The Law of the Iterated Logarithm for p-Random Sequences*

Yongge Wang
Mathematisches Institut
Universität Heidelberg
Im Neuenheimer Feld 294
69120 Heidelberg
Germany
wang@math.uni-heidelberg.de
http://math.uni-heidelberg.de/logic/wang/wang.html

Abstract

The stochastic properties of p-random sequences are studied in this paper. It is shown that the law of the iterated logarithm holds for p-random sequences. This law gives a quantitative characterization of the density of p-random sets. When combined with the invariance property of p-random sequences, this law is also useful in proving that some complexity classes have p-measure 0.

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 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 admissible place selection rules 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 [23] 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. To provide a negative answer to this question, Ville [22] constructed a counterexample in 1939. He showed that, for each countable set of admissible place selection rules, there exists a "Kollektiv" which does not satisfy the law of the iterated logarithm. The example of Ville defeated the plan of von Mises to develop probability theory based on "Kollektivs". Later, admissible place selection rules were further developed by Tornier, Wald, Church, Kolmogorov, Loveland and others. This approach of von Mises to define random sequences is now known as the "stochastic approach".

A completely different approach to the definition of random sequences was proposed by Kolmogorov and, independently, by Chaitin, and further developed by Levin, Schnorr and others (see, e.g., Uspenskii, Semenov and Shen [21]). In this approach, a notion of chaoticness is used for a definition of 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, 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. Later, Schnorr [20] used the martingale con-

*This work is part of my Ph.D thesis under the direction of Prof. Ambos-Spies.

cept to give a uniform description of various notions of randomness. Especially he gave a characterization of Martin-Löf's randomness concept in these terms. He criticized Martin-Löf's concept as being too strong and proposed a less restrictive concept as an adequate formalization of a random sequence instead.

For computational complexity classes, several definitions of pseudorandom sequences have been proposed. Schnorr [20] and Ko [10] introduced resource bounded versions of the notions of Martin-Löf and Kolmogorov randomness, respectively. More recently, Lutz [12, 13] further pursued these ideas and systematically developed a resource bounded measure theory. In particular, he introduced a feasible measure concept, of which he and others have shown that it is a natural tool for the quantitative analysis of the class **E** of exponential time computable sets.

The law of large numbers and the law of the iterated logarithm, both of which require that all random sequences should have some stochastic properties (cf. von Mises' definition of random sequences), are the two most important laws in probability theory. They play a central role in the study of probability theory (see, e.g., [6]) as well as in the study of classical randomness concepts (see, e.g., [9, 14, 20, 22]). In the study of classical randomness concepts, the crucial point is to ensure that each random sequence withstands all "standard" statistical tests, hence satisfies the laws mentioned above. We will show that these two laws hold for p-random sequences also. (In fact, we can show that all the standard laws (e.g., the $\alpha \ln n$-gap law for $\alpha < 1$) in probability theory, which only depend on the 0-1 distributions within the sequences, hold for p-random sequences. However, we do not carry out this tedious work of verification in this paper.) These two laws give a quantitative characterization of the density of p-random sets. It is well known that 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 is obvious that p-random sets have a stochastic distribution on their elements. Hence the density of most intractable sets is just "one half". When combined with the invariance property of p-random sequences, these laws are also useful in proving that some complexity classes have p-measure 0. For details, refer to Wang [25] and Wang [26].

2 Definitions

$N, Q(Q^+)$ and $R(R^+)$ are 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 $(n \geq 0)$ 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 $n \geq -1$, $x[0..n]$ denotes the initial segment of length $n+1$ ($x[0..n] = x$ if $|x| < n+1$) while $x[n]$ denotes the nth bit of x, i.e., $x[0..n] = x[0] \cdots x[n]$. Lower case letters $\cdots, k, l, m, n, \cdots, x, y, z$ from the middle and the end of the alphabet will denote numbers and strings, respectively. The letter b is reserved for elements of Σ, and lower case Greek letters $\xi, \eta, \cdots$ denote infinite sequences from Σ^∞.

A subset of Σ^* is called a language or simply a set. Capital letters are used to denote subsets of Σ^* and boldface capital letters are used to denote subsets of Σ^∞. The cardinality of a language A is denoted by $\|A\|$. We identify a language A with its characteristic function, i.e., $x \in A$ iff $A(x) = 1$. The characteristic sequence of a language A is the infinite sequence $A(z_0)A(z_1)A(z_2)\cdots$. 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 $x \in \Sigma^*$, $A\restriction x$ denotes the finite initial segment of A below x, i.e., $A\restriction x = \{y : y < x \ \& \ y \in A\}$. 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; And $A \subseteq B$ (resp. $A \subset B$) denotes that A is a subset of B (resp. that $A \subseteq B$ and $B \not\subseteq A$).

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, we write $Pr[\mathbf{C}]$ for 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 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.

3 Resource bounded stochasticity and the law of large numbers

Von Mises was the first to suggest identifying the notion of randomness with the notion of stochasticity. But von Mises' "legal selection rules" were not formally given. In the past, works in this area were mainly concentrated on the definition of legal selection rules. For example, Church [4] suggested that legal selection rules should be some recursive processes and Kolmogorov and, independently, Loveland proposed a stronger form which is now known as Kolmogorov-Loveland selection rules (see e.g., [21, 26]). Di Paola [18] considered the notions of stochasticity in subrecursive hierarchies. Based on these works, Wilber [27] introduced a notion of pseudostochasticity for complexity classes, while there exists a Wilber pseudostochastic set which is not **P**-immune. In [2], Ambos-Spies et al. introduced a stronger notion of p-stochasticity. And, at the same time, they showed that this notion of p-stochasticity is weaker than the notion of p-randomness and that all p-stochastic sets are **P**-immune. It is obvious that p-stochastic sequences satisfy the strong law of large numbers, hence p-random sequences satisfy the strong law of large numbers.

We will now introduce a fragment of Lutz's effective measure theory which will be sufficient for our investigation.

Definition 3.1 *(Ville [22]) 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 $\limsup_n F(\xi[0..n-1]) = \infty$. $S^\infty[F]$ denotes the set of sequences on which the martingale F succeeds.*

Definition 3.2 *(Lutz [13]) A set $\mathbf{C}$ of infinite sequences has p-*measure 0 *($\mu_p(\mathbf{C}) = 0$) if there is a polynomial time computable martingale $F : \Sigma^* \to Q^+$ which succeeds on every sequence in $\mathbf{C}$. The set $\mathbf{C}$ has p-*measure 1 *($\mu_p(\mathbf{C}) = 1$) if $\mu_p(\bar{\mathbf{C}}) = 0$ for the complement $\bar{\mathbf{C}} = \{\xi \in \Sigma^\infty : \xi \notin \mathbf{C}\}$ of $\mathbf{C}$.*

Definition 3.3 *(Lutz [13]) A sequence ξ is p-*random *if, for every polynomial time computable martingale F, $\lim_n F(\xi[0..n-1]) < \infty$, that is, F does not succeed on ξ.*

Note that a sequence ξ is p-random if and only if ξ does not belong to any set of p-measure 0, that is, if and only if the singleton $\{\xi\}$ does not have p-measure 0. It should also be noted that Lutz [13] introduced his p-measure in terms of approximable martingales. The following lemma shows that it is equivalent to the above definition.

Definition 3.4 *(Lutz [13]) A function F is p-*approximable *if there exists a polynomial time computable function $h(0^n, x)$ such that $|F(x) - h(0^n, x)| \leq 2^{-n}$ for all $n \in N$ and $x \in \Sigma^*$.*

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

Lemma 3.5 *For each p-approximable martingale F and each number $n \in N$, there exists a polynomial time computable martingale F' such that $F'(x) \geq F(x)$ for all $x \in \Sigma^*$.*

Proof. See Ambos-Spies et al. [3], Juedes and Lutz [8] or Mayordomo [15]. ∎

The above p-randomness concept is defined in terms of typicalness. A p-randomness concept in terms of stochasticity was introduced by Wilber [27] and was strengthened by Ko [10] as follows.

Definition 3.6 *(Ko [10]) A sequence $\xi \in \Sigma^\infty$ is* Ko p-stochastic *if, for every polynomial time computable total function $f : \Sigma^* \to \Sigma$,*

$$\lim_{n\to\infty} \frac{\|\{k < n : f(\xi[0..k-1]) = \xi[k]\}\|}{n} = \frac{1}{2}.$$

In other words, a sequence ξ is Ko p-stochastic if and only if, for each polynomial time computable prediction function f which predicts the nth bit $\xi[n]$ from the previous n bits $\xi[0..n-1]$, the probability of success is no better than tossing an unbiased coin.

Theorem 3.7 *(Ambos-Spies et al. [2]) There exists a Ko p-stochastic set A which is not **P**-immune.*

Theorem 3.7 shows that the notion of Ko p-stochasticity cannot characterize the notion of **P**-immunity. In the next theorem, we will point out the limitation of this notion in terms of martingales.

Definition 3.8 *A sequence ξ is p-*exp-random *if, for every polynomial time computable martingale F and for every real number $c > 1$, $\limsup_n (F(\xi[0..n-1]) - c^n) < 0$.*

Theorem 3.9 *Given a sequence $\xi \in \Sigma^\infty$, ξ is Ko p-stochastic if and only if it is p-exp-random.*

Proof. The proof technique is the same as that in the proof of Schnorr Satz 18.4 in [20], we will omit the details here. ■

By Theorem 3.9, the notion of Ko p-stochasticity is just a little stronger than the notion of non-p-computability, since a sequence $\xi \in \Sigma^\infty$ is polynomial time computable (that is, $\xi[0..n-1]$ is computable in time n^k for some $k \in N$) if and only if there is a polynomial time computable martingale F such that

$$\limsup_n (F(\xi[0..n-1]) - 2^n) \geq 0.$$

The above theorems show some limitations of the notion of Ko p-stochasticity. In [2], Ambos-Spies, Mayordomo, Wang and Zheng introduced yet an even stronger notion of p-stochasticity that can characterize the notion of **P**-immunity.

Definition 3.10 *(Ambos-Spies et al. [2]) A sequence $\xi \in \Sigma^\infty$ is* p-stochastic *if, for every polynomial time computable partial function $f : \Sigma^* \to \Sigma$ such that $\{n : f(\xi[0..n-1])$ is defined$\}$ is an infinite set,*

$$\lim_{n\to\infty} \frac{\|\{k \leq n : f(\xi[0..k-1]) = \xi[k]\}\|}{\|\{k \leq n : f(\xi[0..k-1]) \text{is defined}\}\|} = \frac{1}{2}.$$

Theorem 3.11 *(Ambos-Spies et al. [2]) For a set $A \subseteq \Sigma^*$, if the characteristic sequence ξ of A is p-stochastic, then A is* **E**-*immune.*

The following theorem shows that the notion of resource bounded stochasticity is a weaker notion when compared with the notion of resource bounded typicalness. This coincides with the relationship between the corresponding classical (recursive) notions.

Theorem 3.12 *(Ambos-Spies et al. [2])*

1. *If a sequence is p-random, then it is p-stochastic.*
2. *There is a p-stochastic sequence which is not p-random.*

Corollary 3.13 *(The law of large numbers, Schnorr [20]) For each p-random sequence $\xi \in \Sigma^\infty$,*

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

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

In this section, we prove the law of the iterated logarithm for p-random sequences (p-random sets), which says that both

$$\mathbf{U} = \left\{ A \subseteq \Sigma^* : \limsup_{n\to\infty} \frac{n - 2\|A\upharpoonright z_n\|}{\sqrt{2n \ln\ln n}} = 1 \right\} \text{ and}$$

$$\mathbf{V} = \left\{ A \subseteq \Sigma^* : \liminf_{n\to\infty} \frac{n - 2\|A\upharpoonright z_n\|}{\sqrt{2n \ln\ln n}} = -1 \right\}$$

have p-measure 1.

There are various applications of the law of the iterated logarithm. The notion of polynomial time unsafe approximations for intractable sets was introduced by Yesha [28], and was further investigated by Duris and Rolim [5] and Ambos-Spies [1]. In Wang [25] (see also Wang [26]), the law of the iterated logarithm for p-random sequences was used to prove that both the class of 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 $(i = 0, 1, \cdots)$ be a sequence of uniformly polynomial time computable density functions (the definition will be given below). If $F_i(\lambda) \leq 2^{-i}$ 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 $(i = 1, 2, \cdots)$ such that, for each i

$$F_i(\lambda) \leq i^{-\alpha}$$

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 following proof, the main objective, roughly speaking, is to use p-approximations of $h(n, x) = \sum_{i=1}^n F_i(x) + \int_{n+1}^\infty \frac{dx}{(x-1)^\alpha}$ to define a p-approximation of $F = \sum_{i=1}^\infty F_i$.

Definition 4.1 *A function $F : \Sigma^* \to R^+$ is a* density function *if, for all $x \in \Sigma^*$,*

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

Lemma 4.2 *Given a polynomial time computable function $F(i,x)$ and a nondecreasing, time constructible function $u : N \to N$ satisfying*

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

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

Remark: If we only require that F is p-approximable, then the lemma 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

$$\bigcup_{i=0}^{\infty} S^{\infty}[F_i] \subseteq \bigcup_{i=0}^{\infty} S^{\infty}[F'_i]. \tag{1}$$

Let v be a function defined by the recursion

$$\begin{aligned} v(1) &= u(1) \\ v(k+1) &= \max\{k+1, u(k+1), v(k)\} + 1 \end{aligned}$$

Then 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

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

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

$$S^{\infty}[F_k] \subseteq S^{\infty}[F'_{2^{v(k)}}].$$

Hence (1) holds. ∎

In our following proof, we will use two special functions. The first one is $S : \Sigma^* \to N$ satisfying

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

for all $x \in \Sigma^*$.

The second one is $S^* : \Sigma^* \to R$ satisfying

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

for all $x \in \Sigma^*$.

We will make use of the following variant of DeMoivre-Laplace limit theorem.

Lemma 4.3 *[6] Let $u : N \to R^+$ be a function satisfying*

$$\frac{1}{2}\sqrt{\ln\ln n} \leq u(n) \leq 2\sqrt{\ln\ln n}$$

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

$$\begin{aligned} u^{-2}e^{-u^2/2} &\leq Pr\left[\{\xi : S^*(\xi[0..n-1]) > u(n)\}\right] \\ &\leq e^{-u^2/2}. \end{aligned}$$

The following lemma from Feller [6, p158] is also useful in our proof.

Lemma 4.4 *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 $\mathbf{C}$ is the set of infinite sequences satisfying*

$$S(\xi[0..k-1]) - \frac{k}{2} > u(n)$$

for some $k \leq n$, then

$$Pr[\mathbf{C}] \leq \frac{1}{c_1} Pr\left[\left\{\xi : S(\xi[0..n-1]) - \frac{n}{2} > u(n)\right\}\right].$$

We will now prove our main theorem of this paper.

Theorem 4.5 *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 $\mathbf{Y}_k$ $(k \geq 1)$ be the set of infinite sequences such that

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

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

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

for finitely many n, then

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

has p-measure 0.

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

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

Outline of the Proof: The proof goes on as follows. First, we will show uniformly that every $\mathbf{Y}_k$ has p-measure 0, that is, $\mathbf{Y} = \cup_{k=1}^\infty \mathbf{Y}_k$ has p-measure 0. Then we will use this result to show that $\mathbf{X} = \cup_{k=1}^\infty \mathbf{X}_k$ has p-measure 0. In order to show that $\mathbf{Y}_k$ has p-measure 0, we define a sequence $n_0, n_1, \cdots$ 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 Σ^{n_i}. 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 4.5.
First we show that $\mathbf{Y} = \bigcup_{k=1}^\infty \mathbf{Y}_k$ has p-measure 0.
Let

$$\begin{aligned} \alpha &= 1 + \frac{1}{k} \\ \beta &= 1 + \frac{1}{3k} \\ n_i &= [\beta^i] + 1 \quad (i = 1, 2, \cdots) \end{aligned}$$

Then $1 < \beta < \sqrt{\alpha}$. Let $\mathbf{Y}_{k,i}$ be the set of infinite sequences such that

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

for some $n \in N$ with $n_i \le n < n_{i+1}$, and let

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

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

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

where $Pr[\mathbf{Y}_{k,i}|\mathbf{C}_x]$ 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 4.2, it suffices to define a p-approximable function G and a time constructible function $v : N \to N$ such that, for all $k \in N$ and for all $|x| > v(k)$,

$$\begin{aligned} 2G(k,x) &\ge G(k,x0) + G(k,x1) \\ G(k,x) &\ge F(k,x) \end{aligned}$$

Let

$$G(k,x) = \sum_{i \le \left[\frac{4\ln|x|}{\ln\beta}\right]} Pr[\mathbf{Y}_{k,i}|\mathbf{C}_x] + \sum_{i > \left[\frac{4\ln|x|}{\ln\beta}\right]} \int_i^{i+1} \frac{dx}{c\cdot((x-1)\ln\beta)^\alpha}$$

where c is a constant which will be given below.

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

Proof. Obviously, in the expression of G, the second clause

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

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

If $i \le \left[\frac{4\ln|x|}{\ln\beta}\right]$, then $n_i \le |x|^4 + 1$. Hence, the values of $Pr[\mathbf{Y}_{k,i}|\mathbf{C}_x]$ in the first clause of $G(k,x)$ can be computed using binomial coefficients of base less than $n_{i+1} \le \beta\cdot(|x|^4+1)$. 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 Lemma 4.3, c_1 be the constant in Lemma 4.4, $c = \frac{c_1}{3} > 0$ and $u_1(k) = [6e^{2c_0^2}k^2]$. Then the following conditions hold for all k.*

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

$$Pr[\mathbf{Y}_{k,i}] \le \int_i^{i+1} \frac{dx}{c\cdot((x-1)\ln\beta)^\alpha}.$$

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

$$Pr[\mathbf{Y}_{k,i}|\mathbf{C}_x] \le \int_i^{i+1} \frac{dx}{c\cdot((x-1)\ln\beta)^\alpha}.$$

Proof. 1. By Lemma 4.4,

$$\begin{aligned}
&Pr[\mathbf{Y}_{k,i}] \\
&\le \tfrac{1}{c_1} Pr[\{\xi : S(\xi[0..n_{i+1}-1]) - \tfrac{1}{2}n_{i+1} \\
&\qquad > \alpha\sqrt{\tfrac{1}{2}n_i \ln\ln n_i}\}] \\
&= \tfrac{1}{c_1} Pr[\{\xi : S^*(\xi[0..n_{i+1}-1]) \\
&\qquad > \alpha\sqrt{2\tfrac{n_i}{n_{i+1}} \ln\ln n_i}\}]
\end{aligned}$$

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

$$\begin{aligned}
Pr[\mathbf{Y}_{k,i}] \le \quad & c_1^{-1} Pr[\{\xi : S^*(\xi[0..n_{i+1}-1]) \\
& > \sqrt{2\alpha \ln\ln n_i}\}].
\end{aligned}$$

If $i > 6e^{c_0^2}k^2$, then $\sqrt{2\alpha\ln\ln n_i} > c_0$. By Lemma 4.3, we therefore get, for $i > u_1(k) = [6e^{c_0^2}k^2]$,

$$\begin{aligned}
Pr[\mathbf{Y}_{k,i}] &\le c_1^{-1} e^{-\alpha \ln\ln n_i} \\
&= \frac{1}{c_1(\ln n_i)^\alpha} \\
&< \frac{1}{c(i\ln\beta)^\alpha} \\
&< \int_i^{i+1} \frac{dx}{c\cdot((x-1)\ln\beta)^\alpha}.
\end{aligned}$$

2. First, we note the following fact: for $x \in \Sigma^{\le n_i}$,

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

where $\mathbf{Y}_{k,i,j}$ is the set of infinite sequences such that

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

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

$$\begin{aligned}
& Pr[\mathbf{Y}_{k,i}|\mathbf{C}_x] \\
= \quad & 2^{|x|} Pr[\mathbf{Y}_{k,i} \cap \mathbf{C}_x] \\
\le \quad & 2^{|x|} Pr[\mathbf{Y}_{k,i,|x|} \cap \mathbf{C}_{0^{|x|}}] \\
\le \quad & \textstyle\sum_{y\in\Sigma^{|x|}} Pr[\mathbf{Y}_{k,i,|x|} \cap \mathbf{C}_y] \\
= \quad & Pr[\mathbf{Y}_{k,i,|x|}] \\
\le \quad & c_1^{-1} Pr[\{\xi : S(\xi[0..n_{i+1}-1]) - \tfrac{1}{2}n_{i+1} \\
& \qquad + |x| > \alpha\sqrt{\tfrac{1}{2}n_i\ln\ln n_i}\}] \\
= \quad & c_1^{-1} Pr[\{\xi : S^*(\xi[0..n_{i+1}-1]) \\
& \qquad > \alpha\sqrt{2\tfrac{n_i}{n_{i+1}}\ln\ln n_i} - \tfrac{|x|}{\sqrt{n_{i+1}}}\}] \\
\le \quad & c_1^{-1} Pr[\{\xi : S^*(\xi[0..n_{i+1}-1]) \\
& \qquad > \sqrt{2\alpha\ln\ln n_i} - \tfrac{|x|}{\sqrt{n_{i+1}}}\}] \\
\le \quad & c_1^{-1} e^{-\alpha\ln\ln n_i + \frac{|x|}{\sqrt{n_{i+1}}}\sqrt{2\alpha\ln\ln n_i}} \\
\le \quad & c_1^{-1} e^{\frac{\sqrt[4]{n_{i+1}}\sqrt{2\alpha\ln\ln n_i}}{\sqrt{n_{i+1}}}} e^{-\alpha\ln\ln n_i} \quad \left(\text{By } i > \left[\tfrac{4\ln|x|}{\ln\beta}\right]\right) \\
\le \quad & 3c_1^{-1} e^{-\alpha\ln\ln n_i} \\
= \quad & \frac{3}{c_1(\ln n_i)^\alpha} \\
\le \quad & \frac{3}{c_1(i\ln\beta)^\alpha} \\
= \quad & \frac{1}{c(i\ln\beta)^\alpha} \\
\le \quad & \int_i^{i+1} \frac{dx}{c\cdot((x-1)\ln\beta)^\alpha}.
\end{aligned}$$

□

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

$$\begin{aligned}
2G(k,x) &\ge G(k,x0) + G(k,x1) \\
G(k,x) &\ge F(k,x).
\end{aligned}$$

Proof. If $[\frac{4\ln|x0|}{\ln\beta}] = [\frac{4\ln|x|}{\ln\beta}]$, then it is obvious from

the definition of G that

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

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

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

By Claim 2, for all $|x| > v(k)$ (i.e., $\left[\frac{4\ln|x|}{\ln\beta}\right] > u_1(k)$),

$$\begin{aligned} & G(k,x) - F(k,x) \\ &= \sum_{i>\left[\frac{4\ln|x|}{\ln\beta}\right]} \left(\int_i^{i+1} \frac{dx}{c\cdot((x-1)\ln\beta)^\alpha} - Pr[\mathbf{Y}_{k,i}|\mathbf{C}_x] \right) \\ &\geq 0 \end{aligned}$$

□

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

Next we show that $\mathbf{X} = \bigcup_{k=6}^\infty \mathbf{X}_k$ has p-measure 0.

Let

$$\begin{aligned} \alpha &= 1 - \frac{1}{k} \quad (k > 5) \\ \beta &= k^4 \\ \gamma &= 1 - \frac{1}{k^3} \\ n_i &= \beta^i \quad (i = 1, 2, \cdots) \end{aligned}$$

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 let $\mathbf{X}_{k,i}$ be the set of infinite sequences such that

$$D_i(\xi) - \frac{1}{2}(n_i - n_{i-1}) > \gamma\sqrt{\frac{1}{2}n_i \ln\ln n_i}.$$

Now we show that if $i > e^{c_0^2}$ (where c_0 is the constant in Lemma 4.3), then $Pr[\mathbf{X}_{k,i}] \geq i^{-1}$.

$$\begin{aligned} & Pr[\mathbf{X}_{k,i}] \\ &= Pr\left[\left\{\xi : \frac{2D_i(\xi) - (n_i - n_{i-1})}{\sqrt{n_i - n_{i-1}}} \right.\right. \\ &\qquad \left.\left. > \gamma\sqrt{\frac{2n_i}{n_i - n_{i-1}}\ln\ln n_i}\right\}\right]. \end{aligned}$$

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

$$\begin{aligned} Pr[\mathbf{X}_{k,i}] &\geq Pr[\{\xi : \frac{2D_i(\xi) - (n_i - n_{i-1})}{\sqrt{n_i - n_{i-1}}} \\ &\qquad > \sqrt{2\gamma\ln\ln n_i}\}]. \end{aligned}$$

If $i > e^{c_0^2}$ then $\sqrt{2\gamma\ln\ln n_i} > c_0$. So, by Lemma 4.3, for $i > e^{c_0^2}$,

$$\begin{aligned} Pr[\mathbf{X}_{k,i}] &\geq \frac{1}{2\gamma\ln\ln n_i} e^{-\gamma\ln\ln n_i} \\ &= \frac{1}{2\gamma(\ln\ln n_i)(\ln n_i)^\gamma}. \end{aligned}$$

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 $Pr[\mathbf{X}_{k,i}] \geq i^{-1}$.

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

$$F(k,0,y) = \begin{cases} 0 & y\cdot\Sigma^\infty \subseteq \mathbf{X}_{k,i+1} \\ \frac{i+1}{i}F(k,0,x) & y\cdot\Sigma^\infty \not\subseteq \mathbf{X}_{k,i+1} \end{cases}$$

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

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

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

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

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 4.2, $\mathbf{Z}_{k,0}$ has p-measure 0.

Next, we divide the sequence $\mathbf{X}_{k,i}$ $(i = 1, 2 \cdots)$ into two subsequences $\mathbf{X}_{k,i}^{(1,1)}$ and $\mathbf{X}_{k,i}^{(1,2)}$ such that both $\sum_i Pr[\mathbf{X}_{k,i}^{(1,1)}] = \infty$ and $\sum_i Pr[\mathbf{X}_{k,i}^{(1,2)}] = \infty$. Let

$$\mathbf{Z}_{k,1} = \{\xi : \xi \notin \mathbf{X}_{k,i}^{(1,1)} \text{ for all } i\}$$

$$\bigcup \{\xi : \xi \notin \mathbf{X}_{k,i}^{(1,2)} \text{ for all } i\}.$$

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 sequences $\mathbf{X}_{k,i}^{(1,1)}$ 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 4.2, $\mathbf{Z}$ has p-measure 0.

Let

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

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 $i > n_0$,

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

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,

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

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

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

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

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

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. ■

Acknowledgements

I am grateful to my thesis advisor Professor Ambos-Spies for introducing me into this field and for many crucial discussions during the writing of this paper. At the same time, I am also grateful to Professor Lutz for pointing out an error in Claim 1 and for many suggestions on improving the presentation of this paper.

References

[1] K. Ambos-Spies. On optimal polynomial time approximations: **P**-levelability vs. Δ-levelability. In *Proc. 22nd ICALP*, pages 384–392. Springer Verlag, 1995.

[2] K. Ambos-Spies, E. Mayordomo, Y. Wang, and X. Zheng. Resource-bounded balanced genericity, stochasticity and weak randomness. To appear in *Proc. 13rd STACS*. Springer Verlag, 1996.

[3] K. Ambos-Spies, S. A. Terwijn, and X. Zheng. Resource-bounded randomness and weakly complete problems. In *Proc. ISAAC 94*, Lecture Notes in Comput. Sci., 834, pages 369–377. Springer Verlag, 1994.

[4] A. Church. On the concept of a random sequence. *Bull. Amer. Math. Soc.*, 45:130–135, 1940.

[5] P. Duris and J. D. P. Rolim. **E**-complete sets do not have optimal polynomial time approximations. In *Proc. 19th MFCS*, pages 38–51. Springer Verlag, 1994.

[6] W. Feller. *Introduction to Probability Theory and Its Applications*. Volume I. John Wiley & Sons, Inc., 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., 223, pages 184–195. Springer Verlag, 1986.

[8] D. Juedes and J. H. Lutz. Weak completeness in $\mathbf{E}$ and $\mathbf{E}_2$. *Theoret. Comput. Sci.*, 143:149–158, 1995.

[9] S. Kautz. *Degrees of Random Sets.* PhD thesis, Cornell University, Ithaca, 1991.

[10] K. Ko. On the notion of infinite pseudorandom sequences. *Theoret. Comput. Sci.*, 48:9–33, 1986.

[11] M. van Lambalgen. von Mises' definition of random sequences reconsidered. *J. Symbolic Logic*, 52:725–755, 1987.

[12] J. H. Lutz. Category and measure in complexity classes. *SIAM J. Comput.*, 19:1100–1131, 1990.

[13] J. H. Lutz. Almost everywhere high nonuniform complexity. *J. Comput. System Sci.*, 44:220–258, 1992.

[14] P. Martin-Löf. The definition of random sequences. *Inform. and Control*, 9:602–619, 1966.

[15] E. Mayordomo. *Contributions to the Study of Resource-Bounded Measure.* PhD thesis, Barcelona, 1994.

[16] A. R. Meyer and M. S. Paterson. With what frequency are apparently intractable problems difficult? Technical Report TM-126, Laboratory for Computer Science, MIT, 1979.

[17] R. von Mises. Grundlagen der Wahrscheinlichkeitsrechnung. *Math. Z.*, 5:52–99, 1919.

[18] R. A. Di Paola. Random sets in subrecursive hierarchies. *J. Assoc. Comput. Math.*, 16:621–630, 1969.

[19] C. P. Schnorr. A unified approach to the definition of random sequences. *Math. System Theory*, 5:246–258, 1971.

[20] C. P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit. Eine algorithmische Begründung der Wahrscheinlichkeitstheorie.* Lecture Notes in Math. 218. Springer Verlag, 1971.

[21] V. A. Uspenskii, A. L. Semenov, and A. Kh. Shen. Can an individual sequence of zeros and ones be random? *Russian Math. Surveys*, 45:121–189, 1990.

[22] J. Ville. *Ètude Critique de la Notion de Collectif.* Gauthiers-Villars, Paris, 1939.

[23] A. Wald. Sur la notion de collectif dans le calcul des probabilités. *C. r. Acad. Sci. Paris*, 202:180–183, 1936.

[24] Y. Wang. *Different approaches to the definition of random sequences.* Universität Heidelberg, 1995.

[25] Y. Wang. *Resource bounded category, resource bounded measure and polynomial time approximations.* Universität Heidelberg, 1995.

[26] Y. Wang. *Randomness and Complexity.* Ph.D thesis, Universität Heidelberg, 1995. Available on request or from my WWW homepage.

[27] R. Wilber. Randomness and the density of hard problems. In *Proc. 24th Symp. FOCS*, pages 335–342. IEEE Computer Society Press, 1983.

[28] Y. Yesha. On certain polynomial-time truth-table reducibilities of complete sets to sparse sets. *SIAM J. Comput.*, 12:411–425, 1983.