THE PROCESS COMPLEXITY AND EFFECTIVE RANDOM TESTS.

C. P. Schnorr
Mathematisches Seminar
Universität Frankfurt

Abstract

We propose a variant of the Kolmogorov concept of complexity which yields a common theory of finite and infinite random sequences. The process complexity does not oscillate. We establish some concepts of effective tests which are proved to be equivalent.

1. Notations

Let X^* (X^∞) be the set of all finite (infinite) binary sequences. $\Lambda \in X^*$ denotes the empty sequence. For $x \in X^*$ we denote $|x|$ the length of x. The product $xy \in X^* \cup X^\infty$ denotes the concatenation of sequences $x \in X^*$ and $y \in X^* \cup X^\infty$. Clearly this yields a product $AB \subset X^* \cup X^\infty$ of sets $A \subset X^*$ and $B \subset X^* \cup X^\infty$. For $z \in X^* \cup X^\infty$ we denote $z(n)$ the initial segment of z with length n. $\|A\|$ denotes the cardinality of a set A. We shall write $x \sqsubset y$ iff the sequence x is an initial segment of the sequence y. N (R) denotes the set of natural (real) numbers. For two functions $f,g: Y \to R$ we write $f \dot{\leq} g$ iff $\exists c \in N: \forall x \in Y: f(x) \leq g(x) + c$

$f \doteq g$ iff $f \dot{\leq} g \wedge g \dot{\leq} f$.

μ denotes the product measure on X^∞ 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.

2. THE KOLMOGOROV COMPLEXITY OF FINITE SEQUENCES

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

$$K_A(x) = \min\{|p| \mid A(p) = x\}.$$

Hereby we use the convention $\min \emptyset = \infty$.

It is well-known from |2|,|7| that there exists a universal p.r. function $A: X^* \to X^*$ such that $K_A \dot{\leq} K_B$ for any p.r. function $B: X^* \to X^*$. This implies $K_A \doteq K_B$ 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 $\overline{\lim_n}(n - K_A(z(n))) < \infty$. This would mean that there must not be regularities in any initial segment of z (We consider a sequence x to be regular iff $K_A(x)$ is essentially smaller than $|x|$). This intention failes because of the following theorem of Martin-Löf |4|.

Theorem 1 Let $f: N \to N$ be a rec. function such that $\sum 2^{-f(n)} < \infty$,
then for any $z \in X^\infty$ the following holds:
$\overline{\lim_n}(n - K_A(z(n)) - f(n)) = \infty$.

Since there exist arbitrary long sequences x such that $K_A(x) \geq |x|$ 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

$$K_A(x) \geq |x| \text{ and } K_A(x(n)) < n - f(n).$$

This means that x is irregular although the initial segment x(n) is regular. This fact is hard to conceive 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 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 subsequences 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 his 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 his complexity) is a process itself that proceeds in the same direction.

Definition A p.r. function $f : X^* \to Y^*$ is called a process, if $f(x) \sqsubset f(xy)$ for all x,xy in the domain of f.
Basic properties of processes have been developped independently in |5| and |8|. Processes are called p.r. monotonous functions in |5|. A process $f: X^* \to Y^*$ yields a partial function $\bar{f}: X^\infty \to Y^\infty$ the domain of which is given by

$$D(\bar{f}) = \bigcap_{n \in N} f^{-1}(Y^n Y^*) X^\infty$$

and the values of which are determined by

$$f(z(n)) \sqsubset \bar{f}(z) \quad (z \in D(\bar{f}), n \in N)$$

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

A process $f: X^* \to Y^*$ 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 constructs for any given process an equivalent recursive (primitive rec., resp.) process.

It is obvious 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 $H_i \overline{\text{def}} H(i,)$ 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 $K_P \leq K_B$ for all processes $B: X^* \to X^*$.

Proof Define $P(1^i\ 0\ x) = H(i,x)$ 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^P is to be the program complexity of a fixed universal process P.

Theorem 3
A sequence $z \in X^\infty$ is a Martin-Löf (M.L.) random sequence iff $\overline{\lim_n}(n - K^P(z(n))) < \infty$.

Let us restate the definition of a M.L. random sequence |3|. A rec. sequential test is a r.e. set $Y \subset N \times X^*$ such that $\mu Y_i X^\infty \leq 2^{-i}$ $(i \in N)$. Hereby Y_i is to be $\{x \mid (i,x) \in Y\}$. A rec. sequential test Y yields a null set $\mathfrak{N}_Y = \bigcap_{i \in N} Y_i X^\infty$ which is called a recursive null set. A sequence z is a M.L. random sequence iff z is not contained in any recursive null set.

Proof " => " Assume $\overline{\lim_n}(n - K^P(z(n))) = \infty$. We define $Y_i = \{x \mid K^P(x) \leq |x| - i\}$. We are going to prove that $\mu Y_i X^\infty \leq 2^{-i}$. Assume $\mu Y_i X^\infty > 2^{-i}$. Then there exist sequences $x_1, x_2, \ldots, x_n \in X^*$ such that:

(a) $$\sum_{j=1}^{n} 2^{-|x_j|} > 2^{-i}$$

(b) $x_j X^* \cap x_r X^* = \emptyset \quad (j \neq r)$

(c) $K^P(x_j) \leq |x_j| - i \quad (j = 1,\ldots,n)$

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

(d) $P(w_j) = x_j \quad (j = 1,\ldots,n)$

(e) $|w_j| \leq |x_j| - i \quad (j = 1,\ldots,n)$

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

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

Hence (a), (e), (f) lead to the contradiction $\mu\{\bigcup_{j=1}^{n} w_j X^\infty\} > 1$.

This proves that $\mu Y_i X^\infty \leq 2^{-i}$. Since Y_i can be rec. enumerated (uniformly for any i) this defines a rec. sequential test Y such that $z \in \mathfrak{N}_Y$.

"$\Leftarrow$" Let $Y \subset N \times X^*$ be a rec. sequential test. We construct a process $P : X^* \to X^*$ such that $\lim_n (n - K_P(z(n))) = \infty$ for all $z \in \mathfrak{N}_Y$. We assume $\mathfrak{N}_Y \neq \emptyset$ and $\mu Y_i X^\infty < 2^i$. Then we prove the following

Lemma. To any i we can effectively construct a process P_i such that for any $y \in Y_i X^*$ there is an $x \in X^*$ satisfying. $|x| = |y| - i$, $P_i(x) = y$.

Proof Let $h: N \to Y_i X^*$ be a recursive bijective function. Such a function can easily be found. To $x \in X^*$ we define

$$\tilde{x} := xX^* \cup \{x(i) \mid i \leq |x|\} \subset X^*$$

and we set $U_n := \bigcup_{j \leq n} \widetilde{h(j)}$

We construct a recursive function $g: N \to X^*$ such that $\{(g(i), h(i)) \mid i \in N\}$ is the graph of the process P_i in the lemma. We set $V_n := \bigcup_{j \leq n} \widetilde{g(j)}$.

We choose $g(o) \in X^*$ such that $|g(o)| = |h(o)| - i$. Suppose $g(i)$ is already defined for all $k < j$. We consider two cases cases.

(1) $h(j) \in U_{j-1}$. Then two cases (a) and (b) are possible .

(a) there exists $k < j$ and $w \in X^*$ such that $h(j) = h(k)\,w$. In this case we set $g(j) = g(k)w$.

(b) there exists $k < j$ and w such that $h(k) = h(j)w$. in this case we decompose $h(k)$ such that $h(k) = uv$ with $|v| = |w|$ and we set $g(j) = u$.

(2) $h(j) \notin U_{j-1}$. In this case we choose $g(j)$ such that

$|g(j)| = |h(j)| - i$, $g(j) \notin V_{j-1}$ and

(*) $\|V_j \cap X^k\|$ is minimal for all $k < |h(j)| - i$.

Let us illustrate this last condition. Suppose $V_{j-1} = \widetilde{0001}$ and $|h(j)| - i = 4$, then the above condition implies $g(j) = 0000$. This means that $g(j)$ has to be chosen such that there is a maximal initial segment of $g(j)$ which coincides with an initial segment of some sequence in V_{j-1}.

It can be verified that there exists $g(j)$ satisfying the above conditions iff

(i) $\|V_{j-1} \cap X^{|h(j)|-i}\| < 2^{|h(j)|-i}$.

In this case an appropriate $g(j)$ can be effectively found. We claim that condition (*) implies that for all $j,r \in N$:

$$\|V_j \cap X^r\| = \lceil 2^r \mu(\bigcup_{k \leq j} g(k)X^\infty) \rceil$$

where $\lceil\ \rceil$ denotes the last natural number greater than.

Observe that in fact condition (*) implies that $g(j)$ has to be chosen such that $\|V_j \cap X^k\|$ is minimal for all $k \in N$. Obviously $\lceil 2^r \mu(\bigcup_{k \leq j} g(k)X^\infty) \rceil$ is an lower bound for $\|V_j \cap X\|$ and our construction ensures that this lower bound is attained. Because of $\lceil 2^r \mu(\bigcup_{k \leq j} g(k)X^\infty) \rceil = \lceil 2^{i+r} \mu(\bigcup_{k \leq j} h(k)X^\infty) \rceil \leq$

$2^{i+r} \mu Y_i X^\infty < 2^r$ it follows that (i) holds.

Hence the procedure for g continues for all j. Hence $\{(g(j), h(j)) \mid j \in N\}$ is the graph of a process P_i that satisfies the above lemma.

We continue the proof of Theorem 3. The above lemma implies

$$K_{P_i}(y) = |y| - i \qquad (y \in Y_i X^*).$$

Let us consider the set

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

We can construct a recursive bijective $f: N \to W$ such that $|f(n)| \leq 2\,L(n) + 2$. Finally we construct the process $P: X^* \to X^*$ as follows

$$P(f(i)x) = P_i(x) \text{ for all } x \in D(P_i).$$

This implies $K_P(y) \leq |y| - i + 2\,L(i) + 2$ for all $i \in N$, $y \in Y_i X^*$. Hence

$$\overline{\lim_n}(n - K_P(z(n))) = \infty \quad (z \in \mathfrak{N}_Y), \text{ q.e.d.}$$

It is clear that the identity function $id_{X^*}: X^* \to X^*$ is a process satisfying $K_{id_{X^*}}(x) = |x|$. Hence there exists a natural number c such that for all $x \in X^*$: $K^P(x) \leq |x| + c$. This fact and Theorem 3 yield the following

Corollary 4

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

Let $Y \subset N \times X^*$ be a rec. sequential test. We define the critical level function m_Y

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

hereby we use the convention $\sup \emptyset = 0$. It is known from [3] that there exists a universal rec. sequential test Y such that $m_Y \leq m_{\bar{Y}}$ for any rec. sequential test $\bar{Y}$. Let m be the critical level function of a fixed universal rec. sequential test Y. The proof of Theorem 3 yields the following

Corollary 5

There exists $c \in N$ such that for all $x \in X^*$:

$$-c < m(x) + K^P(x) - |x| < 2\,L(m(x)) + c.$$

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 $n - K^P(z(n))$ is nearly monotonous. This implies that all initial segments of an irregular x (i.e. $K^P(x) \approx |x|$ are irregular too.

Theorem 6 There exists $c \in N$ such that for all $x \in X^*$ and $j \leq |x|$: $|x| - K^P(x) \geq j - K^P(x(j)) - 2\,L(|j - K^P(x(j))|) - c$.

Proof Let $P: X^* \to X^*$ be a process. In order to prove the theorem we construct a process $h: X^* \to X^*$ such that for all $x \in X^*$, $j \leq |x|$:

$$(*) \quad |x| - K_h(x) \geq j - K_P(x(j)) - 2\,L(|j - K_P(x(j))|) - 3.$$

We set

$$Y_i = \{x \in X^* \mid K_P(x) \leq |x| - i\}$$

Hence $\mu Y_i X^\infty \leq 2^{-i}$ and we can effectively construct a process $h_i: X^* \to X^*$ such that for any $y \in Y_i X^*$ there exists $x \in X^*$ satisfying

$$|x| = |y| - i,\ h_i(x) = y.$$

This implies

$$K_{h_i}(y) \leq |y| - i \text{ for all } y \in Y_i X^*.$$

We consider the set

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

We can easily construct a rec. bijective function $f: N \to W$ such that

$$|f(n)| < 2\,L(n) + 3$$

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

$$h(f(i)x) = h_i(x) \quad \text{for all } x \in D(h_i).$$

This implies that the relation (*) holds. Hence Theorem 5 follows from Theorem 2.

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

Theorem 7

There exists a constant c such that for all $x \in X^*$:

$$K^P(x) < K_A(x) + 4\,L|x| + c$$

Proof We set

$$Z_i = \{x \in X^* \mid i < |x| - K_A(x) - 2L|x|\}$$

and

$$Z_i^{(n)} = Z_i \cap X^n$$

$x \in Z_i^{(n)}$ implies $K_A(x) < n - i - 2L(n)$

Hence $\mu Z_i^{(n)} X^\infty \leq 2^{-i-2L(n)}$

It follows $\mu Z_i X^\infty \leq 2^{-i} \sum_{n \in N} n^{-2}$

We choose k such that $2^k > \sum_{n \in N} n^{-2}$ and define a rec. sequential test $Y \subset N \times X^*$ by

$$Y_i = Z_{i+k} \quad (i \in N)$$

It follows from Corollary 5 that there exists $c_1 \in N$ such that for all $x \in X^*$:

$$K^P(x) < |x| - m(x) + 2L|x| + c_1$$

Since $m_Y \leq m$ there exists $c_2 \in N$ such that for all $x \in X^*$:

$$K^P(x) < |x| - m_Y(x) + 2L|x| + c_2$$

It follows from the definition of Z_i that for all $x \in X^*$:

$$m_Y(x) \geq |x| - K_A(x) - 2L|x| - k$$

Hence

$$K^P(x) < K_A(x) + 4L|x| + c_2 + k \quad (x \in X^*), \text{ q.e.d.}$$

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 $Y \subset N \times X^*$ be a recursive sequential test and $x,z \in X^*$. If we know that the critical level function m_Y satisfies $m_Y(x) > m_Y(z)$ than we can say that z withstands the test Y better than x. However, we are able to prove the following

Theorem 8 The critical level function of a universal recursive sequential test must not be recursive.

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

$$x \notin Y_1 X^* \iff m_Y(x) < 1.$$

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

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

If m_Y is recursive than we can construct a recursive function $f: N \to X^*$ such that

(1) $\forall n \in N: (m_Y f(n) < 1 \wedge f(n) \in X^n)$

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

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

This contradicts relation (1). Therefore, the assumption m_Y recursive does not hold, q.e.d.

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

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

Theorem 9

The process complexity is not recursive.

The above theorems constitute a challenge to find a more restrictive concept of random tests. It seems to be natural requiring that an effective recursive sequential test $Y \subset N \times X^*$ is a recursive set. However, it has been shown in [5] that for any rec. sequential test $Y \subset N \times X^*$ there is a rec. sequential test $\overline{Y} \subset N \times X^*$ such that $\mathfrak{N}_Y = \mathfrak{N}_{\overline{Y}}$ and $\overline{Y}$ is a rec. set. Thus, if we would accept this concept of effective test then there

exists an effective test such that any recursive sequence does not withstand this test. Hence such a concept of effective test would not yield a concept of recursive pseudo-random sequences, i.e. recursive sequences withstanding all effective tests that have a bounded computational complexity.

5. Effective Random Tests.

Let $P,B: X^* \to X^*$ be partial functions . Then B is called a right invers (r.i.) of P if $P\,B = id_{X^*}$. A r.i. to P exists if and only if P is surjective. Any r. i. is a total 1-1 function.

A process P together with a recursive r.i. B can be conceived to be an effective test. In case $|z|-|B(z)| > |x|-|B(x)|$ we can say that x withstands this test better than z. This relation can be effectively decided. $|B(x)|$ is a recursive lower bound for $K_P(x)$.

In the following a rec. monotonous and unbounded function $g:N \to N$ shall be called a growth function. We shall use these functions for measuring the increase of real functions.

Definition

A tripel T = (P,B,g) where P is a process, B is a rec. r.i. of P, and g is a growth function, is called an effective random test. $\mathfrak{A}_T = \{z \in X^\infty \mid \overline{\lim_n}(n - |B(z(n))|\,) / g(n) > 0\}$ is defined to be the set of sequences that do not withstand test T.

We say that test T is mortal for the sequences in $\mathfrak{A}_T$. The above definition means that for a sequence z there exists a mortal effective random test if and only if there is a process P such that short programs B(z(n)) for the initial segments z(n) of z can be effectively found and the sequence $n - |B(z(n))|$ increases in an effective way beyond all bounds. Obviously this implies

$$\overline{\lim_n}\ (n - K_P(z(n))) = \infty$$

Next we establish some equivalent concepts of effective random tests.

Let $Y \subset N \times X^*$ be a rec. sequential test. Without restricting generality we shall assume that $Y_0 = X^*$ and $Y_i = Y_i X^*$ for all $i \in N$. A function $h: X^* \to Y$ is called a decode to Y, if $\pi_1 h(x) = x$ for all $x \in X^*$. Hereby $\pi_1: N \times X^* \to N$, $\pi_2: N \times X^* \to X^*$ denote the projections.

A rec. sequential test Y together with a recursive decode can be conceived to be an effective test. In case $\pi_1 h(x) < \pi_1 h(z)$ we can say that x withstands this test better than z. This relation can be effectively decided. $\pi_1 h(x)$ is a recursive lower bound for $m_Y(x)$.

Theorem 10

Let $z \in X^\infty$ be any sequence. Then there exists a mortal effective test for z if and only if there exist a rec. sequential test Y, a (rec.) decode h, and a growth function g, such that $\overline{\lim_n}\ \pi_1 h(z(n))/g(n) > 0$.

Proof (1) Let T = (P,B,g) be an effective test. We define $Y \subset N \times X^*$ as follows:

$$Y_0 = X^* \text{ and } Y_i = \{x \in X^* \mid \exists\, j \leq |x| : |B(x(j))| \leq j - i\}\,.$$

Since P is a process it follows

$$\mu^* Y_i X^\infty \leq 2^{-i}.$$

Hence Y is a rec. sequential test. The decode h is defined by

$$h(x) = \begin{cases} (|x|-|B(x)|\,,x) & \text{if } |x| \geq |B(x)| \\ (0,x) & \text{otherwise} \end{cases}$$

Hence $\overline{\lim_n}(n - |B(z(n))|)/g(n) > 0$

implies $\overline{\lim_n}\pi_1 h(z(n))/g(n) > 0$.

(2) Let $Y \subset N \times X^*$ be a rec. sequential test with $Y_0 = X^*$, h a recursive decode, and g a growth function. We construct a process $P:X^* \to X^*$ as has been done in part (2) of the proof of Theorem 3. It can easily be verified that this construction yields

a recursive r.i. $B:X^* \to X^*$ such for all $x \in X^*$:

$0 \leq \pi_1 h(x) + |B(x)| - |x| \leq 2L(\pi_1 h(x)) + 3$

Hence $\overline{\lim_n} \pi_1 h(z(n))/g(n) > 0$ implies

$$\overline{\lim_n}(n - |B(z(n))|)Lg(n) / g(n) > 0.$$

Obviously this proves the theorem.

Another equivalent concept of effective random tests can be derived from martingales. A function $V:X^* \to R^+$ (R^+ denotes the set of all non-negative real numbers) is called a martingale if it satisfies:

$$V(x) = 2^{-1} (V(x0)+V(x1)) \quad (x \in X^*).$$

A martingale can be conceived to be the capital of a gambler when playing on binary sequences. V(x) denotes the capital after the $|x|$ -th trial when the sequence of the gambling system has the initial segment x. We consider recursive martingales $V:X^* \to Q^+$ where Q^+ is the set of all non-negative rational numbers.

Intuitively a recursive martingale $V:X^* \to Q^+$ constitutes an effective random test. In case $V(x) < V(z)$ we can say that x withstands this test better than z. This relation can be effectively decided. We can prove the following

Theorem 11

Let $z \in X^\infty$ be any sequence. Then there exists a mortal effective test for z if and only if there exists a recursive martingale $V:X^* \to Q^+$ and a growth function g such that $\overline{\lim_n} V(z(n))/g(n) > 0$.

Proof (1) let $V:X^* \to Q^+$ be a recursive martingale and g a growth function. We define a recursive set $Y \subset N \times X^*$ by

$$Y_i = \{x \in X^* | \ \exists j \leq |x| : V(x(j)) > 2^i V(\Lambda)\}$$

The structure of a martingale implies that $\mu Y_i X^\infty \leq 2^{-i}$

Hence Y is a rec. sequential test. We construct a decode h to Y by h(x) =

$$(\max \{i | \ \exists j \leq |x| : V(x(j)) \geq 2^i V(\Lambda)\}, x)$$

It can easily be verified that $\overline{\lim_n} V(z(n))/g(n) > 0$ implies $\overline{\lim_n} \pi_1 h(z(n))/Lg(n) > 0$. This proves one direction of the theorem. The other direction will be proved lateron.

A recursive sequential test $Y \subset N \times X^*$ is called a total recursive sequential test, if $f(i) = \mu Y_i X^\infty$ defines a computable function $f:N \to R$.

Theorem 12

Let $z \in X^\infty$ be any sequence. Then there exists a mortal effective test for z if and only if there exists a total recursive sequential test Y such that $z \in \mathfrak{N}_Y$.

Proof (1) Let T = (P,B,g) be an effective random test. First of all we construct a growth function f such that $\overline{\lim_n} g(n)/f(n) = \infty$. Then we define $Y \subset N \times X^*$ by

$Y_i = \{x \mid |B(x)| \leq |x| - i, |x| - B(x) | > f(|x|)\}$.

Hence $\overline{\lim_n}(n - |B(z(n))|)/g(n) > 0$ implies $z \in \mathfrak{N}_Y$. We prove that Y is a total rec. sequential test. It satisfies showing that $\mu Y_i X^\infty$ can be effectively computed. In order to compute $\mu Y_i X^\infty$ with an error less than 2^{-j} one determines n such that $f(n) > 2^j$. This implies

$$\mu\{z \in X^\infty | \ \exists k \geq n : |B(z(k))| \leq k-i \wedge k-|B(z(k))| > f(k)\} \leq 2^{-j}$$

Hence

$$|\mu Y_i X^\infty - \mu\{z | \exists k < n : |B(z(k))| \leq k-i \wedge k-|B(z(k))| > f(k)\}| \leq 2^{-j}$$

Since

$$\mu\{z \in X^\infty | \ \exists k < n : |B(z(k))| \leq k-i \wedge k-|B(z(k))| > f(k)\}$$

can be recursively computed from i and n it follows that $\mu Y_i X^\infty$ can be effectively computed from i. This proves one direction of the theorem. Those directions of Theorem 10 and 11 that have not yet been proved are a consequence of the following

Theorem 15

Let $z \in X^\infty$ be any sequence. Then the following relations (1) and (2) are

equivalent:

(1) there exists a recursive martingale $V:X^* \to R^+$ and a growth function g such that $\overline{\lim_n} V(z(n))/g(n) > 0$

(2) there exists a total recursive sequential test Y such that $z \in \mathfrak{A}_Y$.

It should be mentioned that all equivalences of this chapter 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 $\mathfrak{M}$ of effective tests we can effectively find a recursive sequence z which withstands all tests in $\mathfrak{M}$.

Because of this theorem it is entirely clear that there cannot exist a universal effective random test. However, the concept of an universal p.r. process (universal rec. sequential test resp.) can also be used relative to effective tests. For instance it can be shown that there exists a universal process $A : X^* \to X^*$ such that for any effective test $\overline{T} = (\overline{A}, \overline{B}\ g)$ one can effectively find a test $T = (A,B,g)$ satisfying $|B| \leq^{\cdot} |\overline{B}|$. Hence all effective test can be referred to A. However, this does not hold for any universal process. It can easily be seen that this only holds for the following concept of admissible universal processes.

Definition

A process $A:X^* \to X^*$ is called admissible universal if for any process $B:X^* \to X^*$ there exists a recursive function $C:X^* \to X^*$ such that $|C| \leq^{\cdot} |id_{X^*}|$ and $A\,C = B$

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

Theorem |8|

Let $A,B:X^* \to X^*$ be two admissible universal processes, then there exists a bijective recursive function $C:X^* \to X^*$ such that $|C| \leq^{\cdot} |id_{X^*}|$ and $A\,C = B$.

REFERENCES

|1| Loveland, D.W.: A variant of the Kolmogorov concept of complexity. Inform. Control 15 (1969), 510-526

|2| Kolmogorov A.N.: Tri podhoda k opredeleniju ponjatija "količestwo informacii" Probl. Peredaci Inform. 1 (1965), 3-11

|3| Martin-Löf,P. : The defination of random sequences. Inform. Control 6 (1966), 602-619

|4| Martin-Löf,P.: Complexity oscillations in infinite binary sequences. Z. Wahrscheinlich. verw. Geb. 19 (1971), 225 - 230

|5| Schnorr, C.P.: Zufälligkeit und Wahrscheinlichkeit. Lecture Notes in Mathematics Vol. 218, Berlin-Heidelberg-New York: Springer 1971

|6| Schnorr, C.P: Optimal Enumerations and optimal Gödel numberings. Technical report. University Frankfurt.

|7| Solomonoff,R.J.: A formal theory of inductive inference, Part I Inform. Control 7 (1964), 1-22

|8| Levin, L. and Zvonkin, A.: Die Komplexität endlicher Objekte und die Begründung der Begriffe der In-

formation und der Zufälligkeit mit Hilfe der Theorie der Algorithmen. (russisch) Uspekhi Matematicheskikh Nauk 156 (1970)

CORRECTION

The case (a) in the proof of the lemma used in the proof of theorem 3 has to be changed as follows:

(a) if there exists $k < j$ such that $h(j) \in h(k)X^*$ then choose a maximal k with this property and choose any $y \in g(k)\, X^* \cap X^{|h(j)| - i}$ which has not yet been used as value of g and set $g(j) = y$.