Process Complexity and Effective Random Tests

C. P. SCHNORR

Mathematisches Seminar, Universität Frankfurt

Received August 3, 1972

We propose a variant of the Kolmogorov concept of complexity which yields a common theory of finite and infinite random sequences. Processes are sequential coding schemes such as prefix coding schemes. The process complexity is the minimal length of the description of a sequence in a sequential coding scheme. The process complexity does not oscillate. We establish some concepts of effective tests which are proved to be equivalent.

1. INTRODUCTION AND NOTATIONS

Several approaches to define randomness have been made recently. Martin-Löf [3] used constructive measure theory to define infinite random sequences, whereas Kolmogorov introduced the concept of program complexity to define finite random sequences. Up to now it has seemed that different approaches have had to be made to handle randomness of finite and infinite sequences. The main obstacle for a common theory of finite and infinite random sequences is the oscillation behaviour of the Kolmogorov program complexity (Theorem 1). Our variant of the program complexity will circumvent these difficulties. A process essentially is a sequential coding scheme such as block coding schemes and prefix coding schemes. The process complexity is the minimal length of the description of a sequence in a sequential coding scheme.

Let $X^*(\infty)$ be the set of all finite (infinite) binary sequences. $A \in X$ denotes the empty sequence. For $x \in X^*$ we denote by $|x|$ the length of $x$. The product $xy \in X^* \cup \infty$ denotes the concatenation of sequences $x \in X^*$ and $y \in X^* \cup \infty$. Clearly this yields a product $AB \subseteq X^* \cup \infty$ of sets $A \subseteq X^*$ and $B \subseteq X^* \cup \infty$. For $z \in X^* \cup \infty$ we denote by $z(n)$ the initial segment of $z$ with length $n$. $|A|$ denotes the cardinality of a set $A$. We shall write $x \subseteq y$ iff the sequence $x$ is an initial segment of the sequence $y$. $N(R)$ denotes the set of natural (real) numbers. For two functions $f, g: Y \rightarrow R$ we write $f \leq g$ iff \( \exists c \in N: \forall x \in Y: f(x) \leq g(x) + c \) and $f \equiv g$ iff $f \leq g \wedge g \leq f$. $\mu$ denotes the product measure on $\infty$ relative to the probabilities $1/2$ for 0 and 1. $L(n)$ denotes the logarithm of $n + 1$ relative to the basis 2. $D(g)$ denotes the domain of the partial function $g$. 

Copyright © 1973 by Academic Press, Inc.
All rights of reproduction in any form reserved.
2. THE KOLMOGOROV COMPLEXITY OF FINITE SEQUENCES

Let \( A : X^* \rightarrow X^* \) be a partial recursive (p.r.) function, then the program complexity \( KA(x) \) of \( x \in X^* \) relative to \( A \) is defined by

\[
KA(x) = \min\{ |p| \mid A(p) = x \}.
\]

Hereby we use the convention \( \min \emptyset = \infty \).

It is well-known from [2], [7] that there exists a universal p.r. function \( A : X^* \rightarrow X^* \) such that \( KA \preceq KB \) for any p.r. function \( B : X^* \rightarrow X^* \). This implies \( KA \equiv KB \) for any two universal p.r. functions \( A \) and \( B \). In the following \( A \) is any fixed universal p.r. function.

The original intention was to define random sequences \( z \in X^\infty \) as those sequences such that

\[
1 - \lim_{n \to \infty} (n - KA(z(n))) < \infty.
\]

This would mean that there must not be regularities in any initial segment of \( z \) (we consider a sequence \( x \) to be regular if \( KA(x) \) is essentially smaller than \( |x| \)). This intention fails because of the following theorem of Martin-Löf [4].

**Theorem 1.** Let \( f : N \rightarrow N \) be a recursive function such that

\[
\sum 2^{-f(n)} = \infty,
\]

then for any \( z \in X^\infty \) the following holds:

\[
\lim_{n \to \infty} (n - KA(z(n)) - f(n)) = \infty.
\]

Since there exist arbitrary long sequences \( x \) such that \( KA(x) \geq |x| \), Theorem 1 implies that for any \( f \) as above and any \( n \in N \) there exist sequences \( x \) of length greater than \( n \) such that

\[
KA(x) \geq |x| \quad \text{and} \quad KA(x(n)) < n - f(n).
\]

This means that \( x \) is irregular although the initial segment \( x(n) \) is regular. This fact is hard to comprehend and is the main obstacle for a common theory of finite and infinite random sequences. The following modification of the concept of program complexity will circumvent these difficulties.

3. THE PROCESS COMPLEXITY

It has already been observed [1] that there must be some difference in the concept of regularity of finite objects which do not involve a direction (for instance a natural number) and the concept of regularity of infinite sequences (as well as finite sub-
sequences of an infinite sequence) where a natural direction is involved. For example, he who wants to understand a book will not read it backwards, since the comments or facts which are given in its first part will help him to understand subsequent chapters (this means they help him to find regularities in the rest of the book). Hence, anyone who tries to detect regularities in a process (for example an infinite sequence or an extremely long finite sequence) proceeds in the direction of the process. Regularities that have ever been found in an initial segment of the process are regularities for ever. Our main argument is that the interpretation of a process (for example to measure the complexity) is a process itself that proceeds in the same direction.

**Definition.** A p.r. function $f: X^* \rightarrow Y^*$ is called a *process* if $f(x) \sqsubset f(xy)$ for all $x, xy$ in the domain of $f$. Basis properties of processes have been developed independently in [5] and [8]. Processes are called p.r. monotonic functions in [5].

**Example 1.** Any homomorphism $f: X^* \rightarrow Y^*$ is a process, i.e., any function satisfying $f(xy) = f(x)f(y)$ for all $x, y \in X^*$.

**Example 2.** Let $C \subseteq X^*$ be any prefix code, i.e., $C$ is a finite set satisfying $C \cap CXX^* = \emptyset$. Then any injective function $f: C \rightarrow X^*$ can be uniquely extended to an injective function $f: C^* \rightarrow X^*$ by $f(xy) = f(x)f(y)$. $f$ as well as the inverse $f^{-1}$ are processes. We call $f^{-1}$ a prefix coding scheme.

A process $f: X^* \rightarrow Y^*$ yields a partial function $f : X^\omega \rightarrow Y^\omega$ the domain of which is given by

$$D(f) = \bigcap_{n \in \mathbb{N}} f^{-1}(Y^nY^*)X^\omega$$

and the values of which are determined by

$$f(x(n)) = f(z) \quad (x \in D(f), n \in \mathbb{N}).$$

Two processes $f, g: X^* \rightarrow Y^*$ are called *equivalent* if $f = g$. For instance, a recursive infinite sequence $z \in X^\omega$ is an equivalence class of processes $f: \{ | \}^* \rightarrow X^*$, where $|$ is a single symbol.

A process $f: X^* \rightarrow Y^*$ is called recursive (primitive recursive, resp.) if the function $f$ is recursive (primitive recursive, resp.) It is known from [5], [8] that there is an algorithm which, given any process, constructs an equivalent recursive process (this algorithm can easily be modified such that it constructs an equivalent primitive recursive process).

It is intuitively obvious and can be proven that the set of processes from $X^*$ to $Y^*$ can be recursively enumerated. This means that there exists a p.r. function
\[ H: N \times X^* \to Y^* \] such that any function \( H_i := \text{det } H(i, \cdot) \) is a process, and such that for any process \( F \) there is an \( i \) such that \( H_i = F \).

This fact implies the following

**Theorem 2.** There exists a universal process \( P: X^* \to X^* \) such that \( K_P \preceq K_B \) for all processes \( B: X^* \to X^* \).

**Proof.** Define \( P(1 \, 0 \, x) = H(i, x) \) for all \( i \in N, \, x \in X^* \).

Next we shall prove that the process complexity circumvents the difficulties involved in the Kolmogorov complexity. The process complexity \( K \) is to be the program complexity of a fixed universal process \( P \). It will turn out that the process complexity circumvents most of the difficulties involved in the Kolmogorov complexity.

To give an example we consider the complexity of the optimal prefix coding scheme of Huffman [9]. Let \( y_1, y_2, \ldots, y_{k^r} \) be all sequences in \( X^k \). We denote by \( p_d(y_i) \) the number of occurrences of \( y_i \) in the sequence \( x = x_1 x_2 \cdots x_r \in X^{kr} \) (where \( x_i \in X^k \)) divided by \( r \).

\[
H(x, k) = - \sum_{i=1}^{2^k} p_d(y_i) \log_2 p_d(y_i)
\]

is the Shannon entropy of \( x \) relative to blocks of length \( k \). Obviously \( H(x, k) \cdot l \geq H(x, k \cdot l) \) for all \( x \in X^{kr} \). We know that there is a prefix coding scheme \( f \) which encodes blocks of length \( k \) such that

\[
K_f(x_1 x_2 \cdots x_r) \leq \sum_{i=1}^{r} K_f(x_i) \leq rH(x, k) + r
\]

for all \( x = x_1 x_2 \cdots x_r \). Assume that \( x \in X^\infty \) satisfies \( \lim \, H(x(kr), k) < ek < k \).

Then \( \lim \, K_f(z(n))/n < c + 1/k \). Hence by choosing a sufficiently large \( k \) one obtains a prefix coding scheme \( f \) such that \( \lim \, K_f(z(n))/n < 1 \).

We shall now compare the behaviour of the process complexity with the notion of random sequence. Several notions of random sequence which are based on recursive function theory have been proposed within literature. A. Church [11] gave a recursive formulation of the von Mises concept of collective which is based on the notion of selection rule. However, Church's notion is not satisfactory since there exist Church random sequences which have definite regularities. For instance it follows from theorems by J. Ville [10] that there exist Church random sequences such that every initial segment has more zeros than ones. A notion of randomness which includes all standard statistical properties, such as the laws of large numbers has first been proposed by Martin-Löf [3]. Martin-Löf uses constructive measure theory in order to formulate the standard statistical properties.

Let us restate the definition of a Martin-Löf (M.L.) random sequence [3]: A rec.
sequential test is a r.e. set \( Y \subseteq N \times X^* \) such that \( \mu Y \subseteq 2^{-i} \) (\( i \in N \)). Hereby \( Y \) is to be \( \{ x \mid (i, x) \in Y \} \). A rec. sequential test \( Y \) yields a null set \( \mathcal{N}_Y = \bigcap_{i \in N} Y_i X^* \) which is called a recursive null set. A sequence \( z \) is a M.L. \textit{random sequence} iff \( z \) is not contained in any recursive null set. It turns out that M.L. random sequences can easily be characterized in terms of the process complexity.

**Theorem 3.** A sequence \( z \in X^* \) is a Martin-Löf (M.L.) random sequence iff

\[
\lim_{n \to \infty} \left( n - K(z(n)) \right) < \infty.
\]

**Proof.** "\( \Rightarrow \)" Assume \( \lim_{n \to \infty} \left( n - K(z(n)) \right) = \infty \). We define \( Y = \{ x \mid K(x) \leq |x| - i \} \).

We are going to prove that \( \mu Y \subseteq 2^{-i} \). Assume \( \mu Y > 2^{-i} \). Then there exist sequences \( x_1, x_2, \ldots, x_n \in X^* \) such that:

\[
\begin{align*}
(a) & \quad \sum_{j=1}^n 2^{-|x_j|} > 2^{-i}, \\
(b) & \quad x_j X^* \cap x_r X^* = \emptyset (j \neq r), \\
(c) & \quad K(x_j) \leq |x_j| - i (j = 1, \ldots, n).
\end{align*}
\]

Let \( P: X^* \to X^* \) be the universal process such that \( K_P = K \). Hence there exist sequences \( w_1, \ldots, w_n \in X^* \) such that

\[
\begin{align*}
(d) & \quad P(w_j) = x_j (j = 1, \ldots, n), \\
(e) & \quad |w_j| \leq |x_j| - i (j = 1, \ldots, n).
\end{align*}
\]

Since \( P \) is a process it follows from (b) that

\[
(f) \quad w_j X^* \cap w_r X^* = \emptyset (j \neq r).
\]

Hence, (a), (c), (f) lead to the contradiction \( \mu \{ \bigcup_{i=1}^n w_i X^* \} > 1 \). This proves that \( \mu Y \subseteq 2^{-i} \). Since \( Y \) can be recursively enumerated (uniformly for any \( i \)) this defines a rec. sequential test \( Y \) such that \( z \in \mathcal{N}_Y \).

The following lemma will be used to prove the other direction of Theorem 3. A \( A \subseteq X^* \) is called prefix-free if \( A \cap A X X^* = \emptyset \).

**Lemma 1.** Given a r.e. set \( U_i \subseteq X^* \) such that \( \sum_{x \in U_i} 2^{-|x|} \leq 2^{-i} \) we can effectively construct a process \( P_i: X^* \to X^* \) such that

\[
\begin{align*}
(1) & \quad \forall x \in D(P_i): |P_i(x)| = |x| + i, \\
(2) & \quad U_i X^* \subseteq P_i(X^*).
\end{align*}
\]

**Proof.** Let a recursive bijective function \( h: N \to U_i \) be given. We construct a recursive \( g: N \to X^* \) such that

\[
\begin{align*}
(a) & \quad \{ g(k) \mid k \in N \} \text{ is prefix-free}, \\
(b) & \quad |g(k)| = |h(k)| - i.
\end{align*}
\]
We denote
\[ W_k = \{ h(j) \mid j \leq k \}, \quad V_k = \{ g(j) \mid j \leq k \} \]
\[ \langle x \rangle = xX^* \cup \{ x(j) \mid j \leq |x| \} \quad (x \in X^*) \]
\[ \langle V_k \rangle = \bigcup_{x \in V_k} \langle x \rangle \]
\[ r(k) = \sum_{x \in W_k} 2^{-|x|} \]

In order to guarantee condition (a) we must construct \( g \) such that \( g(k+1) \notin \langle V_k \rangle \).
We construct \( g \) by recursion on \( k \) such that for all \( k \)
\[ (c) \forall j: ||\langle V_k \rangle \cap X^j || = r(k) 2^{|j|} \]
where \([s]\) denotes the least natural number greater than \( s \).
It can easily be seen that the induction hypothesis (c) for \( k = 0, 1, \ldots, n \) implies
\[ |g(k)| = |h(k)| - i \quad \text{for } k = 0, 1, \ldots, n, \]
\( V_n \) is prefix-free.

Hence, it satisfies to prove by induction on \( k \) that \( g(k) \) can be determined such that (c) holds.

**Construction of \( g \):** \( g(0) \in X^{|h(0)|-i} \) can be chosen arbitrarily. Assume \( g(j) \) with \( j < k \) are known. Let \( h(k) = s \), \( \sum_{x \in U_k} 2^{-|x|} \leq 2^{-i} \) guarantees that \( r(k-1) \leq 2^{-i} - 2^{-s} \). Hence, \( r(k-1) 2^s \leq 2^{s-i} - 1 \).
The induction hypothesis (c) implies that there exists
\[ u \in X^{s-i} - \langle V_{k-1} \rangle. \]
This implies that \( g(k) \in X^{s-i} \) can be determined such that (c) holds.

**Definition of the Process \( P_i \):**
\[ D(P_i) = \bigcup_{k \in N} V_k X \]
\[ \forall x \in X^*; \forall k \in N: P_i(g(k)x) = h(k)x. \]

"\( \prec \)" We continue the proof of Theorem 3. Let \( Y \subseteq N \times X^* \) be a rec. sequential test. We construct a process \( P: X^* \rightarrow X^* \) such that \( \lim_{n \rightarrow \infty} (n - K_p(x(n))) = \infty \) for all \( x \in \mathcal{N}_Y \). It has been proved in (5) that given any r.e. set \( Y_i \subseteq X^* \) we can effectively construct some r.e. set \( U_i \subseteq X^* \) such that \( U_i \cap X^\omega = Y_i \cap X^\omega \) and \( U_i \) is prefix-free. This implies
\[ \sum_{x \in U_i} 2^{-|x|} = \mu U_i X^\omega = \mu Y_i X^\omega \leq 2^{-i}. \]
Hence Lemma 1 can be applied and we construct processes $P_i$ such that

$$K_{P_i}(y) = |y| - i \quad (y \in U_i X^*)$$

Let us consider the set

$$W = \{x_1 x_2 \cdots x_n 01 \mid n \in N, x_i \in X \}.$$  

We can construct a recursive bijective $f: N \to W$ such that $|f(n)| \leq 2L(n) + 2$.  

Finally we construct the process $P: X^* \to X^*$ as follows:

$$P(f(i)x) = P_i(x) \quad (x \in D(P_i)).$$

This implies

$$K_P(y) \leq |y| - i + 2L(i) + 2$$

for all $i \in N, y \in U_i X^*$.

Hence,

$$\lim_{n \to \infty}(n - K_P(z(n))) \geq i - 2L(i) - 2$$

for all $z \in U_i X^\infty = Y_i X^\infty$.

This implies

$$\lim_{n \to \infty}(n - K_P(z(n))) = \infty \quad (z \in \mathcal{N}_y).$$

Q.E.D.

It is clear that the identity function $\text{id}_{X^*}: X^* \to X^*$ is a process satisfying $K_{\text{id}_{X^*}}(x) = |x|$. Hence there exists a natural number $c$ such that for all $x \in X^*$:

$$K(x) \leq |x| + c.$$  

This fact and Theorem 3 yield the following

**Corollary 4.** $x \in X^\infty$ is a M.L. random sequence iff there exists $c \in N$ such that for all $n \in N$: $|K(x(n)) - n| \leq c$.

The following theorem shows that the Kolmogorov complexity $K_A$ and the process complexity $K$ do not differ very much.

**Theorem 5.** $\exists c \in N:\ \forall x \in X^*: K(x) \leq K_A(x) + 4L |x| + c$.

**Proof.** We set

$$Y_i = \{x \in X^* \mid |K_A(x) - |x| + i + 2L |x|| \leq 1\} \quad \text{and} \quad Y_i^{(n)} = Y_i \cap X^n.$$

$x \in Y_i^{(n)}$ implies $K_A(x) \leq n - i - 2L(n) + 1$. Hence,

$$\mu Y_i^{(n)} X^\infty \leq 2^{-(i-2L(n)+1)} = 2^{-i+1}(n + 1)^2.$$
We choose $k \in N$ such that $k > 2 \sum_{n \in N} n^{-2}$. It follows

$$\sum_{x \in Y_i} 2^{-|x|} \leq 2^{-i+k}.$$ 

This guarantees that Lemma 1 can be applied. As in the proof of Theorem 3 we construct a process $P$ such that

$$K_p(x) \leq |x| - i + k + 2L(i) + 2$$

for all $i \geq k$ and $x \in Y_iX^*$. It follows from the definition of $Y_i$:

$$\forall x \in Y_iX^*: K_p(x) \leq K_d(x) + 2L |x| + 2L(i) + k + 3.$$ 

Hence, $K_p(x) \leq K_d(x) + 4L |x| + 3k + 3$ ($x \in Y_iX^*$ implies $i \leq |x| + k$). This proves Theorem 5.

Martin-Löf has pointed out that the Kolmogorov complexity oscillates in a very strange way [4]. Next we are going to prove that the process complexity does not oscillate. We shall show that the function $n - K(z(n))$ is nearly monotonic.

**Theorem 6.**

$$\exists c \in N: \forall x \in X^*: \forall j \leq |x|:\n
| x | - K(x) \geq j - K(x(j)) - 2L(|j - K(x(j))|) - c.$$ 

It follows from Theorem 6 that $j - K(x(j)) \geq 0$ (which means that $x(j)$ is regular) implies $|x| - K(x) \geq 0$ (which means that $x$ is regular, too).

**Proof.** Let $h: X^* \rightarrow X^*$ be a process. In order to prove Theorem 6 we construct a process $P: X^* \rightarrow X^*$ such that $\forall x \in X^*: \forall j \leq |x|:\n
| x | - K_p(x) \geq j - K_h(h(x(j))) - 2L(|j - K_h(x(j))|) - 3.$

We set $Y_i = \{ x | K_h(x) = |x| - i \}$.

We shall construct processes $P_i: X^* \rightarrow X^*$ such that

$$\forall x \in D(P_i): |P_i(x)| = |x| + i$$

$Y_iX^* \subset P_i(X^*)$.

The construction of these processes shall be outlined below. As in the proof of Theorem 3 we can now construct a process $P$ such that

$$K_p(x) \leq |x| - i + 2L(i) + 2 \quad (x \in Y_iX^*).$$

Hence,

$$K_p(x) \leq |x| - j + j - i + 2L(i) + 2.$$
Using the definition of $Y_i$ it follows for all $x(j) \in Y_i$

$$K_p(x) \leq |x| - j + K_h(x(j)) + 2L(|j - K_h(x(j))|) + 2.$$ 

Hence,

$$|x| - K_p(x) \geq j - K_h(x(j)) - 2L(|j - K_h(x(j))|) - 2.$$ 

It remains to construct the processes $P_i$.

Set $Z_i = \{y \in X^* | \|h(y)\| = |y| + i\}$ and let a recursive, surjective function $g: N \rightarrow Z_i$ be given. Let $U_k = \{g(j) | j \leq k\}$. We define by recursion on $k$ the restriction $P_i |_{U_k X^*}$. We start as follows: $\forall x \in X^*: P_i(g(0)x) = h(0)x$.

Let $P_i |_{U_k X^*}$ be given then define $P_i |_{P_i(g(k)x)}$ as follows: We consider three cases:

1. $g(k) \in U_{k-1} X^*$: in this case $P_i |_{P_i(g(k)x)}$ is already defined.
2. $g(k) X^* \cap U_{k-1} X^* = \phi$: We define
   $$\forall x \in X^*: P_i(g(k)x) = h(k)x.$$
3. There remains the case that there exist $j_1, \ldots, j_r < k$ such that
   $$g(k) X^* \cap U_{k-1} X^* = g(j_1) X^* \cup \cdots \cup g(j_r) X^*.$$ 
   Let $s = \max\{|g(j_i)| - |g(k)|\}$. Then there exists a permutation $\sigma: X^* \rightarrow X^*$ such that
   $$\forall x \in X^* (g(k)x \in U_{k-1} X^*): P_i(g(k)x) = h(k) \sigma(x).$$
   We define $\forall x \in X^*$: $\forall k \leq s$:
   $$P_i(g(k)x_1 \cdots x_k) = h(k) \sigma(x_1) \sigma(x_2) \cdots \sigma(x_k).$$
   It can easily be seen that $P_i |_{U_k X^*}$ is a process such that $\forall y \in U_k X^*: |P_i(y)| = |y| + i$.
   This proves that $P_i$ is a suitable process. Q.E.D.

4. Recursive Sequential Tests Are Not Effective

Next we are trying to analyse whether the previously defined random tests are effective. What does "effective" mean? It is our intuition that given an effective random test $T$ and finite sequences $x$ and $z$ we can effectively measure whether $x$ withstands the test $T$ better than $z$. For instance let $Y \subseteq N \times X^*$ be a recursive sequential test. The critical level function $m_T$ is defined by

$$m_T(x) = \sup\{i | x \in Y_i X^*\},$$

hereby we use the convention $\sup \phi = 0$. Let $x, z \in X^*$. If we know that the critical
level function $m_r$ satisfies $m_r(x) > m_r(z)$ we can say that $z$ withstands the test $Y$ better than $x$. For any high value $m_r(x) = i$ of the critical level function means that $x$ does not withstand the test $Y$ at the level $2^{-i}$ and $z \in X^\infty$ withstands the test $Y$ if and only if $m_r(z(n))$ is bounded with respect to $n$. However, we can prove that, in general, the critical level function is not recursive. It is known from [3] that there exists a universal rec. sequential test $Y$ such that $m_r \leq m_r$ for any rec. sequential test $\overline{Y}$. We are able to prove the following

**Theorem 7.** The critical level function of a universal rec. sequential test must not be recursive.

**Proof.** Let $Y \subset N \times X^*$ be a universal rec. random test. Without restricting generality we can assume that $Y_{i+1} \subset Y_i X^*$ $(i \in N)$. This implies

$x \notin Y_i X^* \Leftrightarrow m_r(x) < 1.$

From $\mu Y_1 X^\infty \leq 2^{-1}$ it follows that

$$\forall n \in N: \exists x \in X^n: m_r(x) < 1.$$ 

If $m_r$ is recursive, than we can construct a recursive function $f: N \rightarrow X^*$ such that

1. $\forall n \in N: (m_r f(n) < 1 \land f(n) \in X^n).$

However, the recursive function $f$ yields a rec. sequential test $\overline{Y}$ such that $\overline{Y}_i = \{f(i)\}$. Hence $m_r f(n) = n$. It follows from the universality of $Y$:

$$\exists c \in N: \forall n \in N: m_r f(n) > n - c.$$

This contradicts relation (1). Therefore, the assumption $m_r$ recursive does not hold. Q.E.D.

The same argument proves that the relation $m_r(x) < m_r(z)$ cannot be recursively decided.

We analyse the process complexity $K$ in the same way. If $|x| - K(x) > |z| - K(z)$ than we can say that the sequence $z$ withstands the random test given by $K$ better than $x$. However, the above method of proof also yields the following

**Theorem 8.** The process complexity is not recursive.

5. EFFECTIVE RANDOM TESTS

Let $P$ be a process and $f: X^* \rightarrow N$ a recursive function such that $f(x) \leq |x| - K_P(x)$ for all $x \in X^*$. $f$ is called a recursive lower bound of $|x| - K_P$. The process $P$ together with $f$ can be conceived to be an effective random test. In case $f(z) > f(x)$ we can say that $x$ withstands this test better than $z$. 

In the following recursive monotonic unbounded functions \( g : \mathbb{N} \rightarrow \mathbb{N} \) shall be used to measure the growth of other functions. We call these functions \( g \) growth functions.

A process \( P \), a recursive lower bound \( f \) of \( \| \cdot \| - K_p \) and a growth function \( g \) consists of an effective random test for infinite sequences. \( z \in X^\infty \) does not withstand this test iff \( \liminf_n f(z(n))/g(n) > 0 \).

Next we establish some equivalent concepts of effective random tests. Let \( Y \) be a recursive sequential test and \( f : X^* \rightarrow \mathbb{N} \) be a recursive lower bound of the critical level function \( m_Y \). \( Y \) together with \( f \) can be conceived to be an effective test. In case \( f(x) < f(z) \) we can say that \( x \) withstands this test better than \( z \).

Another concept of effective random test can be derived from martingales. A function \( V : X^* \rightarrow \mathbb{R}^+ \) (\( \mathbb{R}^+ \) denotes the set of all nonnegative real numbers) is called a martingale if it satisfies:

\[
V(x) = \frac{1}{2}(V(x0) + V(x1)) \quad (x \in X^*).
\]

A martingale can be conceived to be the capital of a gambler when playing on binary sequences. \( V(x) \) denotes the capital after the \( x \)-st trial when the sequence of the gambling system has the initial segment \( x \). We consider recursive martingales \( V : X^* \rightarrow \mathbb{Q}^+ \) where \( \mathbb{Q}^+ \) is the set of all nonnegative rational numbers. A recursive martingale \( V : X^* \rightarrow \mathbb{Q}^+ \) constitutes an effective random test. In case \( V(x) < V(z) \) we say that \( x \) withstands this test better than \( z \).

A recursive sequential test \( Y \subset N \times X \) is called a total rec. sequential test if \( \mu Y_i \) defines a computable function \( f : \mathbb{N} \rightarrow \mathbb{R} \). Relative to a total rec. sequential test we can effectively compute the values \( \mu(Y_i X^\infty \cap x X^*) \), and these values are high if \( x \) does not withstand the test \( Y \). Hence total rec. sequential tests can be conceived to be effective random tests.

We shall now prove the following equivalences.

**Theorem 9.** Let \( z \in X^\infty \) be any sequence. Then the following statements are equivalent.

1. There exists a process \( P \), a recursive lower bound \( f \) of \( \| \cdot \| - K_p \) and a growth function \( g \) such that \( \liminf_n f(z(n))/g(n) > 0 \).
2. There exists a rec. sequential test \( Y \), a recursive lower bound \( f \) of \( m_Y \), and a growth function \( g \) such that \( \liminf_n f(z(n))/g(n) > 0 \).
3. There exists a recursive martingale \( V : X^* \rightarrow \mathbb{Q}^+ \) and a growth function \( g \) such that \( \liminf_n V(z(n))/g(n) > 0 \).
4. There exists a total recursive sequential test \( Y \) such that \( z \in \mathcal{M}_Y \).

**Proof.** (1) \( \Rightarrow \) (2): We define a recursive sequential test \( Y \subset N \times X^* \) by

\[
Y_i = \{x \in X^* \mid f(x) \geq i\}.
\]
\( x \in Y_i \) implies \( K_p(x) \leq |x| - i \). \( P \) is a process, it follows \( \mu Y_i X^\infty \leq 2^{-i} \). This proves that \( Y \) is a recursive sequential test. \( f \) is a lower bound of \( m_f \) and therefore (1) \( \Rightarrow \) (2).

(2) \( \Rightarrow \) (4): Let \( r \in \mathbb{Q}_+ \) be any rational. We define a total recursive sequential test \( U \subseteq N \times X^* \) as follows:

\[
U_i = \{ x \in Y_i \mid f(x)g(x) > r \}.
\]

\( U \) is a recursive set and we can compute \( \mu U_i X^\infty \) since \( \mu(U_i \cap X^nX^*) \leq 2^k \) if \( g(n) \geq 2^{kr} \). \( \lim_n f(z(n))g(n) > r \) implies \( z \in N \). Since \( r \in \mathbb{Q}_+ \) can be chosen arbitrarily this proves (2) \( \Rightarrow \) (4).

(3) \( \Rightarrow \) (1): Let \( V : X^* \rightarrow \mathbb{Q}_+ \) be a recursive martingale and \( g \) a growth function. We can assume that \( V(A) = 1 \). Define

\[
Y_i = \{ x \in X^* \mid V(x) \geq 2^i \}.
\]

It follows from the martingale lemma [5] (5.5) that \( \mu Y_i X^\infty \leq 2^{-i} \). Set

\[
U_i = \{ x \in X^* \mid x \in Y_i X X^* \},
\]

i.e., \( U_i \) is prefix-free and \( U_i X^* = Y_i X^* \). Hence,

\[
\sum_{x \in U_i} 2^{-|x|} = \mu U_i X^\infty \leq 2^{-i}.
\]

This proves that \( U \) is a recursive sequential test and Lemma 1 can be applied. As in the proof of Theorem 3 we construct a process \( P \) such that

\[
K_p(x) \leq |x| - i + 2L(i) + 2
\]

for all \( x \in U_i X^* \). \( V(x) > 2^i \) implies \( |x| - K_p(x) \geq i - 2L(i) - 2 \). Hence

\[
\lim_n V(z(n))g(n) > 0 \implies \lim_n(n - K_p(z(n)))/Lg(n) > 0
\]

Since \( U \) is a recursive set, the construction of \( P \) implies that \( K_p \) is a recursive function. Hence, \( |x| - K_p(x) \) is recursive, too. This proves (3) \( \Rightarrow \) (1).

(3) \( \Leftrightarrow \) (4): This has been proved in [5] (9.4), (9.5).

It should be mentioned that all equivalences of Theorem 9 are not merely existential but can be proved by effective methods. Hence, all these concepts of effective random tests do not differ essentially. Finally we restate a theorem of [5] which ensures that our concept of effective tests yields a concept of recursive pseudo-random sequences. An extensive treatment of the theory of pseudo-random sequences as well as some more equivalent concepts of effective tests can be found in [5].
Theorem [5]. Given any rec. enumerable set $\mathcal{M}$ of effective tests we can effectively find a recursive sequence $z$ which withstands all tests in $\mathcal{M}$.

Because of this theorem it is entirely clear that there cannot exist a universal effective random test. However, we can describe all effective random tests by means of a fixed universal process $P$ in the following way. A sequence $z \in X^\omega$ withstands all effective random tests iff there does not exist a recursive lower bound $f$ of $| - K_P$ and a growth function $g$ such that $\lim_{n \to \infty} f(x(n))/g(n) > 0$. Finally we remark that there exist different types of universal processes. A particularly natural class consists of the admissible universal processes.

Definition. A process $P : X^* \to X^*$ is called admissible universal if for any process $\bar{P} : X^* \to X^*$ there exists a recursive function $h : X^* \to X^*$ such that $|h| \leq |\text{id}_{X^*}|$ and $P h = \bar{P}$.

Obviously the process that has been constructed in the proof of Theorem 2 is admissible universal. The methods developed in Schnorr [6] yield the following isomorphism theorem for admissible universal processes:

Theorem [6]. Let $P, \bar{P} : X^* \to X^*$ be two admissible universal processes, then there exists a bijective recursive function $h : X^* \to X^*$ such that $P h = \bar{P}$ and $|h| \leq |\text{id}_{X^*}|$ and $|h^{-1}| \leq |\text{id}_{X^*}|$.

References