y(n)) = \begin{cases} 2^n & y(n) = z(n) \\ 0 & y(n) \neq z(n). \end{cases}$$

(II) Let z be an element of Π_2. This means that $\{n | z_n = 0\}$ is in Σ_2. Hence the above argument also implies that z is not (3)-random.

4. Random Sequences and the Concept of Minimal Program Complexity. We shall prove that the concept of randomness that has been proposed by Loveland [5] is narrower than the definition of random sequences by Martin-Löf.

Let $A\colon X^*\times N \to X^*$ be a partial recursive function satisfying $A(x, n) \in X^n$ for all (x, n) in the domain of A. Kolmogoroff [4] defined the conditional complexity $K_A(x|n)$ of a sequence x with length n relative to the algorithm A:

$$K_A(x|n) = \begin{cases} \infty \text{ if } A(y, n) \neq x \text{ for all } y \in X^*, \\ \min\{\,|y| \;|A(y, n) = x\} \text{ otherwise.} \end{cases}$$

If $A(y, n) = x$, then y is called a program to compute the sequence x by the algorithm A.

Definition 4.1. A function $F\colon X \to Q$ is called a (4)-test if there is a p.r. function $A\colon X^*\times N \to X^*$ as above, such that $F(x) = n - K_A(x|n)$ for all sequences x of length n. $\mathfrak{N}_F = \{z \in X^\infty |\lim\inf_n F(z(n)) > \infty\}$ is the set of sequences that do not withstand the (4)-test F.

This definition of randomness has been explicitly proposed by Loveland in terms of the uniform complexity [5]. (4)-randomness means that for every algorithm A there exist infinitely many initial segments with high program complexity. The original idea was that every random sequence z would satisfy $\lim\sup_n (n - K_A(z(n)|n)) < \infty$ for every algorithm A. However it was shown by Martin-Löf [7] that there exist no sequences that satisfy this property.

Martin-Löf [7] proved that $\mathfrak{N}_F$ is a null set for every (4)-test F. Hence, Definition 4.1 satisfies our axioms (T1) and (T2) of a test function. Moreover, it is known from [7] that every (4)-random sequence is random in the sense of Martin-Löf. We shall prove that the converse of this theorem does not hold.

THEOREM 4.2. *There exists a sequence* $z \in X^\infty$ *and a p.r. function* A: $X^*\times N \to X^*$ *such that* $\lim_n (n - K_A(z(n)|n)) = \infty$ *and* z *is a Martin-Löf random sequence.*

Proof. Let $F\colon X^* \to R^+$ be a universal (1)-test with $F(\Lambda) \leq 1$ that is given by the recursive function $g\colon N\times X^* \to Q$. We consider the (1)-random sequence $z \in \Delta_2$ defined as in the proof of Lemma 3.5. $P\colon X^* \to \{0, 1\}$ is the following predicate in Π_1: $P(x) = 1 \Leftrightarrow \forall_{i\in N}\, g(i, x) \leq 1$. Given P we define z recursively as follows: $z_{i+1} = \min\{j \in X | P(z(i)j) = 1\}$. z is (1)-random and we construct a p.r. function $A\colon X^*\times N \to X^*$ such that $\lim_n (n - K_A(z(n)|n)) = \infty$.

Let $h\colon N \to N\times X^*\times Q$ be the recursive function defined by $h(N) = \{(i, x, q)|g(i, x) = q\}$. There exists a p.r. function $A\colon X^*\times N \to X^*$ such that, for all $x \in X^*$, $A(x, i+|x|) = r(i, x)\, x$. Hereby we define $r(i, x) \in X^i$ recursively as follows:

$$r(0, x) = \Lambda \qquad (x \in X^*),$$

$$r(i+1, x) = r(i, x)s(i, x)$$

with

$$s(i, x) = \min\left\{ j \in X \;\middle|\; \begin{matrix} h(m) = (i, r(i, x)j, q) \\ \text{and } m \leq |x| \Rightarrow q \leq 1 \end{matrix} \right\}.$$

Hereby we suppose that $\min \varnothing = 1$.

Using this construction it can easily be proved that for every $i \in N$ there exists an $n_i \in N$ such that, for all $x \in X^*$ with $|x| \geq n_i$, $A(x, i+|x|) = z(i)x$. Consequently $\lim_n (n - K_A(z(n)|n)) = \infty$.

It is obvious that there is an inconceivable multiplicity of possibilities to define test functions satisfying conditions (T1), (T2). Therefore one problem still remains unsolved, which we shall discuss later. It deals with the question which concept among all possible concepts of test functions is the really "true" one and if such a distinguished concept exists at all.

5. An Objection to the Concept of (4)-Randomness. We shall formulate an objection to the concept of (4)-randomness, although (4)-random sequences possess all standard statistical properties of randomness such as the law of large numbers and the law of the iterated logarithm. Our main objection shall be discussed later. It concerns our feeling that properties of randomness are imposed on (4)-random sequences that have no physical meaning.

Another difficulty arises from the fact that there is no analogue to the martingale property (2.2) regarding (4)-tests.

This lack of an analogue to (2.2) has the consequence that a (4)-random sequence z has infinitely many initial sequences $z(n)$ with high values $F(z(n))$ relative to a universal (4)-test F (high values $F(z(n))$ mean low complexity of $z(n)$). This follows from an argument by Martin-Löf [7] which, when applied to (4)-randomness, shows that there exists no infinite sequence z such that $\limsup_n F(z(n)) < \infty$. Because of Lemma 2.8 this effect is excluded as regards (1)-randomness.

It seems natural to define a hierarchy of complexity for infinite sequences as follows (in a similar manner this has been done by Loveland who used the uniform complexity measure [5]). Let F be a universal (4)-test. Its existence is proved in [4] and [14]. For every non-decreasing function f we denote

$$(5.1) \qquad C_f =_{\text{def}} \{z \in X^\infty \mid \liminf_n (F(z(n)) - f(n)) < \infty\}.$$

If f is bounded, then C_f is exactly the set of all (4)-random sequences. For a slowly increasing unbounded function f the sequences in C_f are expected to be approximately random. This, however, is by no means true. On the contrary, we can prove the following theorem which also holds relative to (4)-random sequences and for the concepts of randomness derived from the unconditional (cf. [4]) and also for uniform complexity measures.

THEOREM 5.2. *Let f: $N \to N$ be a non-decreasing unbounded function. Then there exists a sequence in C_f that does not satisfy the law of large numbers.*

From the statistical point of view the law of large numbers is one of the most basic laws of randomness. There are very simple statistical tests which reject sequences not satisfying this law. Therefore the sequences in C_f, even with a very slowly increasing unbounded f, cannot be viewed as approximately random. And this is an objection to (4)-randomness.

We remark that Theorem 5.2 solves the question of Loveland [5] whether there exists a non-decreasing unbounded f such that C_f is precisely the set of all random sequences. Because of Theorem 5.2 such a function cannot exist.

Proof. Let f: $N \to N$ be an unbounded non-decreasing function and let F be a universal (4)-test. We define $z = z_1 z_2 \cdots z_i \cdots \in X^\infty$ by induction. Suppose that $z(n_i)$ is already defined. Then we set $z_k = 1$ for $n_i < k \leq 2n_i$. It is obvious that there exists a (4)-random sequence x such that the initial sequence $x(2n_i)$ is equal to $z(2n_i)$. Then there is an $m > 2n_i$ such that $F(x(m)) < f(m)$, since otherwise x would be not (4)-random. We define $z(m) = x(m)$. Now take m for n_{i+1} and proceed by induction. The construction obviously implies that $z \in C_f$, and on the other hand the relation $\lim_n (1/n) \sum_{i=1}^{n} z_i = \frac{1}{2}$ cannot be satisfied.

Remark. Theorem 5.2 also holds in this form for the concept of (1)-randomness, that is, if F in (5.1) is a universal (1)-test. However, this is no longer an argument against this concept of random sequences. Since we have used lim sup in the definition of (1)-tests, the appropriate hierarchy of sequences relative to the concept of (1)-randomness has to be defined as follows, where F is a universal (1)-test and $f: N \to N$ is a non-decreasing function:

$$(5.3) \qquad K_f = \{z \in X^\infty \mid \limsup_n (F(z(n)) - f(n)) < \infty).$$

From a theorem in Schnorr [11] it follows that all sequences in K_f satisfy the law of large numbers if $f(n)$ increases less than any exponential function $a^n (a > 1)$. On the other hand, Theorem 5.2 is not a suitable definition relative to a universal (4)-test F. It follows from an argument by Martin-Löf that in this case K_f is empty for all slowly increasing functions f. For instance, the relation $\sum_{n=1}^{\infty} 2^{-f(n)} = \infty$ implies that $K_f = \varnothing$ [7].

6. On the True Concept of Randomness. The deficiency residing in the previous concepts of randomness is, in our opinion, that properties of random sequences are postulated which are of no significance to statistics. Many insufficient approaches have been made until a definition of random sequences was proposed by Martin-Löf which for the first time included all standard statistical properties of randomness. However, the inverse postulate now seems to have been violated.

The acceptable definition of random sequences cannot be any formulation of recursive function theory which contains all relevant statistical properties of randomness, but it has to be precisely a characterization of all those properties of randomness that have a physical meaning. These are intuitively those properties that can be established by statistical experience. This means that a sequence fails to be random in this sense if and only if there is an effective process in which this failure becomes evident. On the other hand, it is clear that if there is no effective process in which the failure of the sequence to be random appears, then the sequence behaves like a random sequence. Therefore the definition of random sequence has to be made in such a way that this sequence is random by definition.

In a series of papers [9, 10, 11, 12] we tried to render clear this intuitive notion of randomness. It turns out that there are rather different approaches to this concept of which all lead to equivalent definitions. This paper has been written to give a comprehensive approach by test functions.

From the point of view of test functions one would consider a sequence to be random if it stands all effective tests. But how are the effective tests to be defined? It is natural to postulate that an effective test $F: X^* \to R$ is computable in the ordinary sense instead of being merely constructive.

Definition 6.1. A function $F\colon X^* \to R$ is computable if there is a recursive function $g\colon N \times X^* \to Q$ such that $|g(n, x) - F(x)| \leq 2^{-n}$ ($x \in X^*$, $n \in N$).

Our considerations in Section 5 should have made clear that a reasonable concept of test function has to include the martingale property (2.2). Computability and the martingale property suffice to characterize effective tests. But which sequences are refused by an effective test? In analogy to (2.3) one would define that a sequence z does not withstand the test F if and only if $\limsup_n F(z(n)) = \infty$. However, if the sequence $F(z(n))$ increases so slowly that no one working with effective methods only would observe its growth, then the sequence z behaves as if it withstands the test F. The definition of $\mathfrak{N}_F$ has to reflect this fact. That is, we have to make constructive the notion $\limsup_n F(z(n)) = \infty$.

Definition 6.2. Let $f\colon N \to N$ be a function. We write $k \limsup_n f(n) = \infty$, if and only if there exists a recursive, monotone and unbounded function $g\colon N \to N$ such that $\limsup_n (f(n) - g(n)) \geq 0$.

Now we present our concept of effective tests [10].

Definition 6.3. A function $F\colon X^* \to R^+$ is an effective test if it is computable and satisfies the martingale property. The set of sequences that do not withstand the test F is defined to be $\mathfrak{N}_F = \{z \in X^\infty \mid k \limsup_n F(z(n)) = \infty\}$.

A sequence is called (0)-random if it withstands all effective tests. It is our thesis that (0)-randomness characterizes all relevant statistical properties of random sequences. To confirm this thesis we shall restate some results from earlier papers.

In [11] we established two interesting classifications of the properties of random sequences. A law of stochasticity is called of order f($f\colon N \to N$ is a non-decreasing function) if there is an effective test $F\colon X^* \to R^+$ such that

$$\limsup_n \,(F(z(n))/f(n)) \geq 0 \tag{6.4}$$

for all $z \in X^\infty$ that do not satisfy this law.

The growth of the function f indicates the importance of the law under consideration. It is shown in [11] that the law of large numbers has a rapidly growing order function. This is in harmony with the fact that the law of large numbers is certainly one of the most basic laws of probability. It is also shown in [11] that the class of laws having the same order as the law of large numbers is a very reasonable class. As is the case with some other concepts of randomness, the set of recursive sequences can be characterized in terms of test functions. A sequence is recursive if and only if it does not satisfy some law of order $f(n) = 2^n$ (as will be proved in [16]).

The above results relative to the order of a law hold for effective tests, as well as for (1)-tests, if a suitable formulation is chosen. However, the second classification of tests which is based on the complexity of test functions (regarding the amount of time and space to compute them [3]) is meaningful for effective tests only.

There is no universal effective test. To every effective test F a recursive sequence not in $\mathfrak{N}_F$ can be constructed. To every effective test $\bar{F}$ there exists an equivalent effective test $F: X^* \rightarrow Z(2)$ that is recursive ($Z(2)$ is the set of all finite dual fractions in R^+). Let us consider a fixed complexity class (according the amount of time or space) of effective test functions $F: X^* \rightarrow Z(2)$. One can construct recursive sequences which will stand every effective test of a fixed complexity class [11].

An infinite sequence z has a certain degree of (0)-randomness if it stands all tests of a corresponding complexity class. The degree of (0)-randomness yields a classification of recursive sequences. Sequences that have a certain degree of (0)-randomness have very interesting properties ([11], [12]).

It is the opinion of the author that this classification of recursive sequences relative to their degree of (0)-randomness is an important argument for the concept of effective tests. The existence of (1)-random sequences as well as that of (0)-random sequences can be proved by non-constructive methods only. These sequences exist only by virtue of the axiom of choice. However, we can approximate the behaviour of (0)-random sequences by constructive methods. This does not hold for (1)-random sequences. Because of Theorem 3.2, (1)-randomness is not equivalent to (0)-randomness (see also [9]).

Another important argument for our thesis which proposes (0)-randomness as the "really true" concept of randomness is that some different approaches lead to an equivalent definition. It is proved in [10, Part I] that a sequence is (0)-random if and only if it is not contained in any null set in the sense of Brouwer. This concept of null set is current in constructive analysis (see, for instance, [1]) and dates back to an intuitionistic formulation of L. E. J. Brouwer [2]. A reasonable characterization of (0)-random sequences by their program complexity can be found in [16]. But what is most surprising is that the original ideas on which von Mises based his concept of collective can be modified to characterize exactly the (0)-random sequences. It is shown in [10] that a sequence z is (0)-random if and only if every sequence y which is an image of z under a constructive measure-preserving map $H: X^\infty \rightarrow X^\infty$ satisfies the law of large numbers. This means that the concept of Stellenauswahl in [8] has to be replaced by the notion of constructive measure-preserving map. All these and some additional results will be included in [16].

REFERENCES

[1] E. Bishop, *Foundations of Constructive Analysis*, McGraw-Hill, New York, 1967.

[2] L. E. J. Brouwer, Begründung der Mengenlehre unabhängig vom logischen Satz vom ausgeschlossenen Dritten. Zweiter Teil. Verh. Niederl. Akad. Wetensch. Afd. Natuurk. Sect. I **12** (1919), 7.

[3] J. Hartmanis and R. E. Stearns, On the computational complexity of algorithms, *Trans. Amer. Math. Soc.* **117** (1965), 285–306.

[4] A. N. Kolmogoroff, Tri podhoda k opredeleniju ponjatija "količestvo informacii", *Problemy Peredači Informacii* **1** (1965), 3–11.

[5] D. Loveland, On minimal program complexity measures, *ACM Symposium on Theory of Computing*, pp. 61–66, May 5–7, 1969.

[6] P. Martin-Löf, The definition of random sequences, *Information and Control* **9** (1966), 602–619.

[7] P. Martin-Löf, Complexity oscillations in infinite binary sequences, unpublished.

[8] R. VON MISES, Grundlagen der Wahrscheinlichkeitstheorie, *Math. Z.* **5** (1919), 52–99.
[9] C. P. SCHNORR, Eine Bemerkung zum Begriff der zufälligen Folge, *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **14** (1969), 27–35.
[10] C. P. SCHNORR, Über die Definition von effektiven Zufallstests, I–II, *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **15** (1970), 297–312, 313–328.
[11] C. P. SCHNORR, Klassifikation der Zufallsgesetze nach Komplexität und Ordnung, *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **16** (1970), 1–21.
[12] C. P. SCHNORR, Über die Zufälligkeit und den Zufallsgrad von Folgen, Symposium on Formale Sprachen und Automatentheorie, Oberwolfach, 1969.
[13] E. SPECKER, Nicht konstruktiv beweisbare Sätze der Analysis, *J. symb. Logic* **14** (1949), 145–158.
[14] R. J. SOLOMONOFF, A formal theory of inductive inference, I, *Information and Control* **7** (1964), 1–22.
[15] J. VILLE, *Étude Critique de la Notion de Collectif*, Gauthiers-Villars, Paris, 1939.
[16] C. P. SCHNORR, Zufälligkeit und Wahrscheinlichkeit, *Lecture Notes in Mathematics* (in preparation).
[17] M. DAVIS, *Computability and Unsolvability*, McGraw-Hill, New York, 1958.

(*Received 24 April 1970, and*
in revised form 11 August 1970)