CDMTCS
Research
Report
Series

Randomness Spaces

Peter Hertling
Department of Computer Science
University of Auckland, New Zealand

Klaus Weihrauch
Theoretical Computer Science I
University of Hagen, Germany

CDMTCS-079
January 1998

Centre for Discrete Mathematics and
Theoretical Computer Science

Randomness Spaces

Peter Hertling*
Department of Computer Science
University of Auckland
Private Bag 92019, Auckland
New Zealand

email: hertling@cs.auckland.ac.nz

Klaus Weihrauch
Theoretische Informatik I
FernUniversität Hagen
58084 Hagen
Germany

email: klaus.weihrauch@fernuni-hagen.de

January 19, 1998

Abstract

Martin-Löf defined infinite random sequences over a finite alphabet via randomness tests which describe sets having measure zero in a constructive sense. In this paper this concept is generalized to separable topological spaces with a measure, following a suggestion of Zvonkin and Levin. After studying basic results and constructions for such randomness spaces a general invariance result is proved which gives conditions under which a function between randomness spaces preserves randomness. This corrects and extends a result by Schnorr. Calude and Jürgensen proved that the randomness notion for real numbers obtained by considering their b-ary representations is independent from the base b. We use our invariance result to show that this notion is identical with the notion which one obtains by viewing the real number space directly as a randomness space. Furthermore, arithmetic properties of random real numbers are derived, for example that every computable analytic function preserves randomness. Finally, by considering the power set of the natural numbers with its natural topology as a randomness space, we introduce a new notion of a random set of numbers. It is different from the usual one which is defined via randomness of the characteristic function, but it can also be characterized in terms of random sequences. Surprisingly, it turns out that there are infinite co-r.e. random sets.

1 Introduction

Random infinite binary sequences have first been introduced by von Mises [27]. His motivation was to lay a foundation for probability theory. He considered sequences as random and called them "Kollektive" if the digits 0 and 1 appear with their expected limiting frequency not only in the sequence but also in any subsequence which could be obtained by applying certain "admissible place selection rules". His approach received a severe blow when Ville [26] showed that there exists a Kollektiv which does not satisfy the law of the iterated logarithm, which a random sequence should certainly satisfy.

*The first author was supported by the DFG Research Grant No. HE 2489/2-1.

A second approach is Martin-Löf's [18] definition of random sequences via typicalness. It is based on the idea that a sequence is typical or random, if it does not lie in any set which is in a constructive sense of measure 0. This idea is formalized by considering randomness tests, which are decreasing recursive sequences $(U_n)_n$ of open sets U_n whose measure tends to 0 with a prescribed convergence rate. The constructive set of measure 0 then consists of the intersection $\bigcap_n U_n$.

Another approach for defining random sequences is based on the idea to consider the program-size complexity of its finite prefixes, defined via universal Turing machines. This idea has been proposed independently by Kolmogorov [13] and Chaitin [8, 9] in different versions (see also Solomonoff [23]) and further developed by Levin, Schnorr and others. It leads to the same notion of random infinite sequences as the second approach.

While the first and the third approach for defining randomness work naturally only for sequences, Martin-Löf's approach can be extended to much more general spaces which allow the formulation of recursive sequences of open sets with fast decreasing measure. This was suggested already by Zvonkin and Levin [31]. We follow this idea and provide rigorous definitions of randomness spaces in Section 3. 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 randomness spaces and random elements are given. In Section 4 we ask under which conditions a function between randomness spaces preserves randomness. Our main invariance result gives sufficient conditions and corrects and extends a corresponding result by Schnorr [21]. In the following section we concentrate on the randomness space 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 [7] 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. The second main result in this section states that every computable analytic function preserves randomness. In the last section we consider another randomness space: the power set of the natural numbers, endowed with its 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.

2 Notation

The power set $\{A \mid A \subseteq X\}$ of all subsets of a set 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. $\mathrm{dom}\, f = X$. For $x \in X$ we write $f(x) \downarrow$ if $x \in \mathrm{dom}\, f$ and $f(x) \uparrow$ or $f(x) = \uparrow$ if $x \notin \mathrm{dom}\, f$. We denote the set of natural numbers by $\mathbb{N} = \{0, 1, 2, \ldots\}$. A *partial recursive function* is a function $f :\subseteq \mathbb{N} \to \mathbb{N}$ which is computable in the usual sense. It is also called *total recursive* if additionally

$\mathrm{dom}\, f = \mathbb{N}$. 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 $k \geq 0$ the finite product $X^k := \{w \mid w : \{1, \ldots, k\} \to X\}$ is the set of all vectors $w = w(1)w(2)\ldots w(k)$ over X of length k. The empty word, the only element of X^0, is denoted by ε.

We use the standard bijection $\langle , \rangle : \mathbb{N}^2 \to \mathbb{N}$ defined by $\langle i, j \rangle := \frac{1}{2}(i+j)(i+j+1)+j$. Higher tupling functions are defined recursively by $\langle n \rangle := n$, $\langle n_1, n_2, \ldots, n_{k+1} \rangle := \langle \langle n_1, \ldots n_k \rangle, n_{k+1} \rangle$. 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 $D : \mathbb{N} \to \{E \subseteq \mathbb{N} \mid E \text{ is finite}\}$ of the set of all finite subset of $\mathbb{N}$, defined by $D^{-1}(E) := \sum \{2^i \mid i \in E\}$. A *topology* on a set X is a class τ of subsets of X which contains the empty set $\emptyset$ and the full set X as elements and which is closed under finite intersection and under arbitrary union (if $\beta \subseteq \tau$ then $\bigcup_{A \in \beta} A = \bigcup \{A \mid A \in \beta\} \in \tau$). The elements of a topology are called *open sets.* A *base* of a topology τ is a subset $\beta \subseteq \tau$ such that any open set is the union of the elements in a subset of β. A *subbase* of a topology τ is a subset $\beta \subseteq \tau$ such that any open set is the union of finite intersections of elements of β. The *σ-algebra* generated by a class $\mathcal{C}$ of subsets of a set X is the smallest class $\mathcal{B}$ of subsets of X which contains $\mathcal{C}$, is closed under complement (if $A \in \mathcal{B}$ then also $X \setminus A \in \mathcal{B}$) and closed under countable union (if $(A_n)_n$ is a sequence of elements in $\mathcal{B}$ then also $\bigcup_{n=0}^\infty A_n \in \mathcal{B}$). A *measure* on a σ-algebra $\mathcal{B}$ is a mapping $\mu : \mathcal{B} \to \{x \in \mathbb{R} \mid x \geq 0\} \cup \{\infty\}$ with $\mu(\emptyset) = 0$ and $\mu(\bigcup_{n=0}^\infty A_n) = \sum_{n=0}^\infty \mu(A_n)$ for any sequence $(A_n)_{n \in \mathbb{N}}$ of pairwise disjoint sets in $\mathcal{B}$. A measure μ on $\mathcal{B}$ is called *σ–finite* if there is a sequence $(A_n)_n$ of sets in $\mathcal{B}$ with $\mu(A_n) < \infty$ for each n whose union is the full space: $X = \bigcup_{n=0}^\infty A_n$. It is called *finite* if $\mu(X) < \infty$ and it is called a *probability measure* if $\mu(X) = 1$. For more details on topology and measure the reader is referred to any standard textbook.

3 Randomness Spaces

Zvonkin and Levin [31], pp. 110–111, observed that Martin–Löf's [18] definition of randomness tests and 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 the necessary definitions and prove elementary results including the existence of a universal randomness test on a randomness space if its measure satisfies a weak effectivity condition. We construct finite products of randomness spaces with σ–finite measures and infinite products of randomness spaces with probability measures. We study randomness on these product spaces. Several examples of randomness spaces and random elements are given.

Definition 3.1 A *randomness space* is a triple (X, B, μ), where X is a topological space, $B : \mathbb{N} \to 2^X$ is a total numbering of a subbase of the topology of X, and μ is a measure defined on the σ-algebra generated by the topology of X (Notation: $B_i := B(i)$).

Random points of a randomness space are defined via randomness tests. Before we define them we introduce the numbering B' of a base, derived from a numbering B of a subbase, and define and discuss computable sequences of open sets.

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*, iff there is an r.e. subset $A \subseteq \mathbb{N}$ such that $V_n = \bigcup_{\langle n,i\rangle \in A} U_i$ for all $n \in \mathbb{N}$.

2. We define a sequence $(U'_n)_n$ of open sets, called the *sequence derived from* U, by $U'_i := U'(i) := \bigcap_{j \in D_i} U_j$, for all $i \in \mathbb{N}$.

3. We say that U satisfies the *intersection property*, iff there is an r.e. set $A \subseteq \mathbb{N}$ with

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

The standard numbering D of the set of all finite subsets of $\mathbb{N}$ has been defined in Section 2. We obtain especially $U'_0 = \bigcap_{j \in D_0} U_j = \bigcap_{j \in \emptyset} U_j = X$ for any sequence $(U_n)_n$ of open sets. If B is a total numbering of a subbase of the topology, then B' is a total numbering of a base. In general, we will deal mostly with B'–computable sequences of open sets. In the following lemma we collect several useful facts about computable sequences of open sets. We omit the proofs.

Lemma 3.3 *Let X be a topological space and $(U_n)_n$, $(V_n)_n$, and $(T_n)_n$ be sequences of open subsets of X.*

1. *If $(U_n)_n$ is V–computable and $(V_n)_n$ is T–computable, then $(U_n)_n$ is T–computable.*

2. *$(U_n)_n$ is U'–computable.*

3. *U satisfies the intersection property, iff the sequence $(U'_n)_n$ is U-computable.*

4. *U' satisfies the intersection property.*

5. *If V satisfies the intersection property, then the following statements are equivalent:*

   (a) $(U_n)_n$ is V–computable.

   (b) $(U_n)_n$ is V'–computable.

   (c) $(U'_n)_n$ is V–computable.

   (d) $(U'_n)_n$ is V'–computable.

The next definition generalizes Martin–Löf's [18] definition of random sequences to points from arbitrary randomness spaces.

Definition 3.4 Let (X, B, μ) be a randomness space.

1. A *randomness test on* X is a B'–computable sequence $(U_n)_n$ of open sets with $\mu(U_n) \leq 2^{-n}$ for all $n \in \mathbb{N}$.

2. An element $x \in X$ is called *non–random*, iff $x \in \bigcap_{n \in \mathbb{N}} U_n$ for some randomness test $(U_n)_n$ on X. It is called *random*, iff it is not non–random.

In the following examples of randomness spaces the numberings B of subbases satisfy the intersection property. By Lemma 3.3 in this case a sequence $(U_n)_n$ of open subsets of X is a randomness test iff it is B–computable and $\mu(U_n) \leq 2^{-n}$ for all n.

Examples 3.5 1. (see Calude, Hertling, Jürgensen, Weihrauch [4]) The simplest examples of randomness spaces are spaces (Σ, B, μ) where $\Sigma = \{s_0, \ldots, s_k\}$ is a finite, non-empty set, the numbering B is given by $B_i := \{s_i\}$ for $i \leq k$ and $B_i := X$ for $i > k$, and the measure μ is given by $\mu(\{s_i\}) = \frac{1}{k+1}$. Notice that this is a probability measure. Every element of Σ is random because the measure of any non-empty open set is at least $\frac{1}{k+1}$.

2. The original randomness spaces are the spaces (Σ^ω, B, μ) of infinite sequences over a finite alphabet Σ with at least two elements (Martin-Löf [18]). The numbering B of a subbase (in fact a base) of the topology is given by $B_i = \nu(i)\Sigma^\omega = \{p \in \Sigma^\omega \mid \nu(i)$ is a prefix of $p\}$, where $\nu : \mathbb{N} \to \Sigma^*$ is the length–lexicographical bijection between $\mathbb{N}$ and the set Σ^* of finite words over Σ. The measure μ is the product measure of the measure in the first example, i.e. given by $\mu(w\Sigma^\omega) = |\Sigma|^{-|w|}$ for $w \in \Sigma^*$. A sequence $p \in \Sigma^\omega$ is called computable, iff there is a computable function $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that $p(i) = s_{f(i)}$ (where $\Sigma = \{s_0, \ldots, s_k\}$). Let p be computable. We claim that p is non-random. Indeed, the sequence $(U_n)_n$ of sets $U_n := p(0) \ldots p(n-1)\Sigma^\omega$ is a randomness test with $p \in \bigcap_n U_n$ because $\mu(U_n) = |\Sigma|^{-n} \leq 2^{-n}$ and $U_n = \bigcup_{\langle n,i\rangle \in A} B_i$ where A is the recursive set $A := \{\langle n, i\rangle \mid \nu(i) = p(0) \ldots p(n-1)\}$).

3. For the real numbers $\mathbb{R}$ we consider the randomness space $(\mathbb{R}, B, \lambda)$, where λ is the usual Lebesgue measure and B is the numbering of a base of the real line topology defined by $B_{\langle i,j\rangle} := \{x \in \mathbb{R} \mid |x - \nu_{\mathbb{D}}(i)| < 2^{-j}\}$. Here $\nu_{\mathbb{D}} : \mathbb{N} \to \mathbb{D}$ is the total numbering of the dyadic numbers

$$\mathbb{D} := \{x \in \mathbb{R} \mid (\exists i, j, k \in \mathbb{N})\ x = (i - j) \cdot 2^{-k}\}$$

defined by $\nu_{\mathbb{D}}\langle i, j, k\rangle := (i - j)/2^k$. When we refer to *random real numbers* we mean random elements of this randomness space. A real number x is computable, iff the set $C_x := \{i \mid x \in B_i\}$ is r.e., see Weihrauch [28]. Let $x \in \mathbb{R}$ be computable. Define $A := \{\langle n, i\rangle \mid i \in C_x, \lambda(B_i) \leq 2^{-n-1}\}$ and $U_n = \bigcup_{\langle n,i\rangle \in A} B_i$. Then $(U_n)_n$ is a randomness test with $\{x\} = \bigcap_{n \in \mathbb{N}} U_n$. Therefore, every computable real number is non–random.

4. For the unit interval $[0, 1]$ we consider the randomness space $([0, 1], \tilde{B}, \tilde{\lambda})$, where $\tilde{B}_i := B_i \cap [0, 1]$ and $\tilde{\lambda}$ denotes the restriction of the Lebesgue measure to the unit interval. Later we shall prove that an element of the unit interval is a random element of the randomness space $([0, 1], \tilde{B}, \tilde{\lambda})$ if and only if it is a random element of the randomness space $(\mathbb{R}, B, \lambda)$.

Our definitions of a randomness space and a randomness test can be specialized or modified in several ways by further conditions:

(B) B is a numbering of a base of the space X.

(IP) B has the intersection property.

(ZL) There exists an r.e. set A such that for all i, $B_i = \bigcup\{B_k \mid \langle i, k\rangle \in A, k > i\}$.

(CB) $(U_n)_n$ is B–computable (instead of B'–computable).

(D) $U_{n+1} \subseteq U_n$ for all $n \in \mathbb{N}$.

(CZL) $U_n = \bigcup\{B_i \mid f(i) \geq n\}$ for some total computable function $f : \mathbb{N} \longrightarrow \mathbb{N}$.

Condition (B), (IP) and (ZL) restrict the class of randomness spaces, and Conditions (CB), (D), and (CZL) restrict the set of randomness tests and non–random elements. In our case, Condition (D) does not restrict the set of non–random elements, i.e. we may assume w.l.o.g. $U_{n+1} \subseteq U_n$ for all $n \in \mathbb{N}$:

Proposition 3.6 *If $(V_n)_n$ is a randomness test, then $(U_n)_n$ with $U_n := \bigcap_{i \leq n} V_i$ is a randomness test with $U_{n+1} \subseteq U_n$ for all n and $\bigcap_{n=0}^{\infty} U_n = \bigcap_{n=0}^{\infty} V_n$.*

Proof. We have to show only that the sequence $(U_n)_n$ is B'–computable. If A is an r.e. set with $V_n = \bigcup_{\langle n,i \rangle \in A} B'_i$, then $\tilde{A} := \{\langle n,i \rangle \mid (\exists i_0, i_1, \ldots, i_n)\ \langle j, i_j \rangle \in A$ for $j = 0, 1, \ldots, n$, and $D_i = \bigcup_{j=0}^{n} D_{i_j}\}$ is an r.e. set with $U_n = \bigcup_{\langle n,i \rangle \in \tilde{A}} B'_i$. □

Obviously, (IP) implies (B). For modelling randomness, (CB) is not very meaningful without (B). Under (IP + CB), (D) can be assumed without loss of generality. Zvonkin and Levin [31] consider (B + ZL + CZL). It is clear that (CZL) implies (CB + D). Does (B + ZL + CB + D) imply (CZL)? Zvonkin's and Levin's [31, p. 110–111] outline does not consider this question. It does also not show in which way the somewhat technically looking assumption (ZL) can be applied to show their invariance proposition 4.2 (c.f. our Proposition 3.8).

In all of the examples of randomness spaces (X, B, μ) considered in this paper the numberings B of subbases satisfy the intersection property (IP). We remind the reader of the fact that in this case a sequence $(U_n)_n$ of open subsets of X is a randomness test iff it is B–computable (this is condition (CB)) and $\mu(U_n) \leq 2^{-n}$ for all n.

In the next section we shall consider randomness preserving mappings between randomness spaces. Here we note that replacing a numbering of a subbase by an "equivalent" numbering of a subbase does not affect the notion of randomness for points in the considered space.

Definition 3.7 Let X be a topological space and let $(B_n)_n$ and $(C_n)_n$ be two sequences of open subsets of X. We say that B *is b–reducible to* C, iff the sequence $(B_n)_n$ is C'–computable. B and C are called *b–equivalent*, iff B is b–reducible to C and C is b–reducible to B.

From Lemma 3.3 one deduces immediately the following

Proposition 3.8 *Let (X, B, μ) be a randomness space and C be a total numbering of a subbase of the topology which is b–equivalent to B. Then a sequence of open subsets of X is a randomness test on (X, B, μ), iff it is a randomness test on (X, C, μ). Consequently, an element of X is random in (X, B, μ), if and only if it is random in (X, C, μ).*

In their context (B + ZL + CZL), Zvonkin and Levin [31, Proposition 4.2] already state (without proof) that equivalent basis numberings induce the same randomness concepts.

It is remarkable that the randomness space $(\Sigma^{\omega}, B, \mu)$ from Example 3.5.2 has a universal randomness test (Martin-Löf [18]), i.e. a randomness test $(U_n)_n$ such that for each randomness test $(V_n)_n$ there exists a constant $c \in \mathbb{N}$ with $V_{n+c} \subseteq U_n$ for all n. We generalize the original definition as follows:

Definition 3.9 A randomness test $(U_n)_n$ on a randomness space (X, B, μ) is called *universal*, iff for any randomness test $(V_n)_n$ on (X, B, μ) there is an increasing, computable function $r : \mathbb{N} \to \mathbb{N}$ with $V_{r(n)} \subseteq U_n$, for all n.

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. Any randomness space whose measure satisfies a certain weak effectivity condition possesses a universal randomness test.

Definition 3.10 We call a measure μ of a randomness space (X, B, μ) *weakly bounded*, iff there are an increasing computable function $d : \mathbb{N} \to \mathbb{N}$ and an r.e. set Z with

$$\mu(B'_{i_1} \cup \ldots \cup B'_{i_k}) \leq 2^{-d(n)} \Longrightarrow \langle k, \langle i_1, \ldots, i_k \rangle, n \rangle \in Z \Longrightarrow \mu(B'_{i_1} \cup \ldots \cup B'_{i_k}) \leq 2^{-n}$$

for all $k, i_1, \ldots, i_k, n \in \mathbb{N}$.

Theorem 3.11 *On every randomness space (X, B, μ) with weakly bounded measure there exists a universal randomness test.*

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

Let $(W_k)_{k \in \mathbb{N}}$ be a standard numbering of all r.e. subsets of $\mathbb{N}$ (compare Rogers [20], Weihrauch [28]). For each $k \in \mathbb{N}$ let $(V_{k,n})_n$ be the k-th computable sequence of open sets, defined by $V_{k,n} := \bigcup \{B'_i \mid \langle n, i \rangle \in W_k\}$. Since $\{\langle n, i, k \rangle \mid \langle n, i \rangle \in W_k\}$ is r.e., there is a computable function $f :\subseteq \mathbb{N}^3 \to \mathbb{N}$ such that $f(k, n, j) \downarrow$ for all $j < i$, if $f(k, n, i) \downarrow$, and $\{i \mid \langle n, i \rangle \in W_k\} = \{f(k, n, l) \mid f(k, n, l) \downarrow\}$. Intuitively, $f(k, n, .)$ enumerates $V_{k,n}$. We cut the sequences $(V_{k,n})_n$ off in order to obtain randomness tests. The function $g :\subseteq \mathbb{N}^3 \to \mathbb{N}$, defined by

$$g(k, n, l) := \begin{cases} f(k, n, l) & \text{if } f(k, n, l) \downarrow \text{ and } \langle l + 1, \langle f(k, n, 0), \ldots, f(k, n, l) \rangle, n \rangle \in Z \\ \uparrow & \text{otherwise,} \end{cases}$$

is computable, because Z is r.e. For each $k \in \mathbb{N}$ define $(T_{k,n})_n$ by

$$T_{k,n} := \bigcup \{B'_i \mid (\exists l)\ g(k, n, l) = i\} .$$

Since by definition $\langle l + 1, \langle g(k, n, 0), \ldots, g(k, n, l) \rangle, n \rangle \in Z$ if $g(k, n, l) \downarrow$, we obtain $\mu(T_{k,n}) \leq 2^{-n}$. Since the function g is computable, the sequence $(T_{k,n})_n$ is a randomness test for each k. On the other hand, let $(S_n)_n$ be a randomness test such that $\mu(S_n) \leq 2^{-d(n)}$ for all n. Then $(S_n)_n = (V_{k,n})_n$ for some k. By the assumption on Z we have $g(k, n, l) = f(k, n, l)$ for all n, l, hence $(T_{k,n})_n = (V_{k,n})_n = (S_n)_n$. That means, such a test $(S_n)_n$ remains unchanged.

Define $U_n := \bigcup_{k=0}^{\infty} T_{k,n+k+1}$ for all n. Then

$$\mu(U_n) \leq \sum_{k=0}^{\infty} \mu(T_{k,n+k+1}) \leq \sum_{k=0}^{\infty} 2^{-(n+k+1)} = 2^{-n} .$$

Furthermore,

$$U_n = \bigcup \{B'_i \mid (\exists k, l \in \mathbb{N})\ g(k, n + k + 1, l) = i\},$$

hence $(U_n)_n$ is B'–computable. Therefore, $(U_n)_n$ is a randomness test. Let $(S_n)_n$ be an arbitrary randomness test. Since $\mu(S_{d(n)}) \leq 2^{-d(n)}$, $(S_{d(n)})_n$ is a randomness test with $(S_{d(n)})_n = (V_{k,n})_n = (T_{k,n})_n$ for some k. With $r(n) := d(n+k+1)$ we obtain:

$$S_{r(n)} = S_{d(n+k+1)} = T_{k,n+k+1} \subseteq U_n \, .$$

We conclude that $(U_n)_n$ is a universal randomness test. □

If the numbering B satisfies the intersection property we can weaken the condition on the measure μ slightly. The following result can be proved by substituting B for B' in the last proof.

Proposition 3.12 *Let (X, B, μ) be a randomness space whose numbering B satisfies the intersection property and whose measure μ satisfies the following property: there are an increasing computable function $d : \mathbb{N} \to \mathbb{N}$ and an r.e. set Z with*

$$\mu(B_{i_1} \cup \ldots \cup B_{i_k}) \leq 2^{-d(n)} \Longrightarrow \langle k, \langle i_1, \ldots, i_k \rangle, n \rangle \in Z \Longrightarrow \mu(B_{i_1} \cup \ldots \cup B_{i_k}) \leq 2^{-n}$$

for all $k, i_1, \ldots, i_k, n \in \mathbb{N}$. Then there exists a universal randomness test on X.

Zvonkin and Levin [31, Proposition 4.1] stated (without proof) that in the framework (B + ZL + CZL) and under the assumption of an effectivity condition for μ, which is stronger than the above one there exists a universal randomness test. It is the following condition: the function $\langle k, \langle i_1, \ldots, i_k \rangle \rangle \mapsto \mu(B_{i_1} \cup \ldots \cup B_{i_k})$ mapping natural numbers to real numbers is a computable function in the usual sense, which means that the set $\{\langle k, \langle i_1, \ldots, i_k \rangle, m, n \rangle \mid \nu_{\mathbb{D}}(m) < \mu(B_{i_1} \cup \ldots \cup B_{i_k}) < \nu_{\mathbb{D}}(n)\}$ is r.e. Considerations in Weihrauch [30] strongly suggest that (under Condition (B)) the property

$$\text{“}\{\langle k, \langle i_1, \ldots, i_k \rangle, m \rangle \mid \nu_{\mathbb{D}}(m) < \mu(B_{i_1} \cup \ldots \cup B_{i_k})\} \text{ is r.e.”}$$

is the canonical computability axiom for randomness spaces in general (Zvonkin and Levin [31], Li and Vitanyi [17], and others call measures with this property “semicomputable”.) Every measure satisfying the above Zvonkin/Levin–condition has this property and satisfies the condition formulated in Proposition 3.12.

We can draw simple conclusions about the set of random elements. In a measure theoretical sense it is large, but topologically it is small if the space has a universal randomness test and the set of non–random elements is a dense subset of X. A subset Y of a topological space X is called *dense in* X if every open subset of X contains an element of Y. It is called *nowhere dense* if its closure does not contain an open set. It is called *meager* if it is the union of countably many nowhere dense sets.

Proposition 3.13 *Let (X, B, μ) be a randomness space.*

1. *The set of random elements in X has μ-measure $\mu(X)$.*

2. *The set of random elements is meager, if the space X has a universal randomness test and its set of non–random elements is dense in X.*

Proof. (1) There are only countable many randomness tests on (X, B, μ). Let

$$(U_n^{(0)})_n,\ (U_n^{(1)})_n,\ (U_n^{(2)})_n, \ldots$$

be a list of them. Each set $\bigcap_{n \in \mathbb{N}} U_n^{(k)}$ has μ-measure 0. Hence the union of these sets has measure 0 as well. The set of random elements is the complement of their union and, thus, has measure $\mu(X)$.

(2) Assume that there is a universal randomness test $(U_n)_n$ and that the set of non–random elements is dense in X. Then each of the sets $X \setminus U_n$ is closed and nowhere dense. The set of random elements is the union $\bigcup_{n \in \mathbb{N}} (X \setminus U_n)$. □

Next, we construct finite products of randomness spaces with σ–finite measures and countable products of randomness spaces with probability measures.

Let $(X^{(0)}, B^{(0)}, \mu^{(0)})$, $(X^{(1)}, B^{(1)}, \mu^{(1)})$, … $(X^{(n)}, B^{(n)}, \mu^{(n)})$, for some $n \in \mathbb{N}$ be a finite list of randomness spaces with σ–finite measures $\mu^{(k)}$. The product $X^{(0)} \times \ldots \times X^{(n)}$ bears the product topology with the *product numbering* $B^{(0)} \times \ldots \times B^{(n)}$ of a subbase defined by

$$(B^{(0)} \times \ldots \times B^{(n)})\langle i_0, \ldots, i_n \rangle := B_{i_0}^{(0)} \times \ldots \times B_{i_n}^{(n)}.$$

Let $\mu^{(0)} \times \ldots \times \mu^{(n)}$ be the usual product measure on $X^{(0)} \times \ldots \times X^{(n)}$. It is well–defined and σ–finite since we assume that all measures $\mu^{(k)}$ are σ–finite. The randomness space

$$\prod_{k=0}^{n} (X^{(k)}, B^{(k)}, \mu^{(k)}) := (X^{(0)} \times \ldots \times X^{(n)}, B^{(0)} \times \ldots \times B^{(n)}, \mu^{(0)} \times \ldots \times \mu^{(n)})$$

is called the *product randomness space* of the spaces $(X^{(0)}, B^{(0)}, \mu^{(0)})$, …, $(X^{(n)}, B^{(n)}, \mu^{(n)})$. We write (X^n, B^n, μ^n) for the product of $n \geq 1$ copies of a randomness space (X, B, μ) with σ–finite measure μ.

Now let $((X^{(k)}, B^{(k)}, \mu^{(k)}))_k$ be a sequence of randomness spaces with probability measures, i.e. $\mu^{(k)}(X^{(k)}) = 1$ for all $k \in \mathbb{N}$. The infinite product $\prod_{k=0}^{\infty} X^{(k)} = \{x : \mathbb{N} \to \bigcup_{k \in \mathbb{N}} X^{(k)} \mid x_k \in X^{(k)} \text{ for all } k\}$ of all sequences $(x_k)_{k \in \mathbb{N}}$ with $x_k \in X^{(k)}$ bears the well–known product topology. A numbering $\prod_{k=0}^{\infty} B^{(k)}$ of a subbase of the topology is defined by

$$\begin{aligned}(\prod_{k=0}^{\infty} B^{(k)})\langle n, \langle i_0, \ldots, i_n \rangle\rangle &:= \prod_{k=0}^{n} B_{i_k}^{(k)} \times \prod_{k=n+1}^{\infty} X^{(k)} \\ &= \{x : \mathbb{N} \to \bigcup_{k \in \mathbb{N}} X^{(k)} \mid x_k \in B_{i_k}^{(k)} \text{ for } 0 \leq k \leq n \text{ and } x_k \in X^{(k)} \text{ for all } k\}\end{aligned}$$

The infinite product measure $\prod_{k=0}^{\infty} \mu^{(k)}$ on $\prod_{k=0}^{\infty} X^{(k)}$ is well–defined and a probability measure since all $\mu^{(k)}$ are assumed to be probability measures. The randomness space

$$\prod_{k=0}^{\infty} (X^{(k)}, B^{(k)}, \mu^{(k)}) := (\prod_{k=0}^{\infty} X^{(k)}, \prod_{k=0}^{\infty} B^{(k)}, \prod_{k=0}^{\infty} \mu^{(k)})$$

is called the *product randomness space* of the spaces $(X^{(k)}, B^{(k)}, \mu^{(k)})$. If all the spaces $(X^{(k)}, B^{(k)}, \mu^{(k)})$ are identical and equal to (X, B, μ) we write $(X^\omega, B^\omega, \mu^\omega)$ for the infinite product.

Remark 3.14 The numberings $B^{(0)} \times \ldots \times B^{(n)}$ and $\prod_{k=0}^{\infty} B^{(k)}$ of subbases are numberings of bases if the $B^{(k)}$ are numberings of bases. The numbering $B^{(0)} \times \ldots \times B^{(n)}$ satisfies the intersection property if the $B^{(k)}$ are numberings of bases satisfying the intersection property. The numbering $\prod_{k=0}^{\infty} B^{(k)}$ satisfies the intersection property if the $B^{(k)}$ uniformly satisfy the intersection property, i.e. if there is an r.e. set $A \subseteq \mathbb{N}$ with $B_i^{(k)} \cap B_j^{(k)} = \bigcup\{B_l^{(k)} \mid \langle k,i,j,l\rangle \in A\}$ for all $k,i,j \in \mathbb{N}$.

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

Theorem 3.15 *1. Let $\prod_{k=0}^{n}(X^{(k)}, B^{(k)}, \mu^{(k)})$ be a product of randomness spaces with finite measures. Let $(i_0, \ldots, i_l)$ be a vector of pairwise different indices i_j with $0 \leq i_j \leq n$. 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 randomness spaces 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 $\prod_{k=0}^{l}(X^{(i_k)}, B^{(i_k)}, \mu^{(i_k)})$.

3. Let $\prod_{k=0}^{\infty}(X^{(k)}, B^{(k)}, \mu^{(k)})$ be a product of randomness spaces with probability measures. Let $r : \mathbb{N} \longrightarrow \mathbb{N}$ 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 $\prod_{k=0}^{\infty}(X^{(r(k))}, B^{(r(k))}, \mu^{(r(k))})$.

Proof. 1. We prove the assertion for the case $l = n-1$. Iterated application gives the general case. By symmetry we may w.l.o.g. assume $(i_0, \ldots, i_l) = (1, \ldots, n)$. Define a projection $f : X^{(0)} \times \ldots \times X^{(n)} \longrightarrow X^{(1)} \times \ldots \times X^{(n)}$ by $f(x_0, \ldots, x_n) := (x_1, \ldots, x_n)$. We show that y is non–random if $f(y)$ is non–random. Let $(V_m)_m$ be a randomness test on $\prod_{k=1}^{n}(X^{(k)}, B^{(k)}, \mu^{(k)})$. Let $B := B^{(0)} \times \ldots \times B^{(n)}$, $C := B^{(1)} \times \ldots \times B^{(n)}$, $\mu := \mu^{(0)} \times \ldots \times \mu^{(n)}$ and $\mu' := \mu^{(1)} \times \ldots \times \mu^{(n)}$. By assumption, $(V_m)_m$ is C'–computable, i.e. $V_m = \bigcup\{C'_j \mid \langle m,j\rangle \in A\}$ for some r.e. set A. Since $f^{-1}(C\langle i_1, \ldots, i_n\rangle) = \bigcup\{B\langle i_0, \ldots, i_n\rangle \mid i_0 \in \mathbb{N}\}$, $(f^{-1}C_i)_i$ is B–computable. From this we conclude that $(f^{-1}C'_j)_j$ is B'–computable and finally that $(f^{-1}(V_m))_m$ is B'–computable. From $f^{-1}(V_m) = X^{(0)} \times V_m$ we obtain $\mu f^{-1}(V_m) = \mu^{(0)}(X^{(0)}) \cdot \mu'(V_m)$. Since $\mu^{(0)}$ is finite, $\mu^{(0)}(X^{(0)}) \leq 2^N$ for some $N \in \mathbb{N}$. Define $W_n := f^{-n}(V_{n+N})$. Then $(W_n)_n$ is a randomness test such that $f(y) \in \bigcap_{m\in\mathbb{N}} V_m$ implies $y \in \bigcap_{n\in\mathbb{N}} W_n$.

2. The proof is similar to that of 1.

3. First notice that B with $B_{\langle k,i\rangle} := \prod_{j=0}^{\infty} Y_j$, where $Y_k := B_i^{(k)}$ and $Y_j := X^{(k)}$ otherwise, is a numbering of a subbase of $\prod_{k=0}^{\infty} X^{(k)}$ which is b–equivalent to $\prod_{k=0}^{\infty} B^{(k)}$. Accordingly, C with $C_{\langle k,i\rangle} := \prod_{j=0}^{\infty} Y_j$, where $Y_k := B_i^{(r(k))}$ and $Y_j := X^{(r(k))}$ otherwise, is a numbering of a subbase of $\prod_{k=0}^{\infty} X^{(r(k))}$ which is b–equivalent to $\prod_{k=0}^{\infty} B^{(r(k))}$.
By Proposition 3.8 we may consider the numberings B and C. Define a projection $f : \prod_{k=0}^{\infty} X^{(k)} \longrightarrow \prod_{k=0}^{\infty} X^{(r(k))}$ by $f(x_0, x_1, \ldots) := (x_{r(0)}, x_{r(1)}, \ldots)$. Let $\mu := \prod_{k=0}^{\infty} \mu^{(k)}$ and $\mu' := \prod_{k=0}^{\infty} \mu^{(r(k))}$. Let $(V_m)_m$ be a randomness test on $(\prod_{k=0}^{\infty} X^{(r(k))}, C, \prod_{k=0}^{\infty} \mu^{(r(k))})$. $(V_m)_m$ is C'–computable. Because of $f^{-1}C_{\langle k,i\rangle} = B_{\langle r(k),i\rangle}$, the sequences $(f^{-1}C'_j)_j$ and $(f^{-1}V_m)_m$ are B'–computable. One checks that for every finite set $E \subseteq \mathbb{N}$ one has $\mu f^{-1}(\bigcup_{i\in E} C'_i) = \mu'(\bigcup_{i\in E} C'_i)$. We conclude $\mu f^{-1}(V_m) = \mu'(V_m)$ for all $m \in \mathbb{N}$. Therefore

$(f^{-1}V_m)_m$ is a randomness test. We conclude that the function f maps random elements to random elements. □

Examples 3.16 1. (see Calude, Hertling, Jürgensen, Weihrauch [4]) Let (Σ, B, μ) be the finite randomness space of Example 3.5.1 and $(\Sigma^\omega, \tilde{B}, \tilde{\mu})$ be the usual randomness space of infinite sequences over Σ, considered in Example 3.5.2. The topologies and measures of the randomness spaces $(\Sigma^\omega, B^\omega, \mu^\omega)$ and $(\Sigma^\omega, \tilde{B}, \tilde{\mu})$ coincide by definition and the numberings B^ω and $\tilde{B}$ are b–equivalent. In fact, they are equivalent in a stronger sense; for details see Calude, Hertling, Jürgensen, Weihrauch [4]. By Proposition 3.8 both spaces have the same random elements. In other words: the infinite product of the finite randomness space (Σ, B, μ) defines the usual randomness concept for infinite sequences in Σ^ω (Calude [3]).

2. The Lebesgue measure on $\mathbb{R}$ is σ–finite. Hence, for any $n \geq 1$ the finite product $(\mathbb{R}^n, B^n, \lambda^n)$ of the randomness space $(\mathbb{R}, B, \lambda)$ is a randomness space again.

3. The infinite product of the randomness space of Example 3.5.4 is a randomness space on the set $[0,1]^\omega$ of infinite sequences of real numbers. It is well–defined since $\tilde{\lambda}([0,1]) = 1$.

We conclude this section with "concrete" examples of random elements of a randomness space.

A sequence $(q_n)_n$ of dyadic rationals is called *computable*, iff there is a total recursive function f with $q_n = \nu_{\mathbb{D}}(f(n))$ for all n (for $\nu_{\mathbb{D}}$ compare Example 3.5.3). A real number x is called *left–computable* (*right–computable*), iff there is a computable non–decreasing (non–increasing) sequence $(q_n)_n$ of dyadic rationals with $\lim_{n\to\infty} q_n = x$, see Weihrauch [28, Ch. 3.8].

Examples 3.17 1. Let Σ be a finite alphabet. A subset $D \subseteq \Sigma^*$ is called *prefix–free* if no element of D is a proper prefix of another element of D. We call a function $f :\subseteq \Sigma^* \to \Sigma^*$ *self-delimiting* if its domain is prefix–free. A partial recursive self-delimiting function $f :\subseteq \Sigma^* \to \Sigma^*$ is called *universal* if for any partial recursive self-delimiting function $g :\subseteq \Sigma^* \to \Sigma^*$ there exists a constant c such that for all $x \in \operatorname{dom} g$ there is a $y \in \operatorname{dom} f$ with $|y| \leq |x| + c$ and $f(y) = g(x)$. Chaitin [9] proved that there exist universal self-delimiting partial recursive functions. The halting probability of a self-delimiting function f is defined by $\Omega_f := \sum_{x\in\operatorname{dom} f} 2^{-|x|}$. Note that this is always a well–defined left–computable number in the unit interval $[0,1]$. Chaitin [9] proved that the halting probability of a universal self-delimiting partial recursive function has a random binary representation. By Theorem 5.1 the halting probability is a random real number, i.e. a random element of the randomness space of Example 3.5.3 and of the space of Example 3.5.4.

2. Let $(U_n)_n$ be a universal randomness test on the space of real numbers $(\mathbb{R}, B, \lambda)$ of Example 3.5.3. 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. The set U_k is recursively open in Ko's [12] terminology. Therefore, by [12, Theorem 2.34] the right–hand boundary of any of these intervals is a left–computable real

number and the left–hand boundary of any of these intervals is a right–computable real number. More on left–computable random numbers can be found in Calude, Hertling, Khoussainov, Wang [6].

3. The construction of the last example can also be carried out on the space (Σ^ω, B, μ) of sequences (Example 3.5.2). For simplicity we consider $\Sigma = \{0, 1\}$. For a larger alphabet the proof is essentially the same. For $p, q \in \Sigma^\omega$ define $p < q :\iff p \neq q$ and $p_i < q_i$ where $i := \mu n[p_n \neq q_n]$, and $p \leq q :\iff p = q$ or $p < q$. For $p, q \in \Sigma^\omega$ with $p \leq q$ the set $[p; q] := \{r \in \Sigma^\omega \mid p \leq r \leq q\}$ is compact and called a *closed interval.* Notice that for the ordered set $(\Sigma^\omega, \leq)$ the supremum $\sup X$ exists for any subset $X \subseteq \Sigma^\omega$. Fix an arbitrary universal randomness test $(U_n)_n$ on Σ^ω. Furthermore fix a computable sequence $p \in \Sigma^\omega$ with $\mu([0^\omega; p]) \leq 1/4$. This sequence is an element of U_1 because U_1 contains all non-random sequences. We claim that the sequence $r := \sup\{q \in \Sigma^\omega \mid [p; q] \subseteq U_1\}$ is a random sequence. For the sake of a contradiction, assume that r is non-random. Then it is an element of U_1. The set U_1 is open. Hence there is a prefix v of r with $v\Sigma^\omega \subseteq U_1$. Let w be the lexicographical successor of v with $|w| = |v|$. It exists because $\mu([0^\omega; p]) \leq 1/4$ and $\mu(U_1) \leq 1/2$ imply that $v \notin \{1\}^*$. We obtain $r < w0^\omega$ and $[p; w0^\omega] \subseteq U_1$, contradicting the definition of r. Hence, r is random. We can approximate r by a non-decreasing computable sequence of words. Let f be a total recursive function with $U_1 = \bigcup\{\nu(f(i))\Sigma^\omega \mid i \in \mathbb{N}\}$. Fix a prefix v of p with $v\Sigma^\omega \subseteq U_1$. For $n \in \mathbb{N}$ define the word w_n by
$$\begin{aligned} |w_n| &= \max(\{|v|\} \cup \bigcup_{i \leq n} \{|\nu f(i)|\}) \quad \text{and} \\ w_n 1^\omega &= \sup\{q \in \Sigma^\omega \mid [p; q] \subseteq v\Sigma^\omega \cup \bigcup_{i \leq n} \nu f(i)\Sigma^\omega\}. \end{aligned}$$
Then the sequence $(w_n)_n$ is a computable sequence of words (that means that there is a computable function $g : \mathbb{N} \to \mathbb{N}$ with $w_n = \nu(g(n))$ for all n) such that for all n either $w_n 1^\omega < w_{n+1} 1^\omega$ or there is a number l with $w_{n+1} = w_n 1^l$. By using the fact that any interval $[p; q] \subseteq U_1$is compact one shows that $(w_n 1^\omega)_n$ converges to r.

4 Randomness Preserving Transformations

The main result of this section is a theorem giving conditions under which a computable function between randomness spaces preserves randomness. This corrects and extends a result by Schnorr [21].

Let Σ and $\tilde{\Sigma}$ be two finite alphabets. A function $g :\subseteq \Sigma^* \to \tilde{\Sigma}^*$ is called *monotonic*, iff $g(vw) \in g(v)\Sigma^*$ for all $v, vw \in \operatorname{dom} g$. And it is called *unbounded on* $p \in \Sigma^\omega$, iff for all $n \in \mathbb{N}$ there is some prefix $v \in \operatorname{dom} f$ of p with $|g(v)| \geq n$. The function $f :\subseteq \Sigma^\omega \to \tilde{\Sigma}^\omega$ *induced* by a monotonic function $g :\subseteq \Sigma^* \to \tilde{\Sigma}^*$ is defined by

1. $\operatorname{dom} f = \bigcap_{n \in \mathbb{N}}(g^{-1}(\tilde{\Sigma}^n \tilde{\Sigma}^*)\Sigma^\omega)$ (i.e. $p \in \operatorname{dom} f$ iff g is unbounded on p),

2. $f(p) \in g(v)\Sigma^\omega$ for any $p \in \operatorname{dom} f$ and for any prefix $v \in \operatorname{dom} g$ of p.

It is clear that f is well-defined by these conditions. A function $f :\subseteq \Sigma^\omega \to \tilde{\Sigma}^\omega$ is called a *computable functional*, iff there is a computable, monotonic function $g :\subseteq \Sigma^* \to \tilde{\Sigma}^*$ which induces f.

Schnorr claimed in [21, Satz 6.5]: *if* $f :\subseteq \{0,1\}^\omega \to \{0,1\}^\omega$ *is a computable functional satisfying* ($\exists$ *constant* K) ($\forall$ *measurable* $A \subseteq \{0,1\}^\omega$) $\mu(f^{-1}(A)) \leq K\mu(A)$, *and if* $x \in \operatorname{dom} f$ *is random, then also* $f(x)$ *is random.* This, as well as Lemma 6.6 and Satz 6.7 in [21], is not completely correct, as was also observed by Wang, see Hertling and Wang [11]. The following proposition gives a counterexample. Note that the function in the following example satisfies the measure–theoretic condition above for any constant K since its domain has measure zero.

Proposition 4.1 *Consider the randomness space from Example 3.5.2 with* $\Sigma = \{0,1\}$. *There exist a random element* $r \in \{0,1\}^\omega$ *and a computable functional* $f :\subseteq \{0,1\}^\omega \to \{0,1\}^\omega$ *with* $\operatorname{dom} f = \{r\}$ *and* $f(r) = 0^\omega$.

Proof. Let $(w_n)_n$ be a computable sequence of words $w_n \in \Sigma^*$ such that the sequence $(w_n 1^\omega)_n$ is non–decreasing and the limit $r = \sup\{w_n 1^\omega \mid n \in \mathbb{N}\}$ in Σ^ω is random, see Example 3.17.3. We define a monotonic computable function $g :\subseteq \Sigma^* \to \Sigma^*$ by

$$g(v) := \begin{cases} 0^{|v|} & \text{if } v \text{ is a prefix of } w_m \text{ for some } m \geq |v| \\ \uparrow & \text{otherwise.} \end{cases}$$

The function f induced by g has the desired properties. □

In fact, one needs an additional condition on the domain of definition of f. For example it would be sufficient to demand that the domain $\operatorname{dom} f$ has measure 1. A more general condition will be formulated in Theorem 4.7 below.

We wish to consider transformations from one randomness space to another one. For such transformations we need a computability notion. 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 subbases. We call a function $f :\subseteq X \to Y$ *computable*, iff there is a B'–computable sequence $(U_n)_n$ of open subsets of X with $f^{-1}(C_n) = U_n \cap \operatorname{dom} f$, for all n.

We observe that this definition generalizes the notion of a computable functional if one does not care about the precise domain of definition. We omit the proof of the following proposition.

Proposition 4.3 *Let* Σ *and* $\tilde{\Sigma}$ *be two finite alphabets and* B *and* C *the corresponding numberings of bases considered in Example 3.5.2. A function* $f :\subseteq \Sigma^\omega \to \tilde{\Sigma}^\omega$ *is computable if and only if there is a computable functional* $g :\subseteq \Sigma^\omega \to \tilde{\Sigma}^\omega$ *with* $f(p) = g(p)$ *for all* $p \in \operatorname{dom} f$.

For the special case of T_0–spaces Definition 4.2 is equivalent to the definition of computable functions via standard representations by Kreitz and Weihrauch [14, 28, 30]. The idea is the same as the classical definition of relative computability via numberings. If X and Y are two sets and $\gamma :\subseteq \Sigma^\omega \to X$ and $\delta :\subseteq \tilde{\Sigma}^\omega \to Y$ are representations, that is, surjective mappings, then a function $f :\subseteq X \to Y$ is called (γ, δ)*–computable*, iff there is a computable functional $g :\subseteq \Sigma^\omega \to \tilde{\Sigma}^\omega$ with $f\gamma(p) = \delta g(p)$ for all $p \in \operatorname{dom} f\gamma$. If (X, B) is a T_0–space (in this case every element of X can be identified by the set of its subbase neighbourhoods), then one defines the *standard representation* $\delta_B :\subseteq \{0,1\}^\omega \to X$ by

$$\delta_B(p) = x \iff \{i \in \mathbb{N} \mid x \in B_i\} = \{i \in \mathbb{N} \mid 10^{i+1}11 \text{ is a subword of } p\}.$$

Theorem 4.4 *Let (X, B) and (Y, C) be two T_0–spaces with total numberings B and C of subbases. Then a function $f :\subseteq X \to Y$ is computable if and only if it is (δ_B, δ_C)–computable.*

Proof. First we assume that f is computable. We wish to construct a computable functional $g :\subseteq \{0,1\}^\omega \to \{0,1\}^\omega$ with $f\delta_B(p) = \delta_C g(p)$ for all $p \in \operatorname{dom} f\delta_B$. Therefore we have to construct a computable function $h :\subseteq \{0,1\}^* \to \{0,1\}^*$ which induces g. Let $A \subseteq \mathbb{N}$ be an r.e. set with $f^{-1}(C_n) = \operatorname{dom} f \cap \bigcup_{\langle n,i\rangle \in A} B'_i$. If A is empty the function f has empty domain and is obviously also (δ_B, δ_C)–computable. So we assume that A is nonempty. Let $(\langle n_k, i_k\rangle)_k$ be a recursive enumeration of A. For a finite word $w \in \{0,1\}^*$ we define $\mathrm{En}(w) := \{j \mid 10^{j+1}11 \text{ is a subword of } w\}$ and a finite set of numbers $S(w)$ by

$$S(w) := \{n_k \mid k \leq |w| \ \&\ D_{i_k} \subseteq \mathrm{En}(w)\} \setminus \bigcup \{S(v) \mid v \text{ is a strict prefix of } w\}.$$

Let $x(w)$ be a finite word which encodes the set $S(w)$: if $S(w) = \emptyset$, we set $x(w) := 1$, otherwise $x(w) := 10^{m_1+1}110^{m_2+1}11 \ldots 10^{m_l+1}11$ where $m_1 < m_2 < \ldots < m_l$ is the ordered list of numbers in $S(w)$. We define the function $h : \{0,1\}^* \to \{0,1\}^*$ by $h(\varepsilon) := \varepsilon$ and $h(vd) := h(v)x(vd)$ for $v \in \{0,1\}^*$ and $d \in \{0,1\}$. We claim that this function h has the desired properties. It is computable, total and monotonic. The induced computable functional $g : \{0,1\}^\omega \to \{0,1\}^\omega$ is also total because $|h(v)| \geq |v|$ for all words v. Assume that $p \in \operatorname{dom} f\delta_B$ and $j \in \mathbb{N}$. We have to show that

$$f\delta_B(p) \in C_j \iff 10^{j+1}11 \text{ is a subword of } g(p).$$

If $f\delta_B(p) \in C_j$, then there is a k with $n_k = j$ and $\delta_B(p) \in B'_{i_k}$. Since the sequence p "enumerates" all numbers l with $\delta_B(p) \in B_l$ there is a smallest prefix w of p with $D_{i_k} \subseteq \mathrm{En}(w)$ and $|w| \geq k$. Hence, the number n_k is an element of $S(w)$ or of $S(v)$ for a strict prefix v of w. The definition of h tells us that $h(w)$ contains the subword $10^{n_k+1}11 = 10^{j+1}11$ (it is either contained in $x(w)$ or in $x(v)$ for some strict prefix v of w). Hence, $g(p)$ contains this word as a subword. If on the other hand $10^{j+1}11$ is a subword of $g(p)$, then it is also a subword of $h(w)$ for some sufficiently large prefix w of p. By definition of h this implies that there is a k with $n_k = j$ and $D_{i_k} \subseteq \mathrm{En}(w)$. But $D_{i_k} \subseteq \mathrm{En}(w)$ implies $\delta_B(p) \in B'_{i_k}$. By the definition of A respectively of $\langle n_k, i_k\rangle$ and with $n_k = j$ we conclude $\delta_B(p) \in f^{-1}(C_j)$, hence $f\delta_B(p) \in C_j$. This finishes the proof of the first half of the theorem.

For the proof of the converse direction we assume that f is (δ_B, δ_C)–computable. We have to construct an r.e. set $A \subseteq \mathbb{N}$ with $f^{-1}(C_n) = \operatorname{dom} f \cap \bigcup_{\langle n,i\rangle \in A} B'_i$ for all n, i. Let $g :\subseteq \{0,1\}^\omega \to \{0,1\}^\omega$ be a computable functional with $f\delta_B(p) = \delta_C g(p)$ for all $p \in \operatorname{dom} f$, and let $h :\subseteq \{0,1\}^* \to \{0,1\}^*$ be a computable function which induces g. We define A by

$$A := \{\langle n, i\rangle \mid (\exists v \in \operatorname{dom} h)\ D_i = \mathrm{En}(v) \ \&\ n \in \mathrm{En}(h(v))\}.$$

It is clear that A is r.e. Fix a number n. We have to show that $f^{-1}(C_n) = \operatorname{dom} f \cap \bigcup_{\langle n,i\rangle \in A} B'_i$. First we show "$\subseteq$". Consider an element $x \in f^{-1}(C_n)$. Then $x \in \operatorname{dom} f$. Choose an arbitrary δ_B–name p for x and set $q := g(p)$. The binary sequence q is a δ_C–name for $f(x)$ and must contain the subword $10^{n+1}11$. Then there must be a prefix $v \in \operatorname{dom} h$ of p such that $10^{n+1}11$ is a subword of $h(v)$, that is, $n \in \mathrm{En}(h(v))$. Certainly, $x \in \bigcap_{j \in \mathrm{En}(v)} B_j$. Hence, if i is a number with $D_i = \mathrm{En}(v)$, then $x \in B'_i$. By definition of A we also have $\langle n, i\rangle \in A$. This shows "$\subseteq$". For the proof of "$\supseteq$" consider a number

$\langle n,i\rangle \in A$ and an element $x \in B'_i \cap \operatorname{dom} f$. There is a word $v \in \operatorname{dom} h$ with $D_i = \operatorname{En}(v)$ and $n \in \operatorname{En}(h(v))$. This word can be extended to a δ_B–name for x. The fact that h induces g implies $f(x) \in C_n$. That was the assertion. □

For real number functions this computability notion derived from the numbering B from Example 3.5.3 is also the usual computability notion considered for example by Grzegorczyk [10], Lacombe [15], Pour-El and Richards [19], Weihrauch and Kreitz [14, 28, 30], Ko [12], and others; for more references see [28, 30].

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 too large sets to too small sets.

Definition 4.5 Let (X, B, μ) be a randomness space. A set $D \subseteq X$ is called *fast enclosable* if it is measurable and if there is a B'–computable sequence $(U_n)_n$ of open sets with $D \subseteq U_n$ and $\mu(U_n \setminus D) \leq 2^{-n}$ for all n.

Definition 4.6 Let (X, B, μ) and $(Y, C, \tilde{\mu})$ be two randomness spaces. A function $f :\subseteq X \to Y$ is called *recursively measure–bounded* if $\operatorname{dom} f$ is measurable and there is a total recursive function r such that for all open sets $V \subseteq Y$:

$$\tilde{\mu}(V) \leq 2^{-r(n)} \Rightarrow \mu(f^{-1}(V)) \leq 2^{-n}\,.$$

In fact, it suffices to require this only for all sets $V = \bigcup_{j \in D_i} C'_j$ $(i \in \mathbb{N})$ where C' is the derived numbering of C. 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 4.7 *Let (X, B, μ) and $(Y, C, \tilde{\mu})$ be randomness spaces. Let $f :\subseteq X \to Y$ be a computable, recursively measure–bounded function with a fast enclosable domain. If $x \in \operatorname{dom} f$ 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

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

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 $f^{-1}(C_n) = \operatorname{dom} f \cap T_n$. Then $f^{-1}(C'_n) = \operatorname{dom} f \cap T'_n$ for each n. The sequence $(T'_n)_n$ is also B'–computable by Lemma 3.3. Let $A_{T'} \subseteq \mathbb{N}$ be an r.e. set which shows that $(T'_n)_n$ is B'–computable. The sequence $(R_n)_n$ with

$$R_n := \bigcup_{\langle n,j\rangle \in A_V} T'_j = \bigcup \{B'_i \mid (\exists j)\langle n,j\rangle \in A_V \text{ and } \langle j,i\rangle \in A_{T'}\}$$

is B'–computable and satisfies $f^{-1}(V_n) = R_n \cap \operatorname{dom} f$. Now let $r : \mathbb{N} \to \mathbb{N}$ be a total recursive function with $\mu(f^{-1}(\tilde{U})) \leq 2^{-n}$ for all open subsets $\tilde{U} \subseteq Y$ with $\tilde{\mu}(\tilde{U}) \leq 2^{-r(n)}$, and let $(S_n)_n$ be a B'–computable sequence of open subsets of X which encloses $\operatorname{dom} f$ in the sense $\operatorname{dom} f \subseteq S_n$ and $\mu(S_n \setminus \operatorname{dom} f) \leq 2^{-n}$ 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 (proof straightforward). It satisfies

$$f^{-1}(V_{r(n+1)}) = U_n \cap \operatorname{dom} f \quad \text{for all } n \tag{2}$$

because of $f^{-1}(V_m) = R_m \cap \operatorname{dom} f$, for all m, and $\operatorname{dom} f \subseteq S_l$, for all l. From (2) we obtain for all n:

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

Finally, (2) implies (1). This ends the proof. □

In our counterexample in Proposition 4.1 the set $\operatorname{dom}(f) = \{r\}$, r random, cannot be fast enclosable. We remark that for infinite sequences Levin [16] 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.

In the rest of this section we assume that Σ is an arbitrary finite alphabet with at least two elements. As an application we show that randomness of a vector or a sequence of elements of Σ^ω can be expressed directly over the randomness space Σ^ω. For $p, q, p^{(1)}, \ldots, p^{(k)} \in \Sigma^\omega$ we define $\langle p \rangle := p$, $\langle p, q \rangle := p(0)q(0)p(1)q(1)p(2)q(2)\ldots$, and recursively $\langle p^{(1)}, \ldots, p^{(k)} \rangle := \langle \langle p^{(1)}, \ldots p^{(k-1)} \rangle, p^{(k)} \rangle$. For a sequence $(p^{(k)})_k$ of sequences we define $\langle p^{(0)}, p^{(1)}, \ldots \rangle(\langle i, j \rangle) := p^{(i)}(j)$ for all i, j.

Corollary 4.8 *1. Let $k \geq 1$. A vector $(p^{(1)}, \ldots, p^{(k)}) \in (\Sigma^\omega)^k$ is random, iff the sequence $\langle p^{(1)}, \ldots, p^{(k)} \rangle \in \Sigma^\omega$ is random.*

2. A sequence $(p^{(k)})_k \in (\Sigma^\omega)^\omega$ of sequences is random, iff the sequence $\langle p^{(0)}, p^{(1)}, \ldots \rangle \in \Sigma^\omega$ is random.

Proof. (1) The mapping $\langle , \rangle : (\Sigma^\omega)^k \to \Sigma^\omega$ is a computable measure invariant homeomorphism and its inverse is computable as well. The assertion follows from Theorem 4.7.

(2) Also the mapping $\langle , \rangle : (\Sigma^\omega)^\omega \to \Sigma^\omega$ is a computable measure invariant homeomorphism and its inverse is computable as well. Again the assertion follows from Theorem 4.7. □

We finish this section by two well–known examples of randomness preserving transformations: given a sequence one chooses a subsequence and rearranges it by applying an injective total recursive function to its coefficients or by choosing only components with indices at which an "independently random" sequence has 1's. The first result seems to be folklore. It is stated for example in Book, Lutz, Martin [1], Lemma 3.4.

Corollary 4.9 *Let $r : \mathbb{N} \to \mathbb{N}$ be a total recursive injective function. If a sequence $p = p(0)p(1)p(2)\ldots \in \Sigma^\omega$ is random, then also the sequence $p(r(0))p(r(1))p(r(2))\ldots$ is random.*

Proof. This is a special case of Theorem 3.15.3. □

The second result is due to van Lambalgen [25, Theorem 5.8]. For considerations which can be used for a proof see [24].

Corollary 4.10 *(van Lambalgen [25]) Let $(p, q) \in (\Sigma^\omega)^2$ be a random pair of sequences. Define a new sequence by erasing out of p all the components $p(i)$ with $q(i) = 0$. The new sequence is random also.*

Proof. First, we observe that the new sequence is well–defined since q contains infinitely many 1's. Therefore notice that the randomness of (p, q) implies that q is random by Theorem 3.15 and, hence, contains infinitely many 1's. The "new" sequence is defined more formally to be the sequence $F(p, q)$ where the function

$$F : \Sigma^\omega \times \{q \in \Sigma^\omega \mid q \text{ contains infinitely many 1's}\} \to \Sigma^\omega$$

is defined by

$$F(p, q)(i) := p(\text{position of the } (i + 1)\text{–th 1 in } q)\,.$$

The function $F :\subseteq (\Sigma^\omega)^2 \to \Sigma^\omega$ is computable. Its domain is fast enclosable because it has μ^2–measure 1 (it is the product of two sets with μ–measure 1). Using Fubini's Theorem one shows that F is measure invariant: it is sufficient to show for $w \in \Sigma^*$ that $\mu^2(F^{-1}(w\Sigma^\omega)) = |\Sigma|^{-|w|}$. This follows from $\int_{\Sigma^\omega} \chi_{F^{-1}(w\Sigma^\omega)}(p, q) d\mu(p) = |\Sigma|^{-|w|}$ for any $q \in \Sigma^\omega$ containing infinitely many 1's and from Fubini's Theorem. Now Theorem 4.7 gives the assertion. □

5 Random Real Numbers

Randomness of real numbers is usually introduced via the the b-ary representations. Calude and Jürgensen [7, 2] 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 the real numbers given in Example 3.5. This is done also for vectors and infinite sequences of reals. Furthermore we show that 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 $b \geq 2$. 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 by

$$\rho_b : \Sigma_b^\omega \to [0, 1], \qquad \rho_b(p(0)p(1)p(2)\ldots) := \sum_{n=0}^{\infty} p(i)b^{-(i+1)}\,.$$

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 rationals 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

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

which we call the b-ary representation of vectors in $[0,1]^k$. In the following theorem we consider the randomness spaces $(\mathbb{R}, B, \lambda)$ and $([0,1], \tilde{B}, \tilde{\lambda})$ introduced in Example 3.5 and their products according to the end of Section 3. The theorem is a slightly more general formulation of a result contained in Weihrauch [29]. For a vector $(x_1, \ldots, x_n)$ of reals the *fractional part* of $(x_1, \ldots, x_n)$ is the unique real vector $(y_1, \ldots, y_n) \in [0,1)^n$ such that the difference $(x_1 - y_1, \ldots, x_n - y_n)$ is a vector of integers.

Theorem 5.1 *Let $n \geq 1$, $b \geq 2$. For a vector $(x_1, \ldots, x_n) \in \mathbb{R}^n$ 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 $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ be an integer vector. The translation $T : (\mathbb{R}^n, B^n) \to (\mathbb{R}^n, B^n)$ with $T(y_1, \ldots, y_n) := (y_1 + z_1, \ldots, y_n + z_n)$ is a total, computable, measure invariant mapping. Hence, by Theorem 4.7, if $(y_1, \ldots, y_n) \in \mathbb{R}^n$ is random (in $(\mathbb{R}^n, B^n, \lambda^n)$), also $(y_1 + z_1, \ldots, y_n + z_n)$ 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 $\operatorname{dom} f = [0,1]^n$ and $f(x) = x$ for all $x \in \operatorname{dom} f$ is computable, measure invariant, and its domain is a fast enclosable subset of $(\mathbb{R}^n, B^n, \lambda^n)$. This, together with Theorem 4.7 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 $\tilde{\lambda}^n((f^{-1})^{-1}(A)) \leq \lambda^n(A)$ for all measurable $A \subseteq \mathbb{R}^n$. Using Theorem 4.7 we conclude "(3) $\Rightarrow$ (2)".

The mapping ρ_b^n itself is computable, total, and measure invariant. Hence, Theorem 4.7 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 $x \in \operatorname{dom} f := [0,1]^n \cap (\mathbb{R} \setminus \mathbb{Q})^n$. 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 4.7 f preserves randomness. If $x \in [0,1]^n$ is random, then it is a vector of random numbers by Theorem 3.15, hence a vector of irrationals, 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:

Theorem 5.2 *(Calude and Jürgensen [7]) For integers $b, c \geq 2$ a real number $x \in [0,1]$ has a random ρ_b–name, iff 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 $b \geq 2$. 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.

Before we turn our attention to the real numbers let us collect a few facts about random infinite sequences of real numbers in $[0,1]^\omega$. A sequence $(x_n)_n \in [0,1]^\omega$ of real numbers is called *uniformly distributed* if for any pair a, b of real numbers with $0 \leq a \leq b \leq 1$ 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 5.4 *Every random sequence of reals in $[0,1]^\omega$ is uniformly distributed.*

Proof. This follows immediately from Theorem 5.3 and from Theorem 3.6 of Calude, Hertling, Khoussainov [5] which states that any sequence of reals in $[0,1]^\omega$ with a random ρ_b^ω-name, $b \geq 2$ arbitrary, is uniformly distributed. □

In Proposition 3.15 we observed that a sequence of reals 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 reals such that all of its components are random? This is true.

Theorem 5.5 *There is a non–random sequence $(x_n)_n$ of reals 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 $0 \leq k < l \leq n$) the vector $(x_{i_0}, \ldots, x_{i_n})$ is random.*

Proof. Let $(y_n)_n$ be an arbitrary random sequence of reals in $[0,1]^\omega$. Then by Theorem 3.15 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 reals 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 $\frac{1}{2}x_n$. 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 $U_n := \{(z_m)_m \in [0,1]^\omega \mid z_n < 2^{-n}\}$). 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. □

We turn our attention to arithmetic properties of random numbers and vectors. We have already remarked 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 all the functions commonly in use.

Theorem 5.6 *Let $n \geq 1$ 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 $x \in \operatorname{dom} f$ is random, then also $f(x)$ is random.*

Proof. Let $z \in \operatorname{dom} f$ be random. Then $f'(z) \neq 0$ by assumption. There is a $k \in \{1, \ldots, n\}$ such that the partial derivative $\frac{\partial f}{\partial x_k}(z) \neq 0$ is non-zero. By symmetry we can assume $k = n$ w.l.o.g. Since the derivative f' is continuous and the domain of f is open there is an open rectangle D with the following properties: (1) $z \in D \subseteq \operatorname{dom} f$, (2) D has rational endpoints, (3) the sidelength of D in any coordinate is at most 1, (4) for all $y \in D$ we have $|\frac{\partial f}{\partial x_n}(y)| \geq c := \frac{1}{2}|\frac{\partial f}{\partial x_n}(z)|$. We claim that the restricted function $g := f|_D$ satisfies all assumptions of Theorem 4.7. 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 is bounded from below by a positive constant on D. We claim that it satisfies

$$\lambda^n(g^{-1}(U)) \leq \frac{2}{c}\lambda(U) \tag{3}$$

for any open subset $U \subseteq \mathbb{R}$. In fact, by taking the sign of $\frac{\partial f}{\partial x_n}(z)$ into account one can show that it satisfies even $\lambda^n(g^{-1}(U)) \leq \frac{1}{c}\lambda(U)$ for any open $U \subseteq \mathbb{R}$. Since any open $U \subseteq \mathbb{R}$ can be written as a disjoint countable union of open intervals (the connected components of U) it is sufficient to prove the claim (3) for open intervals $U = (a, b)$. Fix real numbers $a < b$. Fix a vector $(x_1, \ldots, x_{n-1}) \in \mathbb{R}^{n-1}$ such that there is an $x \in \mathbb{R}$ with $(x_1, \ldots, x_{n-1}, x) \in D$ and consider the function $h :\subseteq \mathbb{R} \to \mathbb{R}$ with $h(x) := g(x_1, \ldots, x_{n-1}, x)$. Note that the domain of h is an open interval. We claim that

$$\lambda(h^{-1}((a, b)) \leq \frac{2}{c}(b - a)\,. \tag{4}$$

If $h^{-1}((a, b))$ is empty this is clearly true. Assume that $h^{-1}((a, b))$ is not empty and fix a real y with $h(y) \in (a, b)$. We shall show

$$h^{-1}((a, b)) \subseteq (y - \frac{1}{c}(b - a), y + \frac{1}{c}(b - a)) \tag{5}$$

This implies (4). Let $x \in h^{-1}((a, b))$. By the Intermediate Value Theorem there is a real number ξ lying in $[y, x]$ if $y \leq x$ respectively in $[x, y]$ if $x \leq y$ with the property

$$h(y) - h(x) = h'(\xi) \cdot (y - x)\,.$$

The point $(x_1, \ldots, x_{n-1}, \xi)$ lies in D, hence $|h'(\xi)| \geq c$ by our fourth assumption on D. We conclude $|h(y) - h(x)| \geq c|y - x|$. Together with $|h(y) - h(x)| \leq b - a$ we obtain

$$b - a \geq c|y - x|$$

and this proves our claim (5), and hence also (4). The inequality (4) is used in the following application of Fubini's Theorem where

$$D' := \{x = (x_1, \ldots, x_{n-1}) \in \mathbb{R}^{n-1} \mid (\exists x \in \mathbb{R})\ (x_1, \ldots, x_{n-1}, x) \in D\}$$

is the projection of D on the first $n - 1$ components:

$$\lambda^n(g^{-1}((a, b))) \;=\; \int_D \chi_{g^{-1}((a,b))}(x_1, \ldots, x_n) d\lambda(x_1, \ldots, x_n)$$

$$\begin{aligned} &= \int_{D'} \left(\int_{\mathbb{R}} \chi_{g^{-1}((a,b))}(x_1,\ldots,x_n) d\lambda(x_n) \right) d\lambda^{n-1}(x_1,\ldots,x_{n-1}) \\ &\leq \int_{D'} \frac{2}{c}(b-a) d\lambda^{n-1}(x_1,\ldots,x_{n-1}) \\ &\leq \frac{2}{c}(b-a)\,. \end{aligned}$$

In the last step we used the assumption that the sidelength of D and hence also of D' in each coordinate of $\mathbb{R}^n$ is at most one. This proves our claim (3) and ends the proof of Theorem 5.6. □

Let $n \geq 1$ 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 $\sum_{k \in \mathbb{N}^n}^{\infty} a_k(x-z)^k$ where $y^k = y_1^{k_1} \cdot \ldots \cdot y_n^{k_n}$ for $y = (y_1,\ldots,y_n) \in \mathbb{R}^n$ and $k = (k_1,\ldots,k_n) \in \mathbb{N}^n$.

Theorem 5.7 *Let $U \subseteq \mathbb{R}$ be open and $f : U \to \mathbb{R}$ be an analytic function which is computable on any compact subset of its domain. If $x \in \operatorname{dom} f$ is random, then also $f(x)$ is random.*

Proof. If f is an analytic function which is computable on any compact subset of its domain U, then its partial derivatives $\frac{\partial f}{\partial x_k}$ (for $k \in \{1,\ldots,n\}$) are also analytic functions and computable on any compact subset of U (their computability can be proved by following the proof of Theorem 2, p. 53 of Pour-El and Richards [19]). Fix a rational compact rectangle K in the domain of f and consider the restriction of f to this set. The set of zeros of f' has measure 0. For each $m \in \mathbb{N}$ (uniformly in m) we can compute a finite union of balls B_i^n in $\mathbb{R}^n$ which cover the set of zeros of f' in K and are contained in $\{x \in U \mid |f'(x)| \leq 2^{-m}\}$. Hence, since the measure of $\{x \in U \mid |f'(x)| \leq 2^{-m}\}$ tends to zero for m tending to infinity, we can construct a randomness test wich contains all zeros of f' in K. Thus, all zeros of f' in K, and therefore all zeros of f' are non–random. The assertion follows now from Theorem 5.6. □

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 5.6), 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 $x := \rho_2(p(0)0p(2)0p(4)0\ldots)$ and $y := \rho_2(0p(1)0p(3)0p(5)\ldots)$ are non–random, but their sum $x+y = \rho_2(p(0)p(1)p(2)\ldots)$ is random.

We end this section with a simple topological observation.

Proposition 5.8 *For $n \geq 2$ 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. □

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 of $\mathbb{N}$ as a randomness space, based on its standard topology. 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 $2^{\mathbb{N}} = \{A \mid A \subseteq \mathbb{N}\}$ 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? One possibility to introduce randomness on $2^{\mathbb{N}}$ is to identify it with the usual randomness space (Σ^ω, B, μ) of Example 3.5.2 via the mapping $\chi : 2^{\mathbb{N}} \to \Sigma^\omega$ 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 $n \notin A$). This mapping is a bijection. Then a set of numbers is random if and only if its characteristic function is random. But the induced topology τ_χ, that is, the topology on $2^{\mathbb{N}}$ induced by the base $\{\chi^{-1}(w\Sigma^\omega) \mid w \in \Sigma^*\}$ is not the standard topology on $2^{\mathbb{N}}$. The standard topology on $2^{\mathbb{N}}$ is usually considered to be the topology induced by the base $\{O_E \mid E \subseteq \mathbb{N} \text{ finite}\}$ where $O_E := \{A \subseteq \mathbb{N} \mid E \subseteq A\}$ for finite subsets E of $\mathbb{N}$. Let us call this topology τ.

Lemma 6.1 *1. The topology τ is a strict 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 words by

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

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 word $w = w(1) \ldots w(|w|) \in \Sigma^*$ 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. □

The topologies τ and τ_χ are not the same. But their σ-algebras are the same. Hence, we can transfer the measure on Σ^ω via χ^{-1} to $2^{\mathbb{N}}$. 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 3.5.2). Notice that $\mu(O_E) = 2^{-|E|}$ for any finite set $E \subseteq \mathbb{N}$. Remember that $D : \mathbb{N} \to \{E \subseteq \mathbb{N} \mid E$ finite$\}$ is a standard numbering of the set of finite subsets of $\mathbb{N}$. Using the numbering O of basic τ-open sets defined by $O_i := O_{D_i}$ we obtain a randomness space

$$(2^{\mathbb{N}}, O, \mu)\,.$$

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

Which properties does this randomness space have? What are its random elements?

It is clear that the randomness space 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 3.6. The measure μ is weakly bounded. This immediately implies by Theorem 3.11 that 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 also.

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 $\mu(U) \geq \mu(O_E) = 2^{-|E|}$. 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 counterintuitive 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 randomness space 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.*

One can express this also negatively:

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

Proof. 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 $\mu(V_n) = \mu(U_n) \leq 2^{-n}$ since χ is measure invariant 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 $U_n = \bigcup\{O_{D_i} \mid \langle n,i\rangle \in \tilde{C}\}$ and, given an index i of a finite set D_i one can compute ν-indices for the finitely many words in the set W_{D_i} considered in the proof of Lemma 6.1, and $V_n = \bigcup\{W_{D_i}\Sigma^\omega \mid \langle n,i\rangle \in \tilde{C}\}$. This ends the proof of the first implication.

Now we are going to 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 $\mu(U_n) = \mu(\chi(U_n)) \leq \mu(V_n) \leq 2^{-n}$ 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

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

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 the lemma following immediately after the proof 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. □

Lemma 6.5 *Let $V \subseteq \Sigma^\omega$ be an open set and $A \subseteq \mathbb{N}$ be a set such that $\chi_B \in V$ for all $B \supseteq A$. Then there is a finite set $E \subseteq A$ with $\chi(O_E) \subseteq V$.*

Note that $E \subseteq A$ is equivalent to $A \in O_E$. The statement of the lemma can also be expressed more elegantly: if a set $A \subseteq \mathbb{N}$ and all sets $B \supseteq A$ are elements of a τ_χ-open subset $U \subseteq 2^{\mathbb{N}}$, then they are already in the τ-interior of U.

Proof. We assume that the assertion is false. Set $E_n := A \cap \{0,\ldots,n\}$ for each n. Then for each n there is a sequence $q_n \in \chi(O_{E_n}) \setminus V$. The set $\Sigma^\omega \setminus V$ is compact. Thus, the sequence $(q_n)_n$ has an accumulation point p in $\Sigma^\omega \setminus V$. We can fix a strictly increasing function $g : \mathbb{N} \to \mathbb{N}$ such that the first $n+1$ digits of $q_{g(n)}$ and of p are identical, for each n. We know $q_{g(n)} \in \chi(O_{E_{g(n)}}) \subseteq \chi(O_{E_n})$ since $g(n) \geq n$ (g is strictly increasing!) implies $E_{g(n)} \supseteq E_n$. Hence, if $i \in E_n$, then $q_{g(n)}(i) = 1$, and thus also $p(i) = 1$. This means $p \in \chi(O_{E_n})$, or in other words, $E_n \subseteq \chi^{-1}(p)$. This, being true for all n, implies $A \subseteq \chi^{-1}(p)$. But the assumption of the lemma was that such a sequence p must lie in V. Contradiction. Hence, there is a finite set $E \subseteq A$ with $\chi(O_E) \subseteq V$. □

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, $(U_n)_n$ is even a universal randomness test on $2^{\mathbb{N}}$ if $(V_n)_n$ is a universal randomness test on Σ^ω. To see this, use the observation in the first part of the proof, namely the observation that $(\chi(\tilde{U}_n))_n$ is a randomness test on Σ^ω if $(\tilde{U}_n)_n$ is a randomness test on $2^{\mathbb{N}}$.

Note that especially randomness of $p \in \Sigma^\omega$ implies randomness of $\chi^{-1}(p)$. The converse is not true: take a random sequence $p = p(0)p(1)p(2)p(3)\ldots \in \Sigma^\omega$. Then the sequence $q = p(0)0p(2)0\ldots$ 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? 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 3.17.3). 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 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 $\mu(U) < 1$. 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 $E_n := \{f(0), \ldots, f(n-1)\}$ 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*, iff it is r.e. and its complement is immune.

Corollary 6.9 *There exist a simple set $A \subseteq \mathbb{N}$ and a random sequence $p \in \Sigma^\omega$ 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 $p(i) := 1 - q(i)$ is random as well and satisfies $\chi^{-1}(p) \subseteq A$. □

Especially in view of Theorem 6.7.2 and the proof of Theorem 6.8 the notion of a random set seems to deserve attention in its own right. Also its connection with random sequences needs to be explored more thoroughly. For example, is there a non–random sequence $p \in \Sigma^\omega$ such that both $\chi^{-1}(p)$ and $\mathbb{N} \setminus \chi^{-1}(p)$ are random? Another topic for which the randomness space $(2^{\mathbb{N}}, O, \mu)$ 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. 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 [22].

Let $a : \mathbb{N} \to \mathbb{N}$ be a total recursive injective function with range $a = A$. We shall define an non–decreasing sequence $(C_n)_n$ of subsets of $\mathbb{N}$ and define in the end $C := \bigcup_n C_n$. Furthermore we will define an non–decreasing sequence $(L_n)_n$ of subsets of A. They contain the indices in A which are in a certain sense "relevant" for the construction. 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 $f_0^{(n)}, \ldots, f_n^{(n)}$ of $n+1$ pairwise different "forbidden" elements (marked). If at stage n the "forbidding" condition of one number $f_k^{(n-1)}$ of the numbers $f_0^{(n-1)}, \ldots, f_{n-1}^{(n-1)}$ from the previous stage is overruled, then all $f_l^{(n-1)}$ with $k \leq l < n$ 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 $C_n \cap \{f_0^{(n)}, \ldots, f_n^{(n)}\} = \emptyset$. It is crucial that each $f_n^{(\cdot)}$ will be changed only at finitely many stages, i.e. for each n there exists a number N such that $f_n^{(k)} = f_n^{(N)}$ for all $k \geq N$. This guarantees that C is co-infinite. It will be clear from the construction that C is r.e. The crucial 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 been listed so far, which are "relevant", and which have the property that the forbidden element is contained in D_i. 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 $\{f_0^{(n-1)}, \ldots, f_{n-1}^{(n-1)}\}$ 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 $j \in \{0, \ldots, n-1\}$ and $f_n^{(n)} := \min(\mathbb{N} \setminus G)$ where

$$G := \bigcup\{D_{a(j)} \mid j \leq n\} \cup \{f_0^{(n-1)}, \ldots, f_{n-1}^{(n-1)}\}\,.$$

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 $l \in \mathbb{N}$ we define

$$S(l, n) := \mu(\bigcup\{O_{D_j} \mid l \in D_j \text{ and } j \in L_n\})\,.$$

The set

$$F_n := \{m \mid 0 \leq m < n \text{ and } \ f_m^{(n-1)} \in D_{a(n)} \text{ and } S(f_m^{(n-1)}, n) > 2^{-m-2}\}$$

can be considered as the set of indices of forbidden elements in $D_{a(n)}$ 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

$$C_n := C_{n-1} \cup (D_{a(n)} \setminus \{f_0^{(n-1)}, \ldots, f_{n-1}^{(n-1)}\}) \cup \{f_m^{(n-1)} \mid m_{F_n} \leq m < n\}\,.$$

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 the same set 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 $i \leq n$. Remember that $(C_n)_n$ is a non–decreasing sequence of sets. Using induction, 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 $(D_{a(n)} \setminus \{f_0^{(n-1)}, \ldots, f_{n-1}^{(n-1)}\}) \cup \{f_m^{(n-1)} \mid m_{F_n} \leq m < n\}$, contains an element from $D_{a(n)}$. This is clear if $D_{a(n)} \not\subseteq \{f_0^{(n-1)}, \dots, f_{n-1}^{(n-1)}\}$. Assume that $D_{a(n)} \subseteq \{f_0^{(n-1)}, \dots, f_{n-1}^{(n-1)}\}$. The set $D_{a(n)}$ is nonempty 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 $m \geq k$. On the other hand, for all $l \in D_{a(n)}$, $S(l,n) \geq \mu(O_{D_{a(n)}}) = 2^{-(k+1)}$. Especially $S(f_m^{(n-1)},n) \geq 2^{-(k+1)} \geq 2^{-(m+1)} > 2^{-m-2}$. This shows that $\{f_l^{(n-1)} \mid m_{F_n} \leq l < n\}$ contains an element from $D_{a(n)}$ if $D_{a(n)} \subseteq \{f_0^{(n-1)}, \dots, f_{n-1}^{(n-1)}\}$. We have proved the second claim.

Finally, we have to prove that $\mathbb{N} \setminus C$ is infinite. We observe that by construction $C_n \cap \{f_0^{(n)}, \dots, f_n^{(n)}\} = \emptyset$ at the end of stage n. The assertion follows from the following claim:

$$\text{for each } n, \text{ there is a number } N \geq n \text{ such that } f_n^{(k)} = f_n^{(N)} \text{ for all } k \geq N. \tag{6}$$

This means that the number $f_n^{(\cdot)}$ 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 n be the smallest natural number such that $f_n^{(\cdot)}$ is changed at infinitely many stages. Let $f_0^{(\infty)}, \dots, f_{n-1}^{(\infty)}$ be the final values of $f_0^{(\cdot)}, \dots, f_{n-1}^{(\cdot)}$, i.e. $f_j^{(\infty)} := \lim_{k\to\infty} f_j^{(k)}$ for $0 \leq j < n$. Note that by construction for each k and each $m \leq k$ we have $S(f_m^{(k)}, k) \leq 2^{-m-2}$ at the end of stage k. We conclude that for $0 \leq j < n$

$$\lim_{k\to\infty} S(f_j^{(\infty)}, k) \leq 2^{-j-2}. \tag{7}$$

For each subset $E \subseteq \{f_0^{(\infty)}, \dots, f_{n-1}^{(\infty)}\}$ and each $m \in \mathbb{N}$ we define

$$\begin{aligned} L^E &:= \{j \in L \mid D_j \cap \{f_0^{(\infty)}, \dots, f_{n-1}^{(\infty)}\} = E\}, \\ L_m^E &:= \{j \in L_m \mid D_j \cap \{f_0^{(\infty)}, \dots, f_{n-1}^{(\infty)}\} = E\} \end{aligned}$$

Let $N_0 \in \mathbb{N}$ be so large such that for all $E \subseteq \{f_0^{(\infty)}, \dots, f_{n-1}^{(\infty)}\}$

$$\mu(L^E) - \mu(L_{N_0}^E) \leq 2^{-(2n+2)} \cdot (1 - 2^{|E|} \cdot \mu(L^E)). \tag{8}$$

There is such an N_0 because for $E = \emptyset$ we have

$$\mu(L^\emptyset) \leq \mu(L) \leq \mu(A) < 1$$

(because of $L^\emptyset \subseteq L \subseteq A$), and because for $E \neq \emptyset$ there is an $f_j^{(\infty)} \in E$ with $j \geq |E| - 1$, hence

$$\begin{aligned} \mu(L^E) &= \mu(\bigcup\{O_{D_i} \mid i \in L^E\}) \\ &\leq \mu(\bigcup O_{D_i} \mid i \in L \text{ and } f_j^{(\infty)} \in D_i\}) \\ &= \lim_{k\to\infty} S(f_j^{(\infty)}, k) \\ &\leq 2^{-j-2} \\ &\leq 2^{-|E|-1} \end{aligned}$$

where we have used (7). We can also assume that N_0 is so large such that $f_k^{(N_0)} = f_k^{(\infty)}$ for all $k \in \{0, \ldots, n-1\}$. Set

$$N_1 := \max(\{f_0^{(\infty)}, \ldots, f_{n-1}^{(\infty)}\} \cup \bigcup \{D_{a(i)} \mid i \leq N_0\}) .$$

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 $\leq N_1$ are added to the set C only at stages $\leq N_2$. We claim that for $j \in L \setminus L_{N_2}$ we have

$$D_j \cap \{0, 1, \ldots, N_1\} \subseteq \{f_0^{(\infty)}, \ldots, f_{n-1}^{(\infty)}\}. \tag{9}$$

To see this, fix a $j \in L \setminus L_{N_2}$. Note that by definition of N_2 no number in $D_j \cap \{0, 1, \ldots, N_1\}$ can be added to C at any stage later than N_2. This is especially true for the stage n_j where $n_j > N_2$ is the (unique) number with $a(n_j) = j$. Therefore we have $D_j \cap \{0, 1, \ldots, N_1\} \subseteq \{f_0^{(n_j - 1)}, \ldots, f_{n_j - 1}^{(n_j - 1)}\}$. We have $f_k^{(n_j - 1)} = f_k^{(\infty)}$ for $0 \leq k < n$, but all numbers $f_k^{(n_j - 1)}$ with $k \geq n$ will be added to C at some stage $\geq n_j$ (because of our assumption that $f_n^{(.)}$ — and hence also $f_k^{(.)}$ for each $k \geq n$ — will be changed infinitely often). Therefore we conclude that (9) is true.

For a moment fix a set $E \subseteq \{f_0^{(\infty)}, \ldots, f_{n-1}^{(\infty)}\}$ 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, 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 $j \in L_{N_0}^E$ we have $E \subseteq D_j \subseteq \{0, 1, \ldots, N_1\}$. On the other hand, from (9) we conclude that for $j \in L^E \setminus L_{N_2}^E$ we have $D_j \cap \{0, 1, \ldots, N_1\} = E$. These two facts imply that in the mentioned probability space the two events

$$O_E \setminus \bigcup \{O_{D_j} \mid j \in L_{N_0}^E\}$$

and

$$O_E \setminus \bigcup \{O_{D_j} \mid j \in L^E \setminus L_{N_2}^E\}$$

are independent. This means

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

A short computation yields the first equality in the following estimation, and (8) gives the last estimate.

$$\begin{aligned} \mu(L^E \setminus L_{N_2}^E) &= \frac{\mu(L_{N_0}^E \cup (L^E \setminus L_{N_2}^E)) - \mu(L_{N_0}^E)}{1 - 2^{|E|} \cdot \mu(L_{N_0}^E)} \\ &\leq \frac{\mu(L^E) - \mu(L_{N_0}^E)}{1 - 2^{|E|} \cdot \mu(L^E)} \\ &\leq 2^{-2n-2} . \end{aligned}$$

Using this inequality for all $E \subseteq \{f_0^{(\infty)}, \ldots, f_{n-1}^{(\infty)}\}$ we obtain

$$\begin{aligned} \mu(L \setminus L_{N_2}) &\leq \sum_{E \subseteq \{f_0^{(\infty)}, \ldots, f_{n-1}^{(\infty)}\}} \mu(L^E \setminus L^E_{N_2}) \\ &\leq \sum_{E \subseteq \{f_0^{(\infty)}, \ldots, f_{n-1}^{(\infty)}\}} 2^{-2n-2} \\ &= 2^{-n-2}. \end{aligned}$$

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

$$S(m,k) \leq \mu(L \setminus L_{N_2}) \leq 2^{-n-2}.$$

Hence, as soon as the number $f_n^{(.)}$ has been set to be larger than N_3, it will never again be changed. This contradicts the assumption that $f_n^{(.)}$ will be changed infinitely often. We have proved the claim (6). This ends the proof of the theorem. □

Acknowledgement

The authors would like to thank Cristian Calude for stimulating discussions on randomness.

References

[1] R. Book, J. Lutz, and M. Martin. The global power of additional queries to random oracles. In *Proc. of STACS 94*, pages 403–414, Berlin, 1994. Springer-Verlag.

[2] C. S. Calude. *Information and Randomness, an Algorithmic Perspective.* Springer-Verlag, Berlin, 1994.

[3] C. S. Calude. Personal communication. March 1997.

[4] C. S. Calude, P. Hertling, H. Jürgensen, and K. Weihrauch. Randomness on shift spaces. In preparation.

[5] C. S. Calude, P. Hertling, and B. Khoussainov. Do the zeros of Riemann's zeta-function form a random sequence? *Bulletin of the EATCS*, 62:199–207, 1997.

[6] C. S. Calude, P. Hertling, B. Khoussainov, and Y. Wang. Recursively enumerable reals and Chaitin ω numbers. In M. Morvan et al., editor, *Proceedings of the 15th Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science, Paris, 1998. Springer-Verlag. to appear.

[7] C. S. Calude and H. Jürgensen. Randomness as an invariant for number representations. In H. Maurer, J. Karhumäki, and G. Rozenberg, editors, *Results and Trends in Theoretical Computer Science*, pages 44–66. Springer-Verlag, Berlin, 1994.

[8] G. J. Chaitin. On the length of programs for computing finite binary sequences. *J. of the ACM*, 13:547–569, 1966.

[9] G. J. Chaitin. A theory of program size formally identical to information theory. *J. of the ACM*, 22:329–340, 1975.

[10] A. Grzegorczyk. On the definitions of computable real continuous functions. *Fund. Math.*, 44:61–71, 1957.

[11] P. Hertling and Y. Wang. Invariance properties of random sequences. *J. UCS*, 3(11):1241–1249, 1997.

[12] K.-I. Ko. *Complexity Theory of Real Functions.* Birkhäuser, Boston, 1991.

[13] A. N. Kolmogorov. Three approaches to the quantitative definition of information. *Problems of Information Transmission*, 1:1–7, 1965.

[14] C. Kreitz and K. Weihrauch. Theory of representations. *Theor. Comp. Science*, 38:35–53, 1985.

[15] D. Lacombe. Extension de la notion de fonction récursive aux fonctions d'une ou plusieurs variables réelles I-III. *Comptes Rendus Académie des Sciences*, 240/241:2478–2480/13–14,151–153, 1955.

[16] L. A. Levin. Randomness conservation inequalities: information and randomness in mathematical theories. *Information and Control*, 61:15–37, 1984.

[17] M. Li and P. Vitanyi. *An Introduction to Kolmogorov Complexity and Its Applications.* Springer–Verlag, New York, 1993.

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

[19] M. B. Pour-El and J. I. Richards. *Computability in Analysis and Physics.* Springer-Verlag, Berlin, Heidelberg, 1989.

[20] H. Rogers, Jr. *Theory of Recursive Functions and Effective Computability.* McGraw–Hill Book Company, New York, 1967.

[21] C.-P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit*, volume 218 of *Lecture Notes in Mathematics.* Springer-Verlag, Berlin, 1971.

[22] R. I. Soare. *Recursively Enumerable Sets and Degrees.* Springer–Verlag, Berlin, 1987.

[23] R. J. Solomonoff. A formal theory of inductive inference I, II. *Information and Control*, 7:1–22, 224–254, 1964.

[24] M. van Lambalgen. Von Mises definition of random sequences reconsidered. *The Journal of Symbolic Logic*, 52(3):725–755, 1987.

[25] M. van Lambalgen. The axiomatization of randomness. *The Journal of Symbolic Logic*, 55(3):1143–1167, 1990.

[26] J. Ville. *Étude Critique de la Notion de Collectif.* Gauthier-Villars, Paris, 1939.

[27] R. von Mises. Grundlagen der Wahrscheinlichkeitsrechnung. *Mathem. Zeitschrift*, 5:52–99, 1919.

[28] K. Weihrauch. *Computability.* Springer–Verlag, Berlin, 1987.

[29] K. Weihrauch. Random real numbers. Preprint, January 1995.

[30] K. Weihrauch. A foundation for computable analysis. In D. S. Bridges et al., editor, *Combinatorics, Complexity, and Logic*, Discrete Mathematics and Theoretical Computer Science, pages 66–89, Singapore, 1997. Springer-Verlag. Proceedings of DMTCS'96, Auckland.

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