ACADEMIC
PRESS

Available at
www.ComputerScienceWeb.com
POWERED BY SCIENCE DIRECT®

Information and Computation 181 (2003) 32–56

Information
and
Computation

www.elsevier.com/locate/ic

Random elements in effective topological spaces with measure

Peter Hertling* and Klaus Weihrauch

Theoretische Informatik I, FernUniversität Hagen, 58084 Hagen, Germany

Received 20 January 1998; revised 29 January 2002

Abstract

Following a suggestion of Zvonkin and Levin, we generalize Martin-Löf's definition of infinite random sequences over a finite alphabet via randomness tests to effective topological spaces with a measure. We show that under weak computability conditions there is a universal randomness test. We prove a theorem on randomness preserving functions which corrects and extends a result by Schnorr and apply it to a number of examples. In particular, we show that a real number is random if, and only if, it has a random b-ary representation, for any $b \geqslant 2$. We show that many computable, continuously differentiable real functions preserve randomness. Especially, all computable analytic functions which are not constant on any open subset of their domain preserve randomness. Finally, we introduce a new randomness concept for subsets of natural numbers, which we characterize in terms of random sequences. Surprisingly, it turns out that there are infinite co-r.e. random sets.

Keywords: Algorithmic randomness; Randomness tests; Random real numbers; Random sets

1. Introduction

Informally, a sequence of zeros and ones is random, if it has no detectable regularity. Precise definitions are based on recursion theory. One possibility for defining random sequences is via the program-size complexity of the finite prefixes; compare, e.g., [13]. Another approach is via randomness tests and due to Martin-Löf [14], who, in fact, gave the first definition of this randomness notion. Martin-Löf's idea was to call a sequence non-typical, i.e., not random, if there is an

[*] Corresponding author.

E-mail addresses: peter.hertling@fernuni-hagen.de (P. Hertling), klaus.weihrauch@fernuni-hagen.de (K. Weihrauch).

0890-5401/02/$ - see front matter © 2002 Elsevier Science (USA). All rights reserved.
PII: S0890-5401(02)00034-2

effectively testable property which the sequence shares only with few other sequences. This is made more precise be demanding that the sequence lies in the intersection of a computable sequence $(U_n)_n$ of open sets U_n whose measure tends to 0 quickly. Martin-Löf's approach has been generalized by Zvonkin and Levin [23] to spaces which allow the formulation of computable sequences of open sets with fast decreasing measure. In this paper, we extend and generalize this work.

In Section 3 we introduce effective topological measure spaces, ETMSs, for short. We prove the existence of a universal randomness test under rather weak conditions, and consider various basic properties of the resulting randomness notion. It should be mentioned that this approach allows for example the introduction of random real numbers without referring to random sequences. Furthermore, some examples of ETMSs and random elements are given. In Section 4 we ask under which conditions a function between ETMSs preserves randomness. Our main invariance result gives sufficient conditions and corrects and extends a corresponding result by Schnorr [17]. In Section 5 we concentrate on the ETMS of real numbers. The invariance result is used to show that the randomness notion introduced directly on the real numbers is identical with the randomness notion for real numbers introduced via randomness of the b-ary representation of a number. This also gives a new proof of the result by Calude and Jürgensen [2] that randomness of a real number defined via randomness of its b-ary representation does not depend on the base b. Furthermore, we consider real vectors and sequences. Further main results in this section state that many computable, continuously differentiable real functions and every computable analytic function which is not constant on any open subset of its domain preserve randomness. In the last section, we consider another ETMS: the power set of the natural numbers, endowed with the natural topology as a complete partial order. This point of view leads to a new and interesting notion of randomness for sets of natural numbers, which is different from the usual one defined via randomness of characteristic functions. The first main result of the section is a characterization of randomness for sets in terms of usual random sequences. The second main result is a theorem which implies that there are infinite random co-r.e. sets.

This paper and the paper Hertling and Weihrauch [7] are abridged versions of the more detailed technical report [8] by Hertling and Weihrauch.

2. Notation

The power set $\{A \mid A \subseteq X\}$ of a set X, containing all subsets of X, is denoted by 2^X. By $f :\subseteq X \to Y$ we mean a (partial or total) function f with domain $\mathrm{dom}(f) \subseteq X$ and range $\mathrm{range}(f) \subseteq Y$. The notation $f : X \to Y$ indicates that the function is total, i.e., $\mathrm{dom}(f) = X$. We denote the set of natural numbers by $\mathbb{N} = \{0, 1, 2, \ldots\}$. We use the notions of a *computable* function $f :\subseteq \mathbb{N} \to \mathbb{N}$ and of an *r.e.* set $A \subseteq \mathbb{N}$ in the usual sense. A *sequence* is a mapping $p : \mathbb{N} \to X$ to some set X and usually written in the form $(p_n)_{n\in\mathbb{N}}$ or just $(p_n)_n$. The infinite product of X is the set of all sequences of elements in X, denoted by $X^\omega := \{p \mid p : \mathbb{N} \to X\}$. For any $k \geqslant 0$ the finite product $X^k := \{w \mid w : \{1, \ldots, k\} \to X\}$ is the set of all vectors $w = w(1)w(2)\cdots w(k)$ over X of length k. The empty word, the only element of X^0, is denoted by ε. The length of a word w is denoted by $|w|$.

We use the standard bijection $\langle , \rangle : \mathbb{N}^2 \to \mathbb{N}$ defined by $\langle i, j\rangle := \frac{1}{2}(i + j)(i + j + 1) + j$. We define higher tupling functions recursively by $\langle n_1, n_2, \ldots, n_{k+1}\rangle := \langle\langle n_1, \ldots, n_k\rangle, n_{k+1}\rangle$, for $k \geqslant 2$. The inverses π_i^k are defined by $\langle \pi_1^k n, \ldots, \pi_k^k n\rangle = n$. We also use the standard bijective numbering $D : \mathbb{N} \to \{E \subseteq \mathbb{N} \,|\, E \text{ is finite}\}$ of the set of all finite subsets of $\mathbb{N}$, defined by $D^{-1}(E) := \sum\{2^i \,|\, i \in E\}$, and the numbering $\nu_{\mathbb{Q}} : \mathbb{N} \to \mathbb{Q}$ of the set of rational numbers defined by $\nu_{\mathbb{Q}}(\langle i,j,k\rangle) := (i-j)/(k+1)$.

For notions like topology, base, subbase, σ-algebra generated by a class of sets, measure, σ-finite measure, finite measure, probability measure, and Lebesgue measure, the reader is referred to standard textbooks on topology and measure theory.

3. Effective topological measure spaces

Zvonkin and Levin [23, pp. 110–111], observed that Martin-Löf's [14] definition of randomness tests and of random elements can easily be generalized from the space of infinite sequences over a finite alphabet to any separable topological space with a given numbering of a base and with a measure. In this section we provide a convenient framework based on the notion of an effective topological measure space. Among other things we prove the existence of a universal randomness test under rather weak assumptions.

The basic setting in which we work is given by the following definition. It is fundamental in effective descriptive set theory. It also fits well into Type-2 Theory of Effectivity; see Weihrauch [22].

Definition 3.1. An *effective topological measure space*, ETMS for short, is a triple (X, B, μ), where X is a topological space, $B : \mathbb{N} \to 2^X$ is a total numbering of a base of the topology of X, and μ is a measure defined on the σ-algebra generated by the topology of X (notation: $B_i := B(i)$).

Fundamental to our approach is the notion of *computability* for sequences of open sets explained in the following definition. Furthermore, often we shall consider ETMSs which satisfy the following *intersection property*.

Definition 3.2. Let X be a topological space and $(U_n)_n$ be a sequence of open subsets of X.

1. A sequence $(V_n)_n$ of open subsets of X is called *U-computable* if, and only if, there is an r.e. set $A \subseteq \mathbb{N}$ such that $V_n = \bigcup_{\langle n,i\rangle \in A} U_i$ for all $n \in \mathbb{N}$.
2. We say that U satisfies the *intersection property* if, and only if, there is an r.e. set $A \subseteq \mathbb{N}$ with

$$U_i \cap U_j = \bigcup \{U_k \,|\, \langle i,j,k\rangle \in A\} \quad \text{for all } i,j \in \mathbb{N}.$$

Remark 3.3. If the numbering B does not satisfy the intersection property, or if one is given only a numbering B of a subbase of the topology (this is the usual setting in Type-2 Theory of Effectivity; see Weihrauch [22]), then one can in a natural way define a numbering $B^{\cap}$ of a base satisfying the intersection property: $B^{\cap}(i) := \bigcap_{j \in D_i} B_j$. It is clear that B is $B^{\cap}$-computable. If B satisfies the intersection property, then $B^{\cap}$ is B-computable as well.

The next definition generalizes Martin-Löf's [14] definition of random sequences to elements from an arbitrary ETMS.

Definition 3.4. Let (X, B, μ) be an ETMS.

1. A *randomness test on X* is a B-computable sequence $(U_n)_n$ of open sets with $\mu(U_n) \leqslant 2^{-n}$ for all $n \in \mathbb{N}$.
2. An element $x \in X$ is called *non-random* if, and only if, $x \in \bigcap_{n\in\mathbb{N}} U_n$ for some randomness test $(U_n)_n$ on X. It is called *random* if, and only if, it is not non-random.

Remark 3.5. Zvonkin and Levin [23] gave a similar generalization of Martin-Löf's randomness tests, though is seems that in their approach the numbering B needs to satisfy an additional technical condition which we do not need.

In the following examples of ETMSs the numberings of bases satisfy the intersection property.

Example 3.6.

1. The simplest example of an ETMS is a finite discrete space (Σ, B, μ), where $\Sigma = \{s_0, \dots, s_{|\Sigma|-1}\}$ is a finite set containing at least 2 elements, where each singleton set has measure $1/|\Sigma|$, and where $B_i := \{s_{i \bmod |\Sigma|}\}$. In this case every non-empty open set has positive measure. Hence, every point in Σ is random.
2. The original ETMSs are the spaces (Σ^ω, B, μ) of infinite sequences over a finite alphabet Σ with at least two elements, where B is the standard numbering of the set $\{w\Sigma^\omega \mid w \in \Sigma^*\}$ given by $B_i := v(i)\Sigma^\omega$ where v is the length-lexicographical bijection between $\mathbb{N}$ and Σ^* (given some ordering on Σ), and where $\mu(w\Sigma^\omega) = |\Sigma|^{-|w|}$ for $w \in \Sigma^*$ [14]. Clearly, every computable sequence $p \in \Sigma^\omega$ is non-random (choose $U_i := p_0p_1\cdots p_{i-1}\Sigma^\omega$).
3. For the real numbers $\mathbb{R}$ we consider the ETMS $(\mathbb{R}, B, \lambda)$, where λ is the usual Lebesgue measure and B is the standard numbering of the set of non-empty open intervals with rational endpoints defined by $B_{\langle i,j\rangle} := (v_{\mathbb{Q}}(i) - v_{\mathbb{Q}_+}(j), v_{\mathbb{Q}}(i) + v_{\mathbb{Q}_+}(j))$, where in addition to $v_{\mathbb{Q}}$ (see Section 2) we use the numbering $v_{\mathbb{Q}_+}$ of the positive rational numbers defined by $v_{\mathbb{Q}_+}(\langle i,k\rangle) := (i+1)/(k+1)$. When we speak about *random real numbers* we mean random elements of this ETMS. A real number x is computable if, and only if, there is a computable function f such that $x \in B_{f(n)}$ and $\mu(B_{f(n)}) \leqslant 2^{-n}$ for all $n \in \mathbb{N}$; see Weihrauch [22]. Clearly, every computable real number is non-random (choose $U_n := B_{f(n)}$).
4. Let the ETMS $([0,1], \tilde{B}, \tilde{\lambda})$ be the canonical restriction of $(\mathbb{R}, B, \lambda)$ from 3 above to the unit interval, that is, $\tilde{B}_i := B_i \cap [0,1]$, and $\tilde{\lambda}(S) := \lambda(S)$, for $S \subseteq [0,1]$.

We state some elementary properties of random elements in ETMSs. Let us call two numberings B and C of bases of a topological space *equivalent* if B is C-computable and C is B-computable.

Proposition 3.7. *Let (X, B, μ) and (X, C, μ) be ETMSs such that B and C are equivalent. Then randomness on the two spaces is the same.*

The proof is straightforward, and we omit it. The next proposition says that one may assume without loss of generality that the sequence $(V_n)_n$ of a randomness test is decreasing if the ETMS satisfies the intersection property.

Proposition 3.8. *Let (X, B, μ) be an ETMS satisfying the intersection property, and let $(V_n)_n$ be a randomness test on X. Then $(U_n)_n$ with $U_n := \bigcap_{i \leqslant n} V_i$ is a randomness test on X with $U_{n+1} \subseteq U_n$ for all n and $\bigcap_{n=0}^{\infty} U_n = \bigcap_{n=0}^{\infty} V_n$.*

Again, the proof is straightforward and omitted.

It is remarkable that the ETMS (Σ^ω, B, μ) from Example 3.6(2) has a universal randomness test [14].

Definition 3.9. A randomness test $(U_n)_n$ on an ETMS (X, B, μ) is called *universal* if, and only if, for any randomness test $(V_n)_n$ on (X, B, μ) there is a number c such that $V_{n+c} \subseteq U_n$ for all $n \in \mathbb{N}$.

Often one needs only the following property of a universal randomness test: if $(U_n)_n$ is a universal randomness test, then the set $\bigcap_{n=0}^{\infty} U_n$ consists exactly of all non-random elements of the space.

Let us call a measure μ on an ETMS *upper semi-computable*, if, and only if,

$$\text{the set}\left\{ \langle j, n \rangle \,\middle|\, \mu\left(\bigcup_{i \in D_j} B_i \right) < \nu_{\mathbb{Q}}(n) \right\}\text{is r.e.} \tag{1}$$

Theorem 3.10. *Every ETMS (X, B, μ) with an upper semi-computable measure has a universal randomness test.*

Proof. First we produce an effective list of randomness tests on (X, B, μ) which contains all randomness tests $(S_n)_n$ satisfying $\mu(S_n) < 2^{-n}$ for all n. Then the universal test will be obtained by a diagonal construction.

The upper semi-computability of the measure implies that also the set

$$Z := \left\{ \langle j, n \rangle \,\middle|\, \mu\left(\bigcup_{i \in D_j} B_i \right) < 2^{-n} \right\}$$

is r.e.. Let $(W_k)_{k \in \mathbb{N}}$ be a standard numbering of all r.e. subsets of $\mathbb{N}$ (compare Rogers [16] or Weihrauch [19]). For each $k \in \mathbb{N}$ let $(U_{k,n})_n$ be the kth computable sequence of open sets, defined by $U_{k,n} := \bigcup_{\langle n,i \rangle \in W_k} B_i = \bigcup_{i \in V_{k,n}} B_i$, where $V_{k,n} := \{ i \,|\, \langle n, i \rangle \in W_k \}$. Since $\{ \langle k, n, i \rangle \,|\, \langle n, i \rangle \in W_k \}$ is r.e. and infinite there is an injective total computable function $h : \mathbb{N} \to \mathbb{N}$ such that $\mathrm{range}(h) = \{ \langle k, n, i \rangle \,|\, \langle n, i \rangle \in W_k \}$. Then $V_{k,n}[m] := \{ i \,|\, (\exists m' \leqslant m) h(m') = \langle k, n, i \rangle \}$ is the set of all those elements in $V_{k,n}$ which have been enumerated by h into $V_{k,n}$ until stage m. We cut the sets $V_{k,n}$ off in order to obtain randomness tests. Therefore we define $\widetilde{V}_{k,n}$ by

$$i \in \widetilde{V}_{k,n} \quad :\Longleftrightarrow \quad i \in V_{k,n} \quad \text{and} \quad \langle D^{-1}(V_{k,n}[\min\{ m \,|\, i \in V_{k,n}[m] \}]), n \rangle \in Z.$$

It is clear that $\widetilde{V}_{k,n} \subseteq V_{k,n}$ and that the set $\{ \langle k, n, i \rangle \,|\, i \in \widetilde{V}_{k,n} \}$ is r.e. We define $\widetilde{U}_{k,n} := \bigcup_{i \in \widetilde{V}_{k,n} B_i}$. Clearly, $\mu(\widetilde{U}_{k,n}) \leqslant 2^{-n}$ by construction. Thus, for each k, the sequence $(\widetilde{U}_{k,n})_n$ is a randomness test. On the other hand, let $(S_n)_n$ be a randomness test such that $\mu(S_n) < 2^{-n}$ for all n. Then $(S_n)_n = (U_{k,n})_n$ for some k. Then $\widetilde{V}_{k,n} = V_{k,n}$, hence $\widetilde{U}_{k,n} = U_{k,n}$, for all n. That means, any such randomness test $(S_n)_n$ occurs in the list $((\widetilde{U}_{k,n})_n)_k$ of randomness tests.

Define $U_n := \bigcup_{k=0}^{\infty} \widetilde{U}_{k,n+k+1}$ for all n. We claim that $(U_n)_n$ is a universal randomness test. It is straightforward to check that $\mu(U_n) \leqslant 2^{-n}$ and that $(U_n)_n$ is B-computable, hence, that $(U_n)_n$ is a randomness test. Let $(S_n)_n$ be an arbitrary randomness test. Then also $(S_{n+1})_n$ is a randomness test. Hence, there is some k such that $U_{k,n} = S_{n+1}$ for all n. Due to $\mu(S_{n+1}) < 2^{-n}$ for all n, we obtain also $\widetilde{U}_{k,n} = S_{n+1}$, hence $S_{n+k+2} \subseteq U_n$, for all n. We conclude that $(U_n)_n$ is a universal randomness test. □

Zvonkin and Levin [23, Proposition 4.1] state without proof that in their framework there exists a universal randomness test if the function $j \mapsto \mu(\bigcup_{i \in D_j})B_i$ mapping natural numbers to real numbers is a computable function in the usual sense, which means that

$$\text{the set} \left\{ \langle j, m, n \rangle \,\middle|\, \nu_{\mathbb{Q}}(m) < \mu\left(\bigcup_{i \in D_j} B_i \right) < \nu_{\mathbb{Q}}(n) \right\} \text{is r.e..}$$

It is interesting that for the existence of a universal randomness test only the upper semi-computability of the measure (Condition (1)) is needed, while in other contexts the complementary condition:

$$\text{the set} \left\{ \langle j, m \rangle \,\middle|\, \nu_{\mathbb{Q}}(m) < \mu\left(\bigcup_{i \in D_j} B_i \right) \right\} \text{is r.e.}$$

seems to be more important, see [13,21,23].

A subset Y of a topological space X is called *dense in* X if, and only if, every open subset of X contains an element of Y. It is called *nowhere dense* if, and only if, its closure does not contain an open set. It is called *meager* if, and only if, it is the union of countably many nowhere dense sets.

Proposition 3.11. *Let (X, B, μ) be an ETMS.*

1. *The set of non-random elements in X has μ-measure 0.*
2. *The set of random elements is meager, if the space X has a universal randomness test and the set of non-random elements is dense in X.*

We leave the simple proof to the reader. This proposition says that, on the one hand, in a measure theoretical sense the set of non-random elements is small. On the other hand, topologically the set of random elements is small, if the space has a universal randomness test, and if the set of non-random elements is a dense subset of X. Of course, the second statement of the proposition is interesting only if the space itself is not meager. For example, all of the ETMSs in Examples 3.6(2)–(4) have these properties.

Is there a canonical definition of the structure of an ETMS on the direct product of finitely or countably many ETMSs? In order to answer this question, remember that an ETMS is given by (1) a topology, (2) a measure on the σ-algebra generated by the topology, and (3) a total numbering of a base of the topology. The construction of the product topology on the direct product of finitely or infinitely many topological spaces is standard. The σ-algebra generated by this topology coincides with the standard product of the σ-algebras. Also, on the direct product of finitely many measure spaces with σ-finite measures one can define in a standard way a measure, which turns out to be σ-finite. Similarly, on a countably infinite product of spaces with probability measures one can define in a standard way a measure, which turns out to be a probability measure. What is left to do, is to define a canonical numbering of a base of the product topology of the direct product of a finite or countably infinite sequence of topological spaces if each of them is endowed with a numbering of a base. This can also be done in a straightforward way as follows. Let $(X^{(i)}, B^{(i)}, \mu^{(i)})$ for $i = 0, 1, 2, \ldots$ be ETMSs. We define a numbering $B^{(0)} \times \cdots \times B^{(n)}$ of a base of the product topology on $X^{(0)} \times \cdots \times X^{(n)}$ and a numbering $(\prod_{k=0}^{\infty} B^{(k)})$ of a base of the product topology on $\prod_{k=0}^{\infty} X^{(k)}$ by

$$(B^{(0)} \times \cdots \times B^{(n)})\langle i_0, \ldots, i_n\rangle := B^{(0)}_{i_0} \times \cdots \times B^{(n)}_{i_n},$$
$$\left(\prod_{k=0}^{\infty} B^{(k)}\right)\langle n, \langle i_0, \ldots, i_n\rangle\rangle := \prod_{k=0}^{n} B^{(k)}_{i_k} \times \prod_{k=n+1}^{\infty} X^{(k)}.$$

If $(X^{(i)}, B^{(i)}, \mu^{(i)}) = (X, B, v)$ for all $i \leqslant n$ (respectively, for all $i \in \mathbb{N}$), then the resulting ETMS is written $(X^{n+1}, B^{n+1}, \mu^{n+1})$ (respectively, $(X^{\omega}, B^{\omega}, \mu^{\omega})$).

Example 3.12. To give an example, consider the ETMS (Σ, B, μ) from Example 3.6(1) and the ETMS $(\Sigma^{\omega}, \tilde{B}, \tilde{\mu})$ from Example 3.6(2). The topology on Σ^{ω} is the product topology of the discrete topology on Σ, the measure $\tilde{\mu}$ on Σ^{ω} is equal to the product measure μ^{ω} of μ, and the numbering $\tilde{B}$ is equivalent (in the sense explained before Proposition 3.7) to the numbering B^{ω} obtained by applying the product construction to B.

By the following result, certain projections of random vectors or sequences are random again. In particular, each component of a finite or infinite random vector is random.

Proposition 3.13.
1. *Let $\prod_{k=0}^{n}(X^{(k)}, B^{(k)}, \mu^{(k)})$ be a product of ETMSs with finite measures. Let $(i_0, \ldots, i_l)$ be a vector of pairwise different indices i_j with $0 \leqslant i_j \leqslant n$. If $(x_0, \ldots, x_n)$ is random in the above space, then $(x_{i_0}, \ldots, x_{i_l})$ is random in $\prod_{k=0}^{l}(X^{(i_k)}, B^{(i_k)}, \mu^{(i_k)})$.*
2. *Let $\prod_{k=0}^{\infty}(X^{(k)}, B^{(k)}, \mu^{(k)})$ be a product of ETMSs with probability measures. Let $(i_0, \ldots, i_l)$ be a vector of pairwise different indices. If $(x_0, x_1, \ldots)$ is random in the above space, then $(x_{i_0}, \ldots, x_{i_l})$ is random in the product space $\prod_{k=0}^{l}(X^{(i_k)}, B^{(i_k)}, \mu^{(i_k)})$.*
3. *Let $\prod_{k=0}^{\infty}(X^{(k)}, B^{(k)}, \mu^{(k)})$ be a product of ETMSs with probability measures. Let $r : \mathbb{N} \to \mathbb{N}$ be an injective computable function. If $(x_0, x_1, \ldots)$ is random in the above space, then $(x_{r(0)}, x_{r(1)}, \ldots)$ is random in the product space $\prod_{k=0}^{\infty}(X^{(r(k))}, B^{(r(k))}, \mu^{(r(k))})$.*

The proof will be given in Section 4.

We conclude this section with "concrete" examples of random elements of an ETMS. A sequence $(q_n)_n$ of rational numbers is called *computable* if, and only if, there is a computable function $f : \mathbb{N} \to \mathbb{N}$ with $q_n = v_{\mathbb{Q}}(f(n))$ for all n. A real number x is called *left-computable* (*right-computable*) if, and only if, there is a computable non-decreasing (non-increasing) sequence $(q_n)_n$ of rational numbers with $\lim_{n\to\infty} q_n = x$; see [22].

Example 3.14.
1. Chaitin's [4] Ω numbers are left-computable real numbers. Chaitin showed that they have a random binary expansion.

2. Let $(U_n)_n$ be a universal randomness test on the space of real numbers $(\mathbb{R}, B, \lambda)$ of Example 3.6(3). Then, for any k, the open set U_k contains all non-random real numbers. This set is also the disjoint union of a countable set of open intervals. The boundaries of these intervals lie outside of U_k, hence they are random real numbers. It is easy to see that the right-hand boundary of any of these intervals is a left-computable real number.
3. The construction of the last example can also be carried out on the space (Σ^ω, B, μ) of sequences (Example 3.6(2)). We consider $\Sigma = \{0, 1\}$. For $p, q \in \Sigma^\omega$ define $p < q :\iff p \neq q$ and $p_i < q_i$ where $i := \min\{j \mid p_j \neq q_j\}$, and $p \leqslant q :\iff p = q$ or $p < q$. In the same way as in Example 3.14(2) one can construct a computable sequence $(w_n)_n$ of finite strings such that $w_n 1^\omega \leqslant w_{n+1} 1^\omega$ for all n and such that $w_n 1^\omega$ converges towards a random binary sequence.

4. Randomness preserving transformations

The main result of this section is a theorem giving conditions under which a computable function between ETMSs preserves randomness. This corrects and extends a result by Schnorr [17].

For a finite alphabet Σ, call a function $g : \Sigma^* \to \Sigma^*$ *monotone* if, and only if, $g(vw) \in g(v)\Sigma^*$ for all $v, w \in \Sigma^*$, and call it *unbounded on* $p \in \Sigma^\omega$ if, and only if, for all $n \in \mathbb{N}$ there is some prefix v of p with $|g(v)| \geqslant n$. The function $g_\omega :\subseteq \Sigma^\omega \to \Sigma^\omega$ *induced* by a monotone function $g : \Sigma^* \to \Sigma^*$ is defined by

1. $p \in \mathrm{dom}(g_\omega)$ if, and only if, g is unbounded on p.
2. $g_\omega(p) \in g(v)\Sigma^\omega$ for any $p \in \mathrm{dom}(g_\omega)$ and for any prefix v of p.

It is clear that g_ω is well-defined by these conditions. A function $f :\subseteq \Sigma^\omega \to \Sigma^\omega$ is called *computable* if, and only if, $f = g_\omega$ for some computable, monotone function $g : \Sigma^* \to \Sigma^*$; see [22].

Schnorr [17, Satz 6.5] claimed: *if* $f :\subseteq \{0,1\}^\omega \to \{0,1\}^\omega$ *is a computable function satisfying* ($\exists$ *constant* K) ($\forall$ *measurable* $A \subseteq \{0,1\}^\omega$) $\mu(f^{-1}(A)) \leqslant K \cdot \mu(A)$, *and if* $x \in \mathrm{dom}(f)$ *is random, then also* $f(x)$ *is random.* This, as well as Lemma 6.6 and Satz 6.7 by Schnorr [17], are not correct, as was also observed by Wang; see [6]. We give a counter-example.

Example 4.1. Let $(w_n)_n$ be a computable sequence of strings $w_n \in \Sigma^*$ as in Example 3.14(3), i.e., such that the sequence $(w_n 1^\omega)_n$ is non-decreasing and converges towards a random sequence $r = \sup\{w_n 1^\omega \mid n \in \mathbb{N}\}$ in Σ^ω. Define a monotone, computable function $g : \Sigma^* \to \Sigma^*$ by $g(\varepsilon) := \varepsilon$ and

$$g(va) := \begin{cases} g(v)0 & \text{if the first } |g(v)| + 1 \text{ symbols of } va \text{ and of } w_{|va|}1^\omega \text{ are equal,} \\ g(v) & \text{otherwise} \end{cases}$$

for all $v \in \Sigma^*$ and $a \in \Sigma$. Then $\mathrm{dom}(g_\omega) = r$ and $g_\omega(r) = 0^\omega$. Therefore, g_ω maps a random sequence to a non-random one. Since $\mu(g_\omega^{-1}(A)) = 0 \leqslant \mu(A)$ for all measurable $A \subseteq \{0,1\}^\omega$, this is a counter-example to the claim above.

In fact, one needs an additional condition on the domain of definition of f. A sufficient condition will be formulated in Theorem 4.5. First, we introduce computability of functions between

ETMSs. A direct and natural definition can be obtained by demanding that the transformation is continuous in an effective way.

Definition 4.2. Let (X, B) and (Y, C) be two topological spaces with total numberings B and C of bases. Let B satisfy the intersection property. We call a function $f :\subseteq X \to Y$ *computable*, if, and only if, there is a B-computable sequence $(U_n)_n$ of open subsets of X with $f^{-1}(C_n) = U_n \cap \mathrm{dom}(f)$, for all n.

Note that we assume that the numbering B satisfies the intersection property. If one does not wish to assume this, then it seems to be more natural to demand that the sequence $(U_n)_n$ is $B^{\cap}$-computable where $B^{\cap}$ is associated with B as in Remark 3.3. If the spaces (X, B) and (Y, C) are T_0-spaces and *computable* in the sense that the sets $\{\langle i,j\rangle \mid B_i = B_j\}$ and $\{\langle i,j\rangle \mid C_i = C_j\}$ are r.e., then Definition 4.2 is equivalent to the definition of computable functions via standard representations as in Weihrauch [22]. For a proof, see [8]. One checks that this definition generalizes the notion of a computable function on Σ^{ω} if one does not care about the precise domain of definition. For real number functions this computability notion derived from the numbering B from Example 3.6(2) is also the usual computability notion considered for example by Grzegorczyk [5], Lacombe [11], Pour-El and Richards [15], Kreitz and Weihrauch [10], Weihrauch [19], Ko [9], and others; for more references see [19,22].

Besides computability we need two additional conditions for a function in order to ensure that it preserves randomness: one saying that we can in some effective, measure-theoretical sense control its domain, and one saying that it may not map large sets to too small sets. With the measure μ on an ETMS (X, B, μ) we associate as usual the outer measure μ^* defined by

$$\mu^*(A) = \inf\left\{ \sum_{i=0}^{\infty} \mu(U_i) \,\middle|\, A \subseteq \bigcup_{i=0}^{\infty} U_i, \text{and } U_i \text{ is an element of the } \sigma\text{-algebra generated by the topology, for all } i \right\}$$

for arbitrary subsets $A \subseteq X$.

Definition 4.3. Let (X, B, μ) be an ETMS. A set $D \subseteq X$ is called *fast enclosable* if, and only if, there is a B-computable sequence $(U_n)_n$ of open sets with $D \subseteq U_n$ and $\mu^*(U_n \setminus D) \leqslant 2^{-n}$ for all n.

Definition 4.4. Let (X, B, μ) and $(Y, C, \tilde{\mu})$ be two ETMSs. A function $f :\subseteq X \to Y$ is called *recursively measure-bounded* if, and only if, there is a total computable function $r : \mathbb{N} \to \mathbb{N}$ such that for all open sets $V \subseteq Y$:

$$\tilde{\mu}(V) \leqslant 2^{-r(n)} \quad \Rightarrow \quad \mu^*(f^{-1}(V)) \leqslant 2^{-n}.$$

Many functions $f :\subseteq X \to Y$ we shall use are even *measure invariant*, that is, $\mu^*(f^{-1}(V)) = \tilde{\mu}(V)$ for all open $V \subseteq Y$. After these preparations we can formulate our theorem on randomness preserving transformations.

Theorem 4.5. *Let (X, B, μ) and $(Y, C, \tilde{\mu})$ be ETMSs. Let B satisfy the intersection property. Let $f :\subseteq X \to Y$ be a computable, recursively measure-bounded function with a fast enclosable domain. If $x \in \mathrm{dom}(f)$ is a random element of X, then $f(x)$ is a random element of Y.*

Informally, a computable, recursively measure-bounded function with a fast enclosable domain preserves randomness.

Proof. It is sufficient to prove the following: if $(V_n)_n$ is a randomness test on $(Y, C, \tilde{\mu})$, then there is a randomness test $(U_n)_n$ on (X, B, μ) with

$$f^{-1}\left(\bigcap_{n\in\mathbb{N}} V_n\right) \subseteq \bigcap_{n\in\mathbb{N}} U_n. \tag{2}$$

Let $(V_n)_n$ be a randomness test on $(Y, C, \tilde{\mu})$, let $A_V \subseteq \mathbb{N}$ be an r.e. set which shows that $(V_n)_n$ is C-computable, i.e., $V_n = \bigcup_{\langle n,j\rangle\in A_V} C_j$, for all n. Let $(T_n)_n$ be a B-computable sequence of open subsets of X with $f^{-1}(C_n) = T_n \cap \mathrm{dom}(f)$. Then the sequence $(R_n)_n$ of subsets of X defined by $R_n := \bigcup_{\langle n,j\rangle\in A_V} T_j$ is B-computable and satisfies $f^{-1}(V_n) = R_n \cap \mathrm{dom}(f)$. Now let $r : \mathbb{N} \to \mathbb{N}$ be a total recursive function with $\mu^*(f^{-1}(\tilde{U})) \leqslant 2^{-n}$ for all open subsets $\tilde{U} \subseteq Y$ with $\tilde{\mu}(\tilde{U}) \leqslant 2^{-r(n)}$, and let $(S_n)_n$ be a B-computable sequence of open subsets of X which encloses $\mathrm{dom}(f)$ in the sense $\mathrm{dom}(f) \subseteq S_n$ and $\mu^*(S_n \setminus \mathrm{dom}(f)) \leqslant 2^{-n}$ for all n. We claim that the sequence $(U_n)_n$ with

$$U_n := S_{n+1} \cap R_{r(n+1)}$$

has the desired properties. It is a sequence of open sets. It is B-computable since both the sequence $(S_{n+1})_n$ and the sequence $(R_{r(n+1)})_n$ are B-computable and the intersection of two B-computable sequences is B-computable again. Note that here one uses the assumption that B satisfies the intersection property. The sequence $(U_n)_n$ satisfies

$$f^{-1}(V_{r(n+1)}) = U_n \cap \mathrm{dom}(f) \quad \text{for all } n \tag{3}$$

because of $f^{-1}(V_m) = R_m \cap \mathrm{dom}(f)$, for all m, and $\mathrm{dom}(f) \subseteq S_l$, for all l. From (3) we obtain for all n:

$$\begin{aligned}\mu(U_n) &\leqslant \mu^*(U_n \cap \mathrm{dom}(f)) + \mu^*(U_n \cap (X \setminus \mathrm{dom}(f)))\\ &\leqslant \mu^*(f^{-1}(V_{r(n+1)})) + \mu^*(S_{n+1} \setminus \mathrm{dom}(f))\\ &\leqslant 2^{-(n+1)} + 2^{-(n+1)} = 2^{-n}.\end{aligned}$$

Finally, (3) implies (2). This ends the proof. □

In our counter-example, Example 4.1, the set $\mathrm{dom}(f) = \{r\}$, r random, cannot be fast enclosable. We remark that for infinite sequences Levin [12] has obtained a randomness preservation result of a different kind. It can roughly be described by saying that certain operators A transform a μ-random sequence into an $A(\mu)$-random sequence where μ belongs to a certain class of measures and $A(\mu)$ is the measure induced by μ and A.

As a first application of Theorem 4.5, we prove Proposition 3.13.

Proof of Proposition 3.13. For the proof of Proposition 3.13(1) consider the canonical projection function f from the product space $\prod_{i=0}^{n}(X^{(i)}, B^{(i)}, \mu^{(i)})$ onto $\prod_{k=0}^{l}(X^{(i_k)}, B^{(i_k)}, \mu^{(i_k)})$. It is computable, total, and satisfies

$$\left(\prod_{i=0}^{k} \mu^{(i)}\right)(f^{-1}(U)) = \left(\prod_{k=0}^{l} \mu^{(i_k)}\right)(U) \cdot \prod_{i \in \{0,\ldots,n\} \setminus \{i_0,\ldots,i_l\}} \mu^{(i)}(X^{(i)})$$

for all open $U \subseteq \prod_{k=0}^{l} X^{(i_k)}$ (remember that the measures $\mu^{(i)}$ are assumed to be finite). Hence, it is recursively measure-bounded. The assertion follows from Theorem 4.5. The assertions 2 and 3 of Proposition 3.13 are proved in the same way. The canonical projection functions which one has to consider here are even measure-preserving. □

In the rest of this section we assume that Σ is an arbitrary finite alphabet with at least two elements. We consider again the randomness space from Example 3.6(2).

Two sequences p and q are sometimes called *independently random* if the sequence

$$\langle p, q \rangle := p_0 q_0 p_1 q_1 p_2 q_2 \cdots$$

is random. Using the notion of the product ETMS $((\Sigma^\omega)^2, B^2, \mu^2)$ as sketched in the end of Section 3, one might also consider sequences p and q such that the pair (p, q) is a random element of this product ETMS. Using the invariance result, Theorem 4.5, it is easy to show that these conditions are equivalent. The reason is that the mapping $(p,q) \mapsto \langle p, q \rangle$ is a computable, measure invariant homeomorphism. Similar statements are true for arbitrary finite vectors of sequences and even for an infinite countable sequence of sequences where for $p^{(0)}, p^{(1)}, p^{(2)}, \ldots \in \Sigma^\omega$ we define

$$\langle p^{(1)}, p^{(2)}, \ldots, p^{(k)} \rangle := p^{(1)}(0) p^{(2)}(0) \cdots p^{(k)}(0) p^{(1)}(1) p^{(2)}(1) \cdots p^{(k)}(1) \cdots,$$

$$\langle p^{(0)}, p^{(1)}, \ldots \rangle(\langle i, j \rangle) := p^{(i)}(j) \quad \text{for all } i, j.$$

5. Random real numbers

Randomness of real numbers is usually introduced via the b-ary representations. Calude and Jürgensen [2] (see also [1] and [13, p. 219]) proved that this leads to a notion independent from the base b. In this section we show that this notion coincides with the direct definition of randomness on real numbers given in Example 3.6(3). This is done also for vectors and infinite sequences of real numbers. Then we show that many computable continuously differentiable real functions preserve randomness. Especially, all non-constant computable analytic functions preserve randomness. Hence, all the common arithmetic functions preserve randomness. We conclude the section with several simple observations on the arithmetic of random real numbers.

Fix a natural number $b \geqslant 2$. The *b-ary representation* of the real numbers in the unit interval is based on the alphabet $\Sigma_b := \{0, 1, \ldots, b-1\}$ and defined to be the mapping

$$\rho_b : \Sigma_b^\omega \to [0, 1] \quad \text{with } \rho_b(p_0 p_1 p_2 \cdots) := \sum_{n=0}^{\infty} p_i b^{-(i+1)}$$

for $p \in \Sigma_b^\omega$. A sequence $p \in \Sigma_b^\omega$ with $\rho_b(p) = x$ is also called *expansion of x to base b*. It is unique for all real numbers in $[0,1]$ except for those rational numbers corresponding to sequences ending on 0's or on an infinite repetition of the digit $b-1$. This definition can directly be extended to a representation ρ_b^k of vectors in $[0,1]^k$ by

$$\rho_b^k : \Sigma_b^\omega \to [0,1]^k, \qquad \rho_b\langle p^{(1)},\dots,p^{(k)}\rangle := (\rho_b(p^{(1)}),\dots,\rho_b(p^{(k)})),$$

which we call the b-ary representation of vectors in $[0,1]^k$. In the following theorem, due to Weihrauch [20], we consider the ETMSs $(\mathbb{R}, B, \lambda)$ and $([0,1], \tilde{B}, \tilde{\lambda})$ introduced in Example 3.6 and their products according to the end of Section 3. For a vector $(x_1,\dots,x_n)$ of real numbers the *fractional part* of $(x_1,\dots,x_n)$ is the unique real vector $(y_1,\dots,y_n) \in [0,1)^n$ such that the difference $(x_1 - y_1,\dots,x_n - y_n)$ is a vector of integers.

Theorem 5.1. *Let $n \geqslant 1$, $b \geqslant 2$. For a vector $(x_1,\dots,x_n) \in \mathbb{R}^n$ the following conditions are equivalent.*
1. *It is a random element of the space $(\mathbb{R}^n, B^n, \lambda^n)$.*
2. *Its fractional part is a random element of the space $(\mathbb{R}^n, B^n, \lambda^n)$.*
3. *Its fractional part is a random element of the space $([0,1]^n, \tilde{B}^n, \tilde{\lambda}^n)$.*
4. *Its fractional part has a random ρ_b^n-name.*

Proof. We prove "(1) $\iff$ (2)", "(2) $\iff$ (3)", and "(3) $\iff$ (4)".

Let $(z_1,\dots,z_n) \in \mathbb{Z}^n$ be an integer vector. The translation $T : (\mathbb{R}^n, B^n) \to (\mathbb{R}^n, B^n)$ with $T(y_1,\dots,y_n) := (y_1 + z_1,\dots,y_n + z_n)$ is a total, computable, measure invariant mapping. Hence, by Theorem 4.5, if $(y_1,\dots,y_n) \in \mathbb{R}^n$ is random (in $(\mathbb{R}^n, B^n, \lambda^n)$), also $(y_1 + z_1,\dots,y_n + z_n)$ is random. The equivalence "(1) $\iff$ (2)" follows.

The mapping $f :\subseteq (\mathbb{R}^n, B^n) \to ([0,1]^n, \tilde{B}^n)$ with $\mathrm{dom}(f) = [0,1]^n$ and $f(x) = x$ for all $x \in \mathrm{dom}(f)$ is computable, measure invariant, and its domain is a fast enclosable subset of $(\mathbb{R}^n, B^n, \lambda^n)$. This, together with Theorem 4.5 proves "(2) $\Rightarrow$ (3)". The inverse mapping $f^{-1} : ([0,1]^n, \tilde{B}^n) \to (\mathbb{R}^n, B^n)$ is computable, total and measure bounded since $\tilde{\lambda}^n((f^{-1})^{-1}(A)) \leqslant \lambda^n(A)$ for all measurable $A \subseteq \mathbb{R}^n$. Using Theorem 4.5 we conclude "(3) $\Rightarrow$ (2)".

The mapping ρ_b^n itself is computable, total, and measure invariant. Hence, Theorem 4.5 yields "(4) $\Rightarrow$ (3)". On the other hand, let now $f :\subseteq [0,1]^n \to \Sigma_b^\omega$ be the mapping which maps each n-vector of irrationals in the unit interval to its (unique!) ρ_b^n-name, i.e., $\rho_b^n(f(x)) = x$ for all $x \in \mathrm{dom}(f) := [0,1]^n \cap (\mathbb{R} \setminus \mathbb{Q})^n$. This mapping is also computable. Since its domain has measure 1 it is fast enclosable. And the function f preserves the measure: $\tilde{\lambda}^n(f^{-1}(A)) = \mu^n(A)$ for all measurable $A \subseteq \Sigma^\omega$. By Theorem 4.5 f preserves randomness. If $x \in [0,1]^n$ is random, then it is a vector of random numbers by Proposition 3.13, hence a vector of irrational numbers, hence in the domain of f, and $f(x)$ is random in Σ_b^ω. This proves "(3) $\Rightarrow$ (4)". □

From the equivalence of 3 and 4 in Theorem 5.1 we obtain:

Corollary 5.2 [2]. *Let $b, c \geqslant 2$ be integers. A real number $x \in [0,1]$ has a random ρ_b-name if, and only if, it has a random ρ_c-name.*

We generalize the equivalence of 3 and 4 in Theorem 5.1 to infinite sequences of real numbers in the unit interval. We define the b-ary representation $\rho_b^\omega : \Sigma^\omega \to [0,1]^\omega$ of such sequences by $\rho_b^\omega\langle p^{(0)}, p^{(1)}, p^{(2)}, \ldots\rangle := (\rho_b(p^{(0)}), \rho_b(p^{(1)}), \rho_b(p^{(2)}), \ldots)$ for $p^{(0)}, p^{(1)}, p^{(2)}, \ldots \in \Sigma^\omega$.

Theorem 5.3. *Let $b \geqslant 2$. A sequence $(x_n)_n$ of real numbers in $[0,1]^\omega$ is a random element of $([0,1]^\omega, \tilde{B}^\omega, \lambda^\omega)$ if, and only if, it has a random ρ_b^ω-name.*

The proof is identical with the proof of the last equivalence in Theorem 5.1.

We turn our attention to arithmetic properties of random numbers and vectors. We remarked already that a computable real number cannot be random. It is well known that a computable real function preserves computability, that is, it maps computable real numbers to computable real numbers. Which real number functions preserve randomness? We give a sufficient condition which seems to cover the most common functions.

Theorem 5.4. *Let $n \geqslant 1$ and $f :\subseteq \mathbb{R}^n \to \mathbb{R}$ be a computable, continuously differentiable function with an open domain such that all zeros of its derivative f' are non-random elements of $\mathbb{R}^n$. If $z \in \mathrm{dom}(f)$ is random, then also $f(z)$ is random.*

Proof. Let $z \in \mathrm{dom}(f)$ be random. Then $f'(z) \neq 0$ by assumption. There is a $k \in \{1, \ldots, n\}$ such that the partial derivative $(\partial f/\partial x_k)(z)$ is non-zero. By symmetry we can assume without loss of generality $k = n$. Since the derivative f' is continuous and the domain of f is open there is a closed rectangle $D = [l_1, r_1] \times \cdots \times [l_n, r_n]$ with the following properties: (1) $z \in D$, (2) $D \subseteq \mathrm{dom}(f)$, (3) D has rational endpoints, (4) the side length of D in any coordinate is at most 1, (5) for all $y \in D$ we have

$$\left|\frac{\partial f}{\partial x_n}(y)\right| \geqslant L := \frac{1}{2}\left|\frac{\partial f}{\partial x_n}(z)\right|.$$

We claim that the restricted function $g := f|_D$ satisfies all assumptions of Theorem 4.5. This, of course, implies that $f(z)$ is random.

It is clear that g is computable and that its domain D is fast enclosable. The only point which has to be proved is that g is recursively measure-bounded. This is a consequence of the fact that the absolute value of the derivative $\partial f/\partial x_n$ is bounded from below by a positive constant L on D. We claim that g satisfies

$$\lambda^n(g^{-1}(U)) \leqslant \frac{\lambda(U)}{L} \tag{4}$$

for any open subset $U \subseteq \mathbb{R}$. Since any open set $U \subseteq \mathbb{R}$ can be written as a disjoint countable union of open intervals (the connected components of U) it is sufficient to prove (4) for non-empty open intervals $U = (c, d)$. Fix a vector

$$(x_1, \ldots, x_{n-1}) \in D' := [l_1, r_1] \times \cdots \times [l_{n-1}, r_{n-1}]$$

and consider the function $h :\subseteq \mathbb{R} \to \mathbb{R}$ with $\mathrm{dom}(h) := [l_n, r_n]$ and $h(x) := g(x_1, \ldots, x_{n-1}, x)$ for $x \in [l_n, r_n]$. Fix real numbers $c < d$. We claim that

$$\lambda(h^{-1}((c,d))) \leqslant \frac{d-c}{L}. \tag{5}$$

Since the partial derivative $(\partial f/\partial x_n)(x)$ is a continuous function and its absolute value is bounded from below by the positive constant L on D, the function h is either strictly increasing or strictly decreasing. Thus, the preimage $h^{-1}([c,d])$ of the closed interval $[c,d]$ is either empty or a single point or a non-degenerate interval. If it is empty or a single point, then claim (5) is clearly true. Assume that it is a non-degenerate interval $[a,b]$. Then $l_n \leqslant a < b \leqslant r_n$ and $|h(b) - h(a)| \leqslant d - c$. By the Intermediate Value Theorem there is a real number ξ lying in (a,b) with

$$h(b) - h(a) = h'(\xi) \cdot (b - a).$$

Since $(x_1, \dots, x_{n-1}, \xi) \in D$, our fifth assumption on D says $|h'(\xi)| \geqslant L$. We obtain

$$\lambda(h^{-1}((c,d))) \leqslant \lambda(h^{-1}([c,d])) = b - a = \frac{h(b) - h(a)}{h'(\xi)} \leqslant \frac{|h(b) - h(a)|}{L} \leqslant \frac{d - c}{L}.$$

This proves our claim (5). The inequality (5) is used in the following application of Fubini's Theorem:

$$\begin{aligned}
\lambda^n(g^{-1}((c,d))) &= \int_D \chi_{g^{-1}((c,d))}(x_1, \dots, x_n)\, \mathrm{d}\lambda^n(x_1, \dots, x_n) \\
&= \int_{D'} \left(\int_{\mathbb{R}} \chi_{g^{-1}((c,d))}(x_1, \dots, x_n)\, \mathrm{d}\lambda(x_n) \right) \mathrm{d}\lambda^{n-1}(x_1, \dots, x_{n-1}) \\
&\leqslant \int_{D'} \frac{d - c}{L} \mathrm{d}\lambda^{n-1}(x_1, \dots, x_{n-1}) \\
&\leqslant \frac{d - c}{L}.
\end{aligned}$$

In the last step we used the assumption that the side length of D and hence also of D' in each coordinate is at most one. This proves our claim (4) and ends the proof of Theorem 5.4. □

Let $n \geqslant 1$ and $U \subseteq \mathbb{R}^n$ be an open set. A function $f : U \to \mathbb{R}$ is *analytic* if for any point $z \in U$ there is a neighbourhood $V \subseteq U$ of z such that in this neighbourhood $f(x)$ can be written as an absolutely convergent power series $\sum_{k \in \mathbb{N}^n} a_k (x - z)^k$ where $y^k = y_1^{k_1} \cdots y_n^{k_n}$ for $y = (y_1, \dots, y_n) \in \mathbb{R}^n$ and $k = (k_1, \dots, k_n) \in \mathbb{N}^n$.

Theorem 5.5. *Let $U \subseteq \mathbb{R}^n$ be open and $f : U \to \mathbb{R}$ be an analytic function which is not constant on any connected component of U and which is computable on any compact subset of U. If $z \in \mathrm{dom}(f)$ is random, then also $f(z)$ is random.*

Proof. If f is an analytic function which is computable on any compact subset of its domain U, then its partial derivatives $\partial f/\partial x_k$ (for $k \in \{1, \dots, n\}$) are also analytic functions and computable on any compact subset of U; see, e.g. [22, Corollary 6.4.8]. Fix a rational compact rectangle K in the domain of f and a slightly larger rational open rectangle V with $K \subseteq V$ and $\overline{V} \subseteq U$. Since we assume that the function f is not constant on any connected component of U, it is also not constant on V. Hence, at least one of the partial derivatives of f, say $\partial f/\partial x_k$, is not identical with the constant zero function on V. Therefore, the set of zeros of $\partial f/\partial x_k$ in V has measure zero. Hence, the measure of $\{x \in V \mid |\partial f/\partial x_k| \leqslant 2^{-m}\}$ tends to zero for m tending to infinity. For each

$m \in \mathbb{N}$ (uniformly in m) we can compute a finite union of rational polycylinders B_i^n in $\mathbb{R}^n$ which cover the set of zeros of $\partial f/\partial x_k$ in K and are contained in $\{x \in V \mid |\partial f/\partial x_k| \leqslant 2^{-m}\}$. Thus, we can construct a randomness test which contains all zeros of $\partial f/\partial x_k$ in K. Thus, all zeros of $\partial f/\partial x_k$ in K, and therefore all zeros of f' in U are non-random. The assertion follows now from Theorem 5.4. □

We conclude that all the common arithmetic functions like addition, subtraction, multiplication, division, taking square roots or higher roots, exp, log, sin, cos, and so on preserve randomness. If for example (x, y) is a random pair of real numbers, then the sum $x + y$ is random as well. But it is important to note that it is insufficient to assume just that both components x and y are random. For example, if x is random, then also $-x$ is random (by Theorem 5.4), but the sum $x + (-x) = 0$ is not random. Hence, addition does not transform random numbers into random numbers. Is the set of non-random numbers closed under addition? No, for we can take a random binary sequence $p(0)p(1)p(2)\ldots \in \{0,1\}^\omega$. The numbers $x := \rho_2(p(0)0p(2)0p(4)0\cdots)$ and $y := \rho_2(0p(1)0p(3)0p(5)\cdots)$ are non-random, but their sum $x + y = \rho_2(p(0)p(1)p(2)\cdots)$ is random.

We conclude this section with several simple observations on random vectors and random sequences of real numbers.

Theorem 5.6. *For $n \geqslant 2$, the set of non-random points in $\mathbb{R}^n$ is connected.*

Proof. Fix a non-random point x in $\mathbb{R}^n$. We choose a sequence of rational points $(q_m)_m$ (that means: all components of q_m are rational) in $\mathbb{R}^n$ converging to x, starting with $q_0 = 0$. By connecting each point q_m via a straight line with q_{m+1} we obtain a path leading from 0 to x. This path contains only non-random points since a straight line segment in $\mathbb{R}^n$ with rational endpoints contains only non-random points. Thus, the set of non-random points in $\mathbb{R}^n$ is connected. □

A sequence $(x_n)_n \in [0,1]^\omega$ of real numbers is called *uniformly distributed* if, and only if, for any pair a, b of real numbers with $0 \leqslant a < b \leqslant 1$ the limit $\lim_{n\to\infty} \frac{1}{n}|\{i < n \mid x_i \in [a,b)\}|$ exists and is equal to $b - a$.

Theorem 5.7. *Every random sequence of real numbers in $[0,1]^\omega$ is uniformly distributed.*

Proof. This follows immediately from Theorem 5.3 and from Calude et al. [3, Theorem 3.6], which states that any sequence of real numbers in $[0,1]^\omega$ with a random ρ_b^ω-name, $b \geqslant 2$ arbitrary, is uniformly distributed. □

In Proposition 3.13 we observed that a sequence of real numbers in $[0,1]$ is already non-random, if one of its components is non-random or a vector formed out of distinct components is non-random. Is there a non-random sequence of real numbers such that all of its components are random? This is true.

Theorem 5.8. *There is a non-random sequence $(x_n)_n$ of real numbers in $[0,1]^\omega$ such that for any $n \in \mathbb{N}$ and any tuple $(i_0,\ldots,i_n)$ of pairwise different indices (i.e., $i_k \neq i_l$ for $0 \leqslant k < l \leqslant n$) the vector $(x_{i_0},\ldots,x_{i_n})$ is random.*

Proof. Let $(y_n)_n$ be an arbitrary random sequence of real numbers in $[0,1]^\omega$. Then by Proposition 3.13 each vector $(y_{j_0},\ldots,y_{j_n})$ for some tuple $(j_0,\ldots,j_n)$ of pairwise different indices is random. Define a sequence $(x_n)_n$ of real numbers in $[0,1]^\omega$ by $x_0 := y_0$ and $x_{n+1} :=$ the first number in the sequence $(y_n)_n$ which is smaller than $x_n/2$. This sequence is well-defined since the sequence $(y_n)_n$ is uniformly distributed. It is non-random since it converges fast to zero (take for example the randomness test $(U_n)_n$ on $[0,1]^\omega$ defined by $U_n := \{(z_m)_m \in [0,1]^\omega \,|\, z_n < 2^{-n}\}$). Each vector of the form $(x_{i_0},\ldots,x_{i_n})$ for any $n \in \mathbb{N}$ and any tuple $(i_0,\ldots,i_n)$ of pairwise different indices is random since it is identical with a vector of the form $(y_{j_0},\ldots,y_{j_n})$ for some tuple $(j_0,\ldots,j_n)$ of pairwise different indices. □

6. Random sets

Usually a set $A \subseteq \mathbb{N}$ of natural numbers is called random if, and only if, its characteristic function is a random sequence. In this section we consider a different notion of a random set which is induced by viewing the power set $2^\mathbb{N}$ of $\mathbb{N}$ as an ETMS, based on the topology which is usually considered when viewing $2^\mathbb{N}$ as a complete partial order; compare Weihrauch [19, Definition 3.1.1, Examples 3.5.2(4)]. The first main result gives a characterization of the resulting randomness notion in terms of randomness for sequences. The second main result is the construction of an infinite co-r.e. random set. Also several simple properties of random sets are observed. In this section we always use Σ for the binary alphabet: $\Sigma = \{0,1\}$. Sets of natural numbers are denoted by literals $A, B, C, \ldots$ while subsets of the power set $2^\mathbb{N} = \{A \,|\, A \subseteq \mathbb{N}\}$ of $\mathbb{N}$ and subsets of Σ^ω are denoted by U, V, W, X, Y, Z.

Which sets of natural numbers should be called random? Before we discuss this question, let us have a look at the possible answers to the same question for computability instead of randomness. The perhaps two most important notions of computability for sets are decidability and recursive enumerability. Both notions can be obtained in a natural way as the computability notions for elements of natural spaces.

If X is a topological space and B a total numbering of a base of X, then we call an element $x \in X$ *computable* if, and only if, the set $\{i \in \mathbb{N} \,|\, x \in B_i\}$ is r.e., that is, if one can effectively enumerate all properties of x that are described by B; compare Weihrauch [22]. The computable elements of the space (Σ^ω, B), obtained from Example 3.6(2) by forgetting the measure μ, are exactly the computable binary sequences. Of course, they correspond to the decidable sets, via the bijection $\chi : 2^\mathbb{N} \to \Sigma^\omega$ which maps a set $A \subseteq \mathbb{N}$ to its characteristic function χ_A (with $\chi_A(n) = 1$ if $n \in A$, $\chi_A(n) = 0$ if $n \notin A$). In the following, we denote the topology on $2^\mathbb{N}$ generated by the base $\chi^{-1}(B_i)$, for $i \in \mathbb{N}$, by τ_χ.

For recursive enumerability the same is possible. We only have to consider a different topology on $2^\mathbb{N}$, and a numbering of a suitable base. In fact, the suitable topology $2^\mathbb{N}$ for this purpose is the topology which one usually considers when viewing $2^\mathbb{N}$ as a complete partial order. It is the topology generated by the base $\{O_E \,|\, E \subseteq \mathbb{N} \text{ finite}\}$ where $O_E := \{A \subseteq \mathbb{N} \,|\, E \subseteq A\}$ for finite subsets E of $\mathbb{N}$. We call this topology τ. The following lemma shows how the topologies τ_χ and τ are related.

Lemma 6.1.

1. *The topology τ is a proper subset of the topology τ_χ.*
2. *The σ-algebra generated by τ is identical with the σ-algebra generated by τ_χ.*

Proof. 1. For any finite set $E \subseteq \mathbb{N}$ we define a finite set W_E of strings by

$$W_E := \{w = w(1) \cdots w(1 + \max E) \in \Sigma^{1+\max E} \mid (\forall i \in E)\ w(1+i) = 1\}.$$

One observes $O_E = \bigcup\{\chi^{-1}(w\Sigma^\omega) \mid w \in W_E\}$. This shows $\tau \subseteq \tau_\chi$. The set $\chi^{-1}(0\Sigma^\omega)$ is an element of $\tau_\chi \setminus \tau$.

2. For any set $F \subseteq \mathbb{N}$ the set $C_F := \{A \subseteq \mathbb{N} \mid A \cap F = \emptyset\}$ is a τ-closed set (that means: $2^{\mathbb{N}} \setminus C_F$ is an element of τ) since $C_{\{n\}} = 2^{\mathbb{N}} \setminus O_{\{n\}}$ for all n and $C_F = \bigcap_{n\in F} C_{\{n\}} = 2^{\mathbb{N}} \setminus \bigcup_{n\in F} O_{\{n\}}$. If, for a string $w = w(1) \cdots w(|w|) \in \Sigma^*$, we set $E := \{i < |w| \mid w(i+1) = 1\}$ and $F := \{i < |w| \mid w(i+1) = 0\}$, then $\chi^{-1}(w\Sigma^\omega) = O_E \cap C_F$. Hence, every basic τ_χ-open set is the intersection of a τ-open and a τ-closed set. The assertion follows. □

In the following, whenever we speak about an open or closed subset of $2^{\mathbb{N}}$, we mean this with respect to the topology τ.

We still need a numbering of a base of τ. Therefore, we use the standard numbering O of basic τ-open sets defined by $O_i := O_{D_i}$. One checks easily that the computable elements of the space $(2^{\mathbb{N}}, O)$ are exactly the r.e. sets.

Thus, both computability notions for sets of natural numbers have arisen naturally as computability notions for elements of natural effective topological spaces. How about randomness? We have defined randomness in general on ETMS. In order to make ETMSs out of the two spaces we only need to introduce a measure. Indeed, on the first space we had already introduced a measure in Example 3.6(2). The resulting randomness notion was the usual Martin-Löf randomness notion for infinite binary sequences. On the second space, we can also introduce a natural measure by transferring the first measure via the bijection χ^{-1}, due to the fact that the σ-algebras of the two topologies τ and τ_χ are the same. We define a measure μ by

$$\mu(X) := \mu(\chi(X))$$

for every set $X \subseteq 2^{\mathbb{N}}$ in the σ-algebra generated by τ (where the μ on the right-hand side of the equation denotes the usual product measure on Σ^ω, considered in Example 3.6(2)). Notice that $\mu(O_E) = 2^{-|E|}$ for any finite set $E \subseteq \mathbb{N}$.

Thus, we have two ETMSs: (Σ^ω, B, μ) and $(2^{\mathbb{N}}, O, \mu)$. While the computable elements of the first ETMS (Σ^ω, B, μ) are the computable binary sequences, which correspond to decidable sets, and its random elements are the usual Martin-Löf random sequences, the computable elements of the second ETMS $(2^{\mathbb{N}}, O, \mu)$ are the r.e. sets. Its random elements are the objects of interest in this section.

Definition 6.2. A set $A \subseteq \mathbb{N}$ is called *random* if, and only if, it is a random element of the ETMS $(2^{\mathbb{N}}, O, \mu)$.

Which properties does this ETMS have? What are its random elements?

It is clear that the numbering O satisfies the intersection property. Hence, whenever one has a randomness test $(U_n)_n$, one can assume that the sequence $(U_n)_n$ is a non-increasing sequence of sets, compare Proposition 3.8. The measure μ is upper semi-computable. Therefore, by Theorem 3.10, the space has a universal randomness test.

Before we characterize randomness of sets in terms of randomness of sequences we make two simple observations.

Proposition 6.3.
1. *Every finite set $E \subseteq \mathbb{N}$ is random.*
2. *Every subset of a random set $A \subseteq \mathbb{N}$ is random as well.*

Proof. 1. Every open set $U \subseteq 2^{\mathbb{N}}$ which contains a finite set $E \subseteq \mathbb{N}$ as an element contains the open set O_E as a subset. Hence $\mu(U) \geqslant \mu(O_E) = 2^{-|E|}$. Thus, there can be no randomness test $(U_n)_n$ on $2^{\mathbb{N}}$ with $E \in \bigcap_{n\in\mathbb{N}} U_n$.

2. We prove the contraposition:

$$\text{if } A \subseteq \mathbb{N} \text{ is non-random and } A \subseteq B, \text{ then also } B \text{ is non-random.}$$

Any open set U that contains A as an element also contains B as an element. Hence, if $A \in \bigcap_n U_n$ for some randomness test $(U_n)_n$, then also $B \in \bigcap_n U_n$, for any $B \supseteq A$. □

Especially the first assertion might seem counter-intuitive at first. But since the finite sets, considered as finite elements in the complete partial order $2^{\mathbb{N}}$, are in some sense very "rough" objects not having any property which is valid only for objects in an open set of very small measure, it makes sense to call them random. In contrast to the ETMS Σ^{ω} where one considers positive and negative information about a set, here we consider only positive information about sets, i.e., information telling us which numbers are in the set. This also gives an intuitive explanation for the second assertion.

The following characterization is the first main result of the section.

Theorem 6.4. *A set $A \subseteq \mathbb{N}$ is random if, and only if, there is a set $B \supseteq A$ such that χ_B is random.*

Another way to express this is:

$$A \subseteq \mathbb{N} \text{ is non-random} \iff (\forall B \supseteq A)\ \chi_B \text{ is non-random.}$$

For the proof of Theorem 6.4 we need a topological lemma.

Lemma 6.5. *If a set $A \subseteq \mathbb{N}$ and all sets $B \supseteq A$ are elements of a τ_χ-open subset $V \subseteq 2^{\mathbb{N}}$, then they are already elements of the τ-interior of V.*

Proof. Let $V \subseteq 2^{\mathbb{N}}$ be a τ_χ-open set and $A \subseteq \mathbb{N}$ be a set such that all sets $B \supseteq A$ are elements of V. It is sufficient to show that there is a finite set $E \subseteq A$ with $O_E \subseteq V$. Set $E_n := A \cap \{0, \dots, n\}$ for each n. Then $\bigcap_n O_{E_n} = \{B \,|\, B \supseteq A\} \subseteq V$, hence, $\bigcap_n \chi(O_{E_n}) \subseteq \chi(V)$. Since for any finite $E \subseteq \mathbb{N}$ the set $\chi(O_E)$ is closed, the sets $\Sigma^{\omega} \setminus \chi(O_{E_n})$ form a non-decreasing sequence of open sets whose union contains $\Sigma^{\omega} \setminus \chi(V)$. Since $\Sigma^{\omega} \setminus \chi(V)$ is compact there exists some n with $\Sigma^{\omega} \setminus \chi(O_{E_n}) \supseteq \Sigma^{\omega} \setminus \chi(V)$, hence with $O_{E_n} \subseteq V$. □

Proof of Theorem 6.4. First we prove that "A non-random" implies "χ_B non-random for all $B \supseteq A$". By Proposition 6.3(2) it is sufficient to prove

$$A \text{ non-random} \Rightarrow \chi_A \text{ non-random}$$

for any $A \subseteq \mathbb{N}$. Fix a non-random set $A \subseteq \mathbb{N}$ and a randomness test $(U_n)_n$ on $2^{\mathbb{N}}$ with $A \in \bigcap_n U_n$. We claim that the sequence $(V_n)_n$ of subsets of Σ^{ω} defined by

$$V_n := \chi(U_n)$$

is a randomness test on Σ^ω with $\chi_A \in \bigcap_n V_n$. The last part of the claim is clear. The sets V_n are open since $\tau \subseteq \tau_\chi$. We have $\mu(V_n) = \mu(U_n) \leqslant 2^{-n}$ by the definition of the measure μ on $2^{\mathbb{N}}$. It is left to prove that there is an r.e. set $C \subseteq \mathbb{N}$ with $V_n = \bigcup\{\nu(i)\Sigma^\omega \mid \langle n,i\rangle \in C\}$ where $\nu : \mathbb{N} \to \Sigma^*$ denotes the standard numbering of Σ^*. This follows since there is an r.e. set $\tilde{C}$ with $U_n = \bigcup\{O_{D_i} \mid \langle n,i\rangle \in \tilde{C}\}$, hence, $V_n = \bigcup\{W_{D_i}\Sigma^\omega \mid \langle n,i\rangle \in \tilde{C}\}$ where the sets W_{D_i} are the sets considered in the proof of Lemma 6.1. Furthermore, given an index i, one can compute ν-indices for the finitely many strings in W_{D_i}. This ends the proof of the first implication.

Now we prove that "χ_B non-random for all $B \supseteq A$" implies "A non-random". Fix a universal randomness test $(V_n)_n$ on Σ^ω. For each n we define U_n to be the τ-interior of $\chi^{-1}(V_n)$:

$$U_n := \bigcup\{O_E \mid E \text{ finite and } \chi(O_E) \subseteq V_n\}.$$

We claim that the sequence $(U_n)_n$ is a randomness test on $2^{\mathbb{N}}$. The sets U_n satisfy $\mu(U_n) = \mu(\chi(U_n)) \leqslant \mu(V_n) \leqslant 2^{-n}$ because χ preserves the measure and $\chi(U_n) \subseteq V_n$. Let $G \subseteq \mathbb{N}$ be an r.e. set with $V_n = \bigcup_{\langle n,j\rangle \in G} \nu(j)\Sigma^\omega$, for all n. We define an r.e. set $H \subseteq \mathbb{N}$ by

$$H := \left\{ \langle n,i\rangle \mid (\exists j_1,\ldots,j_l \in \mathbb{N})\ \langle n,j_k\rangle \in G \text{ for } k = 1,\ldots,l, \text{ and } W_{D_i}\Sigma^\omega \subseteq \bigcup_{k=1}^{l} \nu(j_k)\Sigma^\omega \right\}.$$

Since every set $\chi(O_i) = W_{D_i}\Sigma^\omega$ is compact, we obtain $\langle n,i\rangle \in H \iff \chi(O_i) \subseteq V_n$, for any n and i. This shows $U_n = \bigcup_{\langle n,i\rangle \in H} O_i$, for all n. We have proved that $(U_n)_n$ is a randomness test on $2^{\mathbb{N}}$. Now let $A \subseteq \mathbb{N}$ be a set such that χ_B is non-random for all $B \supseteq A$. This implies $\chi_B \in V_n$ for all $B \supseteq A$ and all n since $(V_n)_n$ is assumed to be a universal randomness test. By Lemma 6.5 we conclude that $A \in U_n$ for all n, hence $A \in \bigcap_n U_n$. This means that A is non-random and proves our assertion. □

Remark 6.6. In the second part of the proof of Theorem 6.4 we started with a randomness test $(V_n)_n$ on Σ^ω and proved that the sequence $(U_n)_n$ consisting of the τ-interiors U_n of the sets $\chi^{-1}(V_n)$ is a randomness test. Actually, if $(V_n)_n$ is a universal randomness test on Σ^ω, then $(U_n)_n$ is a universal randomness test on $2^{\mathbb{N}}$. To see this, use the following observation made in the first part of the proof: if $(\tilde{U}_n)_n$ is a randomness test on $2^{\mathbb{N}}$ then $(\chi(\tilde{U}_n))_n$ is a randomness test on Σ^ω.

Note especially that randomness of $p \in \Sigma^\omega$ implies randomness of $\chi^{-1}(p)$. The converse is not true: take a random sequence $p = p(0)p(1)p(2)p(3)\cdots \in \Sigma^\omega$. Then the sequence $q = p(0)0p(2)0\cdots$ is not random, but the set $\chi^{-1}(q) \subseteq \chi^{-1}(p)$ is random by Proposition 6.3(2) or Theorem 6.4.

Every finite set is random. How simple can infinite random sets be in terms of the arithmetical hierarchy [16,18,19]? We know that there are random sequences $p \in \Sigma^\omega$ such that $\chi^{-1}(p)$ is in Δ_2 (for example the sequences constructed in Example 3.14(3)). Thus, there are infinite random sets in Δ_2. But the set $\chi^{-1}(p)$ associated with a random sequence p can of course not be in Σ_1 or Π_1. Are there infinite random sets even in Σ_1 or Π_1? A set is called *immune* if, and only if, it is infinite and contains no infinite r.e. subset.

Theorem 6.7.

1. *Every random set is either finite or immune.*
2. *There is an infinite random co-r.e. set.*

Hence, there are no infinite random sets in Σ_1, but there are infinite random sets in Π_1. The proof of the first part of the theorem is straightforward. The second part is based on the following theorem, which will be proved at the end of the section.

Theorem 6.8. *Let $A \subseteq \mathbb{N}$ be r.e. and $U := \bigcup\{O_{D_i} \mid i \in A\}$ have measure $\mu(U) < 1$. Then there exists an infinite co-r.e. set $B \notin U$.*

Proof of Theorem 6.7. 1. Assume that a set $A \subseteq \mathbb{N}$ contains an infinite r.e. set B. Fix an injective total recursive function f with range$(f) = B$. Set $E_n := \{f(0), \dots, f(n-1)\}$ for all n. The sequence $(O_{E_n})_n$ is a randomness test on $2^{\mathbb{N}}$ with $A \in \bigcap_n O_{E_n}$.

2. Let $(U_n)_n$ be a universal randomness test on $2^{\mathbb{N}}$. By Theorem 6.8 there exists an infinite co-r.e. subset of $\mathbb{N}$ which is not an element of U_1. This set must be random. □

We deduce a corollary about random sequences. A set $A \subseteq \mathbb{N}$ is called *simple* if, and only if, it is r.e. and its complement is immune.

Corollary 6.9. *There exist a random sequence $p \in \Sigma^\omega$ and a simple set $A \subseteq \mathbb{N}$ with $\chi^{-1}(p) \subseteq A$.*

Proof. By Theorem 6.7(2) there exists an infinite random co-r.e. set $B \subseteq \mathbb{N}$. Its complement $A := \mathbb{N} \setminus B$ is simple by Theorem 6.7(1). By Theorem 6.4 there exists a random sequence $q \in \Sigma^\omega$ with $B \subseteq \chi^{-1}(q)$. The sequence $p \in \Sigma^\omega$ with $p(i) := 1 - q(i)$ for all i is random as well and satisfies $\chi^{-1}(p) \subseteq A$. □

Remark 6.10. Corollary 6.9 gives rise to the question how many sequences p have the property stated in this corollary. The answer is: almost none. Indeed, for any fixed co-infinite set A the set $\{p \in \Sigma^\omega \mid \chi^{-1}(p) \subseteq A\}$ has measure zero. Since there are only countably many r.e. sets, also the set

$$\{p \in \Sigma^\omega \mid (\exists \text{ r.e., co-infinite } A \subseteq \mathbb{N})\ \chi^{-1}(p) \subseteq A\}$$

has measure zero.

Especially in view of Theorem 6.7(2) and the interesting proof of Theorem 6.8 the notion of a random set seems to deserve attention in its own right. Another topic for which the ETMS $(2^{\mathbb{N}}, O, \mu)$ might be very useful and serve as a standard example besides the space of (finite or) infinite sequences is the problem to introduce and study randomness more generally on complete partial orders.

We conclude this section with the proof of Theorem 6.8.

Proof of Theorem 6.8. The assertion is obvious if A is finite. Therefore, from now on we assume that A is infinite. We shall construct an r.e. co-infinite set $C \subseteq \mathbb{N}$ with

$$C \cap D_i \neq \emptyset$$

for all $i \in A$. Its complement proves the assertion. We use a "movable marker" style construction; compare Soare [18]. Let $a : \mathbb{N} \to \mathbb{N}$ be a total recursive injective function with range$(a) = A$. We shall define a non-decreasing sequence $(C[n])_n$ of finite subsets of $\mathbb{N}$ and define in the end

$C := \bigcup_n C[n]$. Furthermore, we shall define a non-decreasing sequence $(L[n])_n$ of finite subsets of A. They contain the indices in A which "require action". We proceed in stages n, for $n \in \mathbb{N}$. The sets $C[n]$ and $L[n]$ will be defined at stage n. Furthermore, at the end of stage n we will have a finite list $f_0[n], \dots, f_n[n]$ of $n+1$ pairwise different "forbidden" numbers (marked). If at stage n the "forbidding" condition of one number $f_k[n-1]$ of the numbers $f_0[n-1], \dots, f_{n-1}[n-1]$ from the previous stage is overruled, then all $f_l[n-1]$ with $k \leqslant l < n$ will be added to the set $C[n-1]$. They will be replaced by new forbidden elements $f_j[n]$ (these markers will be moved); the others are kept. In any case, a new one, the number $f_n[n]$, is defined. They will be defined in such a way that at the end of each stage n we have $C[n] \cap \{f_0[n], \dots, f_n[n]\} = \emptyset$. It is crucial that each $f_k[\cdot]$ will be changed only at finitely many stages, i.e., for each k there exists a number N such that $f_k[n] = f_k[N]$ for all $n \geqslant N$. This guarantees that C is co-infinite. It will be clear from the construction that C is r.e. An important point in the construction is the condition when a "forbidding" condition is overruled. The idea is that this is the case when the measure of the union of the sets O_{D_i} is large enough where the union is taken over those indices i which have required action so far, and which have the property that the forbidden element is contained in D_i. In the correctness proof we will assume that there is some forbidden element which changes infinitely often. We will fix the forbidden element with the smallest index and this property, and then we will show that for this specific forbidden element the measure just described cannot become large enough any more once the forbidden element is large enough. Hence, its forbidding condition cannot be overruled anymore, and the forbidden element cannot change anymore, which is a contradiction. Here is the construction. We start with $C[-1] = \emptyset$ and $L[-1] = \emptyset$.

Stage n:

We can assume that $C[n-1]$, $L[n-1]$ and $\{f_0[n-1], \dots, f_{n-1}[n-1]\}$ are defined. If $D_{a(n)} \cap C$ $[n-1] \neq \emptyset$, then we do the following:

1. We set $L[n] := L[n-1]$.
2. We set $C[n] := C[n-1]$.
3. We define $f_j[n] := f_j[n-1]$ for $j \in \{0, \dots, n-1\}$ and $f_n[n] := \min(\mathbb{N} \setminus G)$ where

$$G := \bigcup \{D_{a(j)} \mid j \leqslant n\} \cup \{f_i[j] \mid 0 \leqslant i \leqslant j < n\}.$$

If $D_{a(n)} \cap C[n-1] = \emptyset$, then we do the following:

1. We set $L[n] := L[n-1] \cup \{a(n)\}$.
2. For every $i \in \mathbb{N}$ we define

$$S(i,n) := \mu\Big(\bigcup \{O_{D_l} \mid i \in D_l \text{ and } l \in L[n]\}\Big).$$

The set

$$F[n] := \{m \mid 0 \leqslant m < n \text{ and } S(f_m[n-1], n) > 2^{-m-2}\}$$

can be considered as the set of indices of forbidden elements whose forbidding condition is overruled. We set

$$m_{F[n]} := \begin{cases} \min F[n] & \text{if } F[n] \text{ is nonempty,} \\ n & \text{otherwise.} \end{cases}$$

and

$$C[n] := C[n-1] \cup (D_{a(n)} \setminus \{f_0[n-1], \ldots, f_{n-1}[n-1]\}) \cup \{f_m[n-1] \mid m_{F[n]} \leqslant m < n\}.$$

3. We do not change the forbidden elements $f_m[n-1]$ with $m < m_{F[n]}$, i.e., for $m < m_{F[n]}$ we define $f_m[n] := f_m[n-1]$. But we define the numbers $f_{m_{F[n]}}[n], \ldots, f_n[n]$ (in this order) to be the smallest pairwise different numbers in $\mathbb{N} \setminus G$ where G is defined in the same way as in the first case.

This ends the description of stage n of the algorithm. Remember that finally we define $C := \bigcup_n C[n]$. The algorithm is complete.

It is clear that the algorithm is well-defined. We only remark that the set G defined above is always finite. We have to show that the set C satisfies all the required conditions:

1. C is r.e.,
2. $C \cap D_i \neq \emptyset$ for all $i \in A$,
3. $\mathbb{N} \setminus C$ is infinite.

The first claim is clear.

For the second claim we show by induction that at the end of stage n we have $C[n] \cap D_{a(i)} \neq \emptyset$ for all $i \leqslant n$. Remember that $(C[n])_n$ is a non-decreasing sequence of sets. Therefore, it is sufficient to show that at the end of stage n we have $C[n] \cap D_{a(n)} \neq \emptyset$. In the first case of the two cases considered in the description of stage n, in the case $D_{a(n)} \cap C[n-1] \neq \emptyset$, this and $C[n] = C[n-1]$ give the assertion. In the second case, in the case $D_{a(n)} \cap C[n-1] = \emptyset$, we must show that the set $(D_{a(n)} \setminus \{f_0[n-1], \ldots, f_{n-1}[n-1]\}) \cup \{f_m[n-1] \mid m_{F[n]} \leqslant m < n\}$ contains an element from $D_{a(n)}$. This is clear if $D_{a(n)} \not\subseteq \{f_0[n-1], \ldots, f_{n-1}[n-1]\}$. Assume that $D_{a(n)} \subseteq \{f_0[n-1], \ldots, f_{n-1}[n-1]\}$. The set $D_{a(n)}$ is non-empty because of $\mu(U) < 1$. Define $k := |D_{a(n)}| - 1$. Then $D_{a(n)}$ must contain a forbidden element $f_m[n-1]$ with $m \geqslant k$. On the other hand, for all $l \in D_{a(n)}$, $S(l, n) \geqslant \mu(O_{D_{a(n)}}) = 2^{-(k+1)}$. Especially $S(f_m[n-1], n) \geqslant 2^{-(k+1)} \geqslant 2^{-(m+1)} > 2^{-m-2}$. Hence, $f_m[n-1]$ is an element of $F[n]$ and also of the set $\{f_l[n-1] \mid m_{F[n]} \leqslant l < n\}$. Thus, this set contains an element from $D_{a(n)}$. We have proved the second claim.

Finally, we have to prove that $\mathbb{N} \setminus C$ is infinite. We observe that by construction the numbers $f_0[n], \ldots, f_n[n]$ are pairwise different and $C[n] \cap \{f_0[n], \ldots, f_n[n]\} = \emptyset$. The assertion follows from the following claim:

$$\text{for each } k, \text{ there is a number } N \text{ such that } f_k[n] = f_k[N] \text{ for all } n \geqslant N. \tag{6}$$

This means that the number $f_k[\cdot]$ will be changed only at finitely many stages. The rest of the proof of the theorem consists of the proof of claim (6). In the proof we shall use $L := \bigcup_n L[n]$. Furthermore, for a subset $M \subseteq \mathbb{N}$ we abbreviate $\mu(\bigcup\{O_{D_i} \mid i \in M\})$ by $\mu(M)$.

Assume that (6) is false. Let k be the smallest natural number such that $f_k[\cdot]$ is changed at infinitely many stages. Let $f_0[\infty], \ldots, f_{k-1}[\infty]$ be the final values of $f_0[.], \ldots, f_{k-1}[.]$, that is, $f_i[\infty] := \lim_{n \to \infty} f_i[n]$ for $0 \leqslant i < k$. Note that by construction for each n and each $m \leqslant n$ we have $S(f_m[n], n) \leqslant 2^{-m-2}$. We conclude that for $0 \leqslant i < k$

$$\lim_{n \to \infty} S(f_i[\infty], n) \leqslant 2^{-i-2}. \tag{7}$$

For each subset $E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}$ and each $n \in \mathbb{N}$ we define

$$L^E := \{l \in L \mid D_l \cap \{f_0[\infty], \ldots, f_{k-1}[\infty]\} = E\},$$
$$L^E[n] := L^E \cap L[n].$$

We claim that

$$\mu(L^E) < 2^{-|E|} \tag{8}$$

for all $E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}$. This is true for $E = \emptyset$ because

$$\mu(L^{\emptyset}) \leqslant \mu(L) \leqslant \mu(A) = \mu(U) < 1$$

(because of $L^{\emptyset} \subseteq L \subseteq A$), and it is true for $E \neq \emptyset$, because for $\emptyset \neq E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}$ there is an $i \in \{|E| - 1, \ldots, k-1\}$ with $f_i[\infty] \in E$, hence

$$\begin{aligned}
\mu(L^E) &= \mu\Big(\bigcup\{O_{D_l} \mid l \in L^E\}\Big)\\
&\leqslant \mu\Big(\bigcup\{O_{D_l} \mid l \in L \text{ and } f_i[\infty] \in D_l\}\Big)\\
&= \lim_{n\to\infty} S(f_i[\infty], n)\\
&\leqslant 2^{-i-2}\\
&\leqslant 2^{-|E|-1},
\end{aligned}$$

where we have used (7). We have proved (8). Hence, we can choose a number $N_0 \geqslant k$ large enough such that for all $E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}$

$$\mu(L^E) - \mu(L^E[N_0]) \leqslant 2^{-(2k+2)} \cdot (1 - 2^{|E|} \cdot \mu(L^E)). \tag{9}$$

We can also assume that N_0 is so large such that $f_i[N_0] = f_i[\infty]$ for all $i \in \{0, \ldots, k-1\}$. Set

$$N_1 := \max\Big(\{f_0[\infty], \ldots, f_{k-1}[\infty]\} \cup \bigcup\{D_{a(i)} \mid i \leqslant N_0\}\Big).$$

Let $N_2 > N_0$ be so large such that

$$C \cap \{0, 1, \ldots, N_1\} = C[N_2] \cap \{0, 1, \ldots, N_1\}.$$

This means that numbers $\leqslant N_1$ are added to the set C only at stages $\leqslant N_2$. We claim that for $l \in L \setminus L[N_2]$ we have

$$D_l \cap \{0, 1, \ldots, N_1\} \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}. \tag{10}$$

To see this, fix an $l \in L \setminus L[N_2]$. Note that by definition of N_2 no number in $D_l \cap \{0, 1, \ldots, N_1\}$ can be added to C at any stage later than N_2. This is especially true for the stage $n_l > N_2$ where n_l is the (unique) number with $a(n_l) = l$. Therefore we have

$$D_l \cap \{0, 1, \ldots, N_1\} \subseteq C[n_l - 1] \cup \{f_0[n_l - 1], \ldots, f_{n_l-1}[n_l - 1]\}.$$

Since $D_l \cap C[n_l - 1] = \emptyset$, due to $l \in L$, we obtain

$$D_l \cap \{0, 1, \ldots, N_1\} \subseteq \{f_0[n_l - 1], \ldots, f_{n_l-1}[n_l - 1]\}.$$

We have $f_i[n_l - 1] = f_i[\infty]$ for $0 \leqslant i < k$, but all numbers $f_i[n_l - 1]$ with $i \geqslant k$ will be added to C at some stage $\geqslant n_l$ (because of our assumption that $f_k[.]$ – and hence also $f_i[\cdot]$ for each $i \geqslant k$ – will be changed infinitely often). Therefore we conclude that (10) is true.

For a moment fix a set $E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}$ and consider the probability space which consists out of (1) the set O_E as the underlying space, (2) the restriction to O_E of the σ-algebra generated by τ, and (3) the probability measure μ_E defined by $\mu_E(U) := 2^{|E|} \cdot \mu(U)$ for all elements

$U \subseteq O_E$ of this σ-algebra. For $l \in L^E[N_0]$ we have $E \subseteq D_l \subseteq \{0, 1, \ldots, N_1\}$. On the other hand, from (10) we conclude that for $l \in L^E \setminus L^E[N_2]$ we have $D_l \cap \{0, 1, \ldots, N_1\} = E$. These two facts imply that in the mentioned probability space the two events

$$\bigcup\{O_{D_l} \mid l \in L^E[N_0]\} \quad \text{and} \quad \bigcup\{O_{D_l} \mid l \in L^E \setminus L^E[N_2]\}$$

are independent. Then also their complements

$$O_E \setminus \bigcup\{O_{D_l} \mid l \in L^E[N_0]\} \quad \text{and} \quad O_E \setminus \bigcup\{O_{D_l} \mid l \in L^E \setminus L^E[N_2]\}$$

are independent. Hence, the probability of the joint occurrence is equal to the product of the two probabilities, that is,

$$1 - 2^{|E|} \cdot \mu\big(L^E[N_0] \cup (L^E \setminus L^E[N_2])\big) = \big(1 - 2^{|E|} \cdot \mu(L^E[N_0])\big) \cdot \big(1 - 2^{|E|} \cdot \mu(L^E \setminus L^E[N_2])\big).$$

A short computation yields the first equality in the following estimation, and (9) gives the last estimate

$$\begin{aligned} \mu(L^E \setminus L^E[N_2]) &= \frac{\mu(L^E[N_0] \cup (L^E \setminus L^E[N_2])) - \mu(L^E[N_0])}{1 - 2^{|E|} \cdot \mu(L^E[N_0])} \\ &\leqslant \frac{\mu(L^E) - \mu(L^E[N_0])}{1 - 2^{|E|} \cdot \mu(L^E)} \\ &\leqslant 2^{-2k-2}. \end{aligned}$$

Using this inequality for all $E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}$ we obtain

$$\begin{aligned} \mu(L \setminus L[N_2]) &\leqslant \sum_{E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}} \mu(L^E \setminus L^E[N_2]) \\ &\leqslant \sum_{E \subseteq \{f_0[\infty], \ldots, f_{k-1}[\infty]\}} 2^{-2k-2} \\ &= 2^{-k-2}. \end{aligned}$$

Finally set $N_3 := \max(\bigcup\{D_{a(i)} \mid i \leqslant N_2\})$. For all $i > N_3$ and stages $n \in \mathbb{N}$ we have

$$S(i, n) \leqslant \mu(L \setminus L[N_2]) \leqslant 2^{-k-2}.$$

Hence, as soon as the number $f_k[\cdot]$ has been set to be larger than N_3, it will never again be changed. This contradicts the assumption that $f_k[\cdot]$ will be changed infinitely often. We have proved (6). This ends the proof of the theorem. □

Acknowledgments

During the preparation of the paper, the first author was supported by the DFG Research Grant No. HE 2489/2-1 and a member of the Computer Science Department of the University of Auckland, New Zealand. The authors thank Cristian Calude for stimulating discussions on randomness and the anonymous referees for useful comments.

References

[1] C. Calude, Information and Randomness, Monographs in Theoretical Computer Science, Springer, Berlin, 1994.

[2] C. Calude, H. Jürgensen, Randomness as an invariant for number representations, in: H. Maurer, et al. (Eds.), Results and Trends in Theoretical Computer Science, Springer, Berlin, 1994, pp. 44–66.

[3] C.S. Calude, P. Hertling, B. Khoussainov, Do the zeros of Riemann's Zeta-function form a random sequence?, Bulletin of the European Association for Theoretical Computer Science 62 (1997) 199–207.

[4] G.J. Chaitin, A theory of program size formally identical to information theory, Journal of the Association for Computing Machinery 22 (1975) 329–340.

[5] A. Grzegorczyk, On the definitions of computable real continuous functions, Fundamenta Mathematicae 44 (1957) 61–71.

[6] P. Hertling, Y. Wang, Invariance properties of random sequences, Journal of Universal Computer Science 3 (11) (1997) 1241–1249.

[7] P. Hertling, K. Weihrauch, Randomness spaces, in: K.G. Larsen, S. Skyum, G. Winske (Eds.), Automata, Languages and Programming, Lecture Notes in Computer Science, vol. 1443, Springer, Berlin, 1998, pp. 796–807, 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 1998.

[8] P. Hertling and K. Weihrauch, Randomness spaces, Technical Report 079, CDMTCS, Auckland, Jan. 1998.

[9] K.-I. Ko, Complexity Theory of Real Functions, Progress in Theoretical Computer Science, Birkhäuser, Boston, 1991.

[10] C. Kreitz, K. Weihrauch, Theory of representations, Theoretical Computer Science 38 (1985) 35–53.

[11] D. Lacombe, Classes récursivement fermés et fonctions majorantes, Comptes Rendus Académie des Sciences Paris, 240:716–718, June 1955. Théorie des fonctions.

[12] L.A. Levin, Randomness conservation inequalities: information and independence in mathematical theories, Information and Control 61 (1984) 15–37.

[13] M. Li, P. Vitányi, An Introduction to Kolmogorov Complexity and Its Applications, second ed., Graduate Texts in Computer Science, Springer, New York, 1997.

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

[15] M.B. Pour-El, J.I. Richards, Computability in Analysis and Physics, Perspectives in Mathematical Logic, Springer, Berlin, 1989.

[16] H. Rogers, Theory of Recursive Functions and Effective Computability, McGraw-Hill, New York, 1967.

[17] C.P. Schnorr, Zufälligkeit und Wahrscheinlichkeit, Lecture Notes in Mathematics, vol. 218, Springer, Berlin, 1971.

[18] R.I. Soare, Recursively Enumerable Sets and Degrees, Perspectives in Mathematical Logic, Springer, Berlin, 1987.

[19] K. Weihrauch, Computability, EATCS Monographs on Theoretical Computer Science, vol. 9, Springer, Berlin, 1987.

[20] K. Weihrauch, Random real numbers, Informatik Berichte 219, FernUniversität Hagen, Hagen, June 1997.

[21] K. Weihrauch, Computability on the probability measures on the Borel sets of the unit interval, Theoretical Computer Science 219 (1999) 421–437.

[22] K. Weihrauch, Computable Analysis, Springer, Berlin, 2000.

[23] A. Zvonkin, L. Levin, The complexity of finite objects and the development of the concepts of information and randomness by means of the theory of algorithms, Russian Mathematical Surveys 25 (6) (1970) 83–124.