Journal of Universal Computer Science, vol. 3, no. 11 (1997), 1241-1249
submitted: 8/8/97, accepted: 16/10/97, appeared: 28/11/97

Invariance Properties of Random Sequences [1]

Peter Hertling
(Department of Computer Science, The University of Auckland,
Private Bag 92019, Auckland, New Zealand
Email: hertling@cs.auckland.ac.nz)

Yongge Wang
(Department of Computer Science, The University of Auckland,
Private Bag 92019, Auckland, New Zealand
Email: wang@cs.auckland.ac.nz)

Abstract: We present invariance characterizations of different types of random sequences. We correct Schnorr's original, incorrect characterization of Martin-Löf random sequences, compare it with Schnorr's corresponding characterization of his own randomness concept, and give a similar, new characterization of Kurtz random sequences. That is, we show that an infinite sequence ξ is Kurtz random if and only if for every partial, computable, measure-invariant function $\Phi : \Sigma^\omega \to \Sigma^\omega$ the sequence $\Phi(\xi)$ is not recursive.

Key Words: Randomness, invariance properties

Category: F.1

1 Introduction and Notation

Random sequences were first introduced by von Mises [von Mises 1919] as a foundation for probability theory. Von Mises thought that random sequences were a type of disordered sequences, called "Kollektive". The two features characterizing a Kollektiv are: the existence of limiting relative frequencies within the sequence and the invariance of these limits under the operation of an "admissible place selection rule". Here an admissible place selection rule is a procedure for selecting a subsequence of a given sequence ξ in such a way that the decision to select a term $\xi[n]$ does not depend on the value of $\xi[n]$. But von Mises' definition of an "admissible place selection rule" is not rigorous according to modern mathematics. After von Mises introduced the concept of "Kollektive", the first question raised was whether this concept is consistent. Wald [Wald 1936] answered this question affirmatively by showing that, for each countable set of admissible place selection rules, the corresponding set of "Kollektive" has Lebesgue measure 1. The second question raised was whether all "Kollektive" satisfy the standard statistical laws. For a negative answer to this question, Ville [Ville 1939] constructed a counterexample in 1939. He showed that, for each countable set of admissible place selection rules, there exists a "Kollektiv" which does not satisfy the law of the iterated logarithm. The example of Ville defeated the plan of von Mises to develop probability theory based on "Kollektive", that is, to give an axiomatisation of probability theory with "random sequences" (i.e., "Kollektive") as a

[1] Proceedings of the *First Japan-New Zealand Workshop on Logic in Computer Science*, special issue editors D.S. Bridges, C.S. Calude, M.J. Dinneen and B. Khoussainov.

primitive term. Later, admissible place selection rules were further developed by Tornier, Wald, Church, Kolmogorov, Loveland and others. This approach of von Mises to define random sequences is now known as the "stochastic approach".

Finally, Martin-Löf [Martin-Löf 1966] developed a quantitative (measure-theoretic) approach to the notion of random sequences. This approach is free from those difficulties connected with the frequency approach of von Mises. The idea underlying this approach is to identify the notion of randomness with the notion of typicalness. A sequence is typical if it lies in every "large" set of sequences, that is, if it is not in any "small" set of sequences. Of course, if we take "small" sets as Lebesgue measure 0 sets, then no typical sequence exists. The solution to this problem given by Martin-Löf is to define the "small" sets to be certain *constructive* null sets.

A different characterization of Martin-Löf's randomness concept was given by Solovay (see, e.g. [Chaitin 1987] or [Kautz 1991]), which is in the style of the first Borel-Cantelli Lemma. Later, the notion of "typicalness" was further studied by Schnorr, Kurtz and others.

Schnorr [Schnorr 1971] used the martingale concept to give a uniform description of various notions of randomness. Moreover, he criticized Martin-Löf's concept as being too strong and proposed a less restrictive concept as an adequate formalization of a random sequence. Kurtz [Kurtz 1981] introduced a notion of weak randomness using recursively open sets of Lebesgue measure one.

In [Wang 1996, Wang 1997], the second author obtained a complete characterization of the relations among these notions of randomness mentioned above. That is, the following diagram is shown:

$$\mathbf{M\text{-}RAND} \subset \mathbf{S\text{-}RAND} \subset \mathbf{W\text{-}RAND},$$

where these sets are the sets of Martin-Löf, Schnorr and Kurtz random sequences, respectively.

Note that a completely different approach to the definition of random sequences was proposed by Chaitin [Chaitin 1975], and further developed by others (see [Calude 1994]). In this approach, a notion of complexity is used for a definition of random sequences: The complexity of a finite string x is defined to be the length of the minimal string y from which x can be generated effectively. Then an infinite sequence is random if all of its initial segments have the maximal possible complexity (modulo some additive constant).

Schnorr and Chaitin [Chaitin 1975] showed that a sequence is random in Chaitin's sense if and only if it is Martin-Löf random. But it is still open whether one can define a concrete set of place selection rules so that the notion of stochasticity and the notion of typicalness coincide. Some partial results have been obtained in this line for abstract selection rules.

In this paper we give a summary of Schnorr's characterization of Martin-Löf's randomness concept (respectively Schnorr's randomness concept) in terms of invariance properties. Note that Schnorr's original characterization of Martin-Löf's randomness concept in terms of invariance properties is not correct. We will give a correct version in this paper. And we prove a similar characterization of Kurtz's randomness concept.

We close this section by introducing some notation we will use.

N is the set of natural numbers. $\Sigma = \{0, 1\}$ is the binary alphabet, Σ^* is the set of (finite) binary strings, Σ^n is the set of binary strings of length n, Σ^ω is the set of infinite binary sequences, and $\Sigma^\infty = \Sigma^* \cup \Sigma^\omega$. The length of a string x is denoted by $|x|$. λ is the empty string. $<$ is the length-lexicographical ordering on Σ^* and z_n ($n \geq 0$) is the nth string under this ordering. For strings $x, y \in \Sigma^*$, xy is the concatenation of x and y. For a sequence $x \in \Sigma^\omega$ and an integer number $n \geq -1$, $x[0..n]$ denotes the initial segment of length $n+1$ of x ($x[0..n] = x$ if $|x| \leq n+1$) and $x[i]$ denotes the ith bit of x, i.e., $x[0..n] = x[0] \cdots x[n]$. Lower case letters $\cdots, k, l, m, n, \cdots, x, y, z$ from the middle and the end of the alphabet will denote numbers and strings, respectively. Lower case Greek letters $\xi, \eta, \cdots$ denote infinite sequences from Σ^ω.

A subset of Σ^* is called a language or simply a set. Capital letters are used to denote subsets of Σ^* and boldface capital letters are used to denote subsets of Σ^ω. For sets A and B, $A \subseteq B$ (respectively $A \subset B$) denotes that A is a subset of B (respectively $A \subseteq B$ and $B \not\subseteq A$).

If X is a set of strings and $\mathbf{C}$ is a set of infinite sequences, then $X \cdot \mathbf{C}$ denotes the set $\{w\xi \ : \ w \in X, \xi \in \mathbf{C}\}$. For a set $\mathbf{C}$ of infinite sequences, we write $\mathrm{Prob}[\mathbf{C}]$ for the probability that $\xi \in \mathbf{C}$ when ξ is chosen by a random experiment in which an independent toss of a fair coin is used to decide whether $\xi[n] = 1$. This is the usual product measure on Σ^ω and defined for all measurable sets $\mathbf{C}$ with respect to this measure.

We fix a standard recursive bijection $\lambda x, y < x, y >$ on Σ^*. For a set $A \subseteq \Sigma^*$, we set $A^{[i]} = \{x \ : < x, z_i > \in A\}$.

A *Martin-Löf test* is a recursively enumerable set $A \subseteq \Sigma^*$ satisfying

$$\mathrm{Prob}[A^{[i]} \cdot \Sigma^\omega] \leq 2^i$$

for all $i \in N$. An infinite sequence ξ is *random* if it *withstands* every Martin-Löf test A, that is $\xi \notin \bigcap_i A^{[i]} \cdot \Sigma^\omega$. Let **M-NULL** be the set of sequences which do not withstand some Martin-Löf test, and let **M-RAND** $= \Sigma^\omega \setminus$ **M-NULL** be the set of Martin-Löf random sequences.

Schnorr modified Martin-Löf's randomness concept as follows. A *Schnorr test* is a pair (U, g) consisting of a recursively enumerable set $U \subseteq \Sigma^*$ and a recursive function g, together with a recursive enumeration $\{U_s\}_{s \in N}$ of U (that is, each $U_s \subseteq \Sigma^*$ contains exactly s words, $U_s \subseteq U_{s+1}$ for all s, $\bigcup_s U_s = U$, and the sequence $\{U_s\}_s$ is recursive) such that, for each k and j,

1. $\mathrm{Prob}[U^{[k]} \cdot \Sigma^\omega] \leq 2^{-k}$.
2. $\mathrm{Prob}[(U^{[k]} \setminus U^{[k]}_{g(k,j)}) \cdot \Sigma^\omega] \leq 2^{-j}$.

An infinite sequence ξ *does not withstand* the Schnorr test (U, g) if $\xi \in U^{[k]} \cdot \Sigma^\omega$ for all $k \in N$. A sequence ξ is *Schnorr random* if it withstands all Schnorr tests. Let **S-NULL** be the set of sequences which do not withstand some Schnorr test, and let **S-RAND** $= \Sigma^\omega \setminus$ **S-NULL** be the set of Schnorr random sequences.

Kurtz [Kurtz 1981] further defined a notion of weak randomness in terms of recursively open sets of Lebesgue measure 1. A *Kurtz test* is a recursively enumerable set $U \subseteq \Sigma^*$ such that $\mathrm{Prob}[U \cdot \Sigma^\omega] = 1$. A sequence ξ *does not withstand* the Kurtz test U if $\xi \notin U \cdot \Sigma^\omega$. A sequence ξ is *Kurtz random* if it withstands all Kurtz tests. Let **W-NULL** be the set of sequences that do not withstand some Kurtz test, and let **W-RAND** $= \Sigma^\omega \setminus$ **W-NULL** be the set of Kurtz random sequences.

In [Wang 1996, Wang 1997], the second author has given an alternative definition of Kurtz random sequences in terms of Martin-Löf statistical tests. An *mw-test* is a pair (U, g) where $U \subseteq \Sigma^*$ is a recursive set and g is a recursive function such that, for all k, the following two conditions hold:

1. $U^{[k]} \subseteq \Sigma^{\leq g(k)}$.
2. $\text{Prob}[U^{[k]} \cdot \Sigma^\omega] \leq 2^{-k}$.

A sequence ξ *does not withstand* the mw-test (U, g) if $\xi \in U^{[k]} \cdot \Sigma^\omega$ for all $k \in N$. A sequence ξ is *mw-random* if it withstands all mw-tests.

Theorem 1. *[Wang 1996, Wang 1997] An infinite sequence ξ is Kurtz random if and only if it is mw-random.*

2 Main Results

In this section we formulate a characterization of Martin-Löf's randomness concept in terms of invariance properties and compare it with Schnorr's characterization of his own randomness concept. Note that Schnorr's original characterization of Martin-Löf's randomness concept is not correct. And we will give a similar characterization of Kurtz's randomness concept.

Definition 2. A partial function $\varphi : \Sigma^* \to \Sigma^*$ is *monotone* if $\varphi(xy) \in \varphi(x) \cdot \Sigma^*$ for all $x, xy \in \text{dom}(\varphi)$.

A partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is continuous with respect to the product topology on Σ^ω if, for each set $A \subseteq \Sigma^*$, there exists a set $B \subseteq \Sigma^*$ such that $\Phi^{-1}(A \cdot \Sigma^\omega) = (B \cdot \Sigma^\omega) \cap \text{dom}(\Phi)$, where $\text{dom}(\Phi)$ is the domain of Φ. This can also be expressed in another way.

Definition 3. [Schnorr 1971] A partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is *induced* by a partial, monotone function $\varphi : \Sigma^* \to \Sigma^*$ if $\text{dom}(\Phi) = \bigcap_n (\varphi^{-1}(\Sigma^n \cdot \Sigma^*) \cdot \Sigma^\omega)$ and, for each $\xi \in \text{dom}(\Phi)$ and $n \in N$, $\Phi(\xi) \in \varphi(\xi[0..n-1]) \cdot \Sigma^\omega$.

It is easy to see that a partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is continuous if and only if there is a partial, monotone function $\varphi : \Sigma^* \to \Sigma^*$ such that Φ is a restriction of the function induced by φ.

Definition 4. [Schnorr 1971]

1. A partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is called *computable* if it is induced by some partial recursive, monotone function $\varphi : \Sigma^* \to \Sigma^*$.
2. A partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is called *strongly computable* if it is induced by some total recursive, monotone function $\varphi : \Sigma^* \to \Sigma^*$, and there is a total recursive function $h : N \to N$ such that $\text{dom}(\Phi) = \{\xi \in \Sigma^\omega : |\varphi(\xi[0..h(n)-1])| \geq n, n \in N\}$.

In [Schnorr 1971] computable functions are called sub-computably continuous, and strongly computable functions are called computably continuous. It is easy to see that a partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is computable if and only if it is induced by some total recursive, monotone function $\varphi : \Sigma^* \to \Sigma^*$ ([Schnorr 1971], Lemma 6.3). For total functions Φ computability and strong computability are equivalent.

Lemma 5. *A total function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is computable if and only if it is strongly computable.*

Proof. Let $\Phi : \Sigma^\omega \to \Sigma^\omega$ be a total computable function. W.l.o.g. we can assume that Φ is induced by a total recursive monotone function $\varphi : \Sigma^* \to \Sigma^*$. We define $h : N \to N$ by $h(n) = \min\{m : |\varphi(x)| \geq n \text{ for all } x \in \Sigma^m\}$. By compactness of Σ^ω, the function h is well-defined and total. It is computable. The pair (φ, h) shows that Φ is strongly computable. □

Definition 6. [Schnorr 1971]

1. A partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is *measure bounded* if, for each Lebesgue measurable set $\mathbf{C} \subseteq \Sigma^\omega$, there exists a constant c such that
$$\mathrm{Prob}[\Phi^{-1}(\mathbf{C})] \leq c \cdot \mathrm{Prob}[\mathbf{C}].$$
2. A partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is *measure-nondecreasing* (note that Schnorr used a different word: massverkleinernd) if, for each Lebesgue measurable set $\mathbf{C} \subseteq \Sigma^\omega$,
$$\mathrm{Prob}[\Phi^{-1}(\mathbf{C})] \leq \mathrm{Prob}[\mathbf{C}].$$
3. A partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is *measure-invariant* if, for each Lebesgue measurable set $\mathbf{C} \subseteq \Sigma^\omega$,
$$\mathrm{Prob}[\Phi^{-1}(\mathbf{C})] = \mathrm{Prob}[\mathbf{C}].$$

After these preliminary definitions, we can introduce von Mises style characterizations of the notions of Martin-Löf randomness and Schnorr randomness. In [Schnorr 1971], Satz 6.7, Schnorr claimed:

> Given a recursive sequence $\eta \in \Sigma^\omega$, a sequence $\xi \in \Sigma^\omega$ is Martin-Löf random if and only if there is no partial, computable, measure-nondecreasing function $\Phi : \Sigma^\omega \to \Sigma^\omega$ such that $\Phi(\xi) = \eta$.

This is not correct. For counterexamples to Schnorr's claim the reader is referred to [Hertling and Weihrauch 1997] and [Wang 1996, Wang 1997]. In the following, we prove a correct version of Schnorr's result.

Definition 7. [Hertling and Weihrauch 1997] A set $\mathbf{D} \subseteq \Sigma^\omega$ is a *fast enclosable G_δ-set* if there is an r.e. set $A \subseteq \Sigma^*$ satisfying the following conditions:

1. $\mathbf{D} = \bigcap_{i \in N} (A^{[i]} \cdot \Sigma^\omega)$,
2. $\mathrm{Prob}[A^{[i]} \cdot \Sigma^\omega \setminus \mathbf{D}] \leq 2^{-i}$ for all $i \in N$.

Theorem 8. *Given a recursive sequence $\eta \in \Sigma^\omega$, a sequence $\xi \in \Sigma^\omega$ is Martin-Löf random if and only if there is no partial, computable, measure-nondecreasing function $\Phi : \Sigma^\omega \to \Sigma^\omega$ with $\Phi(\xi) = \eta$ whose domain* $\mathrm{dom}(\Phi)$ *is a fast enclosable G_δ-set.*

Proof. The reader is referred to [Hertling and Weihrauch 1997] for the implication "$\Rightarrow$". For the implication "$\Leftarrow$", we proceed (almost) as in the proof of the second part of Satz 6.7 in [Schnorr 1971] and construct a partial computable function $\Phi : \Sigma^\omega \to \Sigma^\omega$ with $\mathrm{dom}(\Phi) = \Sigma^\omega \setminus \mathbf{M\text{-}RAND}$ and $\Phi(\beta) = \eta$ for all $\beta \in \Sigma^\omega \setminus \mathbf{M\text{-}RAND}$. Note that $\Sigma^\omega \setminus \mathbf{M\text{-}RAND}$ is a fast enclosable G_δ-set. The function Φ is measure-nondecreasing since $\mathrm{Prob}[\mathrm{dom}(\Phi)] = 0$.

Namely, it is well-known that there is a universal Martin-Löf test $A \subseteq \Sigma^*$ with $\bigcap_i A^{[i]} \cdot \Sigma^\omega = \Sigma^\omega \setminus \mathbf{M\text{-}RAND}$. Furthermore, we can assume that A is recursive and satisfies $A^{[i+1]} \subseteq A^{[i]} \cdot \Sigma^*$ for all i. We define a partial recursive monotone function $\varphi : \Sigma^* \to \Sigma^*$ by

$$\varphi(x) = \eta[0 \dots n-1] \quad \text{where} \quad n = \max\{j : \text{a prefix of } x \text{ is in } A^{[j]}\},$$

for all $x \in \Sigma^*$. Then the partial function $\Phi : \Sigma^\omega \to \Sigma^\omega$ which is induced by φ is computable, has domain

$$\mathrm{dom}(\Phi) = \bigcap_k A^{[k]} \cdot \Sigma^\omega = \Sigma^\omega \setminus \mathbf{M\text{-}RAND}$$

and satisfies $\Phi(\xi) = \eta$ for all $\xi \in \mathrm{dom}(\Phi)$. □

The following results give a characterization of Schnorr's randomness concept in terms of invariance properties. Remember that a total function $\Phi : \Sigma^\omega \to \Sigma^\omega$ is computable if and only if it is strongly computable.

Theorem 9. *[Schnorr 1971] Let $\Phi : \Sigma^\omega \longrightarrow \Sigma^\omega$ be a partial, computable, measure-invariant function. Then $\mathbf{S\text{-}RAND} \subseteq \mathrm{dom}(\Phi)$ and $\Phi(\mathbf{S\text{-}RAND}) \subseteq \mathbf{S\text{-}RAND}$.*

Theorem 10. *[Schnorr 1971] Let $\Phi : \Sigma^\omega \to \Sigma^\omega$ be a total, computable, measure-bounded function. Then $\Phi(\mathbf{S\text{-}RAND}) \subseteq \mathbf{S\text{-}RAND}$.*

Let $\mathbf{C}_1$ be the set of total, computable, measure-bounded functions $\Phi : \Sigma^\omega \to \Sigma^\omega$, $\mathbf{C}_2$ be the set of total, computable, measure-nondecreasing functions $\Phi : \Sigma^\omega \to \Sigma^\omega$, $\mathbf{C}_3$ be the set of partial, computable, measure-invariant functions $\Phi : \Sigma^\omega \to \Sigma^\omega$, and $\mathbf{C}_4$ be the set of total, computable, measure-invariant functions $\Phi : \Sigma^\omega \to \Sigma^\omega$.

Theorem 11. *[Schnorr 1971] For $i = 1, 2, 3, 4$, a sequence $\xi \in \Sigma^\omega$ is Schnorr random if and only if, for all $\Phi \in \mathbf{C}_i$ with $\xi \in \mathrm{dom}(\Phi)$, $\Phi(\xi)$ satisfies the law of large numbers.*

By our characterization of Kurtz's randomness concept in Theorem 1, a similar characterization as Theorem 11 can be given for Kurtz's concept. The proofs of the following theorems are minor modifications of the proofs of Theorem 9, Theorem 10 and Theorem 11.

Theorem 12. *Let $\Phi : \Sigma^\omega \to \Sigma^\omega$ be a partial, computable, measure-invariant function. Then $\Phi(\mathbf{W\text{-}RAND} \cap \mathrm{dom}(\Phi)) \subseteq \mathbf{W\text{-}RAND}$.*

Proof. It suffices to show that, for each mw-test (U, g), there is another mw-test (V, f) such that

$$\Phi^{-1}(\mathbf{NULL}_{(U,g)}) \subseteq \mathbf{NULL}_{(V,f)} \tag{1}$$

where $\mathbf{NULL}_{(U,g)}$ (respectively $\mathbf{NULL}_{(V,f)}$) is the set of sequences that do not withstand the mw-test (U, g) (respectively (V, f)).

W.l.o.g., we may assume that Φ is induced by a total recursive, monotone function $\varphi : \Sigma^* \to \Sigma^*$. First, for all $k \in \mathbf{N}$, define the set $A^{[k]} \subseteq \Sigma^*$ to be the smallest set with the following properties:

1. $\text{Prob}[A^{[k]} \cdot \Sigma^\omega] \geq 1 - 2^{-k}$,
2. if $x \in A^{[k]}$ then $|\varphi(x)| \geq g(k)$,
3. if $z_n \in A^{[k]}$, $j \leq n$ and $|\varphi(z_j)| \geq g(k)$ then $z_j \in A^{[k]}$.

These sets $A^{[k]}$ are well-defined and finite because Φ is measure-invariant. Let $l(k) = \max\{|x| : x \in A^{[k]}\}$, $C^{[k]} = \Sigma^{l(k)} \setminus A^{[k]} \cdot \Sigma^*$, $V^{[k]} = C^{[k+1]} \cup \{x \in A^{[k+1]} : \varphi(x) \in U^{[k+1]} \cdot \Sigma^*\}$, and $f(n) = l(n+1)$. Then it is easily checked that (V, f) is an mw-test and $\Phi^{-1}(U^{[k+1]} \cdot \Sigma^\omega) \subseteq V^{[k]} \cdot \Sigma^\omega$. Whence (1) holds. This completes the proof of the theorem. □

Theorem 13. *Let $\Phi : \Sigma^\omega \to \Sigma^\omega$ be a total, computable, measure-bounded function. Then $\Phi(\mathbf{W\text{-}RAND}) \subseteq \mathbf{W\text{-}RAND}$.*

Proof. It suffices to show that, for each mw-test (U, g), there is another mw-test (V, f) such that (1) holds. By Lemma 5 the function Φ is strongly computable. Let $\varphi : \Sigma^* \to \Sigma^*$ and $h : N \to N$ be a pair of total functions which witness that Φ is strongly computable. Fix a number c such that, for all Lebesgue measurable sets $\mathbf{C} \subseteq \Sigma^\omega$, $\text{Prob}[\Phi^{-1}(\mathbf{C})] \leq 2^c \cdot \text{Prob}[\mathbf{C}]$.

For all k, define $f(k) = h(g(k+c))$ and $V^{[k]} = \{x \in \Sigma^{f(k)} : \varphi(x) \in U^{[k+c]} \cdot \Sigma^*\}$. Since $|\varphi(x)| \geq g(k+c)$ for all $x \in \Sigma^{f(k)}$ we see $V^{[k]} \cdot \Sigma^\omega = \Phi^{-1}(U^{[k+c]} \cdot \Sigma^\omega)$, hence

$$\text{Prob}[V^{[k]} \cdot \Sigma^\omega] \leq 2^c \cdot \text{Prob}[U^{[k+c]} \cdot \Sigma^\omega] \leq 2^{-k}$$

for all $k \in N$. Hence, the pair (V, f) is an mw-test satisfying (1). This completes the proof of the theorem. □

Theorem 14. *Let (U, g) be an mw-test and $\eta \in \Sigma^\omega$ be a recursive sequence. Then there exists a total, strongly computable, measure-invariant function $\Phi : \Sigma^\omega \to \Sigma^\omega$ such that $\Phi(\xi) = \eta$ for all $\xi \in \mathbf{NULL}_{(U,g)}$.*

Proof. W.l.o.g., we may assume that, for all k, the following hold:

1. g is strictly increasing,
2. $U^{[k]} \subseteq \Sigma^{g(k)}$,
3. for all $x \in U^{[k+1]}$, there is a prefix y of x such that $y \in U^{[k]}$,
4. $\text{Prob}[U^{[k]} \cdot \Sigma^\omega] = 2^{-k}$.

In the following we define a total recursive, monotone function $\varphi : \Sigma^* \to \Sigma^*$ such that the induced function $\Phi : \Sigma^\omega \to \Sigma^\omega$ satisfies our requirements.

At first, we define sequences $C_{(k,0)}, \cdots, C_{(k,2^k-1)}$ of sets of strings and sequences $x_{(k,0)}, \cdots, x_{(k,2^k-1)}$ of strings by induction on k.

Let $C_{(0,0)} = \{\lambda\}$ and $x_{(0,0)} = \{\lambda\}$.

Let $C_{(k+1,0)}, \cdots, C_{(k+1,2^{k+1}-1)}$ be a sequence of subsets of $\Sigma^{g(k+1)}$ such that

1. $(C_{(k+1,2i)} \cup C_{(k+1,2i+1)}) \cdot \Sigma^\omega = C_{(k,i)} \cdot \Sigma^\omega$ for $i < 2^k$,
2. $C_{(k+1,0)} = U^{[k+1]}$,
3. $C_{(k+1,i)} \cap C_{(k+1,j)} = \emptyset$ for $i \neq j$,
4. $\mathrm{Prob}[C_{(k+1,i)} \cdot \Sigma^\omega] = 2^{-(k+1)}$ for $i < 2^{k+1}$,

and let $x_{(k+1,0)}, \cdots, x_{(k+1,2^{k+1}-1)}$ be an enumeration of all strings in Σ^{k+1} such that

1. $x_{(k+1,0)} = \eta[0..k]$,
2. $x_{(k,i)} \cdot \Sigma^\omega = \{x_{(k+1,2i)}, x_{(k+1,2i+1)}\} \cdot \Sigma^\omega$ for all $i < 2^k$.

Now the function $\varphi : \Sigma^* \to \Sigma^*$ is defined by $\varphi(\lambda) = \lambda$ and

$$\varphi(yb) = \begin{cases} x_{(k,i)} & \text{if } yb \in C_{(k,i)} \text{ for some } k, i \in N \\ \varphi(y) & \text{otherwise} \end{cases}$$

where $y \in \Sigma^*$ and $b \in \Sigma$.

The function φ is total recursive and monotone. It is straightforward to check that the induced function $\Phi : \Sigma^\omega \to \Sigma^\omega$ by φ is total, strongly computable and measure-invariant. Moreover, for all $\xi \in \mathbf{NULL}_{(U,g)}$, $\Phi(\xi) = \eta$. □

Now we are ready to characterize the notion of Kurtz randomness in terms of invariance properties. By combining previous theorems, we obtain the following theorem.

Theorem 15. *For $i = 1, 2, 3, 4$ and a recursive sequence $\eta \in \Sigma^\omega$, a sequence $\xi \in \Sigma^\omega$ is Kurtz random if and only if $\Phi(\xi) \neq \eta$ for all $\Phi \in \mathbf{C}_i$ with $\xi \in \mathrm{dom}(\Phi)$.*

Proof. This follows from Theorem 12, Theorem 13, Theorem 14, and from the fact that no recursive sequence is Kurtz random. □

The topic of this paper is related to the independence properties of subsequences of a random sequence and is also related to the independent random sequences. A number of general independence properties for subsequences of a random sequence are established by Kautz [Kautz 1991] and van Lambalgen [van Lambalgen 1987b, van Lambalgen 1987a] et al. There are various applications of independence properties and independent random sequences. For example Lutz [Lutz 1992] used the independent random oracles to characterize complexity classes, and Kautz and Miltersen [Kautz and Miltersen 1994] used independence properties of Martin-Löf random sequences to show that relative to a random oracle, **NP** is not small in the sense of Lutz p-measure.

Acknowledgements

We would like to thank Professor Cristian Calude for many discussions and for his suggestions to improve the presentation of this paper.

The first author is supported by DFG Research Grant No. HE 2489/2-1. The second author is supported by a postdoctoral fellowship (supervisor: Professor Cristian Calude) of the University of Auckland.

References

[Calude 1994] C. Calude: "Information and Randomness: An Algorithmic Perspective"; Springer Verlag, Berlin, 1994.

[Chaitin 1975] G. J. Chaitin: "A theory of program size formally identical to information theory", J. Assoc. Comput. Mach., 22 (1975), 329–340.

[Chaitin 1987] G. J. Chaitin: "Incompleteness theorems for random reals"; Adv. in Appl. Math., 8 (1987), 119–146.

[Hertling and Weihrauch 1997] P. Hertling, K. Weihrauch: "Randomness spaces"; in preparation.

[Kautz 1991] S. Kautz: "Degrees of Random Sets"; PhD thesis, Cornell University, Ithaca, (1991).

[Kautz and Miltersen 1994] S. Kautz and P. Miltersen: "Relative to a random oracle, **NP** is not small"; in: Proc. 9th Conf. on Structure in Complexity Theory, IEEE Computer Society Press (1994), 162–174.

[Kolmogorov 1965] A. N. Kolmogorov: "Three approaches to the definition of the concept *quantity of information*"; *Problemy Inform. Transmission*, 1 (1965), 3–7.

[Kurtz 1981] S. Kurtz: "Randomness and Genericity in the Degrees of Unsolvability"; PhD thesis, University of Illinois at Urbana-Champaign (1981).

[Lutz 1992] J. H. Lutz: "On independent random oracles"; Theoret. Comput. Sci., 92 (1992) 301–307.

[Martin-Löf 1966] P. Martin-Löf: "The definition of random sequences"; Inform. and Control, 9 (1966), 602–619.

[Schnorr 1971] C. P. Schnorr: "Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie"; Lecture Notes in Math. 218. Springer Verlag (1971).

[van Lambalgen 1987a] M. van Lambalgen: "Random Sequences"; PhD thesis, University of Amsterdam (1987).

[van Lambalgen 1987b] M. van Lambalgen: "Von Mises' definition of random sequences reconsidered"; J. Symbolic Logic, 52 (1987), 725–755.

[Ville 1939] J. Ville: "Ètude Critique de la Notion de Collectif"; Gauthiers-Villars, Paris (1939).

[von Mises 1919] R. von Mises: "Grundlagen der Wahrscheinlichkeitsrechnung"; Math. Zeitschrift, 5 (1919), 52–99.

[Wald 1936] A. Wald: "Sur la notion de collectif dans le calcul des probabilités"; C. R. Acad. Sci. Paris, 202 (1936), 180–183.

[Wang 1996] Y. Wang: "Randomness and Complexity"; PhD thesis, Universität Heidelberg, Germany (1996).

[Wang 1997] Y. Wang: "A comparison of some randomness concepts"; to appear in: J. Symbolic Logic (1997).