Journal of Universal Computer Science, vol. 11, no. 12 (2005), 1970-1985
submitted: 14/10/05, accepted: 15/11/05, appeared: 28/12/05 © J.UCS

Nonrandom Sequences between Random Sequences[1]

Peter Hertling[2]
(Institut für Theoretische Informatik und Mathematik, Universität der Bundeswehr München, 85577 Neubiberg, Germany
Email: hertling@informatik.unibw-muenchen.de)

Abstract: Let us say that an infinite binary sequence q lies *above* an infinite binary sequence p if q can be obtained from p by replacing selected 0's in p by 1's. We show that above any infinite binary Martin-Löf random sequence p there exists an infinite binary nonrandom sequence q above which there exists an infinite binary random sequence r. This result is of interest especially in connection with the new randomness notion for sets of natural numbers introduced in [Hertling and Weihrauch 1998, Hertling and Weihrauch 2003] and in connection with its relation to the Martin-Löf randomness notion for infinite binary sequences.

Key Words: Algorithmic information theory, algorithmic randomness, random binary sequences, random sets

Category: F.1, H.1.1

1 Introduction

The today perhaps most widely used notion of randomness for infinite binary sequences is due to Martin-Löf [Martin-Löf 1966]. His definition is based on the idea that a sequence should be called random if it does not satisfy any law which can be verified effectively and which is valid only for a small subset of all sequences. Here "small" is meant in a measure-theoretic sense. Technically, this can be expressed by so-called "randomness tests". Precise definitions will be given in Section 3. One can characterize this notion of randomness of an infinite binary sequence also via the program-size complexity of the finite prefixes of the infinite binary sequence. For more background information about randomness notions the reader is referred to [Calude 2002] and [Li and Vitanyi 1997].

In this paper we prove a new property of Martin-Löf random infinite binary sequences. Consider some random binary sequence p. Is it possible, by first replacing some 0's in p by 1's, to arrive at a nonrandom sequence q, and then, by repeating this process, i.e., by replacing some 0's in q by 1's, to arrive at a random sequence r again? It is the main result of this paper that this is indeed possible, even for all random binary sequences p. Note that this is by no means obvious. In the first step of replacing 0's by 1's one has to introduce some nonrandomness, i.e., some effectively testable law, into the original random binary sequence. But in the second step, by replacing even more 0's by 1's, one has to destroy this law again, and to make sure that the resulting sequence does not satisfy any effectively testable law. If, for example, in the first step one makes

[1] C. S. Calude, H. Ishihara (eds.). *Constructivity, Computability, and Logic. A Collection of Papers in Honour of the 60th Birthday of Douglas Bridges.*

[2] This work was supported by DFG (446 CHV 113/240/0-1) and NSFC (10420130638).

sure that $q(n) = 1$ for all n which are a power of 2, then certainly q is a nonrandom sequence. But any sequence obtained by changing even more 0's to 1's will satisfy the same law, and, hence, will also be nonrandom.

While we believe that the result stated above in terms of infinite binary sequences is interesting itself already, the motivation which led to this result was a question arising in the study of random sets of numbers. Which sets of natural numbers should be called random? Of course, one might take the randomness notion for infinite binary sequences and transfer it to sets by identifying a set with its characteristic sequence. Another, new notion of randomness for sets was introduced in [Hertling and Weihrauch 1998, Hertling and Weihrauch 2003]. It is obtained by defining randomness tests on the power set $2^{\mathbb{N}}$ of the set $\mathbb{N}$ of all natural numbers similarly to Martin-Löf's randomness tests, but with respect to the topology on $2^{\mathbb{N}}$ as a complete partial order in the usual sense, not with respect to the topology on $2^{\mathbb{N}}$ induced by identifying $2^{\mathbb{N}}$ with the space of all infinite binary sequences. The precise definition will be given in a later section. The relation between random binary sequences and random sets has something in common with the relation between decidable sets and computably enumerable sets. For random binary sequences one considers any effectively testable law that can be expressed in terms of finite $0, 1$-strings. But for random sets one considers only effectively testable laws that can be expressed in terms of finite sets, i.e., in terms of finite combinations of 1's. Thus, while for random sequences one considers positive (1's) and negative (0's) information, for random sets one considers only positive (1's) information. The situation is similar for decidable sets (positive and negative information) and computably enumerable sets (only positive information). It is a fundamental fact that a set is decidable if and only if both the set and its complement are computably enumerable. Is a similar statement true for random sequences and random sets, that is, is it true that a sequence is random if and only if the corresponding set and its complement are random? It is easy to see that randomness of the characteristic sequence of a set implies randomness of the set and of its complement. But it is a corollary of the result stated above that the converse is not true: there exists a set such that both the set and its complement are random but the corresponding characteristic binary sequence is nonrandom. In fact, we can derive a much stronger result: For any random set A, there exists a superset $B \supseteq A$ such that both B and $\mathbb{N} \setminus B$ are random, but the characteristic sequence of B is not random.

In the following section we introduce some basic, general notation. In Section 3 we remind the reader of Martin-Löf's randomness notion for infinite binary sequences and state the main result of the paper in a more formal way. In Section 4 we repeat the definition of random sets of natural numbers, introduced in [Hertling and Weihrauch 1998, Hertling and Weihrauch 2003], and restate and derive the statement mentioned above about the relation between random sets and random binary sequences. Section 5 contains the proof of the main result.

2 Notation

We denote the set of natural numbers by $\mathbb{N} = \{0, 1, 2, \ldots\}$. The cardinality of a finite set E is denoted by $\#(E)$. Throughout the paper, Σ denotes the binary alphabet: $\Sigma = \{0, 1\}$. The set of all finite strings over Σ is denoted Σ^*. The length of a finite string w is denoted $\mathrm{length}(w)$. The symbols of w are usually written $w(0), \dots, w(\text{length}(w)-1)$. By $\#_1(w)$ we denote the number of 1's in w. For sets $A, B \subseteq \Sigma^*$, by AB we denote the set of all concatenations of strings in A and strings in B (in this order). A possibly partial function mapping elements of a set X to elements of a set Y is denoted $f :\subseteq X \to Y$. For a function $f :\subseteq X \to Y$ and an element $x \in X$, we write $f(x)\downarrow$ if, and only if, x is in the domain of definition $\text{dom}(f)$ of f, and $f(x)\uparrow$ otherwise. If $\text{dom} f = X$, we may write $f : X \to Y$. We use the notions of a computable, possibly partial, function $f :\subseteq \mathbb{N}^k \to \mathbb{N}$ and of a computably enumerable (*c.e.*) set $A \subseteq \mathbb{N}^k$ in the usual sense, for $k \geq 1$. By identifying the sets Σ^* and $\mathbb{N}$ via the length-lexicographical ordering we obtain computability notions also on Σ^* and on products of $\mathbb{N}$ and Σ^*. A *sequence* is a total mapping $p : \mathbb{N} \to X$ to some set X and usually written in the form $(p_n)_n$ or $(p(n))_n$. The infinite product $\Sigma^\omega := \{p \mid p : \mathbb{N} \to \Sigma\}$ of Σ is the set of all infinite binary sequences. For $0 \leq n \leq m$ and $p \in \Sigma^\omega$, by $p[n \dots m-1]$ we denote the string of length $m - n$ consisting of the symbols $p(n) \dots p(m-1)$. The set Σ^ω is a topological space with a basis consisting of the sets $w\Sigma^\omega = \{p \in \Sigma^\omega \mid p[0 \dots \text{length}(w)-1] = w\}$, for $w \in \Sigma^*$. For $A \subseteq \Sigma^*$, we use $A\Sigma^\omega = \bigcup_{w \in A} w\Sigma^\omega$. We denote by μ the usual uniform measure on Σ^ω given by $\mu(w\Sigma^\omega) = 2^{-\text{length}(w)}$, for $w \in \Sigma^*$.

3 Random Infinite Binary Sequences

In this section we remind the reader of Martin-Löf's [Martin-Löf 1966] definition of random binary sequences and state the main results of the paper in a more formal way.

Definition 1. 1. A sequence $(U_n)_n$ of subsets of Σ^ω is called *uniformly c.e. open* if there is a c.e. set $A \subseteq \mathbb{N} \times \Sigma^*$ with $U_n = A_n\Sigma^\omega$ for all n, where

$$A_n := \{w \in \Sigma^* \mid (n, w) \in A\} \ .$$

2. A *randomness test on* Σ^ω is a uniformly c.e. open sequence $(U_n)_n$ of subsets of Σ^ω satisfying additionally $\mu(U_n) \leq 1/(n+1)$ for all $n \in \mathbb{N}$.
3. A sequence $p \in \Sigma^\omega$ is called *nonrandom* if there exists a randomness test $(U_n)_n$ on Σ^ω with $p \in \bigcap_n U_n$. A sequence $p \in \Sigma^\omega$ is called *random* if it is not nonrandom.

Often, for example in the original paper [Martin-Löf 1966], instead of the condition $\mu(U_n) \leq 1/(n+1)$ the condition $\mu(U_n) \leq 2^{-n}$ is used. It is clear that our choice does not lead to a different randomness notion. The only reason for our choice is that with respect to notation it is more convenient for some proofs later on.

One of the striking properties of this randomness notion is the existence of a universal randomness test: we call a randomness test $(U_n)_n$ *universal* if $\bigcap_n U_n$ contains all nonrandom sequences $p \in \Sigma^\omega$.

Proposition 2 ([Martin-Löf 1966]). *There exists a universal randomness test on* Σ^ω.

Let us define the bijection $\chi : 2^{\mathbb{N}} \to \Sigma^\omega$ by

$$\chi(A)_n = \begin{cases} 1 & \text{if } n \in A, \\ 0 & \text{if } n \notin A, \end{cases}$$

for all $A \subseteq \mathbb{N}$ and $n \in \mathbb{N}$, i.e., for $A \subseteq \mathbb{N}$ the sequence $\chi(A)$ is the characteristic sequence of A.

Definition 3. We define a partial order relation $\leq$ on Σ^ω by

$$p \leq q :\iff \chi^{-1}(p) \subseteq \chi^{-1}(q) \ ,$$

for any $p, q \in \Sigma^\omega$.

The following theorem, first stated in the technical report [Hertling 2001], is the main result of the paper.

Theorem 4. *For every random sequence $p \in \Sigma^\omega$ there exist two sequences $q, r \in \Sigma^\omega$ with the following properties: q is nonrandom, r is random, $p \leq q$, and $q \leq r$.*

The proof will be given in Section 5.

4 Random Sets of Numbers

In [Hertling and Weihrauch 1998, Hertling and Weihrauch 2003] a randomness notion for sets of natural numbers was introduced in a similar way as randomness for infinite binary sequences, namely via randomness tests. For a finite set $E \subseteq \mathbb{N}$ we define

$$O(E) := \{A \subseteq \mathbb{N} \mid E \subseteq A\} \ .$$

The sets $O(E)$ for finite E form a basis of a topology on $2^{\mathbb{N}}$. This topology gives $2^{\mathbb{N}}$ a well-researched structure of a "complete partial order"; see e.g. [Weihrauch 1987]. It is different from the topology on $2^{\mathbb{N}}$ induced by identifying $2^{\mathbb{N}}$ via χ with the topological space Σ^ω, but both topologies generate the same σ-algebra; see [Hertling and Weihrauch 2003, Lemma 6.1]. Therefore, we can translate the measure μ on Σ^ω via χ to $2^{\mathbb{N}}$. 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 subsets of $\mathbb{N}$, defined by $D^{-1}(E) := \sum_{i \in E} 2^i$.

Definition 5.
1. A sequence $(U_n)_n$ of subsets of $2^{\mathbb{N}}$ is called *uniformly c.e. open* if there is a c.e. set $R \subseteq \mathbb{N}^2$ with $U_n = \bigcup_{i \in R_n} O(D_i)$ for all n, where
$$R_n := \{i \in \mathbb{N} \mid (n, i) \in R\} \ .$$
2. A *randomness test on* $2^{\mathbb{N}}$ is a uniformly c.e. open sequence $(U_n)_n$ of subsets of $2^{\mathbb{N}}$ satisfying additionally $\mu(U_n) \leq 1/(n+1)$ for all n.
3. A set $A \subseteq \mathbb{N}$ is called *nonrandom* if there exists a randomness test $(U_n)_n$ on $2^{\mathbb{N}}$ with $p \in \bigcap_n U_n$. A set $A \subseteq \mathbb{N}$ is called *random* if it is not nonrandom.

The randomness notions for infinite binary sequences and for sets are closely related.

Proposition 6 ([Hertling and Weihrauch 1998]). *A set $A \subseteq \mathbb{N}$ is random if, and only if, there is a set $B \supseteq A$ such that $\chi(B)$ is random.*

For a proof of this result see [Hertling and Weihrauch 2003].

For any $A \subseteq \mathbb{N}$ the sequence $\chi(A)$ is random if and only if, the sequence $\chi(\mathbb{N} \setminus A)$ is random. Therefore, Proposition 6 implies that if $\chi(A)$ is random then both A and $\mathbb{N} \setminus A$ are random. Is the converse true? From Theorem 4 and Proposition 6 we can deduce that this is not the case. In fact, we can deduce the following much stronger result.

Corollary 7. *For any random set $A \subseteq \mathbb{N}$ there exists a superset $B \supseteq A$ of natural numbers with the following properties: both the set B and its complement $\mathbb{N} \setminus B$ are random, but the characteristic sequence $\chi(B)$ of B is not random.*

Proof. Let A be an arbitrary random set. By Proposition 6, there exists a random sequence p with $A \subseteq \chi^{-1}(p)$. By Theorem 4 there exist a nonrandom sequence q and a random sequence r with $p \leq q \leq r$. Set $B := \chi^{-1}(q)$. Then $A \subseteq \chi^{-1}(p) \subseteq B$. Since r is random and $B \subseteq \chi^{-1}(r)$, by Proposition 6, B is random. Since p is random, also the sequence $\overline{p}$ obtained by replacing all 0's in p by 1's and all 1's in p by 0's, is random. Hence, since $\mathbb{N} \setminus B \subseteq \chi^{-1}(\overline{p})$, by Proposition 6, $\mathbb{N} \setminus B$ is random. □

5 The Proof of Theorem 4

This section contains the proof of Theorem 4. The first subsection contains the construction and the main body of the proof. The remaining three subsections contain proofs of lemmata formulated in the first subsection.

5.1 The Construction and the Main Body of the Proof

We need the following simple notions and statements.

Definition 8. 1. For $S \subseteq \Sigma^\omega$ we set

$$\mathrm{up}(S) := \{q \in \Sigma^\omega \mid \exists p \in S \,.\, p \leq q\} \ .$$

2. For $S \subseteq \Sigma^\omega$ we set

$$\mathrm{down}(S) := \{p \in \Sigma^\omega \mid \exists q \in S \,.\, p \leq q\} \ .$$

3. A set $S \subseteq \Sigma^\omega$ is called *upwards closed* if $\mathrm{up}(S) \subseteq S$.
4. A set $S \subseteq \Sigma^\omega$ is called *downwards closed* if $\mathrm{down}(S) \subseteq S$.

Lemma 9. *1. If S is open, so are* $\mathrm{up}(S)$ *and* $\mathrm{down}(S)$.
2. If S is closed, so are $\mathrm{up}(S)$ *and* $\mathrm{down}(S)$.

Proof. The first statement is obvious. The second follows from the compactness of Σ^ω. We prove the second statement for $\mathrm{up}(S)$ in detail. The proof for $\mathrm{down}(S)$ is similar. Let $S \subseteq \Sigma^\omega$ be a closed set. Let q be an element of the closure of $\mathrm{up}(S)$. We have to show that q is in $\mathrm{up}(S)$. For each n, let $q^{(n)} \in \mathrm{up}(S)$ be a sequence with $q^{(n)}[0 \ldots n-1] = p[0 \ldots n-1]$. For each n, let $p^{(n)} \in S$ be a sequence with $p^{(n)} \leq q^{(n)}$. Since S is closed, and, due to the compactness of Σ^ω, also compact, there is an accumulation point $p \in S$ of the sequence $(p^{(n)})_n$. We claim that $p \leq q$. Indeed, for any m there exists some $n \geq m$ with $p^{(n)}[0 \ldots m-1] = p[0 \ldots m-1]$. Using also $p^{(n)} \leq q^{(n)}$ and $q^{(n)}[0 \ldots m-1] = q[0 \ldots m-1]$ we obtain $p[0 \ldots m-1]0^\omega \leq q[0 \ldots m-1]0^\omega$. This shows $p \leq q$. Thus, $p \in \mathrm{up}(S)$. We have proved that $\mathrm{up}(S)$ is closed. □

For $l \in \mathbb{N}$ and $0 \leq z \leq l$ we set

$$S(l, z) := \{w \in \Sigma^l \mid \#_1(w) = z\} \ .$$

For each $l, m \in \mathbb{N}$ and $i \in \{0, \ldots, m\}$ let $g(l, m, i)$ be the smallest number j with the following property:

$$\frac{\#(\{w \in \Sigma^l \mid \#_1(w) \leq j\})}{\#(\Sigma^l)} \geq \frac{i}{m} \ .$$

The partial function $g :\subseteq \mathbb{N}^3 \to \mathbb{N}$ defined in this way is obviously computable. Clearly,

$$0 = g(l, m, 0) \leq \ldots \leq g(l, m, i) \leq g(l, m, i+1) \leq \ldots \leq g(l, m, m) = l$$

for $l, m \in \mathbb{N}$, $i \in \{0, \ldots, m-1\}$.

We define three computable sequences $(l_k)_k$, $(m_k)_k$, and $(n_k)_k$ of natural numbers by

$$l_k := 2 \cdot (k+1)^6, \qquad n_k := \sum_{i=0}^{k-1} l_i,$$
$$m_k := (k+1)^2 \ .$$

For $k \in \mathbb{N}$ we define

$$T(k) := \bigcup_{i=0}^{m_k} S(l_k, g(l_k, m_k, i))$$

and

$$C_k := \{p \in \Sigma^\omega \mid p[n_k \ldots n_{k+1} - 1] \in T(k)\} \ .$$

For each k, the set C_k is closed and open. It is clear that the sequence $(C_k)_k$ is uniformly c.e. open.

Lemma 10. *For each $k \in \mathbb{N}$, $\mu(C_k) \leq 1/(k+1)$.*

This lemma is proved by estimating the number of strings in $T(k)$. This is done by using a version of Stirling's formula with an error estimate. The proof is given in Subsection 5.2.

Hence, any sequence p contained in $\bigcap_{j=k}^{\infty} C_j$, for some k, is nonrandom.

Let $(V_n)_n$ be a universal randomness test on Σ^ω; see Proposition 2. We define for each k

$$U_k := \left\{ p \in \Sigma^\omega \;\middle|\; \mathrm{up}\left(\mathrm{up}\,(\{p\}) \cap \bigcap_{j=k}^{\infty} C_j \right) \subseteq V_k \right\} \ .$$

Lemma 11. *The sequence $(U_k)_k$ is uniformly c.e. open.*

This lemma is proved in Subsection 5.3. The proof is based on the following observations. On the one hand, the sequence $(V_k)_k$ is uniformly c.e. open, thus, it can be approximated uniformly from below by basic open sets. On the other hand, the set $\mathrm{up}\left(\mathrm{up}\,(\{p\}) \cap \bigcap_{j=k}^{\infty} C_j\right)$ is compact and it can be approximated uniformly from above by compact sets that are described by finite information. This set is compact, because each C_j is compact, therefore also their intersection, and because of Lemma 9, applied twice. It can be approximated from above by the compact sets $\mathrm{up}\left(\mathrm{up}\,(w\Sigma^\omega) \cap \bigcap_{j=k}^{i} C_j\right)$ for longer and longer prefixes w of p and for growing i.

Lemma 12. *For each $k \in \mathbb{N}$, $\mu(U_k) \leq 2/(k+1)$.*

The proof of this lemma is the longest part of the proof. The main idea is that, although for j tending to infinity the measure $\mu(C_j)$ tends to zero, the measure $\mu(A \cup B)$ of any union $A \cup B$ of a measurable, downwards closed set A and a measurable, upwards closed set B such that $A \cup B$ contains C_j can be bounded from below effectively by a number tending to 1 for j tending to infinity. The proof of Lemma 12 is given in Subsection 5.4.

From these lemmata we can deduce the assertion of Theorem 4. Let $p \in \Sigma^\omega$ be a random sequence. We have to show that there exist two sequences $q, r \in \Sigma^\omega$ with the following properties: q is nonrandom, r is random, $p \leq q$, and $q \leq r$.

According to Lemma 11 and Lemma 12, the sequence $(U_{2 \cdot k+1})_k$ is a randomness test. Since p is random, there is some k_0 with $p \notin U_{k_0}$. Hence, there is some sequence $r \in \mathrm{up}\left(\mathrm{up}(\{p\}) \cap \bigcap_{j=k_0}^{\infty} C_j\right)$ with $r \notin V_{k_0}$. Since $(V_k)_k$ is a universal randomness test, $r \notin V_{k_0}$ implies that r is random. There must also exist some sequence $q \in \mathrm{up}(\{p\}) \cap \bigcap_{j=k_0}^{\infty} C_j$ with $q \leq r$. The condition $q \in \mathrm{up}(\{p\})$ is equivalent to $p \leq q$. And the condition $q \in \bigcap_{j=k_0}^{\infty} C_j$ implies that q is nonrandom, due to Lemma 10 and the fact that the sequence $(C_k)_k$ is uniformly c.e. open. This ends the proof of Theorem 4.

We still have to prove Lemma 10, Lemma 11, and Lemma 12. This will be done in the following subsections.

5.2 Proof of Lemma 10

For $k = 0$ the assertion is trivial. Let us fix some $k \geq 1$. It is clear that

$$\begin{aligned} 2^{l_k} \cdot \mu(C_k) &= \#(T(k)) \\ &= \sum_{i=0}^{m_k} \#(S(l_k, g(l_k, m_k, i))) \\ &= \sum_{i=0}^{m_k} \binom{l_k}{g(l_k, m_k, i)} \\ &= 2 + \sum_{i=1}^{m_k - 1} \binom{l_k}{g(l_k, m_k, i)} \ . \end{aligned}$$

For the terms in the sum we use the following uniform estimate:

$$\binom{l_k}{j} = \frac{l_k!}{j! \cdot (l_k - j)!} \leq \frac{l_k!}{(l_k/2)! \cdot (l_k/2)!} \ ,$$

valid for any $j \in \{0, \ldots, l_k\}$. Note that l_k is even. The last term on the right hand side can be estimated using the following two-sided estimate for the factorial function:

$$\sqrt{2\pi n} \cdot n^n \cdot \mathrm{e}^{-n} < n! < \sqrt{2\pi n} \cdot n^n \cdot \mathrm{e}^{-n} \cdot \exp\left(\frac{1}{12(n-1)}\right) \ ,$$

valid for $n \geq 2$. This is a version of Stirling's formula together with an error estimate. For a proof see e.g. Forster [Forster 1983]. Since $l_k/2 \geq 2$ for $k \geq 1$, we obtain

$$\begin{aligned} l_k! &< \sqrt{2\pi l_k} \cdot l_k^{l_k} \cdot \mathrm{e}^{-l_k} \cdot \exp\left(\frac{1}{12(l_k - 1)}\right), \\ (l_k/2)! &> \sqrt{2\pi(l_k/2)} \cdot (l_k/2)^{l_k/2} \cdot \mathrm{e}^{-l_k/2} \ , \end{aligned}$$

hence,

$$\begin{aligned} \frac{l_k!}{(l_k/2)! \cdot (l_k/2)!} &\leq \frac{\sqrt{2\pi l_k} \cdot l_k^{l_k} \cdot \mathrm{e}^{-l_k} \cdot \exp\left(\frac{1}{12(l_k-1)}\right)}{\pi \cdot l_k \cdot (l_k/2)^{l_k} \cdot \mathrm{e}^{-l_k}} \\ &= \sqrt{\frac{2}{\pi \cdot l_k}} \cdot 2^{l_k} \cdot \exp\left(\frac{1}{12(l_k - 1)}\right) \ . \end{aligned}$$

Thus, we obtain

$$\begin{aligned} \mu(C_k) &\leq \frac{2}{2^{l_k}} + (m_k - 1) \cdot \sqrt{\frac{2}{\pi \cdot l_k}} \cdot \exp\left(\frac{1}{12(l_k - 1)}\right) \\ &= \frac{2}{2^{2 \cdot (k+1)^6}} + \frac{((k+1)^2 - 1)}{(k+1)^3} \cdot \sqrt{\frac{1}{\pi}} \cdot \exp\left(\frac{1}{12(2 \cdot (k+1)^6 - 1)}\right) \\ &\leq 1/(k+1) \ . \end{aligned}$$

That was to be shown.

5.3 Proof of Lemma 11

Let $h : \mathbb{N}^2 \to \Sigma^*$ be a total computable function with $V_k = \{h(k,i) \mid i \in \mathbb{N}\}\Sigma^\omega$ for all k. We define

$$V_k[i] := \{h(k,j) \mid 0 \le j < i\}\Sigma^\omega$$

for all k, i. It is clear that the set

$$\widetilde{D} := \left\{ (k,i,w) \in \mathbb{N}^2 \times \Sigma^* \;\middle|\; i \ge k \text{ and } \operatorname{up}\left(\operatorname{up}(w\Sigma^\omega) \cap \bigcap_{j=k}^{i} C_j\right) \subseteq V_k[i] \right\}$$

is decidable. Hence, the set $D \subseteq \mathbb{N} \times \Sigma^*$ defined by

$$D := \left\{ (k,w) \in \mathbb{N} \times \Sigma^* \;\middle|\; \exists i \ge k \,.\, (k,i,w) \in \widetilde{D} \right\}$$

is computably enumerable. The assertion of Lemma 11 follows from this fact and from the following lemma, where we use $D_k := \{w \in \Sigma^* \mid (k,w) \in D\}$.

Lemma 13. *$U_k = D_k\Sigma^\omega$ for all $k \in \mathbb{N}$.*

Proof. Let us fix some $k \in \mathbb{N}$. It is obvious that $D_k\Sigma^\omega \subseteq U_k$. For the inverse inclusion fix some $p \in U_k$. We have to show $p \in D_k\Sigma^\omega$.

Since all sets C_j are closed, so is the set $\bigcap_{j=k}^{\infty} C_j$. Since the singleton set $\{p\}$ is closed, so is the set $\operatorname{up}(\{p\})$, according to Lemma 9. Thus, also the set $\operatorname{up}(\{p\}) \cap \bigcap_{j=k}^{\infty} C_j$ is closed, and again according to Lemma 9, also the set $\operatorname{up}(\operatorname{up}(\{p\}) \cap \bigcap_{j=k}^{\infty} C_j)$. It is even compact because Σ^ω is compact. Since $p \in U_k$, there must exist some i (without loss of generality $i \ge k$) with

$$\operatorname{up}\left(\operatorname{up}(\{p\}) \cap \bigcap_{j=k}^{\infty} C_j\right) \subseteq V_k[i] \ .$$

Let z be the smallest natural number such that

$$n_z \ge \max\{\operatorname{length}(h(k,j)) \mid 0 \le j < i\} \ .$$

We claim that even

$$\operatorname{up}\left(\operatorname{up}(p[0\ldots n_z - 1]\Sigma^\omega) \cap \bigcap_{j=k}^{z-1} C_j\right) \subseteq V_k[i] \ . \tag{1}$$

This, of course, implies $p \in D_k\Sigma^\omega$. In order to prove (1), fix a sequence

$$r \in \operatorname{up}\left(\operatorname{up}(p[0\ldots n_z - 1]\Sigma^\omega) \cap \bigcap_{j=k}^{z-1} C_j\right) \ .$$

We have to show $r \in V_k[i]$. Fix also a sequence

$$q \in \mathrm{up}(p[0 \dots n_z - 1]\Sigma^\omega) \cap \bigcap_{j=k}^{z-1} C_j$$

with $q \le r$. Set

$$q' := q[0 \dots n_z - 1]1^\omega \quad \text{and}$$
$$r' := r[0 \dots n_z - 1]1^\omega \ .$$

Then $q' \in \mathrm{up}(\{p\}) \cap \bigcap_{j=k}^{\infty} C_j$ and $q' \le r'$. We conclude $r' \in V_k[i]$. There must be some $j < i$ with $r' \in h(k,j)\Sigma^\omega$. Since $\mathrm{length}(h(k,j)) \le n_z$, we conclude that also $r \in h(k,j)\Sigma^\omega$, hence, $r \in V_k[i]$. That ends the proof. □

5.4 Proof of Lemma 12

We start with a simple property of downwards respectively upwards closed sets.

Lemma 14. *1. For every string $v \in \Sigma^*$, every $l \ge 1$, every $z \in \{0, \dots, l-1\}$, and every downwards closed, measurable set $A \subseteq \Sigma^\omega$,*

$$\frac{\mu(A \cap vS(l,z)\Sigma^\omega)}{\mu(vS(l,z)\Sigma^\omega)} \ge \frac{\mu(A \cap vS(l,z+1)\Sigma^\omega)}{\mu(vS(l,z+1)\Sigma^\omega)} \ .$$

2. For every string $v \in \Sigma^*$, every $l \ge 1$, every $z \in \{1, \dots, l\}$, and every upwards closed, measurable set $B \subseteq \Sigma^\omega$,

$$\frac{\mu(B \cap vS(l,z)\Sigma^\omega)}{\mu(vS(l,z)\Sigma^\omega)} \ge \frac{\mu(B \cap vS(l,z-1)\Sigma^\omega)}{\mu(vS(l,z-1)\Sigma^\omega)} \ .$$

Proof. This result follows from the symmetry of the sets $S(l,z)$. We show only the first statement. The second is proved in the same way. Fix some $l \ge 1$ and some $z \in \{0, \dots, l-1\}$. Since A is downwards closed, for any $w \in S(l,z)$,

$$\begin{aligned}\mu(A \cap vw\Sigma^\omega) &\ge \max\{\mu(A \cap vx\Sigma^\omega) \mid x \in S(l,z+1) \text{ and } w \le x\} \\ &\ge \frac{\sum_{x \in S(l,z+1),\, w \le x} \mu(A \cap vx\Sigma^\omega)}{\#\{x \in S(l,z+1) \mid w \le x\}} \\ &= \frac{1}{l-z} \cdot \sum_{x \in S(l,z+1),\, w \le x} \mu(A \cap vx\Sigma^\omega) \ .\end{aligned}$$

Here $w \le x$ has the obvious meaning for strings w and x of the same length: $w(i) \le x(i)$ for all $i < \mathrm{length}(w)$. In other words, $w \le q \iff w0^\omega \le x0^\omega$, for string w and x of the same length. Summation over all $w \in S(l,z)$ and interchanging the summations on the right hand side yields:

$$\begin{aligned}\mu(A \cap vS(l,z)\Sigma^\omega) &\geq \frac{1}{l-z} \cdot \sum_{w \in S(l,z)} \sum_{x \in S(l,z+1),\, w \leq x} \mu(A \cap vx\Sigma^\omega) \\ &= \frac{1}{l-z} \cdot \sum_{x \in S(l,z+1)} \sum_{w \in S(l,z),\, w \leq x} \mu(A \cap vx\Sigma^\omega) \\ &= \frac{1}{l-z} \cdot \sum_{x \in S(l,z+1)} (z+1) \cdot \mu(A \cap vx\Sigma^\omega) \\ &= \frac{z+1}{l-z} \cdot \mu(A \cap vS(l,z+1)\Sigma^\omega) \ .\end{aligned}$$

The assertion follows because

$$\mu(vS(l,z)\Sigma^\omega) = \frac{z+1}{l-z} \cdot \mu(vS(l,z+1)\Sigma^\omega) \ .$$

□

Lemma 15. *Fix a string $v \in \Sigma^*$ and a number $k \in \mathbb{N}$. Let $A \subseteq \Sigma^\omega$ be a downwards closed, measurable set and $B \subseteq \Sigma^\omega$ be an upwards closed, measurable set. Let $\gamma \in [0,1]$ be a real number such that*

$$\frac{\mu(A \cap vw\Sigma^\omega) + \mu(B \cap vw\Sigma^\omega)}{\mu(vw\Sigma^\omega)} \geq \gamma \qquad \text{for all } w \in T(k). \tag{2}$$

Then

$$\frac{\mu(A \cap v\Sigma^\omega) + \mu(B \cap v\Sigma^\omega)}{\mu(v\Sigma^\omega)} \geq \gamma \cdot \left(1 - \frac{1}{m_k}\right) \ .$$

Proof. Throughout the proof, a string $v \in \Sigma^*$, a number $k \in \mathbb{N}$, a downwards closed set $A \subseteq \Sigma^\omega$, an upwards closed set $B \subseteq \Sigma^\omega$, and a real number $\gamma \in [0,1]$ satisfying (2) are fixed.

Lemma 14 implies for all $i \leq m_k$, and all $z \leq g(l_k, m_k, i)$,

$$\frac{\mu(A \cap vS(l_k,z)\Sigma^\omega)}{\mu(vS(l_k,z)\Sigma^\omega)} \geq \frac{\mu(A \cap vS(l_k, g(l_k,m_k,i))\Sigma^\omega)}{\mu(vS(l_k, g(l_k,m_k,i))\Sigma^\omega)} \ . \tag{3}$$

Considering the definition of $g(l_k, m_k, i)$ one deduces

$$\frac{\mu(A \cap v\Sigma^\omega)}{\mu(v\Sigma^\omega)} \geq \frac{1}{m_k} \cdot \sum_{i=1}^{m_k} \frac{\mu(A \cap vS(l_k, g(l_k,m_k,i))\Sigma^\omega)}{\mu(vS(l_k, g(l_k,m_k,i))\Sigma^\omega)} \ . \tag{4}$$

Before we prove this claim in detail, we continue with the main body of the proof of Lemma 15. Similarly to (4), one obtains

$$\frac{\mu(B \cap v\Sigma^\omega)}{\mu(v\Sigma^\omega)} \geq \frac{1}{m_k} \cdot \sum_{i=0}^{m_k-1} \frac{\mu(B \cap vS(l_k, g(l_k,m_k,i))\Sigma^\omega)}{\mu(vS(l_k, g(l_k,m_k,i))\Sigma^\omega)} \ . \tag{5}$$

Adding (4) and (5) and taking for every $i \in \{1, \ldots, m_k - 1\}$ into account:

$$\frac{\mu(A \cap vS(l_k, g(l_k, m_k, i)\Sigma^\omega) + \mu(B \cap vS(l_k, g(l_k, m_k, i)\Sigma^\omega)}{\mu(vS(l_k, g(l_k, m_k, i)\Sigma^\omega)} \geq \gamma$$

(this follows from the assumption (2)), we obtain

$$\frac{\mu(A \cap v\Sigma^\omega) + \mu(B \cap v\Sigma^\omega)}{\mu(v\Sigma^\omega)} \geq \frac{1}{m_k} \cdot (m_k - 1) \cdot \gamma \ .$$

That was to be shown.

We still wish to give a detailed proof of (4). The inequality (5) can be proved in the same way. We prove only (4). First, using

$$\delta_i := \frac{\mu(A \cap vS(l_k, g(l_k, m_k, i))\Sigma^\omega)}{\mu(vS(l_k, g(l_k, m_k, i))\Sigma^\omega)}$$

we rewrite (3) as follows:

$$\mu(A \cap vS(l_k, z)\Sigma^\omega) \geq 2^{-\mathrm{length}(v) - l_k} \cdot \delta_i \cdot \#(S(l_k, z)) \tag{6}$$

(this is valid for $0 \leq i \leq m_k$ and $0 \leq z \leq g(l_k, m_k, i)$). We observe

$$\begin{aligned} \mu(A \cap v\Sigma^\omega) &= \sum_{z=0}^{l_k} \mu(A \cap vS(l_k, z)\Sigma^\omega) \\ &= \sum_{i=0}^{m_k} \mu(A \cap vS(l_k, g(l_k, m_k, i))\Sigma^\omega) && (7) \\ &\quad + \sum_{i=1}^{m_k} \sum_{g(l_k, m_k, i-1) < z < g(l_k, m_k, i)} \mu(A \cap vS(l_k, z)\Sigma^\omega) \ . && (8) \end{aligned}$$

The terms in the sum in (8), the double sum, are estimated using (6) directly. For the estimate of the terms in the sum in (7) we define numbers α_i for $i \in \{0, \ldots, m_k\}$:

$$\alpha_i := \frac{\#(\{w \in \Sigma^{l_k} \mid \#_1(w) \leq g(l_k, m_k, i)\}) - \frac{i}{m_k} \cdot \#(\Sigma^{l_k})}{\#(S(l_k, g(l_k, m_k, i)))} \ .$$

Note that $0 \leq \alpha_i \leq 1$ for each $i \in \{0, \ldots, m_k\}$, and especially $\alpha_0 = 1$, $\alpha_{m_k} = 0$. By induction over i one observes for all $i \in \{1, \ldots, m_k\}$

$$\begin{aligned} \frac{1}{m_k} \cdot \#(\Sigma^{l_k}) \ &= \ \alpha_{i-1} \cdot \#(S(l_k, g(l_k, m_k, i-1))) \\ &\quad + \sum_{g(l_k, m_k, i-1) < z < g(l_k, m_k, i)} \#(S(l_k, z)) && (9) \\ &\quad + (1 - \alpha_i) \cdot \#(S(l_k, g(l_k, m_k, i))) \ . \end{aligned}$$

For the terms in the sum in (7) we use the following estimate, according to (6) valid for all $i \in \{0, \ldots, m_k - 1\}$:

$$\mu(A \cap vS(l_k, g(l_k, m_k, i))\Sigma^\omega) \\ \geq\ 2^{-\text{length}(v)-l_k} \cdot \big((1-\alpha_i)\cdot\delta_i + \alpha_i \cdot \delta_{i+1}\big) \cdot \#(S(l_k, g(l_k, m_k, i)))\ .$$

Due to $\alpha_{m_k} = 0$, this expression makes sense and is true also for $i = m_k$. For the term $\mu(A \cap v\Sigma^\omega)$ we obtain

$$\begin{aligned}&\mu(A \cap v\Sigma^\omega)\\ &\geq \sum_{i=0}^{m_k} 2^{-\text{length}(v)-l_k} \cdot \big((1-\alpha_i)\cdot\delta_i + \alpha_i\cdot\delta_{i+1}\big)\cdot \#(S(l_k, g(l_k, m_k, i)))\\ &\quad + \sum_{i=1}^{m_k} \sum_{g(l_k,m_k,i-1)<z<g(l_k,m_k,i)} 2^{-\text{length}(v)-l_k} \cdot \delta_i \cdot \#(S(l_k, z))\\ &= \frac{1}{m_k} \cdot 2^{-\text{length}(v)} \cdot \sum_{i=1}^{m_k} \delta_i\ .\end{aligned}$$

The last equality follows by rearranging, by using $\alpha_0 = 1$ and $\alpha_{m_k} = 0$, and by applying (9). This ends the proof of (4) and the proof of Lemma 15. □

Corollary 16. *Fix a string $v \in \Sigma^*$, a number $k \in \mathbb{N}$, and a number $i \geq k$. Let $A \subseteq \Sigma^\omega$ be a downwards closed, measurable set and $B \subseteq \Sigma^\omega$ be an upwards closed, measurable set. Let $\gamma \in [0, 1]$ be a real number such that*

$$\frac{\mu(A \cap vw\Sigma^\omega) + \mu(B \cap vw\Sigma^\omega)}{\mu(vw\Sigma^\omega)} \geq \gamma$$

for all $w \in T(k)\ldots T(i)$. Then

$$\frac{\mu(A \cap v\Sigma^\omega) + \mu(B \cap v\Sigma^\omega)}{\mu(v\Sigma^\omega)} \geq \gamma \cdot \prod_{j=k}^{i} \left(1 - \frac{1}{m_j}\right)\ .$$

Proof. This follows by induction from Lemma 15. □

Corollary 17. *Fix a number $k \in \mathbb{N}$, and a number $i \geq k$. Let $A \subseteq \Sigma^\omega$ be a downwards closed, measurable set and $B \subseteq \Sigma^\omega$ be an upwards closed, measurable set such that*

$$\bigcap_{j=k}^{i} C_j \subseteq A \cup B\ .$$

Then

$$\mu(A) + \mu(B) \geq \prod_{j=k}^{i} \left(1 - \frac{1}{m_j}\right)\ .$$

Proof. This follows from Corollary 16 by considering $\gamma = 1$ and all strings v of length n_k, and by taking the sum over all these strings. □

Corollary 18. *Fix a number $k \in \mathbb{N}$. Let $A \subseteq \Sigma^\omega$ be an open, downwards closed set and $B \subseteq \Sigma^\omega$ be an open, upwards closed set such that*

$$\bigcap_{j=k}^{\infty} C_j \subseteq A \cup B \ .$$

Then

$$\mu(A) + \mu(B) \geq \frac{k}{k+1} \ .$$

Proof. There exist sets $W_A, W_B \subseteq \Sigma^*$ with $A = W_A\Sigma^\omega$ and with $B = W_B\Sigma^\omega$. Since the set $\bigcap_{i=k}^{\infty} C_j$ is compact there exists a number $l \in \mathbb{N}$ such that

$$\bigcap_{j=k}^{\infty} C_j \subseteq \{w \in W_A \mid \text{length}(w) \leq l\}\Sigma^\omega \cup \{w \in W_B \mid \text{length}(w) \leq l\}\Sigma^\omega \ .$$

Set $i := \min\{z \in \mathbb{N} \mid z \geq k \ \& \ n_{z+1} \geq l\}$. Then, clearly,

$$\bigcap_{j=k}^{i} C_j \subseteq \{w \in W_A \mid \text{length}(w) \leq l\}\Sigma^\omega \cup \{w \in W_B \mid \text{length}(w) \leq l\}\Sigma^\omega \ .$$

We conclude from Corollary 17

$$\begin{aligned}\mu(A) + \mu(B) &\geq \prod_{j=k}^{i}\left(1 - \frac{1}{m_j}\right) \\ &\geq \prod_{j=k}^{\infty}\left(1 - \frac{1}{m_j}\right) \\ &= \prod_{j=k}^{\infty}\left(1 - \frac{1}{(j+1)^2}\right) \\ &= \frac{k}{k+1}.\end{aligned}$$

□

Lemma 19. *Let $A \subseteq \Sigma^\omega$ be a closed, downwards closed set, and fix some $\varepsilon > 0$. There is an open, downwards closed set A' with $A \subseteq A'$ and $\mu(A') \leq \mu(A) + \varepsilon$.*

Proof. The complement $\Sigma^\omega \setminus A$ of A is an open, upwards closed set. There exists a finite set $W \subseteq \Sigma^\omega$ such that $W\Sigma^\omega \subseteq \Sigma^\omega \setminus A$ and $\mu(W\Sigma^\omega) \geq \mu(\Sigma^\omega \setminus A) - \varepsilon$. The set $W\Sigma^\omega$ is closed. So is the set $\text{up}(W\Sigma^\omega)$. This set is also contained in $\Sigma^\omega \setminus A$. Therefore, the set $A' := \Sigma^\omega \setminus \text{up}(W\Sigma^\omega)$ is open, it contains A, and it satisfies

$$\mu(A') = 1 - \mu(\text{up}(W\Sigma^\omega)) \leq 1 - \mu(W\Sigma^\omega) \leq 1 - (\mu(\Sigma^\omega \setminus A) - \varepsilon) = \mu(A) + \varepsilon.$$

□

Corollary 20. *Fix a number $k \in \mathbb{N}$. Let $A \subseteq \Sigma^\omega$ be a closed, downwards closed set and $B \subseteq \Sigma^\omega$ be an open, upwards closed set such that*

$$\bigcap_{j=k}^{\infty} C_j \subseteq A \cup B \ .$$

Then

$$\mu(A) + \mu(B) \geq \frac{k}{k+1} \ .$$

Proof. The assertion follows by applying first Lemma 19 to A and some $\varepsilon > 0$, then Corollary 18, and then by letting ε tend to zero. □

Let us fix some $k \in \mathbb{N}$. The set

$$\widetilde{V_k} := \{q \in \Sigma^\omega \mid \mathrm{up}(\{q\}) \subseteq V_k\}$$

is upwards closed. It is open because for any $q \in \Sigma^\omega$ the set $\mathrm{up}(\{q\})$ is compact, according to Lemma 9. Using it, we can describe U_k in the following way:

$$U_k = \left\{ p \in \Sigma^\omega \;\middle|\; \mathrm{up}\left(\{p\}\right) \cap \bigcap_{j=k}^{\infty} C_j \subseteq \widetilde{V_k} \right\} \ .$$

We conclude that U_k is upwards closed as well and that

$$\bigcap_{j=k}^{\infty} C_j \subseteq (\Sigma^\omega \setminus U_k) \cup \widetilde{V_k}.$$

Since U_k is upwards closed, $\Sigma^\omega \setminus U_k$ is downwards closed. And since U_k is open, $\Sigma^\omega \setminus U_k$ is closed. Thus, Corollary 20 tells us

$$\mu(\Sigma^\omega \setminus U_k) + \mu(\widetilde{V_k}) \geq k/(k+1).$$

Using additionally $\mu(\widetilde{V_k}) \leq \mu(V_k) \leq 1/(k+1)$ we obtain $\mu(U_k) \leq 2/(k+1)$. That was to be shown. This ends the proof of Theorem 4.

Remark. One can avoid to use Lemma 19 if one uses the sets

$$U_{k,i} := \left\{ p \in \Sigma^\omega \;\middle|\; \mathrm{up}\left(\mathrm{up}\left(\{p\}\right) \cap \bigcap_{j=k}^{i} C_j \right) \subseteq V_k \right\} \ .$$

defined for any $k \in \mathbb{N}$ and $i \geq k$. They are upwards closed, and satisfy $U_{k,i} \subseteq U_{k,i+1}$ for all k, i, $\bigcup_{i \in \mathbb{N}} U_{k,i} = U_k$ for all k, and

$$\bigcap_{j=k}^{i} C_j \subseteq (\Sigma^\omega \setminus U_{k,i}) \cup \widetilde{V_k}.$$

Thus, one can directly apply Corollary 17.

References

[Calude 2002] Calude, C.: "Information and Randomness"; 2nd ed., Springer, Berlin, 2002.

[Forster 1983] Forster, O.: "Analysis I"; 4th ed., Vieweg, Braunschweig, 1983.

[Hertling 2001] Hertling, P.: "Random sets versus random sequences"; Informatik-Berichte 288, Fernuniversität Hagen, Hagen, Sept. 2001.

[Hertling and Weihrauch 1998] Hertling, P., Weihrauch, K.: "Randomness spaces"; In Larsen K., Skyum, S., and Winskel, G., editors, "Automata, Languages and Programming", volume 1443 of Lecture Notes in Computer Science, pages 796–807, Berlin, 1998. Springer. 25th International Colloquium, ICALP'98, Aalborg, Denmark, July 1998.

[Hertling and Weihrauch 2003] Hertling, P., Weihrauch, K.: "Random elements in effective topological spaces with measure"; Information and Computation, 181 (2003), 32–56.

[Li and Vitanyi 1997] Li, M., Vitanyi, P.: "An Introduction to Kolmogorov Complexity and Its Applications"; 2nd ed., Springer, New York, 1997.

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

[Weihrauch 1987] Weihrauch, K.: "Computability"; Springer, Berlin, 1987.