ELSEVIER

Theoretical Computer Science 237 (2000) 33–55

Theoretical Computer Science

www.elsevier.com/locate/tcs

Resource bounded randomness and computational complexity

Yongge Wang

Department of Electrical Engineering and Computer Science, University of Wisconsin-Milwaukee, P.O. Box 784, Milwaukee, WI 53201, USA

Received February 1996; revised February 1998
Communicated by J. Díaz

Abstract

The following is a survey of resource bounded randomness concepts and their relations to each other. Further, we introduce several new resource bounded randomness concepts corresponding to the classical randomness concepts, and show that the notion of polynomial time bounded Ko randomness is independent of the notions of polynomial time bounded Lutz, Schnorr and Kurtz randomness. Lutz has conjectured that, for a given time or space bound, the corresponding resource bounded Lutz randomness is a proper refinement of resource bounded Schnorr randomness. This conjecture is answered for the case of polynomial time bound. Moreover, we will show that polynomial time bounded Schnorr randomness is a proper refinement of polynomial time bounded Kurtz randomness. In contrast to this result, we show that the notions of polynomial time bounded Lutz, Schnorr and Kurtz randomness coincide in the case of recursive sets, thus it suffices to study the notion of resource bounded Lutz randomness in the context of complexity theory. The stochastic properties of resource bounded random sequences will be discussed in detail. Schnorr has already shown that the law of large numbers holds for p-random sequences. We will show that another important law in probability theory, the law of the iterated logarithm, holds for p-random sequences too. Hence almost all sets in the exponential time complexity class are "hard" from the viewpoint of statistics.

Keywords: Computational complexity; Randomness; p-randomness; p-measure; Law of the iterated logarithm

1. Introduction

Random sequences were first introduced by von Mises [17] as a foundation for probability theory. Von Mises thought that random sequences were a type of disordered

E-mail address: wang@cs.uwm.edu (Y. Wang).

0304-3975/00/$ - see front matter
PII: S0304-3975(98)00119-4

sequences, called "Kollektivs". The two features characterizing a Kollektiv are: the existence of limiting relative frequencies within the sequence and the invariance of these limits under the operation of an "admissible place selection". Here an admissible place selection is a procedure for selecting a subsequence of a given sequence ξ in such a way that the decision to select a term $\xi[n]$ does not depend on the value of $\xi[n]$. But von Mises' definition of an "admissible place selection" is not rigorous according to modern mathematics. After von Mises introduced the concept of "Kollektivs", the first question raised was whether this concept is consistent. Wald [21] answered this question affirmatively by showing that, for each countable set of "admissible place selection" rules, the corresponding set of "Kollektivs" has Lebesgue measure 1. The second question raised was whether all "Kollektivs" satisfy the standard statistical laws. Ville [20] showed that this was not possible by constructing a counterexample in 1939. He showed that, for each countable set of "admissible place selection" rules, there exists a "Kollektiv" which does not satisfy the law of the iterated logarithm. Ville's example defeated von Mises' plan to develop probability theory based on "Kollektivs". "Admissible place selection" rules were further developed by Tornier, Wald, Church, Kolmogorov, Loveland and others. This approach of von Mises to define random sequences is now known as the "stochastic approach".

A completely different approach to the definition of random sequences was proposed by Kolmogorov and Chaitin independently, and was further developed by Levin, Schnorr and others (see, e.g., [19]). In this approach, a notion of chaoticness is used when defining random sequences: the entropy of a finite string x is defined to be the length of the minimal string y from which x can be generated effectively. Then an infinite sequence is chaotic if all of its initial segments have the maximal possible entropy (modulo some additive constant).

Finally, Martin–Löf [14] developed a third, quantitative (measure-theoretic) approach to the notion of random sequences. This approach is free from those difficulties connected with the frequency approach of von Mises. The idea underlying this approach is to identify the notion of randomness with the notion of typicalness. A sequence is typical if it is in every large set of sequences, that is to say, if it is not in any small set of sequences. Of course, if we take small sets as the Lebesgue measure 0 sets, then no typical sequence exists. The solution to this problem given by Martin–Löf is to define the small sets to be certain *constructive* null sets.

Schnorr [18] used the martingale concept to give a uniform description of various notions of randomness. He used this concept to characterize Martin–Löf's randomness. However, he criticized Martin–Löf's concept as being too strong and proposed a less restrictive concept as an adequate formalization of a random sequence.

In this paper we will study applications of randomness concepts in complexity theory. For computational complexity classes, several definitions of pseudorandom sequences have been proposed. Blum and Micali [5], and Yao [26] gave a relatively weak definition of resource bounded random sequences. Schnorr [18] and Ko [10] introduced resource bounded versions of the notions of Martin–Löf and Kolmogorov randomness. More recently, Lutz [12, 13] pursued these ideas and systematically developed a

resource bounded measure theory. In particular, he introduced a feasible measure concept, for which he and others have shown that it is a natural tool for the quantitative analysis of the class **E**. For example, Mayordomo [15] and Juedes and Lutz [8] have shown that both the class of **P**-bi-immune sets and the class of p-incompressible sets have measure 1 in **E**.

In Section 3, we will introduce various notions of resource bounded randomness in terms of typicalness, and we investigate their relations to each other. We will show that:

(1) For polynomial time bounds, the notion of Lutz randomness is stronger than the notion of Schnorr randomness and the notion of Schnorr randomness is stronger than the notion of Kurtz randomness. The former was conjectured to be true by Lutz [13]. We will show, however, that if one considers only recursive sets, then these randomness concepts coincide.

(2) For polynomial time bounds, the notion of Ko randomness is independent of the notions of Lutz randomness, Schnorr randomness and Kurtz randomness.

In Section 4, we will study the stochastic properties of p-random sequences. The law of large numbers and the law of the iterated logarithm, which require that all random sequences should have some stochastic properties (cf. von Mises' definition of a randomness concept), play a central role in the study of probability theory (see, e.g., [6]) and in the study of classical randomness concepts (see e.g., [14, 18, 20]). Schnorr [18] showed that the first law holds for p-random sequences. In this paper we will show that the second law holds for p-random sequences too. In fact, we can show that all the standard laws of probability theory which depend only on the 0–1 distributions within the sequences hold for p-random sequences. However, the tedious work of verification is omitted in this paper. The two laws mentioned above give a quantitative characterization of the density of p-random sets. It is well known that all p-random sets have symmetric density. By the law of large numbers and by the law of the iterated logarithm for p-random sequences, it follows that all p-random sets have stochastic distributions on their elements, hence the density of most intractable sets is just "one-half". When combined with the invariance property of p-random sequences (see [22, 24]), these laws are also useful in proving that some complexity classes have p-measure 0. Note that the invariance property of p-random sequences says that if one selects a subsequence from a p-random sequence using a polynomial time bounded selection function then the selected subsequence is also p-random.

2. Notation

Let N, $Q(Q^+)$ and $R(R^+)$ denote the set of natural numbers, the set of (nonnegative) rational numbers and the set of (nonnegative) real numbers, respectively. For a real number $\alpha \in R$, $[\alpha]$ denotes the greatest integer less than or equal to α. $\Sigma = \{0, 1\}$ is the binary alphabet, Σ^* is the set of (finite) binary strings, Σ^n is the set of binary strings of length n, and Σ^∞ is the set of infinite binary sequences. The length of a string x

is denoted by $|x|$. $<$ is the length-lexicographical ordering on Σ^*, and z_n $(n \geqslant 0)$ is the nth string under this ordering. λ is the empty string. For strings $x, y \in \Sigma^*$, xy is the concatenation of x and y, $x \sqsubseteq y$ denotes that x is an initial segment of y. For a sequence $x \in \Sigma^* \cup \Sigma^\infty$ and an integer number $n \geqslant -1$, $x[0..n]$ denotes the initial segment of length $n+1$ of x ($x[0..n] = x$ if $|x| \leqslant n+1$) while $x[n]$ denotes the nth bit of x, i.e., $x[0..n] = x[0] \ldots x[n]$. Lowercase letters $\ldots, k, l, m, n, \ldots, x, y, z$ from the middle and the end of the alphabet will denote numbers and strings, respectively. The letter b is reserved for elements of Σ, and lowercase Greek letters $\xi, \eta, \ldots$ denote infinite sequences from Σ^∞.

A subset of Σ^* is called a language, a problem, or simply a set. Capital letters are used to denote subsets of Σ^* and boldface capital letters are used to denote subsets of Σ^∞. The cardinality of a language A is denoted by $\|A\|$. We identify a language A with its characteristic function, i.e., $x \in A$ if and only if $A(x) = 1$. The characteristic sequence of a language A is the infinite sequence $A(z_0)A(z_1)A(z_2)\ldots$ We freely identify a language with its characteristic sequence and the class of all languages with the set Σ^∞. For a language $A \subseteq \Sigma^*$ and a string $x \in \Sigma^*$, $A \upharpoonright x$ denotes the finite initial segment of A below x, i.e., $A \upharpoonright x = \{y : y < x \ \& \ y \in A\}$. For languages A and B, $\bar{A} = \Sigma^* - A$ is the complement of A, $A \Delta B = (A - B) \cup (B - A)$ is the symmetric difference of A and B; $A \subseteq B$ (resp., $A \subset B$) denotes that A is a subset of B (resp., $A \subseteq B$ and $B \nsubseteq A$. For a number n, $A^{=n} = \{x \in A : |x| = n\}$ and $A^{\leqslant n} = \{x \in A : |x| \leqslant n\}$.

If X is a set of strings (i.e., a language) and $\mathbf{C}$ is a set of infinite sequences (i.e., a class of languages), then $X \cdot \mathbf{C}$ denotes the set $\{w\xi : w \in X, \xi \in \mathbf{C}\}$. For each string w, $\mathbf{C}_w = \{w\} \cdot \Sigma^\infty$ is called the basic open set defined by w.

For a class $\mathbf{C}$ of languages, $Prob[\mathbf{C}]$ denotes the probability that $A \in \mathbf{C}$ when A is chosen by a random experiment in which an independent toss of a fair coin is used to decide whether a string is in A. This probability is defined whenever $\mathbf{C}$ is measurable under the usual product measure on Σ^∞.

We fix a standard polynomial time computable and invertible pairing function $\lambda x, y \langle x, y \rangle$ on Σ^*. For a set U, let $U^{[k]} = \{x : \langle k, x \rangle \in U\}$. We will use $\mathbf{P}$, $\mathbf{E}$, and $\mathbf{E}_2$ to denote the complexity classes $DTIME(poly)$, $DTIME(2^{linear})$, and $DTIME(2^{poly})$, respectively. Finally, we fix a recursive enumeration $\{P_e : e \geqslant 0\}$ of $\mathbf{P}$ such that $P_e(x)$ can be computed in $O(2^{|x|+e})$ steps (uniformly in e and x). We will abuse our notation by using the same notation for classes of sets and classes of functions ($\mathbf{P}$, etc.).

3. Resource bounded typicalness

In this section, we will introduce various notions of resource bounded randomness in terms of typicalness, and will investigate their relations to each other. In particular, we will show that the notions of resource bounded Lutz, Schnorr and Kurtz randomness coincide in the case of recursive sets. Hence, it suffices to consider the notion of resource bounded Lutz randomness in the context of complexity classes.

3.1. Resource bounded Lutz, Schnorr and Kurtz randomness

First we introduce the notions of resource bounded Lutz, Schnorr and Kurtz randomness; these notions are obtained from the corresponding classical notions by putting resource bounds on them. In the rest of the paper, unless otherwise stated, $\mathscr{C}$ denotes some given class of functions.

Definition 1 (*Ville* [20]). A *martingale* is a function $F:\Sigma^* \to R^+$ such that, for all $x \in \Sigma^*$,

$$F(x) = \frac{F(x1) + F(x0)}{2}.$$

A martingale F succeeds on a sequence $\xi \in \Sigma^\infty$ if $\limsup_n F(\xi[0..n-1]) = \infty$. $\mathbf{NULL}_F$ denotes the set of sequences on which the martingale F succeeds.

Definition 2 (*Schnorr* [18] *and Lutz* [13]). A *Lutz $\mathscr{C}$-test* is a martingale $F \in \mathscr{C}$. An infinite sequence ξ *does not withstand* the Lutz $\mathscr{C}$-test F if F succeeds on ξ. A sequence ξ is *Lutz $\mathscr{C}$-random* if it withstands all Lutz $\mathscr{C}$-tests.

Let $\mathscr{C}$-**L-NULL** be the set of sequences which do not withstand some Lutz $\mathscr{C}$-test, and let $\mathscr{C}$-**L-RAND** $= \Sigma^\infty -$ $\mathscr{C}$-**L-NULL** be the set of Lutz $\mathscr{C}$-random sequences.

Definition 3. A *Schnorr $(\mathscr{C}_1, \mathscr{C}_2)$-test* is a pair (F,h) of functions such that $F \in \mathscr{C}_1$ is a martingale and $h \in \mathscr{C}_2$ is an unbounded, nondecreasing function from N to N. An infinite sequence ξ does not withstand the Schnorr $(\mathscr{C}_1, \mathscr{C}_2)$-test (F,h) if $\limsup_n(F(\xi[0..n-1]) - h(n)) \geqslant 0$, i.e., if $F(\xi[0..n-1]) \geqslant h(n)$ *i.o.* A sequence ξ is *Schnorr $(\mathscr{C}_1, \mathscr{C}_2)$-random* if it withstands all Schnorr $(\mathscr{C}_1, \mathscr{C}_2)$-tests.

Let $(\mathscr{C}_1, \mathscr{C}_2)$-**S-NULL** be the set of sequences which do not withstand some Schnorr $(\mathscr{C}_1, \mathscr{C}_2)$-test, and let $(\mathscr{C}_1, \mathscr{C}_2)$-**S-RAND** $= \Sigma^\infty - (\mathscr{C}_1, \mathscr{C}_2)$-**S-NULL** be the set of Schnorr $(\mathscr{C}_1, \mathscr{C}_2)$-random sequences.

Definition 4. A *Kurtz $(\mathscr{C}_1, \mathscr{C}_2)$-test* is a pair (F,h) of functions such that $F \in \mathscr{C}_1$ is a martingale and $h \in \mathscr{C}_2$ is an unbounded, nondecreasing function from N to N. An infinite sequence ξ *does not withstand* the Kurtz $(\mathscr{C}_1, \mathscr{C}_2)$-test (F,h) if $\liminf_n(F(\xi[0..n-1]) - h(n)) \geqslant 0$, i.e., if $F(\xi[0..n-1]) \geqslant h(n))$ a.e. A sequence ξ is *Kurtz $(\mathscr{C}_1, \mathscr{C}_2)$-random* if it withstands all Kurtz $(\mathscr{C}_1, \mathscr{C}_2)$-tests.

Let $(\mathscr{C}_1, \mathscr{C}_2)$-**W-NULL** be the set of sequences which do not withstand some Kurtz $(\mathscr{C}_1, \mathscr{C}_2)$-test, and let $(\mathscr{C}_1, \mathscr{C}_2)$-**W-RAND** $= \Sigma^\infty - (\mathscr{C}_1, \mathscr{C}_2)$-**W-NULL** be the set of Kurtz $(\mathscr{C}_1, \mathscr{C}_2)$-random sequences.

The following relations among resource bounded Lutz, Schnorr and Kurtz randomness are immediate by definition.

Lemma 5. *For any function classes* $\mathscr{C}_1$ *and* $\mathscr{C}_2$,

$$\mathscr{C}_1\text{-}\mathbf{L}\text{-}\mathbf{RAND} \subseteq (\mathscr{C}_1, \mathscr{C}_2)\text{-}\mathbf{S}\text{-}\mathbf{RAND} \subseteq (\mathscr{C}_1, \mathscr{C}_2)\text{-}\mathbf{W}\text{-}\mathbf{RAND}$$

Moreover,

$$\mathscr{C}_1\text{-}\mathbf{L}\text{-}\mathbf{RAND} = (\mathscr{C}_1, \mathbf{all})\text{-}\mathbf{S}\text{-}\mathbf{RAND}$$

where **all** *is the class of all functions.*

Proof. It follows from the definitions. □

Lemma 6. *For any function classes* $\mathscr{C}_1$, $\mathscr{C}_2$, $\mathscr{C}_1'$ *and* $\mathscr{C}_2'$ *such that* $\mathscr{C}_1 \subseteq \mathscr{C}_1'$ *and* $\mathscr{C}_2 \subseteq \mathscr{C}_2'$,

$$(\mathscr{C}_1', \mathscr{C}_2')\text{-}\mathbf{S}\text{-}\mathbf{RAND} \subseteq (\mathscr{C}_1, \mathscr{C}_2)\text{-}\mathbf{S}\text{-}\mathbf{RAND}$$

and

$$(\mathscr{C}_1', \mathscr{C}_2')\text{-}\mathbf{W}\text{-}\mathbf{RAND} \subseteq (\mathscr{C}_1, \mathscr{C}_2)\text{-}\mathbf{W}\text{-}\mathbf{RAND}.$$

Proof. It follows from the definitions. □

Next we will give separation results for these concepts, where we restrict our results to the polynomial time case.

Theorem 7 (Schnorr [18, Satz 16.2]). *Let* $f_1, f_2 \in \mathbf{P}$ *be two functions such that* f_1/f_2 *converges to* 0 *monotonically. Then* $(\mathbf{P}, OL(f_1))\text{-}\mathbf{S}\text{-}\mathbf{RAND} \subset (\mathbf{P}, OL(f_2))\text{-}\mathbf{S}\text{-}\mathbf{RAND}$, *where* $OL(f_i) = \{cf_i : c \in N\}$.

Proof. Schnorr [18, Satz 16.2] proved that

$$(\mathbf{REC}, OL(f_1))\text{-}\mathbf{S}\text{-}\mathbf{RAND} \subset (\mathbf{REC}, OL(f_2))\text{-}\mathbf{S}\text{-}\mathbf{RAND}$$

where **REC** is the class of recursive functions. It is easily checked that his proof works for the function class **P** too. □

We showed in Wang [22] that $\mathbf{REC}\text{-}\mathbf{L}\text{-}\mathbf{RAND} \subset (\mathbf{REC}, \mathbf{REC})\text{-}\mathbf{S}\text{-}\mathbf{RAND}$ by constructing a martingale F and a sequence ξ such that F succeeds on ξ and $\xi \in (\mathbf{REC}, \mathbf{REC})\text{-}\mathbf{S}\text{-}\mathbf{RAND}$. In fact, the martingale F constructed there is computable in time n^3, whence we obtain the following theorem.

Theorem 8. *Let* $\mathscr{C}$ *be a class of recursive functions such that* $DTIME(n^3) \subseteq \mathscr{C}$. *Then* $\mathscr{C}\text{-}\mathbf{L}\text{-}\mathbf{RAND} \subset (\mathscr{C}, \mathbf{REC})\text{-}\mathbf{S}\text{-}\mathbf{RAND} \subseteq (\mathscr{C}, \mathscr{C})\text{-}\mathbf{S}\text{-}\mathbf{RAND}$.

Theorem 9 (Schnorr [18] and Kurtz [11]). $(\mathbf{P}, \mathbf{P})\text{-}\mathbf{S}\text{-}\mathbf{RAND} \subset (\mathbf{P}, \mathbf{P})\text{-}\mathbf{W}\text{-}\mathbf{RAND}$.

Proof. By Lemma 5, $(\mathbf{P},\mathbf{P})$-**S-RAND** $\subseteq (\mathbf{P},\mathbf{P})$-**W-RAND**. It was observed by Kurtz [11] that there exists a Kurtz random sequence ξ which does not satisfy the law of large numbers, whereas Schnorr showed that $(\mathbf{P},\mathbf{P})$-random sequences satisfy the law of large numbers. Whence the theorem is proved. □

The above theorems show that, in many important cases, the resource bounded Lutz randomness is stronger than the resource bounded Schnorr randomness which is again stronger than the resource bounded Kurtz randomness.

3.2. Resource bounded measure

In the rest of the paper, we will use the following notation.

(1) Let n^k-**L-RAND**, n^k-**S-RAND** and n^k-**W-RAND** denote $DTIME(n^k)$-**L-RAND**, $(DTIME(n^k),\mathscr{C}_k)$-**S-RAND** and $(DTIME(n^k),\mathscr{C}_k)$-**W-RAND**, respectively, where $\mathscr{C}_k$ is the class of n^k-time computable (with respect to the unary representation of numbers), unbounded, nondecreasing functions from N to N.
(2) A martingale F is an n^k-martingale if it is computable within a time bound in $O(n^k)$.
(3) We will say that a sequence ξ is Lutz p-random, if it is n^k-random for all $k \in N$.

In this section we will introduce a fragment of Lutz's effective measure theory which will be sufficient for our investigation.

Definition 10 (*Lutz* [13]). A class $\mathbf{C}$ of sets has *p-measure* 0 ($\mu_p(\mathbf{C}) = 0$) if there is a polynomial time computable martingale F which succeeds on every set in $\mathbf{C}$. The class $\mathbf{C}$ has *p-measure* 1 ($\mu_p(\mathbf{C}) = 1$) if $\mu_p(\bar{\mathbf{C}}) = 0$ for the complement $\bar{\mathbf{C}} = \{A \subseteq \Sigma^* : A \notin \mathbf{C}\}$ of $\mathbf{C}$.

It should be noted that Lutz [13] introduced his p-measure in terms of approximable martingales. However, the following lemma shows that it is equivalent to the above definition.

Definition 11 (*Lutz* [13]). A function F is *p-approximable* if there exists a polynomial time computable function $h(0^n,x)$ such that $|F(x) - h(0^n,x)| \leqslant 2^{-n}$ for all $n \in N$ and $x \in \Sigma^*$.

For the reason of convenience, we will use $h(n,x)$ to denote $h(0^n,x)$ in the rest of the paper unless otherwise stated.

Lemma 12 (Ambos-Spies et al. [3], Juedes and Lutz [9], and Mayordomo [15]). *For each p-approximable martingale F, there exists a polynomial time computable martingale F' such that $F'(x) \geqslant F(x)$ for all $x \in \Sigma^*$.*

The following theorem gives a characterization of p-measure 0 sets in terms of Lutz n^k-randomness concept.

Theorem 13 (Ambos-Spies et al. [3]). *Let $\mathscr{C}$ be a class of languages. Then $\mathscr{C}$ has p-measure 0 if and only if there exists a number $k \in N$ such that there is no Lutz n^k-random set in $\mathscr{C}$.*

It was proved by Ambos-Spies et al. [3] that, for each $k \in N$, there exist Lutz n^k-random sets in **E**. Hence we have the following theorem.

Theorem 14 (Lutz [13]). **E** *does not have p-measure* 0.

It has been shown that p-measure (whence Lutz n^k-randomness concept) is a natural tool for the quantitative analysis of the class **E**. We can also introduce p-measure in terms of Schnorr and Kurtz n^k-randomness concepts. In the next section, we will show that, in the context of complexity classes, the p-measures based on Schnorr and Kurtz randomness concepts coincide with the above p-measure based on Lutz randomness concept.

3.3. Resource bounded randomness and computational complexity

In this section we will show that a recursive set is polynomial time Lutz random if and only if it is polynomial time Schnorr random, and if and only if it is polynomial time Kurtz random.

In order to show that the notions of polynomial time bounded Lutz, Schnorr and Kurtz randomness coincide in the case of recursive sets, we need the following lemma which is essentially due to Allender and Strauss [1]. We will state and prove the lemma in a different fashion.

Lemma 15 (Allender and Strauss [1]). *Let F be an n^k-martingale. Then there exists and n^{k+1}-martingale F' and an n^{k+1}-time computable function $u : \Sigma^* \to N$ such that:*
(1) *For all $x \sqsubseteq y$, $u(x) \leqslant u(y)$.*
(2) *For all x, $F'(x) \geqslant u(x)$.*
(3) *For any sequence $\xi \in \Sigma^\infty$, if $\limsup_n F(\xi[0..n-1]) = \infty$, then $\lim_n u(\xi[0..n-1]) = \infty$.*

Proof. We construct u and F' in stages, where at stage s we define $F'(x)$ and $u(x)$ for all strings of length s. W.l.o.g., we may assume that $F(\lambda) = 1$.

Stage 0. Let $F'(\lambda) = F(\lambda) = 1$ and let $u(\lambda) = F(\lambda) - 1 = 0$.

Stage $s+1$. Fix a string x of length s and, for $b \in \Sigma$, let $l(xb) = F(xb)/F(x)$ if $F(x) \neq 0$ and let $l(xb) = 0$ otherwise. For the definition of $F'(xb)$ and $u(xb)$, we distinguish the following two cases.

Case 1. $u(x) + 1 \geqslant F'(x)$. Let $F'(xb) = u(x) + (F'(x) - u(x))l(xb)$ and $u(xb) = u(x)$.

Case 2. $u(x) + 1 < F'(x)$. Let $F'(xb) = u(x) + 1 + (F'(x) - u(x) - 1)l(xb)$ and $u(xb) = u(x) + 1$.

End of construction.

We show that the above constructed functions F' and u have the required properties by establishing a series of claims.

Claim 1. *F' is an n^{k+1}-martingale.*

Proof of Claim 1. By the construction, F' is n^{k+1}-computable. It is easily checked that F' has the martingale property. □

Claim 2. *For all $x \sqsubseteq y$, $u(x) \leqslant u(y)$.*

Proof of Claim 2. It follows from the construction. □

Claim 3. *For all $x \in \Sigma^*$, $F'(x) \geqslant u(x)$.*

Proof of Claim 3. The claim can be proven using a simple induction. □

Claim 4. *Given two strings $x, y \in \Sigma^*$, if $u(x) < F'(x) \leqslant u(x)+1$ and $F'(xy') \leqslant u(x)+1$ for all $y' \sqsubseteq y$, then*

$$F'(xy) = \frac{F(xy)}{F(x)} \cdot (F'(x) - u(x)) + u(x).$$

Proof of Claim 4. If $y \in \Sigma$, then the claim follows from the construction. We can assume that

$$F'(xy) = \frac{F(xy)}{F(x)} \cdot (F'(x) - u(x)) + u(x)$$

and $F'(xy) \leqslant u(x)+1$. Then, by the construction, $u(xy) = u(x)$ and

$$\begin{aligned} F'(xyb) &= u(xy) + (F'(xy) - u(xy))l(xyb) \\ &= u(xy) + (F'(xy) - u(xy))\frac{F(xyb)}{F(xy)} \\ &= u(x) + \left(\frac{F(xy)}{F(x)} \cdot (F'(x) - u(x)) + u(x) - u(x)\right) \cdot \frac{F(xyb)}{F(xy)} \\ &= u(x) + \frac{F(xyb)}{F(x)} \cdot (F'(x) - u(x)) \end{aligned}$$

where $b = 0, 1$. □

Claim 5. *For a sequence $\xi \in \Sigma^\infty$, if $\limsup_n F(\xi[0..n-1]) = \infty$, then $\lim_n u(\xi[0..n-1]) = \infty$.*

Proof of Claim 5. We prove by induction that, for each $k \in N$, there exists $n \in N$ such that $u(\xi[0..n-1]) > k$.

By the construction, $u(\lambda) \geqslant 0$.

We can assume that $k+1 \geqslant F'(\xi[0..n_1-1]) > u(\xi[0..n_1-1]) = k$ for some $n_1 \in N$. Then, by Claim 4,

$$F'(\xi[0..n-1]) = \frac{F(\xi[0..n-1])}{F(\xi[0..n_1-1])} \cdot (F'(\xi[0..n_1-1]) - u(\xi[0..n_1-1])) + u(\xi[0..n_1-1])$$

for $n \geqslant n_1$ until $F'(\xi[0..n-1]) > u(\xi[0..n_1-1]) + 1 = k+1$. Because $\limsup_n F(\xi[0..n-1]) = \infty$, there exists $n_2 > n_1$ such that

$$F(\xi[0..n_2-1]) > \frac{F(\xi[0..n_1-1])}{F'(\xi[0..n_1-1]) - u(\xi[0..n_1-1])}.$$

Hence, there exists $n_3 \leqslant n_2$ such that $F'(\xi[0..n_3-1]) > u(\xi[0..n_1-1]) + 1 = k+1$ and $u(\xi[0..n_3]) \geqslant k+1$. □

Theorem 16. *Let $k \geqslant 2$ and let ξ be an infinite recursive sequence which is Kurtz n^k-random. Then ξ is Lutz n^{k-1}-random.*

Proof. For a contradiction assume that ξ is not Lutz n^{k-1}-random. Let M be a Turing machine computing the sequence ξ, and let F be an n^{k-1}-martingale which succeeds on ξ. Let F' and u be the n^k-martingale and the n^k-time computable function corresponding to F according to Lemma 15. Define a function h as follows. □

Stage 0. Let $h(0) = 0$.

Stage $s+1$. Use at most $s+1$ steps to search for a string $x \sqsubseteq \xi[0..s]$ (using the Turing machine M) such that $u(x) \geqslant h(|x|) + 1 = h(s) + 1$. If such an x is found, then let $h(s+1) = h(s) + 1$. Otherwise let $h(s+1) = h(s)$. Go to Stage $s+2$.

End of construction.

It is straightforward to check that h is an n^2-time computable (with respect to the unary representation of numbers), unbounded, nondecreasing function and $F'(\xi[0..n-1]) \geqslant h(n)$ a.e. Hence ξ is not Kurtz n^k-random contrary to assumption. □

Corollary 17. *For any recursive sequence ξ, ξ is Lutz p-random if and only if ξ is Schnorr p-random, if and only if ξ is Kurtz p-random. That is to say,*

$$\textbf{P-L-RAND} \cap \textbf{REC} = (\textbf{P},\textbf{P})\textbf{-S-RAND} \cap \textbf{REC} = (\textbf{P},\textbf{P})\textbf{-W-RAND} \cap \textbf{REC}.$$

Corollary 17 shows that if suffices to study resource bounded Lutz randomness in the context of complexity classes. In the rest of the paper, unless otherwise stated, we will study resource bounded Lutz randomness and omit the prefix name of person.

3.4. Resource bounded Ko randomness

In the previous sections, we have studied the resource bounded randomness concepts based on martingales. In this section, we will discuss the resource bounded Ko randomness concept which is based on the constructive null covers.

Definition 18 (*Ko* [10]). A *Ko* $(\mathscr{C}_1,\mathscr{C}_2)$-*test* is a pair (U,g) where $U\in\mathscr{C}_1$ is a subset of Σ^* (notice that we identify a set with its characteristic function) and $g\in\mathscr{C}_2$ is an unbounded, nondecreasing function from N to N such that the following conditions hold.

(1) $U^{[0]}=\Sigma^*$.

(2) $U^{[k+1]}\subseteq U^{[k]}$.

(3) $Prob[U^{[k]}\cdot\Sigma^\infty]\leqslant 2^{-k}$.

A sequence ξ *does not withstand* a Ko $(\mathscr{C}_1,\mathscr{C}_2)$-test (U,g) if $\max\{m:\xi[0..n-1]\in U^{[m]}\}>g(n)$ i.o. A sequence ξ is Ko $(\mathscr{C}_1,\mathscr{C}_2)$-*random* if it withstands all Ko $(\mathscr{C}_1,\mathscr{C}_2)$-tests.

Let $(\mathscr{C}_1,\mathscr{C}_2)$-**K-NULL** be the set of sequences that do not withstand some Ko $(\mathscr{C}_1,\mathscr{C}_2)$-test, and let $(\mathscr{C}_1,\mathscr{C}_2)$-**K-RAND** $=\Sigma^\infty-(\mathscr{C}_1,\mathscr{C}_2)$-**K-NULL** be the set of Ko $(\mathscr{C}_1,\mathscr{C}_2)$-random sequences.

In the following theorems, we will show that the notion of polynomial time bounded Ko randomness is independent of the notions of polynomial time bounded Schnorr, Lutz and Kurtz randomness.

First we introduce the notion of Kolmogorov complexity. A self-delimiting Turing machine is a Turing machine whose domain is prefix free. Given a universal self-delimiting Turing machine U, the Kolmogorov complexity of a string x is defined as $KM(x)=\min\{|y|:U(y)=x\}$. An infinite sequence ξ is called Martin–Löf random if there is a constant c such that $KM(\xi[0..n-1])>n-c$ for all $n\in N$.

Lemma 19 (Ko [10, Corollary 3.9]). *Let ξ be an infinite sequence such that $KM^{2^{2n}}(\xi[0..n-1])>n-[4\log n]$ a.e., where $KM^{2^{2n}}(x)$ is the 2^{2n}-time bounded monotonic Kolmorogov complexity of x. Then $\xi\in(\mathbf{P},\log)$-**K-RAND**.*

Lemma 20. $(\mathbf{P},\log)$-**K-RAND** $\not\subseteq$ $(\mathbf{P},\log)$-**W-RAND**.

Proof. Let ξ_1 be a Martin–Löf random sequence. Define a sequence ξ by

$$\xi[n]=\begin{cases}\xi_1[n] & \text{if } n\leqslant 1,\\ 0 & \text{if } n=2^i \text{ for some } i>0,\\ \xi_1[n-[\log n]] & \text{otherwise.}\end{cases}$$

Then

$$\begin{aligned}KM^{2^{2n}}(\xi[0..n-1]) &\geqslant KM(\xi[0..n-1])\\ &\geqslant KM(\xi_1[0..n-[\log n]-1])-c_1\\ &\geqslant n-[\log n]-c\\ &\geqslant n-[4\log n] \quad \text{a.e.}\end{aligned}$$

Hence, by Lemma 19, $\xi\in(\mathbf{P},\log)$-**K-RAND**.

It remains to show that $\xi \notin (\mathbf{P}, \log)$-**W-RAND**. Define a martingale F by

$$F(\lambda) = 1,$$
$$F(xb) = \begin{cases} 2(1-b)F(x) & \text{if } |x| = 2^i \text{ for some } i > 0, \\ F(x) & \text{otherwise,} \end{cases}$$

where $b = 0, 1$. Then $F(\xi[0..n-1]) \geqslant n/2$ for all $n \in N$. Whence $\xi \notin (\mathbf{P}, \log)$-**W-RAND**. □

As a corollary of the proof of Lemma 20, we have the following result.

Corollary 21. *There exists a Ko* $(\mathbf{P}, \log)$*-random set which is not* **P***-immune.*

Remark. Using Meyer and McCreight's weighted priority diagonalization, Ko [10] showed some stronger results about resource bounded Kolmogorov complexity, which can be used to produce a sequence in the double exponential time complexity class (w.r.t. the length of the initial segment of the sequence) which is an element of $(\mathbf{P}, \log)$-**K-RAND** $\cap$ $(\mathbf{P}, \log)$-**W-NULL**.

Lemma 22. *Let* $A \in \mathbf{E}_2$. *Then* $A \notin (\mathbf{P}, \log)$-**K-RAND**.

Proof. Assume that $A \in \mathrm{DTIME}(2^{n^k})$, and let ξ be the characteristic sequence of A. Then $\xi[0..n-1]$ can be computed in $n^{1+(\log n)^k} \leqslant 2^n$ steps for almost all n.

Let $U^{[i]} = \{\xi[0..i-1]x : \xi[0..i-1]$ can be computed in $i + |x|$ steps$\}$. Then $U \in \mathbf{P}$ and the following conditions hold.

(1) $U^{[i+1]} \subseteq U^{[i]}$.

(2) $Prob[U^{[i]} \cdot \Sigma^\infty] = 2^{-i}$.

(3) For almost all n, $\xi[0..n-1] \in U^{[[\log n]]}$, that is to say, $\max\{m : \xi[0..n-1] \in U^{[M]}\} \geqslant [\log n]$ for almost all n.

Hence $\xi \notin (\mathbf{P}, \log)$-**K-RAND**. □

Lemma 23. **P-L-RAND** $\not\subseteq (\mathbf{P}, \log)$-**K-RAND**.

Proof. Lutz [13] has shown that there is a p-random set A in $\mathrm{DTIME}(2^{n^2})$. Whence the lemma follows from Lemma 22. □

By Lemmas 20 and 23, we get the following independence results.

Theorem 24. (1) **P-L-RAND** *and* $(\mathbf{P}, \log)$-**K-RAND** *are independent.*

(2) $(\mathbf{P}, \log)$-**S-RAND** *and* $(\mathbf{P}, \log)$-**K-RAND** *are independent.*

(3) $(\mathbf{P}, \log)$-**W-RAND** *and* $(\mathbf{P}, \log)$-**K-RAND** *are independent.*

4. The law of the iterated logarithm for p-random sequences

In this section we will study the stochastic properties of p-random sequences. We will show that the law of the iterated logarithm holds for p-random sequences. Note that Schnorr has already shown that the law of large numbers holds for p-random sequences.

Definition 25. An infinite sequence $\xi \in \Sigma^\infty$ satisfies *the law of large numbers* if

$$\lim_n \frac{\sum_{i=0}^{n-1} \xi[i]}{n} = \frac{1}{2}.$$

Theorem 26 (Schnorr [18]). *Let $\xi \in \Sigma^\infty$ be an n^2-random sequence. Then ξ satisfies the law of large numbers.*

For a nonempty string $x \in \Sigma^*$, let

$$S(x) = \sum_{i=0}^{|x|-1} x[i]$$

denote the *number* of 1's in x, and let

$$S^*(x) = \frac{2 \cdot S(x) - |x|}{\sqrt{|x|}}$$

denote the *reduced number* of 1's in x. Note that $S^*(x)$ amounts to measuring the deviations of $S(x)$ from $|x|/2$ in units of $\frac{1}{2}\sqrt{|x|}$. In probability theory, $S(x)$ is called the *number of successes* and $S^*(x)$ is called the *reduced number of successes*.

The law of large numbers says that, for an n^2-random sequences ξ, the limit of $S(\xi[0..n-1])/n$ is $\frac{1}{2}$. But it says nothing about the reduced deviation $S^*(\xi[0..n-1])$. It is intuitively clear that, for a random sequence ξ, $S^*(\xi[0..n-1])$ will sooner or later take on arbitrary large values. Moderate values of $S^*(\xi[0..n-1])$ are most probable, but the maxima will slowly increase. How fast? Can we give an optimal upper bound for the fluctuations of $S^*(\xi[0..n-1])$? The law of the iterated logarithm, which was first discovered by Khintchine for the classical cases, gives a satisfactory answer for the above questions.

Definition 27. A sequence $\xi \in \Sigma^\infty$ satisfies *the law of the iterated logarithm* if

$$\limsup_{n\to\infty} \frac{2\sum_{i=0}^{n-1} \xi[i] - n}{\sqrt{2n \ln\ln n}} = 1$$

and

$$\liminf_{n\to\infty} \frac{2\sum_{i=0}^{n-1} \xi[i] - n}{\sqrt{2n \ln\ln n}} = -1.$$

In this section, we will prove that the law of the iterated logarithm holds for p-random sequences also.

There are various applications of the law of the iterated logarithm. For example, in [22, 24], we used this law to prove that both the class of $\mathbf{P}$-Δ-levelable sets and the class of sets which have optimal polynomial time unsafe approximations have p-measure 0, hence p-random sets are not Δ-levelable. That is to say, for every p-random set $A \in \mathbf{E}_2$ and for every polynomial time computable set B, there is another polynomial time computable set B' such that

$$\forall k \in N\ \exists n \in N\ (\|(A \Delta B) \upharpoonright z_n\| > \|(A \Delta B') \upharpoonright z_n\| + k).$$

In other words, no polynomial time computable set can approximate a p-random set optimally.

We will now introduce some technical tools for the proof of the law of the iterated logarithm.

In the traditional proof of the law of the iterated logarithm for random sequences, the first and the second Borel–Cantelli lemmas are used. Lutz [12] has proved the first Borel–Cantelli lemma for p-measure. Roughly speaking, let F_i $(i = 0, 1, \ldots)$ be a sequence of uniformly polynomial time computable density functions (the definition will be given below). If $F_i(\lambda) \leqslant 2^{-i}$ for all i, then we can define a martingale $F = \sum_{i=0}^{\infty} F_i$ which is p-approximable by $h(n, x) = \sum_{i=0}^{n} F_i(x)$ such that, for each sequence $\xi \in \Sigma^{\infty}$, if ξ is covered by infinitely many F_i, then F succeeds on ξ.

But in the proof of the law of the iterated logarithm, we can only define a sequence of density functions F_i $(i = 1, 2, \ldots)$ such that $F_i(\lambda) \leqslant i^{-\alpha}$ where $\alpha > 1$. And $h(n, x) = \sum_{i=1}^{n} F_i(x)$ is not a p-approximation of $F = \sum_{i=1}^{\infty} F_i$. Hence, we cannot use Lutz-Borel–Cantelli lemma to prove this law directly. In our next proof, the main objective, roughly speaking, is to use p-approximations of $h(n, x) = \sum_{i=1}^{n} F_i(x) + \int_{n+1}^{\infty} \mathrm{d}m/(m-1)^{\alpha}$ to define a p-approximation of $F = \sum_{i=1}^{\infty} F_i$.

Definition 28 (*Lutz* [12]). A function $F : \Sigma^* \to R^+$ is a *density function* if, for all $x \in \Sigma^*$,

$$F(x) \geqslant \frac{F(x0) + F(x1)}{2}.$$

Note that the density functions defined in the Definition 28 is classically known as supermartingales.

Lemma 29. *Given a polynomial time computable function $F(i, x)$ and a nondecreasing, time constructible function $u : N \to N$ satisfying*

$$2F(i, x) \geqslant F(i, x0) + F(i, x1)$$

for all i and all $|x| \geqslant u(i)$, the set $\bigcup_{i=0}^{\infty} \mathbf{NULL}_{F_i}$ has p-measure 0, where $\mathbf{NULL}_{F_i} = \{\xi \in \Sigma^{\infty} : \limsup_n F(i, \xi[0..n-1]) = \infty\}$.

Remark. If we only require that F be p-approximable, then Lemma 29 still holds.

Proof. By the p-union lemma of Lutz [13], it suffices to show that there exists a polynomial time computable function $F'(i,x)$ such that $F'_i(x)=F'(i,x)$ is a density function for each i and

$$\bigcup_{i=0}^{\infty} \mathbf{NULL}_{F_i} \subseteq \bigcup_{i=0}^{\infty} \mathbf{NULL}_{F'_i}. \tag{1}$$

Let v be a function defined by the recursion

$$v(1) = u(1),$$
$$v(k+1) = \max\{k+1, u(k+1), v(k)\} + 1.$$

We define the function F' as follows. If $i \neq 2^{v(k)}$ for any $k \in N$, then let $F'(i,x)=0$ for all $x \in \Sigma^*$. If $i = 2^{v(k)}$ for some $k \in N$, then $F'(i,x)$ is defined by

$$F'(i,x) = \begin{cases} \sum_{|y|=u(k)-|x|} 2^{|x|-u(k)} F(k,xy) & \text{if } |x| < u(k), \\ F(k,x) & \text{if } |x| \geqslant u(k). \end{cases}$$

It is obvious that, for every k, $F'_k(x)=F'(k,x)$ is a density function and

$$\mathbf{NULL}_{F_i} \subseteq \mathbf{NULL}_{F'_{2^{v(k)}}}.$$

Hence (1) holds. □

In our next proof, we will use the following variant of DeMoivre–Laplace limit theorem.

Theorem 30 (Feller [6, p. 144]). *Let $u: N \to R^+$ be a function satisfying*

$$\tfrac{1}{2}\sqrt{\ln\ln n} \leqslant u(n) \leqslant 2\sqrt{\ln\ln n}$$

for all n. Then there exists a constant c_0 which is independent of u such that, for all $u(n) > c_0$.

$$u^{-2}\mathrm{e}^{-u^2/2} \leqslant Prob[\{\xi \in \Sigma^\infty\colon S^*(\xi[0..n-1]) > u(n)\}] \leqslant \mathrm{e}^{-u^2/2}.$$

We will also use the following lemma from Feller [6, p. 158].

Lemma 31 (Feller [6, p. 158]). *Let $u: N \to R^+$ be a function. Then there exists a constant c_1 which is independent of both u and n such that if*

$$\mathbf{C} = \{\xi \in \Sigma^\infty\colon S(\xi[0..k-1]) - \tfrac{1}{2}k > u(n) \text{ for some } k \leqslant n\},$$

then

$$Prob[\mathbf{C}] \leqslant \frac{1}{c_1} Prob[\{\xi \in \Sigma^\infty\colon S(\xi[0..n-1]) - \tfrac{1}{2}n > u(n)\}].$$

Now we are ready to prove our main theorem of this section.

Theorem 32. *Let*

$$\mathbf{U} = \left\{ \xi \in \Sigma^\infty : \limsup_{n\to\infty} \frac{S^*(\xi[0..n-1])}{\sqrt{2\ln\ln n}} = 1 \right\}.$$

Then $\mathbf{U}$ *has p-measure* 1. *This means that if we let* $\mathbf{Y}_k$ $(k \geqslant 1)$ *be the set of infinite sequences such that*

$$S(\xi[0..n-1]) > \tfrac{1}{2}n + \left(1 + \frac{1}{k}\right)\sqrt{\tfrac{1}{2}n\ln\ln n}$$

for infinitely many n, and let $\mathbf{X}_k$ $(k \geqslant 1)$ *be the set of infinite sequences such that*

$$S(\xi[0..n-1]) > \tfrac{1}{2}n + \left(1 - \frac{1}{k}\right)\sqrt{\tfrac{1}{2}n\ln\ln n}$$

for finitely many n, then

$$\Sigma^\infty - \mathbf{U} = \left(\bigcup_{k=1}^{\infty} \mathbf{X}_k\right) \cup \left(\bigcup_{k=1}^{\infty} \mathbf{Y}_k\right)$$

has p-measure 0.

For reasons of symmetry, the above theorem implies that the following set has p-measure 1:

$$\mathbf{V} = \left\{ \xi \in \Sigma^\infty : \liminf_{n\to\infty} \frac{S^*(\xi[0..n-1])}{\sqrt{2\ln\ln n}} = -1 \right\}.$$

Proof (*Outline*). The proof goes on as follows. First, we will show uniformly that every $\mathbf{Y}_k$ has p-measure 0, that is to say, $\mathbf{Y} = \bigcup_{k=1}^{\infty} \mathbf{Y}_k$ has p-measure 0. Then we will use this result to show that $\mathbf{X} = \bigcup_{k=1}^{\infty} \mathbf{X}_k$ has p-measure 0. In order to show that $\mathbf{Y}_k$ has p-measure 0, we define a sequence $n_0, n_1, \ldots$ of natural numbers. For each n_i, we define a martingale $F_k(i,x)$ in such a way that, for all $m > l > n_i$, $F_k(i,x[0..l]) = F_k(i,x[0..m])$. That is to say, $F_k(i,x)$ is defined to check the 0–1 distributions on strings in $\Sigma^{n_{i+1}-1}$. If a string $x \in \Sigma^{n_i}$ seems to be an initial segment of some sequences in $\mathbf{Y}_k$, $F_k(i,x)$ is then given a large value; Otherwise, $F_k(i,x)$ is given a small value. Lastly, $F_k(x) = \sum_{i=0}^{\infty} F_k(i,x)$ succeeds on every sequence in $\mathbf{Y}_k$. All we need to do is to choose n_i and to define $F_k(i,x)$ appropriately so that our proving process is uniformly polynomial time computable and $F_k(x)$ succeeds on all sequences in $\mathbf{Y}_k$.

Proof of Theorem 32. First we show that $\mathbf{Y} = \bigcup_{k=1}^{\infty} \mathbf{Y}_k$ has p-measure 0.

Let $\alpha = 1 + 1/k$, $\beta = 1 + 1/3k$ and $n_i = [\beta^i] + 1$ $(i = 1, 2, \ldots)$. Then $1 < \beta < \sqrt{\alpha}$. Let

$$\mathbf{Y}_{kj} = \{\xi \in \Sigma^\infty : S(\xi[0..n-1]) - \tfrac{1}{2}n > \alpha\sqrt{\tfrac{1}{2}n_i \ln\ln n_i} \text{ for some } n_i \leqslant n < n_{i+1}\}$$

and

$$\mathbf{Y}'_k = \{\xi \in \Sigma^\infty : \xi \in \mathbf{Y}_{k,i} \text{ for infinitely many } i\}.$$

Then $\mathbf{Y}_k \subseteq \mathbf{Y}'_k$. So it suffices to show that $\mathbf{Y}' = \bigcup_{k=1}^{\infty} \mathbf{Y}'_k$ has p-measure 0.

Let

$$F_i(k,x) = Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x],$$

where $Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x]$ is the conditional probability of $\mathbf{Y}_{k,i}$ under the condition $\mathbf{C}_x$, and let

$$F(k,x) = \sum_{i=0}^{\infty} F_i(k,x).$$

It is straightforward that, for each $k \in N$, $F_k(x) = F(k,x)$ is a martingale and, for each $\xi \in \mathbf{Y}'_k$, $F_k(x) = F(k,x)$ succeeds on ξ.

By the remark of Lemma 29, it suffices to construct a p-approximable function G and a time constructible function $v : N \to N$ such that, for all $k \in N$ and for all $|x| > v(k)$,

$$2G(k,x) \geqslant G(k,x0) + G(k,x1),$$

$$G(k,x) \geqslant F(k,x).$$

Let

$$G(k,x) = \sum_{i \leqslant [4\ln|x|/\ln\beta]} Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x] + \sum_{i > [4\ln|x|/\ln\beta]} \int_i^{i+1} \frac{\mathrm{d}n}{c((n-1)\ln\beta)^{\alpha}}$$

where c is a constant which will be given below.

Claim 1. *$G(k,x)$ is p-approximable (w.r.t. $k + |x|$).*

Proof of Claim 1. In the expression of G, the second clause

$$\sum_{i > [4\ln|x|/\ln\beta]} \int_i^{i+1} \frac{\mathrm{d}n}{c \cdot ((n-1)\ln\beta)^{\alpha}} = \frac{1}{c(\ln\beta)^{\alpha}(\alpha-1)} \left(\left[\frac{4\ln|x|}{\ln\beta} \right] \right)^{1-\alpha}$$

is p-approximable (w.r.t. $k + |x|$).

If $i \leqslant [4\ln|x|/\ln\beta]$, then $n_i \leqslant |x|^4 + 1$. Hence, the values of $Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x]$ in the first clause of $G(k,x)$ can be computed using binomial coefficients of base less than $n_{i+1} \leqslant \beta \cdot (|x|^4 + 1)$. That is to say, the first clause of $G(k,x)$ can be computed in time polynomial in $k + |x|$. □

Claim 2. *Let c_0 be the constant in Theorem 30, c_1 be the constant in Lemma 31, $c = c_1/3 > 0$ and $u_1(k) = [6e^{2c_0^2}k^2]$. Then the following conditions hold for all k.*

(1) *For all $i > u_1(k)$,*

$$Prob[\mathbf{Y}_{k,i}] \leqslant \int_i^{i+1} \frac{\mathrm{d}n}{c((n-1)\ln\beta)^{\alpha}}.$$

(2) *For all $i > \max\{u_1(k), [4\ln|x|/\ln\beta]\}$,*

$$Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x] \leqslant \int_i^{i+1} \frac{\mathrm{d}n}{c((n-1)\ln\beta)^{\alpha}}.$$

Proof of Claim 2. (1) By Lemma 31,

$$\begin{aligned} Prob[\mathbf{Y}_{k,i}] &\leqslant \frac{1}{c_1} Prob[\{\xi \in \Sigma^\infty\colon\ S(\xi[0..n_{i+1}-1]) - \tfrac{1}{2}n_{i+1} > \alpha\sqrt{\tfrac{1}{2}n_i \ln\ln n_i}\}] \\ &= \frac{1}{c_1} Prob\left[\left\{\xi \in \Sigma^\infty\colon\ S^*(\xi[0..n_{i+1}-1]) > \alpha\sqrt{2\frac{n_i}{n_{i+1}}\ln\ln n_i}\right\}\right]. \end{aligned}$$

By a simple computation, it can be shown that if $i > 6k^2$ then $n_i\alpha^2/n_{i+1} > \alpha$. Hence, for $i > 6k^2$,

$$Prob[\mathbf{Y}_{k,i}] \leqslant c_1^{-1} Prob[\{\xi \in \Sigma^\infty\colon\ S^*(\xi[0..n_{i+1}-1]) > \sqrt{2\alpha\ln\ln n_i}\}].$$

If $i > 6e^{c_0^2}k^2$, then $\sqrt{2\alpha\ln\ln n_i} > c_0$. By the DeMoivre–Laplace limit theorem (Theorem 30) we get, therefore, for $i > u_1(k) = [6e^{c_0^2}k^2]$,

$$\begin{aligned} Prob[\mathbf{Y}_{k,i}] &\leqslant c_1^{-1}\mathrm{e}^{-\alpha\ln\ln n_i} \\ &= \frac{1}{c_1(\ln n_i)^\alpha} \\ &< \frac{1}{c(i\ln\beta)^\alpha} \\ &< \int_i^{i+1} \frac{\mathrm{d}n}{c((n-1)\ln\beta)^\alpha}. \end{aligned}$$

(2) First we notice the following fact: for $x \in \Sigma^{\leqslant n_i}$,

$$\begin{aligned} Prob[\mathbf{Y}_{k,i}|\mathbf{C}_{0^{|x|}}] &\leqslant Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x] \\ &\leqslant Prob[\mathbf{Y}_{k,i}|\mathbf{C}_{1^{|x|}}] \\ &= Prob[\mathbf{Y}_{k,i,|x|}|\mathbf{C}_{0^{|x|}}], \end{aligned}$$

where

$$\begin{aligned} Y_{k,i,j} = \{\xi \in \Sigma^\infty\colon\ & S(\xi[0..n-1]) - \tfrac{1}{2}n + j \\ & > \alpha\sqrt{\tfrac{1}{2}n_i\ln\ln n_i} \text{ for some } n,\ n_i \leqslant n < n_{i+1}\} \end{aligned}$$

for $i, j \in N$.

It is easily checked that if $i > u_1(k) = [6e^{2c_0^2}k^2]$ then $n_i\alpha^2/n_{i+1} > \alpha$ and $\sqrt{2\alpha\ln\ln n_i} - |x|/\sqrt{n_{i+1}} > c_0$. Hence, in the same way as in (1), we can show that

$$\begin{aligned} Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x] &= 2^{|x|} Prob[\mathbf{Y}_{k,i} \cap \mathbf{C}_x] \\ &\leqslant 2^{|x|} Prob[\mathbf{Y}_{k,i,|x|} \cap \mathbf{C}_{0^{|x|}}] \\ &\leqslant \sum_{y\in\Sigma^{|x|}} Prob[\mathbf{Y}_{k,i,|x|} \cap \mathbf{C}_y] \\ &= Prob[\mathbf{Y}_{k,i,|x|}] \\ &\leqslant c_1^{-1} Prob[\{\xi \in \Sigma^\infty\colon\ S(\xi[0..n_{i+1}-1]) - \tfrac{1}{2}n_{i+1} + |x| \\ &\qquad > \alpha\sqrt{\tfrac{1}{2}n_i\ln\ln n_i}\}] \end{aligned}$$

$$
\begin{aligned}
&= c_1^{-1} Prob\left[\left\{\xi \in \Sigma^\infty:\ S^*(\xi[0..n_{i+1}-1])\right.\right.\\
&\qquad \left.\left. > \alpha\sqrt{2\frac{n_i}{n_{i+1}}\ln\ln n_i} - \frac{2|x|}{\sqrt{n_{i+1}}}\right\}\right]\\
&\leqslant c_1^{-1} Prob\left[\left\{\xi \in \Sigma^\infty:\ S^*(\xi[0..n_{i+1}-1])\right.\right.\\
&\qquad \left.\left. > \sqrt{2\alpha\ln\ln n_i} - \frac{2|x|}{\sqrt{n_{i+1}}}\right\}\right]\\
&\leqslant c_1^{-1}\mathrm{e}^{-\alpha\ln\ln n_i + (2|x|/\sqrt{n_{i+1}})\sqrt{2\alpha\ln\ln n_i}}\\
&\leqslant c_1^{-1}\mathrm{e}^{(2\sqrt[4]{n_{i+1}}\sqrt{2\alpha\ln\ln n_i}/\sqrt{n_{i+1}})}\mathrm{e}^{-\alpha\ln\ln n_i} \qquad \left(\text{by } i > \left[\frac{4\ln|x|}{\ln\beta}\right]\right)\\
&\leqslant 3c_1^{-1}\mathrm{e}^{-\alpha\ln\ln n_i}\\
&= \frac{3}{c_1(\ln n_i)^\alpha}\\
&\leqslant \frac{3}{c_1(i\ln\beta)^\alpha}\\
&= \frac{1}{c(i\ln\beta)^\alpha}\\
&\leqslant \int_i^{i+1}\frac{\mathrm{d}n}{c((n-1)\ln\beta)^\alpha}. \qquad \square
\end{aligned}
$$

Claim 3. *Let $v(k)\geqslant\beta^{u_1(k)/4}$ be a time constructible function. Then, for all $k\in N$ and for all $|x|>v(k)$,*

$$2G(k,x) \geqslant G(k,x0) + G(k,x1),$$
$$G(k,x) \geqslant F(k,x).$$

Proof of Claim 3. If $[4\ln|x0|/\ln\beta] = [4\ln|x|/\ln\beta]$, then from the definition of G,

$$2G(k,x) = G(k,x0) + G(k,x1),$$

For $|x|>v(k)$, if $m=[4\ln|x0|/\ln\beta]=[4\ln|x|/\ln\beta]+1$, then $m>u_1(k)$. So, by Claim 2 and by the definition of G, we have

$$
\begin{aligned}
2G(k,x) - G(k,x0) - G(k,x1) = \int_m^{m+1}\frac{2\mathrm{d}n}{c\cdot((n-1)\ln\beta)^\alpha} &- Prob[\mathbf{Y}_{k,m}|\mathbf{C}_{x0}]\\
&- Prob[\mathbf{Y}_{k,m}|\mathbf{C}_{x1}] \geqslant 0.
\end{aligned}
$$

By Claim 2, for all $|x|>v(k)$ (i.e., $[4\ln|x|/\ln\beta]>u_1(k)$), we have

$$G(k,x) - F(k,x) = \sum_{i>[4\ln|x|/\ln\beta]}\left(\int_i^{i+1}\frac{\mathrm{d}n}{c\cdot((n-1)\ln\beta)^\alpha} - Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x]\right) \geqslant 0.$$

$\square$

All these claims complete the proof that $\bigcup_k \mathbf{Y}_k$ has p-measure 0.

Next we show that $\mathbf{X} = \bigcup_{k=6}^{\infty} \mathbf{X}_k$ has p-measure 0. Note that $\mathbf{X}_1, \ldots, \mathbf{X}_5$ are all included in $\mathbf{X}_6$.

Let $\alpha = 1 - (1/k)$ $(k > 5)$, $\beta = k^4$, $\gamma = 1 - (1/k^3)$ and $n_i = \beta^i$ $(i = 1, 2, \ldots)$. Then

$$\frac{\beta - 1}{\beta} > \gamma > \alpha.$$

Let

$$D_i(\xi) = S(\xi[0..n_i - 1]) - S(\xi[0..n_{i-1} - 1])$$

and

$$\mathbf{X}_{k,i} = \{\xi \in \Sigma^{\infty} : \ D_i(\xi) - \tfrac{1}{2}(n_i - n_{i-1}) > \gamma\sqrt{\tfrac{1}{2} n_i \ln\ln n_i}\}.$$

We first show that if $i > e^{c_0^2}$ (where c_0 is the constant in Theorem 30), then $Prob[\mathbf{X}_{k,i}] \geqslant i^{-1}$.

$$Prob[\mathbf{X}_{k,i}] = Prob\left[\left\{\xi \in \Sigma^{\infty} : \ \frac{2D_i(\xi) - (n_i - n_{i-1})}{\sqrt{n_i - n_{i-1}}} > \gamma\sqrt{2\frac{n_i}{n_i - n_{i-1}} \ln\ln n_i}\right\}\right].$$

Here $n_i/(n_i - n_{i-1}) = \beta/(\beta - 1) < \gamma^{-1}$. Hence

$$Prob[\mathbf{X}_{k,i}] \geqslant Prob\left[\left\{\xi \in \Sigma^{\infty} : \ \frac{2D_i(\xi) - (n_i - n_{i-1})}{\sqrt{n_i - n_{i-1}}} > \sqrt{2\gamma \ln\ln n_i}\right\}\right].$$

If $i > e^{c_0^2}$, then $\sqrt{2\gamma \ln\ln n_i} > c_0$. So, by the DeMoivre–Laplace limit theorem (Theorem 30), for $i > e^{c_0^2}$,

$$Prob[\mathbf{X}_{k,i}] \geqslant \frac{1}{2\gamma \ln\ln n_i} \mathrm{e}^{-\gamma \ln\ln n_i} = \frac{1}{2\gamma (\ln\ln n_i)(\ln n_i)^{\gamma}}.$$

Since $n_i = \beta^i$ and $\gamma < 1$, there is a time constructible function $u_2(k) > e^{c_0^2}$ such that if $i > u_2(k)$ then $Prob[\mathbf{X}_{k,i}] \geqslant i^{-1}$.

Let

$$\mathbf{Z}_{k,0} = \{\xi \in \Sigma^{\infty} : \ \xi \notin \mathbf{X}_{k,i} \text{ for all } i\},$$

and let F be a density function defined as follows. For all $x \in \Sigma^{n_i}$ and $y \in \Sigma^{n_{i+1}}$ with $x \sqsubseteq y$, let

$$F(k, 0, y) = \begin{cases} 0 & \text{if } y \cdot \Sigma^{\infty} \subseteq \mathbf{X}_{k,i+1}, \\ \dfrac{i+1}{i} F(k, 0, x) & \text{if } y \cdot \Sigma^{\infty} \notin \mathbf{X}_{k,i+1}. \end{cases}$$

For all other $z \in \Sigma^*$ with $x \sqsubseteq z \sqsubseteq y$, let

$$F(k, 0, z) = \frac{F(k, 0, z0) + F(k, 0, z1)}{2}.$$

Using binomial coefficients, we can compute $F(k,0,x)$ in time polynomial in $k+|x|$ and, for all $k \in N$ and $|x| > \beta^{e^{c_0^2}}$,

$$2F(k,0,x) \geqslant F(k,0,x0) + F(k,0,x1).$$

And, for all $\xi \in \mathbf{Z}_{k,0}$,

$$F(k,0,\xi[0..n_i - 1]) = \frac{2}{1} \cdot \frac{3}{2} \cdots \frac{i}{i-1} = i.$$

Hence, by Lemma 29, $\mathbf{Z}_{k,0}$ has p-measure 0.

Next, divide the class $\mathbf{X}_{k,i}$ $(i = 1,2,\ldots)$ into two subclasses $\mathbf{X}_{k,i}^{(1,1)}$ and $\mathbf{X}_{k,i}^{(1,2)}$ such that both $\sum_i Prob[\mathbf{X}_{k,i}^{(1,1)}] = \infty$ and $\sum_i Prob[\mathbf{X}_{k,i}^{(1,2)}] = \infty$. Let

$$\mathbf{Z}_{k,1} = \{\xi \in \Sigma^\infty\colon\ \xi \notin \mathbf{X}_{k,i}^{(1,1)} \text{ for all } i\} \cup \{\xi \in \Sigma^\infty\colon\ \xi \notin \mathbf{X}_{k,2}^{(1,2)} \text{ for all } i\}.$$

In the same way as showing that $\mathbf{Z}_{k,0}$ has p-measure 0, we can define a density function $F(k,1,x)$ to show that $\mathbf{Z}_{k,1}$ has p-measure 0.

Applying, in turn, this statement to the classes $\mathbf{X}_{k,i}^{(1,1)}$ and $\mathbf{X}_{k,i}^{(1,2)}$, we can define p-measure 0 sets $\mathbf{Z}_{k,3}$ and $\mathbf{Z}_{k,4}$, and so on. Let

$$\mathbf{Z} = \bigcup_k \bigcup_i \mathbf{Z}_{k,i}.$$

Then $\mathbf{Z}$ is a p-union of p-measure 0 sets $\mathbf{Z}_{k,i}$ $(k,i \in N)$. Hence, by Lemma 29, $\mathbf{Z}$ has p-measure 0.

Let

$$\mathbf{X}'_k = \{\xi \in \Sigma^\infty\colon\ \xi \in \mathbf{X}_{k,i} \text{ for finitely many } i\}.$$

Then $\mathbf{X}' = \bigcup_{k=6}^\infty \mathbf{X}'_k \subseteq \mathbf{Z}$, hence $\mathbf{X}'$ has p-measure 0.

The last step of the proof is to show that, in the definition of $\mathbf{X}_{k,i}$, the term $S(\xi([0..n_{i-1} - 1])$ can be neglected. From the part (1) of this theorem, we know that $\mathbf{Y}$ has p-measure 0, hence $\mathbf{Y} \cup \mathbf{X}'$ has p-measure 0. For each $\xi \in \Sigma^\infty - (\mathbf{Y} \cup \mathbf{X}')$, we can find a large enough n_0 so that, for all $i > n_0$,

$$|S(\xi[0..n_{i-1} - 1]) - \tfrac{1}{2}n_{i-1}| < 2\sqrt{\tfrac{1}{2}n_{i-1} \ln\ln n_{i-1}}.$$

By the choice of γ,

$$1 - \gamma < \left(\frac{\gamma - \alpha}{2}\right)^2.$$

So

$$4n_{i-1} = 4\frac{n_i}{\beta} < n_i(\gamma - \alpha)^2.$$

Hence

$$S(\xi[0..n_{i-1} - 1]) - \tfrac{1}{2}n_{i-1} > -(\gamma - \alpha)\sqrt{\tfrac{1}{2}n_i \ln\ln n_i}. \tag{2}$$

Because $\xi \notin \mathbf{X}', \xi \in \mathbf{X}_{k,i}$ for infinitely many i, i.e.,

$$D_i(\xi) - \tfrac{1}{2}(n_i - n_{i-1}) > \gamma\sqrt{\tfrac{1}{2}n_i \ln\ln n_i} \text{ i.o.} \tag{3}$$

Adding (2) to (3), we obtain that, for each sequence $\xi \in \Sigma^\infty - (\mathbf{X}' \cup \mathbf{Y})$, there are infinitely many n such that

$$S(\xi[0..n-1]) > \tfrac{1}{2}n + \alpha\sqrt{\tfrac{1}{2}n \ln\ln n}.$$

So $\Sigma^\infty - (\mathbf{X}' \cup \mathbf{Y}) \subseteq \Sigma^\infty - \mathbf{X}$, i.e., $\mathbf{X} \subseteq \mathbf{X}' \cup \mathbf{Y}$. Hence $\mathbf{X}$ has p-measure 0. □

Corollary 33. *There exists a number $k \in N$ such that every n^k-random sequence satisfies the law of the iterated logarithm.*

Acknowledgements

I am grateful to my thesis advisor Professor Ambos-Spies for introducing me to this field and for the many crucial discussions during the writing of this paper. I am also grateful to Professor Lutz for pointing out an error in Claim 1 of the Section 4 and for many suggestions on the presentation of my paper [23] which consists of the Section 4 of this paper. Lastly, I would like to thank Professor Mayordomo for the discussions and thank Doctor Brian King for helping me improve the presentation of this paper.

References

[1] E. Allender, M. Strauss, Measure on **P**: robustness of the notion, in: Proc. MFCS '95, Lecture Notes in Computer Science, vol. 969, Springer, Berlin, 1995, pp. 129–138.
[2] K. Ambos-Spies, E. Mayordomo, Y. Wang, X. Zheng, Resource-bounded balanced genericity, stochasticity and weak randomness, in: Proc. STACS '96, Lecture Notes in Computer Science, vol. 1046, Springer, Berlin, 1996, pp. 63–74.
[3] K. Ambos-Spies, S.A. Terwijn, X. Zheng, Resource-bounded randomness and weakly complete problems, in: Proc. ISAAC '94, Lecture Notes in Computer Science, vol. 834, Springer, Berlin, 1994, pp. 369–377.
[4] J.L. Balcázar, J. Díaz, J. Gabarró, Structural Complexity I, Springer, Berlin, 1988.
[5] M. Blum, S. Micali, How to generate cryptographically strong sequences of pseudorandom bits, SIAM J. Comput. 13 (1984) 850–864.
[6] W. Feller, Introduction to Probability Theory and Its Applications, vol. I, Wiley, New York, 1968.
[7] D.T. Huynh, Resource bounded Kolmogorov complexity of hard languages, in: Proc. 1st Conf. on Structure in Complexity Theory, Lecture Notes in Comput. Sci., vol. 223, Springer, Berlin, 1986, pp. 184–195.
[8] D. Juedes, J.H. Lutz, The complexity and distribution of hard problem, SIAM J. Comput. 24 (1995) 279–295.
[9] D. Juedes, J.H. Lutz, Weak completeness in **E** and $\mathbf{E}_2$, Theoret. Comput. Sci. 143 (1995) 149–158.
[10] K. Ko, On the notion of infinite pseudorandom sequences, Theoret. Comput. Sci. 48 (1986) 9–33.
[11] S. Kurtz, Randomness and genericity in the degrees of unsolvability, Ph.D. Thesis, Department of Mathematics, University of Illinois at Urbana-Champaign, 1981.
[12] J.H. Lutz, Category and measure in complexity classes, SIAM J. Comput. 19 (1990) 1100–1131.
[13] J.H. Lutz, Almost everywhere high nonuniform complexity, J. Comput. System Sci. 44 (1992) 220–258.

[14] P. Martin–Löf, The definition of random sequences, Inform. and Control 9 (1966) 602–619.
[15] E. Mayordomo, Contributions to the study of resource-bounded measure, Ph.D. Thesis, University of Barcelona, 1994.
[16] E. Mayordomo, Almost every set in exponential time is **P**-bi-immune, Theoret. Comput. Sci. 136 (1994) 487–506.
[17] R. von Mises, Grundlagen der wahrscheinlichkeitsrechnung, Math. Z. 5 (1919) 52–99.
[18] C.P. Schnorr, Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie, Lecture Notes in Mathematics, vol. 218, Springer, Berlin, 1971.
[19] V.A. Uspenskii, A.L. Semenov, A.Kh. Shen, Can an individual sequence of zeros and ones be random? Russian Math. Surveys 45 (1990) 121–189.
[20] J. Ville, Étude Critique de la Notion de Collectif, Gauthiers-Villars, Paris, 1939.
[21] A. Wald, Sur la notion de collectif dans le calcul des probabilités, C.R. Acad. Sci. Paris 202 (1936) 180–183.
[22] Y. Wang, Randomness and complexity, Ph.D. Thesis, Mathematics Institute, Universität Heidelberg, 1996.
[23] Y. Wang, The law of the iterated logarithm for p-random sequences, in: Proc. 11th Conf. Computational Complexity (formerly Conf. on Structure in Complexity Theory), IEEE Computer Society Press, Silver Spring, MD, 1996, pp. 180–189.
[24] Y. Wang, Genericity, randomness, and polynomial-time approximations, SIAM J. Comput. 28 (1999) 394–408.
[25] R. Wilber, Randomness and the density of hard problems, in: Proc. FOCS '83, IEEE Computer Society Press, Silver Spring, 1983, pp. 335–342.
[26] A.C. Yao, Theory and applications of trapdoor functions, in: Proc. FOCS '82, IEEE Computer Society Press, Silver Spring, 1982, pp. 80–91.