Inaugural Dissertation

zur

Erlangung der Doktorwürde

der

Naturwissenschaftlich-Mathematischen Gesamtfakultät

der

Ruprecht-Karls-Universität

Heidelberg

vorgelegt von

Yongge Wang

aus Gansu, China

1996

Randomness and Complexity

Gutachter: Prof. Dr. Klaus Ambos-Spies
Prof. Dr. Jack Lutz

Tag der mündlichen Prüfung: August 30, 1996

Preface

This thesis was written when I was studying at the University of Heidelberg from October 1993 to March 1996. First of all I am indebted to my thesis advisor Prof. Klaus Ambos-Spies for his guidance and support, for many fruitful discussions during the writing of this thesis, and for spending much time on the presentation of this thesis.

I would like to thank Prof. Guoding Hu of the Nankai University for arranging my participation in the academic exchange program between the Nankai University and the University of Heidelberg.

I would also like to express my appreciation to Klaus Ambos-Spies, Steven Kautz, Ker-I Ko, Stuart Kurtz, Michiel van Lambalgen, Jack Lutz, Elvira Mayordomo and Claus Schnorr for their mathematical work, upon which I directly depend.

For helpful discussions and correspondence, I would like to thank Prof. R. Beigel, Prof. R. Book, Prof. S. Kautz, Prof. J. Lutz and Dr. E. Mayordomo. Dr. Frank Stephan read an earlier version of this manuscript carefully and gave me helpful comments.

Finally I would like to thank my colleagues: Levke Bentzien, Bernd Borchert, Gunther Mainhardt, Wolfgang Merkle, Frank Stephan and Xizhong Zheng, for many discussions and for offering a good environment to study here.

Abstract

The topic of this thesis is the study of randomness concepts and their applications in computational complexity theory. In Chapter 3, we discuss the classical notions of randomness. We give a systematic study of various notions of randomness, especially, of the following concepts defined in terms of typicalness: Martin-Löf randomness, rec-randomness, Schnorr randomness, Ko randomness, and Kurtz randomness. We study each notion of typicalness by using three different approaches: the approach based on constructive null covers, the approach based on martingales and the approach based on Solovay style criteria (the first Borel-Cantelli lemma-like condition).

Schnorr has shown that Martin-Löf randomness is a proper refinement of rec-randomness, and he left open the question whether rec-randomness is a proper refinement of Schnorr randomness. In the sequel, the later was conjectured to be true by van Lambalgen and Lutz. We prove this conjecture, thereby completely clarifying the relations among the above cited important randomness concepts. At the same time, we will show that there is a Schnorr random sequence which is not Church stochastic.

In Chapter 4, we extend Kurtz recursion theoretic notion of n-randomness to the recursion theoretic notions of rec- and Schnorr n-randomness.

Notions of resource bounded randomness have been introduced by several authors. Though it was known that most of these notions are different, the relations among them were not fully understood. In Chapter 5, we give a survey of these notions and show their relations to each other. Moreover, we introduce several new notions of resource bounded randomness corresponding to the classical notions of randomness discussed in Chapter 3. We show that the notion of polynomial time bounded Ko randomness is independent of the notions of polynomial time bounded rec-, Schnorr and Kurtz randomness. Lutz has conjectured that, for a given time or space bound, the corresponding resource bounded rec-randomness is a proper refinement of resource bounded Schnorr randomness. We answer this conjecture affirmatively. Moreover, we show that resource bounded Schnorr randomness is a proper refinement of resource bounded Kurtz randomness too. In contrast to this result, however, we also show that the notions of polynomial time bounded rec-, Schnorr and Kurtz randomness coincide in the case of recursive sets, whence it suffices to study the notion of resource bounded rec-randomness in the context of complexity theory.

The stochastic properties of resource bounded random sequences (i.e., resource bounded typical sequences) will be discussed in detail. Schnorr has already shown that the law of large numbers holds for p-random sequences. We show that another important law in probability theory, the law of the iterated logarithm, holds for p-random sequences too. (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.) Hence almost all sets in the exponential time complexity class are "hard" from the viewpoint of statistics. These laws also give a quantitative characterization of the density of p-random sets. And, when combined with an invariance property of p-random sets, these laws are useful in proving that some classes of sets have p-measure 0.

Polynomial time safe and unsafe approximations for intractable sets were introduced by Meyer, Paterson, Yesha, Duris, Rolim and Ambos-Spies, respectively. The question of

which sets have optimal safe and unsafe approximations has been investigated extensively. Recently, Duris, Rolim and Ambos-Spies showed that the existence of optimal polynomial time approximations for the safe and unsafe cases is independent. Using the law of the iterated logarithm for p-random sequences discussed in Chapter 5, we extend this observation by showing that both the class of $\mathbf{\Delta}$-levelable sets and the class of sets which have optimal polynomial time unsafe approximations have p-measure 0. Hence p-random sets do not have optimal polynomial time unsafe approximations. We will also show the relations between resource bounded genericity concepts (introduced by Ambos-Spies et al., Fenner and Lutz) and the polynomial time safe (unsafe) approximation concept.

In the last chapter, we show that no $\mathbf{P}$-selective set is $\leq^p_{tt}$-hard for $\mathbf{NP}$ unless $\mathbf{NP}$ is small.

Contents

Chapter 1

Introduction and Notation

1.1 Introduction

Random sequences were first introduced by von Mises [79] 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 rule". Here an admissible place selection rule 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 rule" 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 [99] 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. For a negative answer to this question, Ville [98] 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", that is to say, to give an axiomatisation of probability theory with "random sequences" (i.e., "Kollektivs") as a primitive term. 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 [97]). In this approach, a notion of chaoticness is used for a definition of random sequences: The complexity 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 complexity (modulo some additive constant).

Finally, Martin-Löf [74] 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. A different characterization of Martin-Löf's randomness concept was given by Solovay (see, e.g., Chaitin [30] or Kautz [44]), which is in the style of the first Borel-Cantelli Lemma. Later, the notion of "typicalness" was further studied by Schnorr, Kurtz, Ko, Solovay, Lutz and others.

Schnorr [89] used the martingale concept to give a uniform description of various notions of randomness. In particular, he gave a characterization of Martin-Löf's randomness concept in these terms. Moreover, 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 addition Schnorr introduced a refinement of Martin-Löf randomness and some intermediate notion between Martin-Löf and Schnorr randomness. This latter concept coincides with the notion of rec-randomness introduced by van Lambalgen [57] and Lutz [65]. Schnorr left open the question whether rec-randomness is a proper refinement of Schnorr randomness, which was conjectured to be true by van Lambalgen and Lutz. We will show that rec-randomness is strictly weaker than Martin-Löf randomness and that it is strictly stronger than Schnorr randomness, thereby proving van Lambalgen and Lutz's conjecture. At the same time, we will show that there is a Schnorr random sequence ξ and a recursive place selection rule φ in the sense of Church such that the selected subsequence of ξ by φ is $111\cdots$. This shows that the notion of Schnorr randomness seems to us less adequate to our intuition than the notions of Martin-Löf and rec-randomness.

Ko [48] introduced a pseudorandomness concept which is based on the notion of efficient tests. In this thesis, we introduce the randomness concept corresponding to Ko's pseudorandomness concept, and we prove that this concept coincides with Schnorr's randomness concept. Using this new concept, we give a characterization of Schnorr's randomness concept in terms of finite unions of basic open sets instead of recursively open sets, which can be used to give a Solovay style criterion for the notion of Schnorr randomness.

Kurtz [54] introduced a notion of weak randomness using recursively open sets of Lebesgue measure one. We characterize this notion in terms of constructive null covers, martingales and a Solovay style criterion.

In Chapter 3, we study the notions of classical randomness mentioned above and we analyze the relations among them. We characterize the concepts of Martin-Löf, Lutz, Schnorr, Ko and Kurtz typical sequences in different equivalent ways (for example, in terms of martingales, in terms of Borel-Cantelli Lemma style criteria, and in terms of constructive null covers). The main theorem of this chapter is Theorem 3.2.2: rec-randomness is a proper refinement of Schnorr randomness. Together with other theorems in this chapter, we obtain a complete characterization of the relations among these notions of typicalness mentioned above. That is to say, we have the following diagram:

$$\mathbf{M\text{-}RAND} \subset \mathbf{L\text{-}RAND} \subset \mathbf{K\text{-}RAND} = \mathbf{S\text{-}RAND} \subset \mathbf{W\text{-}RAND},$$

where these sets are the sets of Martin-Löf, Lutz, Ko, Schnorr and Kurtz random sequences, respectively.

At the end of Chapter 3, we discuss notions of randomness in terms of chaoticness and stochasticity. In particular, we address the invariance properties of random sequences. We list some of Schnorr's [89] results about the invariance properties of random sequences and, as an analog, we show the invariance properties of Kurtz random sequences.

Chapter 4 is devoted to notions of n-randomness. These refinements of effective randomness, which correspond to the levels of the arithmetical hierarchy, are of interest in recursion theory. The results in this chapter can be considered as relativizations of the results in Chapter 3.

In the second part of this thesis we study applications of randomness concepts in complexity theory. For computational complexity classes, several definitions of pseudorandom sequences have been proposed. Blum and Micali [18] and Yao [115] gave a relatively weak definition of resource bounded random sequences. Schnorr [89] and Ko [48] introduced resource bounded versions of the notions of Martin-Löf and Kolmogorov randomness. More recently, Lutz [63, 65] 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**. For example, Mayordomo [76] and Juedes and Lutz [42] have shown that both the class of **P**-bi-immune sets and the class of p-incompressible sets have p-measure 1.

Chapter 5 is devoted to the study of notions of resource bounded randomness. First, we introduce various notions of resource bounded randomness in terms of typicalness and investigate their relations to each other. We will show that:

1. For polynomial time bounds, the notion of rec-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 [65]. We also show, however, that if we consider only recursive sets, then these randomness concepts coincide.

2. For polynomial time bounds, the notion of Ko randomness is independent of the notions of rec-randomness, Schnorr randomness and Kurtz randomness.

Moreover, we study notions of resource bounded stochasticity. Here we concentrate our attention on the stochastic properties of resource bounded rec-random sequences and we show that the important laws in probability theory hold for 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 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., [33]) and in the study of classical randomness concepts (see, e.g., [44, 74, 89, 98]). 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 two laws mentioned above. We will show that these two laws hold for p-random sequences also. (In particular, 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 thesis.) These two laws 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 is obvious that all p-random sets have a stochastic distribution on their elements, hence the density of most intractable sets is just “one half”. When combined with an invariance property of p-random sequences, these laws are also useful in proving that some complexity classes have p-measure 0.

Chapter 6 will establish the relations between the concepts of resource bounded randomness and the concepts of approximations. The notion of polynomial time safe approximations was introduced by Meyer and Paterson in [78] (see also [49]). In Orponen et al. [83], the existence of optimal safe approximations was phrased in terms of **P**-levelability. The notion of unsafe approximations was introduced by Yesha in [116]. Duris and Rolim [32] and Ambos-Spies [4] further investigated unsafe approximations and introduced two levelability concepts, Δ-levelability and weak Δ-levelability, respectively. In this thesis, we study a little different version of unsafe approximations.

Resource bounded measure and category are useful in the study of typical properties of intractable complexity classes. It was shown in Ambos-Spies et al. [9] that the generic sets of Ambos-Spies are **P**-immune, and that the class of sets which have optimal safe approximations is comeager in the sense of resource bounded Ambos-Spies category. Mayordomo [75] has shown that the class of **P**-immune sets is neither meager nor comeager in the sense of resource bounded Lutz category and in the sense of resource bounded Fenner category. We extend this result by showing that the class of sets which have optimal safe approximations is neither meager nor comeager both in the sense of resource bounded Lutz category and in the sense of resource bounded Fenner category. Moreover, we will show the following relationships between unsafe approximations and resource bounded categories.

1. The class of weakly Δ-levelable sets is neither meager nor comeager in the sense of resource bounded Ambos-Spies category [9].

2. The class of weakly Δ-levelable sets is comeager in the sense of resource bounded general Ambos-Spies [5], Fenner [34] and Lutz [63] categories.

3. The class of Δ-levelable sets is neither meager nor comeager in the sense of resource bounded general Ambos-Spies [5], Fenner [34] and Lutz [63] categories.

In the last section of Chapter 6, we will show the relations between polynomial time approximations and p-measure. Mayordomo [76] has shown that the class of **P**-bi-immune sets has p-measure 1. It follows that the class of sets which have optimal polynomial time safe approximations has p-measure 1. Using the law of the iterated logarithm for p-random sequences which we have proved in Chapter 5, we will show that:

1. The class of Δ-levelable sets has p-measure 0.

2. The class of sets which have optimal polynomial time unsafe approximations has p-measure 0.

3. p-Random sets are weakly Δ-levelable but not Δ-levelable.

Hence typical sets in the sense of Lutz measure theory do not have optimal polynomial time unsafe approximations.

Chapter 7 is devoted the study of **P**-selective hard sets for **NP**. Selman [91] showed that if $\mathbf{NP} \subseteq \mathbf{P}_m(\mathbf{SELECT})$, where **SELECT** is the class of **P**-selective sets, then $\mathbf{P} = \mathbf{NP}$. Recently, Agrawal and Arvind [1], Beigel, Kummer and Stephan [15] and Ogihara [81] showed that if $\mathbf{NP} \subseteq \mathbf{P}_{n^\alpha\text{-}tt}(\mathbf{SELECT})$ for some real $\alpha < 1$, then $\mathbf{P} = \mathbf{NP}$. It seems difficult to remove the condition $\alpha < 1$ in the above result. In this chapter, however, we will remove this condition under a stronger but reasonable hypothesis. That is, we show that if **NP** does not have p-measure 0, then no $\leq^p_{tt}$-hard set for **NP** is **P**-selective. We also give a partial affirmative answer to a conjecture by Beigel, Kummer and Stephan [15]. They conjectured that every $\leq^p_{tt}$-hard set for **NP** is p-superterse unless $\mathbf{P} = \mathbf{NP}$. We will prove that every $\leq^p_{tt}$-hard set for **NP** is p-superterse unless **NP** has p-measure 0.

1.2 Summary of Main Contributions

The main contributions in Chapter 3 are:

- We give Solovay style characterizations (in terms of martingales) of notions of Martin-Löf, Lutz, Schnorr and Kurtz randomness, respectively.

- We give a martingale characterization and an effective null cover characterization of the notion of Kurtz randomness.

- We show that the set of rec-random sequences is a proper subset of the set of Schnorr random sequences. This question has been left open by Schnorr [89], and later was conjectured to be true by van Lambalgen [57] and Lutz [65].

- We show that there is a sequence which is Schnorr random, but not Church stochastic.

The main contributions in Chapter 4 are:

- We introduce notions of n-randomness corresponding to the notions of rec-randomness and Schnorr randomness.

- We give martingale characterizations of the notions of Martin-Löf, rec-, Schnorr and Kurtz n-randomness, respectively. It should be noted that Kurtz [54] introduced the notions of Martin-Löf and Kurtz n-randomness in terms of effective null covers.

The main contributions in Chapter 5 are:

- We establish the relations among various notions of resource bounded randomness, for example, the relations among the notions of resource bounded Ko, rec-, Schnorr and Kurtz randomness.

- We study the notions of resource bounded stochasticity. In particular, we show that all “standard” statistical laws hold for p-random sequences.

The main contributions in Chapter 6 are:

- We establish the relations between resource bounded genericity concepts (resp. resource bounded randomness concepts) and the unsafe approximation concept. In particular, we show that p-random sets do not have optimal polynomial time unsafe approximations.

The main contribution in Chapter 7 is:

- We show that all $\leq^p_{tt}$-hard sets for **NP** are p-superterse unless **NP** is small.

1.3 Notation

For the most part our notation is standard, following that used by Soare [93] and Balcázar *et al.* [11]. We assume that the reader is familiar with the basics of recursion theory.

$N, Q(Q^+)$ 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 $n+1$ of x ($x[0..n] = x$ if $|x| < n+1$) and $x[n]$ 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, 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., $x \in A$ 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., $A\restriction x = \{y : y < x \;\&\; y \in A\}$, and we identify this initial segment with its characteristic string, i.e., $A\restriction z_n = A(z_0)\cdots A(z_{n-1}) \in \Sigma^*$. 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 $B \not\subseteq A$), and $A =^* B$ (resp. $A \subseteq^* B$) denotes that $A\Delta B$ (resp. $A - B$) is finite. For a number n, $A^{=n} = \{x \in A : |x| = n\}$ and $A^{\leq n} = \{x \in A : |x| \leq n\}$.

A class $\mathbf{C}$ of languages is closed under finite variation iff, for all languages A and B, if $A =^* B$, then $A \in \mathbf{C}$ iff $B \in \mathbf{C}$. 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. An open set is a (finite or infinite) union of basic open sets, that is, a set $X \cdot \Sigma^\infty$ where $X \subseteq \Sigma^*$. A closed set is the complement of an open set. A class of languages is recursively open if it is of the form $X \cdot \Sigma^\infty$ for some recursively enumerable set $X \subseteq \Sigma^*$. A class of languages is recursively closed if it is the complement of some recursively open set.

For a class $\mathbf{C}$ of languages, we write $Prob[\mathbf{C}]$ 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 fix a standard polynomial time computable and invertible pairing function $\lambda x, y < x, y >$ on Σ^* such that, for a string x, there is a real $\alpha(x) > 0$ satisfying

$$\|\Sigma^{[x]} \cap \Sigma^n\| \geq \alpha(x) \cdot 2^n \text{ for almost all } n$$

where $\Sigma^{[x]} = \{< x, y >: y \in \Sigma^*\}$ and $\Sigma^{[\leq x]} = \{< x', y >: x' \leq x \ \& \ y \in \Sigma^*\}$. For a set U, let $U^{[k]} = \{x :< k, x >\in U\}$. 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. For a function $f : \Sigma^* \rightarrow N$, $O(f)$ denotes the class $\{g : g \leq cf \text{ for some } c \in N\}$ of functions. Finally, we fix a recursive enumeration $\{P_e : e \geq 0\}$ of $\mathbf{P}$ such that $P_e(x)$ can be computed in $O(2^{|x|+e})$ steps (uniformly in e and x).

Chapter 2

Basics of Lebesgue Measure Theory

In this chapter we review some of the basic concepts of Lebesgue measure theory which we need in this thesis. In particular, we give an alternative definition (by Ville [98]) of Lebesgue measure in terms of martingales.

2.1 Lebesgue Measure Theory

We identify the unit interval $[0,1]$ with the set Σ^∞ of infinite 0-1 sequences. For two infinite sequences $\xi, \eta \in \Sigma^\infty$, we write $\xi < \eta$ if there exists $n \in N$ such that $\xi[0..n-1] = \eta[0..n-1]$ and $\xi[n] < \eta[n]$, and we write $\xi \leq \eta$ if $\xi = \eta$ or $\xi < \eta$. (ξ, η) denotes the corresponding open interval inside $[0,1]$.

The *measure* (or *probability*) of a basic open set $\mathbf{C}_x = x \cdot \Sigma^\infty$ is defined as $Prob[\mathbf{C}_x] = 2^{-|x|}$.

A sequence of basic open sets $\{\mathbf{C}_{x_n} : n \in N\}$ is said to *cover* a set $\mathbf{C} \subseteq \Sigma^\infty$ if its union contains $\mathbf{C}$. The greatest lower bound of the sums $\sum_{n \in N} Prob[\mathbf{C}_{x_n}]$, for all sequences $\{\mathbf{C}_{x_n} : n \in N\}$ that cover $\mathbf{C}$, is called the *outer measure* (or *outer probability*) of $\mathbf{C}$, and is denoted by $Prob^*[\mathbf{C}]$. I.e.,

$$Prob^*[\mathbf{C}] = \inf \left\{ \sum_{n \in N} Prob[\mathbf{C}_{x_n}] : \mathbf{C} \subseteq \cup_{n \in N} \mathbf{C}_{x_n} \right\}.$$

The *inner measure* (or *inner probability*) of a set $\mathbf{C} \subseteq \Sigma^\infty$ is defined as $Prob_*[\mathbf{C}] = 1 - Prob^*[\bar{\mathbf{C}}]$. A set $\mathbf{C} \subseteq \Sigma^\infty$ is *Lebesgue measurable* if $Prob^*[\mathbf{C}] = Prob_*[\mathbf{C}]$. For a Lebesgue measurable set $\mathbf{C}$, $Prob[\mathbf{C}] = Prob^*[\mathbf{C}]$ is called the *measure* (or *probability*) of $\mathbf{C}$.

Lemma 2.1.1 *A set $\mathbf{C} \subset \Sigma^\infty$ has Lebesgue measure 0 if and only if, for each $n \in N$, there is a set $A \subseteq \Sigma^*$ such that the following hold.*

1. $\sum_{x \in A} Prob[\mathbf{C}_x] \leq 2^{-n}$.

2. $\mathbf{C} \subseteq A \cdot \Sigma^\infty = \cup_{x \in A} \mathbf{C}_x$.

Proof. Straightforward. ■

We often call a set $\mathbf{C}$ a null set if it has Lebesgue measure 0. It is obvious that singletons are null sets and that any subset of a null set is a null set. Any countable union of null sets is also a null set.

Theorem 2.1.2 *(Borel) If a finite or infinite sequence* $\{\mathbf{C}_{x_n} : n \in N\}$ *of basic open sets covers a basic open set* $\mathbf{C}_x$*, then* $Prob[\mathbf{C}_x] \leq \sum_{n\in N} Prob[\mathbf{C}_{x_n}]$.

Proof. Straightforward. ■

The following two theorems are useful in the study of Lebesgue measure.

Theorem 2.1.3 *(The first Borel-Cantelli Lemma) Let* $\mathbf{C}_0, \mathbf{C}_1, \cdots$ *be an infinite sequence of Lebesgue measurable sets such that* $\sum_{n\in N} Prob[\mathbf{C}_n]$ *converges. Then*

$$\mathbf{C} = \{\xi : \xi \textit{ belongs to infinitely many } \mathbf{C}_n\}$$

is a null set.

Proof. Choose $n_0, n_1, \cdots$ so that, for each $i \in N$, $\sum_{j\geq n_i} Prob[\mathbf{C}_j] \leq 2^{-i}$. Obviously, for each $i \in N$,

$$\mathbf{C} \subseteq \cup_{j\geq n_i} \mathbf{C}_j.$$

Hence, by Lemma 2.1.1 and Theorem 2.1.2, $\mathbf{C}$ is a null set. ■

The following theorem is a "converse" of the above theorem for the special case of mutually independent $\mathbf{C}_n$.

Theorem 2.1.4 *(The second Borel-Cantelli Lemma) Let* $\mathbf{C}_0, \mathbf{C}_1, \cdots$ *be an infinite sequence of independent, Lebesgue measurable sets, i.e.,* $Prob[\mathbf{C}_i] \cdot Prob[\mathbf{C}_j] = Prob[\mathbf{C}_i \cap \mathbf{C}_j]$ *for* $i \neq j$*, such that* $\sum_{n\in N} Prob[\mathbf{C}_n]$ *diverges. Then*

$$\mathbf{C} = \{\xi : \xi \in \mathbf{C}_n \textit{ for infinitely many } n \in N\},$$

has probability 1.

Remark. The proof of this theorem can be found in many textbooks. In the proof of the law of the iterated logarithm for p-random sequences (Chapter 5), the idea underlying the following proof will be used.

Proof. Let $c_n = Prob[\mathbf{C}_n]$ and

$$\mathbf{A}_n = \{\xi : \xi \notin \mathbf{C}_i \text{ for all } i \leq n\}.$$

Then, by the independence property of the sequence $\{\mathbf{C}_n : n \in N\}$, $Prob[\mathbf{A}_n] \leq (1 - c_0) \cdots (1 - c_n) < e^{-(c_0+\cdots+c_n)}$. Hence the set

$$\mathbf{B}_1 = \{\xi : \xi \in \mathbf{C}_n \text{ for at least one } n \in N\}$$

has probability 1.

Next, divide the sequence $\mathbf{C}_0, \mathbf{C}_1, \cdots$ into two subsequences $\mathbf{C}'_0, \mathbf{C}'_1, \cdots$ and $\mathbf{C}''_0, \mathbf{C}''_1, \cdots$ so that both series $\sum_{n \in N} Prob[\mathbf{C}'_n]$ and $\sum_{n \in N} Prob[\mathbf{C}''_n]$ diverge. Applying our above result to the two subsequences we obtain that

$$\mathbf{B}_2 = \{\xi : \xi \in \mathbf{C}_n \text{ for at least two } n \in N\}$$

has probability 1. Applying, in turn, this statement to the sequences $\mathbf{C}'_0, \mathbf{C}'_1, \cdots$ and $\mathbf{C}''_0, \mathbf{C}''_1, \cdots$, and going on this procedure, we can show that, for every $i \in N$, the set

$$\mathbf{B}_i = \{\xi : \xi \in \mathbf{C}_n \text{ for at least } i \text{ numbers } n \in N\}$$

has probability 1. Hence $\mathbf{C} = \cap_{i=1}^{\infty} \mathbf{B}_i$ has probability 1. ■

2.2 Martingales

Following Ville [98], in this section we give an alternative definition of Lebesgue measure based on martingales.

Definition 2.2.1 *A* martingale *is a function $F : \Sigma^* \rightarrow R^+$ such that, for all $x \in \Sigma^*$,*

$$F(x) = \frac{F(x1) + F(x0)}{2}. \tag{2.1}$$

A martingale F covers *a set $\mathbf{C}$ of infinite sequences if, for each $\xi \in \mathbf{C}$, $\liminf_n F(\xi[0..n-1]) \geq 1$. A martingale F* succeeds *on an infinite sequence $\xi \in \Sigma^\infty$ if $\limsup_n F(\xi[0..n-1]) = \infty$. $\mathbf{NULL}_F$ denotes the set of infinite sequences on which F succeeds.*

Ville [98] has shown that Lebesgue measure can be defined in terms of martingales. In particular, a set of infinite sequences has Lebesgue measure 0 if and only if there is a martingale which succeeds on all sequences in the set.

For each basic open set $\mathbf{C}_x$, define a martingale F_x by

$$F_x(y) = \begin{cases} 2^{|y|-|x|} & y \sqsubseteq x \\ 1 & x \sqsubseteq y \\ 0 & \text{otherwise} \end{cases}$$

Then $F_x(\lambda) = Prob[\mathbf{C}_x]$ and, for all $y \in x \cdot \Sigma^*$, $F_x(y) = 1$. That is to say, $\mathbf{C}_x$ is covered by F_x. In the same way, it is easy to prove the following lemma.

Lemma 2.2.2 *For each open set $\mathbf{C} \subseteq \Sigma^\infty$, there is a martingale F such that $F(\lambda) = Prob[\mathbf{C}]$ and $\mathbf{C}$ is covered by F.*

Proof. Straightforward. ■

Lemma 2.2.3 *For each null set $\mathbf{C}$, there is a martingale F which succeeds on $\mathbf{C}$.*

Proof. Because $\mathbf{C}$ is a null set, by Lemma 2.1.1, for each n, there is an open set $\mathbf{C}_n$ such that $\mathbf{C} \subseteq \mathbf{C}_n$ and $Prob[\mathbf{C}_n] \leq 2^{-n}$. By Lemma 2.2.2, there is a martingale F_n such that $F_n(\lambda) \leq 2^{-n}$ and $\mathbf{C}_n$ is covered by F_n. Let $F(x) = \sum_{n\in N} F_n(x)$. Then F is a martingale which succeeds on $\mathbf{C}$. ■

Lemma 2.2.4 *(Ville [98]) Let F be a martingale and $F_k = \{x \in \Sigma^* \ : \ F(x) > k\}$. Then $Prob[F_k \cdot \Sigma^\infty] \leq F(\lambda)k^{-1}$.*

Proof. Let F'_k be a prefix free set (i.e. $F'_k \cap F'_k\Sigma\Sigma^* = \emptyset$) satisfying $F_k \cdot \Sigma^\infty = F'_k \cdot \Sigma^\infty$. Then

$$F(\lambda) \geq \sum_{x\in F'_k} F(x)2^{-|x|} \geq k \cdot Prob[F_k \cdot \Sigma^\infty].$$

Consequently,

$$Prob[F_k \cdot \Sigma^\infty] \leq F(\lambda)k^{-1}.$$

■

By combining Lemma 2.2.3 and Lemma 2.2.4, we get

Corollary 2.2.5 *A set $\mathbf{C} \subset \Sigma^\infty$ is a null set if and only if there exists a martingale F such that F succeeds on $\mathbf{C}$.*

Corollary 2.2.5 shows that we can give an alternative definition of Lebesgue measure in terms of martingales. As an example, we rephrase the first Borel-Cantelli lemma in terms of martingales.

Theorem 2.2.6 *(The first Borel-Cantelli Lemma) Let $F_0, F_1, \cdots$ be an infinite sequence of martingales such that $\sum_{n\in N} F_n(\lambda)$ converges. Then the martingale $F = \sum_{n\in N} F_n$ succeeds on*

$$\mathbf{C} = \{\xi : \xi \textit{ is covered by infinitely many } F_n\}.$$

Hence $\mathbf{C}$ is a null set.

Proof. Straightforward ■

Chapter 3

A Comparison of Classical Randomness Concepts

3.1 Typicalness

We have already mentioned in the introduction that Martin-Löf defined a notion of randomness in terms of typicalness, that is, he identified the notion of randomness with the notion of typicalness. Since every single sequence has Lebesgue measure 0, we can not use Lebesgue measure to define the notions of "small sets" and "large sets". So Martin-Löf [74] introduced the notion of an "effectively null set", which can be used for a definition of random sequences. Each constructive null set can be considered as an effective statistical test (see Martin-Löf [74]), and it is more intuitive to give definitions of randomness concepts in terms of effective tests. In the style of the first Borel-Cantelli Lemma, a variant definition of Martin-Löf's randomness concept was given by Solovay (see, e.g., Chaitin [30] or Kautz [46]).

Schnorr [88, 89] characterized Martin-Löf's effective tests in terms of martingales, and criticized Martin-Löf's concepts as being too strong. Using ideas from intuitionistic mathematics by L. E. J. Brouwer, he modified Martin-Löf's notion of randomness by adding some additional requirements to the effective tests, and got a new weaker notion of randomness.

Ko [48] has tried to introduce a notion of pseudorandomness along the line of Martin-Löf, but he observed that this approach does not work if we only replace the effective tests with polynomial time tests: A sequence does not withstand some effective test if and only if it does not withstand some polynomial time test. Ko succeeded in defining a meaningful concept of pseudorandmoness, however, by additionally taking into account the resources which is needed to check whether a sequence withstands an effective test. Roughly speaking, a sequence is Ko pseudorandom if it cannot be *easily* rejected by any *efficient* method of testing randomness. Here we introduce a recursive version of Ko's pseudorandomness concept by replacing *easily* and *efficient* with *effectively* and *effective*, respectively. We characterize this notion in terms of effective null covers consisting of finite unions of basic open sets and in terms of martingales. From these characterizations, it is easy to show that this notion coincides with the notion of Schnorr randomness and to give a Solovay style characterization of this notion.

Using martingale concepts, Lutz [63, 65] introduced an effective version of Lebesgue measure. He and others have studied this subject systematically. For example, Lutz [65] has shown the first Borel-Cantelli Lemma for his effective measure, from which it is easy to give a Solovay style criterion for the notion of rec-randomness.

Kurtz [54] has further studied a randomness concept based on the notion of "typicalness". He defined that a sequence is weakly random if and only if it is not in any recursively closed set of Lebesgue measure 0. We characterize this notion in terms of constructive null covers, martingales and a Solovay style criterion.

3.1.1 Martin-Löf randomness

For a definition of random sequences, many insufficient approaches have been made until a definition was proposed by Martin-Löf, which for the first time included all standard statistical properties of random sequences.

Definition 3.1.1 *(Martin-Löf [74]) A* Martin-Löf test *is a recursively enumerable set U with the property that $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$ for all $k \in N$. An infinite sequence ξ* does not withstand *the Martin-Löf test U if $\xi \in U^{[k]} \cdot \Sigma^\infty$ for all $k \in N$. A sequence ξ is* Martin-Löf random *if it withstands all Martin-Löf tests.*

Let **M-NULL** be the set of sequences which do not withstand some Martin-Löf test, and let **M-RAND** $= \Sigma^\infty -$ **M-NULL** be the set of Martin-Löf random sequences.

In the following, we show that, in the definition of Martin-Löf's random sequences, we can require that the Martin-Löf test U be polynomial time computable (this fact was first observed by Ko [48]).

Definition 3.1.2 *(Ko [48]) An* m-1-test *is a Martin-Löf test U which is polynomial time computable. A sequence ξ is* m-1-random *if it withstands all m-1-tests.*

Let **M-1-NULL** be the set of sequences which do not withstand some m-1-test, and let **M-1-RAND** $= \Sigma^\infty -$ **M-1-NULL** be the set of m-1-random sequences.

The above definition of Martin-Löf's randomness concept is based on effective tests, which are given by recursively open sets. As shown by Schnorr [88, 89], the martingale concept can be used to characterize effective tests also. Schnorr [88, 89] used various types of martingales to characterize effective tests and to give a uniform approach to definitions of various randomness concepts. In particular, he characterized the notion of Martin-Löf randomness in terms of martingales.

Definition 3.1.3 *(Schnorr [88, 89]) A total function $F : \Sigma^* \to R$ is* weakly approximable *if there is a recursive function $h : N \times \Sigma^* \to Q$ such that*

1. *For each $n \in N$ and $x \in \Sigma^*$, $h(n, x) \leq h(n + 1, x)$.*
2. *For each $x \in \Sigma^*$, $\lim_n h(n, x) = F(x)$.*

Definition 3.1.4 *(Schnorr [88, 89]) An* m-2-test *is a weakly approximable martingale F. An infinite sequence ξ* does not withstand *the m-2-test F if F succeeds on ξ. A sequence ξ is* m-2-random *if it withstands all m-2-tests.*

Let **M-2-NULL** be the set of sequences which do not withstand some m-2-test, and let **M-2-RAND** $= \Sigma^\infty -$ **M-2-NULL** be the set of m-2-random sequences.

Now we introduce Solovay's characterization of Martin-Löf's randomness concept. Solovay's original characterization is based on open covers, whereas the following one is based on martingales.

Definition 3.1.5 *A* Solovay test *is a recursive function $F : N \times \Sigma^* \to Q^+$ with the properties that*

1. $\sum_{i=0}^{\infty} F(i, \lambda) < \infty$.
2. *For each $i \in N$, $F_i(x) = F(i, x)$ is a martingale.*

An infinite sequence ξ does not withstand *the Solovay test F if it is covered by infinitely many F_i. A sequence ξ is* Solovay random *if it withstands all Solovay tests.*

Let **So-M-NULL** be the set of sequences which do not withstand some Solovay test, and let **So-M-RAND** $= \Sigma^\infty -$ **So-M-NULL** be the set of Solovay random sequences.

The following theorem shows that the above defined randomness concepts coincide.

Theorem 3.1.6 *(Ko [48] and Schnorr [88, 89])* **M-RAND** = **M-1-RAND** = **M-2-RAND** = **So-M-RAND**.

Remark. **M-RAND** = **M-1-RAND** was proved by Ko [48] and **M-RAND** = **M-2-RAND** was proved by Schnorr [88, 89]. We include proofs of these facts here only for the sake of completeness.

Proof. In order to show **M-NULL** = **M-1-NULL** = **M-2-NULL** = **So-M-NULL**, it is sufficient to show the following implications.

M-1-NULL $\subseteq$ **So-M-NULL** $\subseteq$ **M-2-NULL** $\subseteq$ **M-NULL** $\subseteq$ **M-1-NULL**.

(1). **M-1-NULL** $\subseteq$ **So-M-NULL**

Let U be an m-1-test. W.l.o.g. we may assume that $U^{[k]}$ is prefix-free for all $k \in N$, that is, for each $x \in U^{[k]}$, there is no nonempty string y such that $xy \in U^{[k]}$. Define a recursive function F by

$$F(<k, l>, x) = \begin{cases} 2^{-|y|} & \text{if } xy = x_{<k,l>} \text{ for some } y \in \Sigma^* \\ 1 & \text{if } x = x_{<k,l>}y \text{ for some } y \in \Sigma^* \\ 0 & \text{otherwise} \end{cases}$$

where $x_{<k,l>}$ is the lth element of $U^{[k]}$.

It is straightforward to verify that the following hold.

1. $\sum_{<k,l>\in N} F(<k,l>,\lambda) = \sum_{i\in N} \mathit{Prob}[U^{[i]}\cdot\Sigma^\infty] \leq \sum_{i\in N} 2^{-i} = 2$.

2. $F : N \times \Sigma^* \to Q$ is recursive.

3. For each i, $F_i(x) = F(i,x)$ is a martingale.

So F is a Solovay test. Moreover, for each $<k,l>$, if $\xi \in x_{<k,l>}\cdot\Sigma^\infty$, then ξ is covered by $F_{<k,l>}$. Hence, for every ξ which does not withstand the m-1-test U, ξ is covered by infinitely many F_i, that is, ξ does not withstand the Solovay test F.

(2). **So-M-NULL $\subseteq$ M-2-NULL**

Let $F(i,x)$ be a Solovay test. Define a function F' by

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

Then F' is a martingale which is weakly approximable as witnessed by $h(n,x) = \sum_{i=0}^{n} F(i,x)$, and, for every sequence ξ, if ξ is covered by infinitely many $F_i(x) = F(i,x)$, then F' succeeds on ξ.

(3). **M-2-NULL $\subseteq$ M-NULL**

Let F be an m-2-test and let h be the recursive function witnessing the weak approximability of F. W.l.o.g. we may assume that $F(\lambda) \leq 1$. Define a recursively enumerable set U by

$$U = \{<k,x>: \exists n\ (h(n,x) \geq 2^k)\}.$$

By Lemma 2.2.4, $\mathit{Prob}[U^{[k]}\cdot\Sigma^\infty] \leq 2^{-k}$ for all $k \in N$. Hence U is a Martin-Löf test and $\mathbf{NULL}_F \subseteq U^{[k]}\cdot\Sigma^\infty$ for all $k \in N$. That is, no sequence in $\mathbf{NULL}_F$ withstands the Martin-Löf test U.

(4). **M-NULL $\subseteq$ M-1-NULL**

Given a Martin-Löf test U, for each k, let $U_s^{[k]}$ be the set of all strings which have been enumerated in $U^{[k]}$ by the end of the sth step of a fixed recursive enumeration of U, and let

$$V = \{<k,x>: \text{ there exists } y \sqsubseteq x \text{ such that } y \in U_{|x|}^{[k]}\}.$$

Then V is polynomial time computable and $V^{[k]}\cdot\Sigma^\infty = U^{[k]}\cdot\Sigma^\infty$ for all $k \in N$. That is, V is an m-1-test and every sequence that does not withstand the Martin-Löf test U does not withstand the m-1-test V. ■

We close this section with the observation that there is a universal Martin-Löf test.

Theorem 3.1.7 *(Martin-Löf [74] and Schnorr [88, 89]) There exists a universal m-2-test F, that is, there is a weakly approximable martingale F such that* **M-2-NULL= NULL**$_F$.

Proof. See Schnorr [88, 89]. ■

3.1.2 Rec-randomness

Schnorr [88, 89] objected to Martin-Löf's randomness concepts, because the algorithmic structure of an m-2-test F is not symmetrical. He thought that there is no reason why we should require that the martingale F be weakly approximable but at the same time may allow that $-F$ is not weakly approximable. So Schnorr proposed the following definition.

Definition 3.1.8 *(Schnorr [88, 89]) A* rec-1-test *is a martingale F such that $-F$ is weakly approximable. An infinite sequence ξ* does not withstand *the rec-1-test F if F succeeds on ξ. A sequence ξ is* rec-1-random *if it withstands all rec-1-tests.*

Let **rec-1-NULL** be the set of sequences which do not withstand some rec-1-test, and let **rec-1-RAND** $= \Sigma^\infty -$ **rec-1-NULL** be the set of rec-1-random sequences.

By the martingale property (2.1), a rec-1-test can be characterized by a recursive martingale.

Lemma 3.1.9 *(Schnorr [89]) For each rec-1-test F, there exists a recursive martingale $F' : \Sigma^* \to Q^+$ such that $F'(x) > F(x)$ for all $x \in \Sigma^*$.*

Proof. Let F be a rec-1-test which is given by a recursive function $h : N \times \Sigma^* \to Q^+$, that is, $\lim_n h(n,x) = F(x)$ and $h(n+1,x) \leq h(n,x)$ for all $n \in N$ and $x \in \Sigma^*$. W.l.o.g. we may assume that $F(x) < h(n,x)$ for all $n \in N$ and $x \in \Sigma^*$. (If h does not have this property, replace h by $h'(n,x) = h(n,x) + 2^{-n}$.)

We inductively define a recursive martingale F' such that $F'(x) > F(x) + 2^{-|x|}$ for all strings x. Let

$$F'(\lambda) = h(0,\lambda) + 1.$$

Then $F'(\lambda) = h(0,\lambda) + 2^{-|\lambda|} > F(x) + 2^{-|\lambda|}$. For the inductive step, fix x and assume that $F'(x)$ has been defined. Let

$$F'(x1) = h(n,x1) + 2^{-|x|-1}.$$

where $n = \min\{i : h(i,x1) + h(i,x0) < 2(F'(x) - 2^{-|x|})\}$, and let

$$F'(x0) = 2F'(x) - F'(x1).$$

By the recursiveness of h, the above n can be found effectively, whence F' is recursive. Moreover, by definition, $F'(x1) > F(x1) + 2^{-|x1|}$. So it suffices to show that $F'(x0) > F(x0) + 2^{-|x0|}$. This is shown as follows.

$$\begin{aligned} F'(x0) &= 2F'(x) - F'(x1) \\ &= 2F'(x) - h(n,x1) - 2^{-|x|-1} \\ &> h(n,x0) + 2^{-|x|-1} \quad \text{(by the choice of } n\text{)} \\ &> F(x0) + 2^{-|x0|}. \end{aligned}$$

■

By Lemma 3.1.9, we can rephrase the definition of rec-1-randomness in terms of recursive martingales. The following definition was introduced by van Lambalgen [57] and Lutz [65].

Definition 3.1.10 *(van Lambalgen [57] and Lutz [65]) A* rec-test *is a recursive martingale $F : \Sigma^* \to Q^+$. An infinite sequence ξ* does not withstand *the rec-test F if F succeeds on ξ. A sequence ξ is* rec-random *if it withstands all rec-tests.*

Let **rec-NULL** be the set of sequences which do not withstand some rec-test, and let **rec-RAND**$= \Sigma^\infty -$ **rec-NULL** be the set of rec-random sequences.

It should be noted that Lutz [65] introduced his resource bounded measure theory and resource bounded randomness concepts in terms of approximable martingales. However, the following lemma shows that it is enough to consider recursive martingales.

Definition 3.1.11 *(Schnorr [89]) A function $F : \Sigma^* \to R$ is* approximable *if there is a recursive function $h : N \times \Sigma^* \to Q$ such that, for all n,*

$$|F(x) - h(n, x)| \leq 2^{-n}.$$

By the martingale property (2.1), the approximable martingales do not have additional power in characterizing effective tests when compared with recursive martingales.

Lemma 3.1.12 *(Schnorr [89, Satz 9.3]) For each approximable martingale $F : \Sigma^* \to R^+$, there exists a recursive martingale $F' : \Sigma^* \to Q^+$ such that $F'(x) \geq F(x)$ for all $x \in \Sigma^*$.*

Proof. Let $h : N \times \Sigma^* \to Q$ be a function such that $|h(n, x) - F(x)| \leq 2^{-n}$ for all $n \in N$ and $x \in \Sigma^*$. We inductively define a function h_1 by letting $h_1(0, x) = h(0, x) + 2$ for all $x \in \Sigma^*$, and by letting

$$h_1(n + 1, x) = \min\{h_1(0, x), \cdots, h_1(n, x), h(n + 1, x) + 2^{-n}\}$$

for all $n \in N$ and $x \in \Sigma^*$. Then $\lim_n h_1(n, x) = F(x)$ and $F(x) \leq h_1(n + 1, x) \leq h_1(n, x)$ for all $n \in N$ and $x \in \Sigma^*$. By Lemma 3.1.9, there is a recursive martingale $F' : \Sigma^* \to Q^+$ such that $F'(x) \geq F(x)$ for all $x \in \Sigma^*$. ■

Corollary 3.1.13 *A sequence ξ is rec-random if and only if, for each approximable martingale F, F does not succeed on ξ.*

We can also give a Solovay style characterization of rec-randomness concept as follows.

Definition 3.1.14 *A* So-rec-test *is a recursive function $F : N \times \Sigma^* \to Q^+$ such that*

1. *$\sum_{i=0}^{\infty} F(i, \lambda) < \infty$ is computable, that is, we can recursively find a number n_k for each $k \in N$ such that $\sum_{i=n_k}^{\infty} F(i, \lambda) < 2^{-k}$.*
2. *For each i, $F_i(x) = F(i, x)$ is a martingale.*

An infinite sequence does not withstand *the So-rec-test F if it is covered by infinitely many F_i. A sequence ξ is* So-rec-random *if it withstands all So-rec-tests.* **So-rec-NULL**$_F$ *denotes the set of sequences that do not withstand the So-rec-test F.*

Let **So-rec-NULL** be the set of sequences which do not withstand some So-rec-test, and let **So-rec-RAND** $= \Sigma^\infty -$ **So-rec-NULL** be the set of So-rec-random sequences.

Theorem 3.1.15 rec-RAND=So-rec-RAND=rec-1-RAND.

Proof. By Lemma 3.1.9, **rec-RAND=rec-1-RAND**. Hence it suffices to show that **rec-NULL =So-rec-NULL**.

(1). **rec-NULL** $\subseteq$**So-rec-NULL**

Given a recursive martingale F, define a function F' by

$$F'(i,x) = \frac{1}{2^i}F(x).$$

Then F' is a So-rec-test and **rec-NULL**$_F$ $\subseteq$ **So-rec-NULL**$_{F'}$.

(2). **So-rec-NULL**$\subseteq$ **rec-NULL**

Given a So-rec-test F, define a martingale F' by

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

Then F' is approximable and **So-rec-NULL**$_F$ $\subseteq$ **rec-NULL**$_{F'}$. Moreover, by Lemma 3.1.12, there is a recursive martingale F'' such that **So-rec-NULL**$_F$ $\subseteq$ **rec-NULL**$_{F''}$. ∎

3.1.3 Schnorr and Ko randomness

After characterizing Martin-Löf's statistical tests in terms of martingales, Schnorr [88] remarked:

> Computability and the martingale property (2.1) suffice to characterize effective tests. But which sequences are refused by an effective test? $\cdots$ one would define that a sequence ξ does not withstand the test F if and only if $\limsup_n F(\xi[0..n-1]) = \infty$. However, if the sequence $F(\xi[0..n-1])$ increases so slowly that no one working with effective methods only would observe its growth, then the sequence ξ behaves as if it withstands the test F. The definition of **NULL**$_F$ has to reflect this fact. That is, we have to make constructive the notion $\limsup_n F(\xi[0..n-1]) = \infty$. (From Schnorr [88, p256])

Using ideas from intuitionistic mathematics by L. E. J. Brouwer, Schnorr [89] developed a randomness concept by adding some additional requirements to the notion of martingale-succeeding on a sequence.

Definition 3.1.16 *(Schnorr [89]) An* s-test (Schnorr test) *is a pair* (F, h) *of functions such that* F *is a recursive martingale and* $h : N \to N$ *is an unbounded, nondecreasing, recursive function. A sequence* ξ does not withstand *the s-test* (F, h) *if* $\limsup_n(F(\xi[0..n-1]) - h(n)) \geq 0$*, i.e., if* $F(\xi[0..n-1]) \geq h(n)$ *i.o. A sequence* ξ *is* s-random (Schnorr random) *if it withstands all s-tests.* $\mathbf{S\text{-}NULL}_{(F,h)}$ *denotes the set of sequences that do not withstand the s-test* (F, h)*.*

Let **S-NULL** be the set of sequences which do not withstand some s-test, and let **S-RAND** $= \Sigma^\infty -$ **S-NULL** be the set of s-random sequences.

In the following, we will list some characterizations of Schnorr randomness. The equivalence of these concepts will be proved at the end of this section. We start with Schnorr's characterization of his randomness concept in terms of Martin-Löf style statistical tests.

Definition 3.1.17 *(Schnorr [89]) An* s-1-test *is a pair* (U, g) *consisting of a recursively enumerable set* U *and a recursive function* g*, together with a recursive enumeration* $\{U_s\}_{s\in N}$ *of* U *such that, for each* k *and* j*,*

1. $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.
2. $Prob[(U^{[k]} - U^{[k]}_{g(k,j)}) \cdot \Sigma^\infty] \leq 2^{-j}$.

An infinite sequence ξ does not withstand *the s-1-test* (U, g) *if* $\xi \in U^{[k]} \cdot \Sigma^\infty$ *for all* $k \in N$*. A sequence* ξ *is* s-1-random *if it withstands all s-1-tests.*

Let **S-1-NULL** be the set of sequences which do not withstand some s-1-test, and let **S-1-RAND** $= \Sigma^\infty -$ **S-1-NULL** be the set of s-1-random sequences.

The additional constraint 2 in an s-1-test (which is absent in a Martin-Löf test) has the implication that $\lim_s Prob[U^{[k]}_s \cdot \Sigma^\infty]$ not only converges to a number less than 2^{-k}, but converges effectively also.

As we will show below, in the definition of s-1-tests, we can require that the set U be polynomial time computable.

Definition 3.1.18 *An* s-2-test *is a pair* (U, g) *where* U *is a polynomial time computable set and* g *is a recursive function such that, for each* k *and* j*,*

1. $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.
2. $Prob[(U^{[k]} \cap \Sigma^{g(k,j)}\Sigma^*) \cdot \Sigma^\infty] \leq 2^{-j}$.

An infinite sequence ξ does not withstand *the s-2-test* (U, g) *if* $\xi \in U^{[k]} \cdot \Sigma^\infty$ *for all* $k \in N$*. A sequence* ξ *is* s-2-random *if it withstands all s-2-tests.*

Let **S-2-NULL** be the set of sequences which do not withstand some s-2-test, and let **S-2-RAND** $= \Sigma^\infty -$ **S-2-NULL** be the set of s-2-random sequences.

There is also a Solovay style characterization of Schnorr's randomness concept.

Definition 3.1.19 *A* So-s-test *is a pair (F, h) of functions with the properties that both $F : N \times \Sigma^* \to Q^+$ and $h : N \to N$ are recursive functions satisfying*

1. *$\sum_{i=0}^{\infty} F(i, \lambda) < \infty$ is computable, that is, we can recursively find a number n_k for each k such that $\sum_{i=n_k}^{\infty} F(i, \lambda) < 2^{-k}$.*

2. *For each i, $F_i(x) = F(i, x)$ is a martingale.*

A sequence $\xi \in \Sigma^\infty$ is covered *by F_i with respect to h if $F_i(\xi[0..n-1]) \geq 1$ for all $n > h(i)$. A sequence ξ* does not withstand *the So-s-test (F, h) if it is covered by infinitely many F_i w.r.t. h. A sequence ξ is* So-s-random *if it withstands all So-s-tests.* $\textbf{So-S-NULL}_{(F,h)}$ *denotes the set of sequences that do not withstand the So-s-test (F, h).*

Let **So-S-NULL** be the set of sequences which do not withstand some So-s-test, and let **So-S-RAND** $= \Sigma^\infty -$ **So-S-NULL** be the set of So-s-random sequences.

Ko [48] introduced a notion of pseudorandomness in terms of efficient tests. Intuitively, in an efficient Ko test, we reject the hypothesis that ξ is random on the significance level 2^{-k} if ξ does not pass the test by examining only the first $g^{-1}(k)$ bits of ξ, where g belongs to some specified set of functions. In the following, we will introduce a recursive version of this notion by letting g^{-1} be any recursive function.

Definition 3.1.20 *(Ko [48]) A* k-test *is a pair (U, g) where U is a recursive set and g is an unbounded, nondecreasing, recursive function such that $U^{[0]} = \Sigma^*$ and, for all k, the following hold.*

1. *For $x, y \in \Sigma^*$, if $x \in U^{[k]}$, then $xy \in U^{[k]}$.*

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

3. *$Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.*

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

Let **K-NULL** be the set of sequences that do not withstand some k-test, and let **K-RAND** $= \Sigma^\infty -$ **K-NULL** be the set of k-random sequences.

It is possible to define k-tests in terms of finite sets, which is useful for a Solovay style characterization of Ko's randomness concept.

Definition 3.1.21 *A* k-1-test *is a pair (U, g) where U is a recursive set and g is a recursive function such that the following hold.*

1. *$U^{[k]} \subseteq \Sigma^{\leq g(k)}$.*

2. *$Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.*

A sequence ξ does not withstand *the k-1-test (U, g) if $\xi \in U^{[k]} \cdot \Sigma^\infty$ i.o. A sequence ξ is* k-1-random *if it withstands all k-1-tests.*

Let **K-1-NULL** be the set of sequences that do not withstand some k-1-test, and let **K-1-RAND** $= \Sigma^\infty -$ **K-1-NULL** be the set of k-1-random sequences.

The following theorem shows that these notions of randomness defined above coincide.

Theorem 3.1.22 S-RAND = S-1-RAND = S-2-RAND = So-S-RAND = K-RAND = K-1-RAND.

Remark. **S-1-RAND = S-RAND** was proved by Schnorr [89], and part (2) of the following proof is taken from Schnorr [89]. We include it here only for the sake of completeness.

Proof. It suffices to show the following implications.

S-2-NULL $\subseteq$ **S-1-NULL** $\subseteq$ **S-NULL** $\subseteq$ **K-1-NULL** $\subseteq$ **K-NULL** $\subseteq$ **K-1-NULL** $\subseteq$ **So-S-NULL** $\subseteq$ **K-1-NULL** $\subseteq$ **S-2-NULL**.

(1). **S-2-NULL** $\subseteq$ **S-1-NULL**

Straightforward.

(2). **S-1-NULL** $\subseteq$ **S-NULL**

Let (U,g) be an s-1-test. W.l.o.g., assume that, for each k, $U^{[k]}$ is prefix-free. Let $B = \cup_{k\in N} U^{[k]}$ and let $f(n)$ be an unbounded, nondecreasing, recursive function satisfying

$$\sum_{x\in B\cap\Sigma^n\Sigma^*} 2^{-|x|} \leq 2^{-2f(n)}.$$

(Note that $\sum_{x\in B\cap\Sigma^n\Sigma^*} 2^{-|x|}$ converges to zero, whence such a function f exists.) Then

$$\sum_{\substack{x\in B\\ f(|x|)=m}} 2^{-|x|}2^{f(|x|)} \leq 2^{-2m}2^m = 2^{-m},$$

i.e.,

$$\sum_{x\in B} 2^{-|x|}2^{f(|x|)} \leq \sum_{n=0}^{\infty} 2^{-n} = 2.$$

Hence there exists an unbounded, nondecreasing, recursive function $h : N \to N$ such that

$$\sum_{x\in B\cap\Sigma^{h(n)}\Sigma^*} 2^{-|x|}2^{f(|x|)} \leq 2^{-n}.$$

For $k \in N$, let $V^{[k]} = B \cap \Sigma^{h(k)}\Sigma^*$. Then it is straightforward that $\cap_{k\in N}(U^{[k]}\cdot\Sigma^\infty) = \cap_{k\in N}(V^{[k]}\cdot\Sigma^\infty)$. Define a function F by

$$F(x) = \sum_{k\in N}\left(\sum_{xy\in V^{[k]}} 2^{-|y|}2^{f(|xy|)} + \sum_{\substack{x[0..n-1]\in V^{[k]}\\ n<|x|}} 2^{f(n)}\right).$$

Firstly we show that F is a martingale.

By the definition of f and V,

$$F(\lambda) = \sum_{k \in N} \sum_{x \in V^{[k]}} 2^{-|x|} 2^{f(|x|)} \leq \sum_{k \in N} 2^{-k} < \infty.$$

It is straightforward that, for each $x \in \Sigma^*$, $F(x0) + F(x1) = 2F(x)$.

Secondly, we show that F is approximable.

Obviously, F is weakly approximable. $F(\lambda)$ is approximable because

$$\left| F(\lambda) - \sum_{k=0}^{n} \sum_{x \in V^{[k]}} 2^{-|x|} 2^{f(|x|)} \right| \leq 2^{-n}$$

and

$$\left| \sum_{x \in V^{[k]}} 2^{-|x|} 2^{f(|x|)} - \sum_{x \in V^{[k]} \cap \Sigma^{h(j)} \Sigma^*} 2^{-|x|} 2^{f(|x|)} \right| \leq 2^{-j}.$$

In order to compute $F(x0)$ and $F(x1)$, we compute $F(x)$ with error less than $\frac{\varepsilon}{4}$ and find $u_0 \leq F(x0)$, $u_1 \leq F(x1)$ such that

$$|2F(x) - u_0 - u_1| < \frac{\varepsilon}{2}.$$

Then $|F(x0) - u_0| < \varepsilon$ and $|F(x1) - u_1| < \varepsilon$. Because $F(\lambda)$ is approximable and F is weakly approximable, F is approximable.

By the construction of F, it is straightforward that, for each sequence ξ that does not withstand the s-1-test (U, g), $\xi \in$ **S-NULL**$_{(F,f)}$. By Lemma 3.1.12, there is a recursive martingale F' such that **S-NULL**$_{(F,f)} \subseteq$ **S-NULL**$_{(F',f)}$.

(3). **S-NULL** $\subseteq$ **K-1-NULL**

Let (F, f) be an s-test. W.l.o.g., assume that $F(\lambda) \leq 1$.

Let $h(n) = \mu m(f(m) \geq 2^{n+1})$ and $U^{[k]} = \{x \in \Sigma^{\leq h(k)} : F(x) \geq 2^k\}$. Then, for each k,

1. $U^{[k]} \subseteq \Sigma^{\leq h(k)}$.
2. $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.

It follows that, for each sequence $\xi \in$ **S-NULL**$_{(F,f)}$, ξ does not withstand the k-1-test (U, h).

(4). **K-1-NULL** $\subseteq$ **K-NULL**

Given a k-1-test (U, g), let

$$\begin{aligned} g'(n) &= \max\{g(i) : i \leq n\}, \\ h(n) &= \min\{m : g'(m) > n\} - 1, \end{aligned}$$

and, for each k, let

$$V^{[k]} = \cup_{i \geq k+1} \{xy : x \in U^{[i]}, y \in \Sigma^*\}.$$

Then it is easily checked that (V, h) is a k-test.

Let ξ be a sequence that does not withstand the k-1-test (U, g). For each k_0, there exist $n \geq k > k_0$ such that $\xi[0..n-1] \in U^{[k]}$. Hence

$$\begin{aligned}
\max\{m : \xi[0..n-1] \in V^{[m]}\} &\geq k - 1 \\
&\geq \min\{m : \xi[0..n-1] \in U^{[m]}\} - 1 \\
&\geq \min\{m : g(m) \geq n\} - 1 \\
&\geq \min\{m : g'(m) \geq n\} - 1 \\
&= h(n).
\end{aligned}$$

That is, ξ does not withstand the k-test (V, h).

(5). **K-NULL $\subseteq$ K-1-NULL**

Given a k-test (U, h), let

$$h_1(n) = \max\{m : h(m) < n + 1\},$$

and

$$V = \{< k, x >: x \in U^{[k]} \cap \Sigma^{\leq h_1(k)}\}.$$

Then, obviously, (V, h_1) is a k-1-test. It suffices to show that the sequences $\xi \in \Sigma^\infty$ that do not withstand the k-test (U, h) do not withstand the k-1-test (V, h_1).

Given a sequence $\xi \in \Sigma^\infty$ that does not withstand the k-test (U, h), for each $n_0 \in N$, there exists $n > n_0$ such that

$$\max\{m : \xi[0..n-1] \in U^{[m]}\} \geq h(n),$$

that is, there exists $m_1 \geq h(n)$ such that $\xi[0..n-1] \in U^{[m_1]}$. But then

$$h_1(m_1) = \max\{m : h(m) < m_1 + 1\} \geq n,$$

so $\xi[0..n-1] \in U^{[m_1]} \cap \Sigma^{\leq h_1(m_1)} = V^{[m_1]}$. Hence $\xi \in V^{[k]} \cdot \Sigma^\infty$ i.o. That is, ξ does not withstand the k-1-test (V, h_1).

(6). **K-1-NULL $\subseteq$ So-S-NULL**

Let (U, h) be a k-1-test. W.l.o.g., assume that, for each i, $U^{[i]}$ is prefix-free.

Define a function F by

$$F(i, x) = \sum_{xy \in U^{[i]}} 2^{-|y|} + \sum_{\substack{x[0..n-1] \in U^{[i]} \\ n < |x|}} 1.$$

Then it is straightforward that (F, h) is a So-s-test.

For $\xi \in \Sigma^\infty$, if $\xi \in U^{[i]} \cdot \Sigma^\infty$, then ξ is covered by F_i with respect to h. So, for each ξ that does not withstand the k-1-test (U, h), ξ is covered by infinitely many F_i with respect to h. Hence $\xi \in \textbf{So-S-NULL}_{(F,h)}$.

(7). **So-S-NULL** $\subseteq$ **K-1-NULL**
Let (F, h) be a So-s-test and $n_0, n_1, \cdots$ be a sequence of numbers such that, for all k,

$$\sum_{i=n_k}^{\infty} F(i, \lambda) \leq 2^{-k}.$$

For each i, let

$$U^{[i]} = \{x \in \Sigma^{\leq h(j)} : F(j, x) \geq 1, n_i \leq j < n_{i+1}\}.$$

Obviously, (U, h) is a k-1-test and, for each $\xi \in \Sigma^\infty$, if ξ is covered by some martingale F_j $(n_i \leq j < n_{i+1})$ w.r.t. h, then $\xi \in U^{[i]} \cdot \Sigma^\infty$. Hence, for each $\xi \in$ **So-S-NULL**$_{(F,h)}$, ξ does not withstand the k-1-test (U, h).

(8). **K-1-NULL** $\subseteq$ **S-2-NULL**
Given a k-1-test (U, h), let

$$V_1 = \{< k, x >: x \in U^{[i]} \text{ for some } i \geq k + 1\}$$

and let M be a Turing machine which accepts the recursive set V_1. Let

$$V = \{< k, x >: \text{ there exists } y \sqsubseteq x \text{ such that } M \text{ accepts } < k, y > \text{ in } |x| \text{ steps } \},$$

and $r(k, j) = t(j + 2 + \max\{h(i) : i \leq j + 2\})$, where t is the time bound of M. Then V is polynomial time computable and

1. $Prob[V^{[k]} \cdot \Sigma^\infty] = Prob[V_1^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.
2. $Prob[(V^{[k]} \cap \Sigma^{r(k,j)}\Sigma^*) \cdot \Sigma^\infty] \leq 2^{-j}$.

Hence (V, r) is an s-2-test and the sequences that do not withstand the k-1-test (U, h) do not withstand the s-2-test (V, r). ■

3.1.4 Weak randomness

Kurtz [54] defined a notion of weak randomness in terms of recursively open sets of Lebesgue measure 1.

Definition 3.1.23 *(Kurtz [54]) A* Kurtz test *is a recursively enumerable set U such that $Prob[U \cdot \Sigma^\infty] = 1$. A sequence ξ* does not withstand *the Kurtz test U if $\xi \notin U \cdot \Sigma^\infty$. A sequence ξ is* Kurtz random *if it withstands all Kurtz tests.*

Let **W-NULL** be the set of sequences that do not withstand some Kurtz test, and let **W-RAND** $= \Sigma^\infty -$ **W-NULL** be the set of Kurtz random sequences.

Now we develop alternative definitions of Kurtz random sequences in terms of Martin-Löf style statistical tests, martingales and a Solovay style criterion.

Definition 3.1.24 *An* mw-test *is a pair (U, g) where U is a recursive set and g is a recursive function such that, for all k, the following hold.*

1. $U^{[k]} \subseteq \Sigma^{\leq g(k)}$.

2. $Prob[U^{[k]} \cdot \Sigma^{\infty}] \leq 2^{-k}$.

A sequence ξ does not withstand *the mw-test* (U, g) *if* $\xi \in U^{[k]} \cdot \Sigma^{\infty}$ *a.e. A sequence* ξ *is* mw-random *if it withstands all mw-tests.*

Let **MW-NULL** be the set of sequences that do not withstand some mw-test, and let **MW-RAND** $= \Sigma^{\infty} -$ **MW-NULL** be the set of mw-random sequences.

Definition 3.1.25 *An* sw-test *is a pair* (F, h) *of functions such that* F *is a recursive martingale and* $h : N \to N$ *is an unbounded, nondecreasing, recursive function. A sequence* ξ does not withstand *the sw-test* (F, h) *if* $\liminf_n (F(\xi[0..n-1]) - h(n)) \geq 0$*, i.e., if* $F(\xi[0..n-1]) \geq h(n)$ *a.e. A sequence* ξ *is* sw-random *if it withstands all sw-tests.* **SW-NULL**$_{(F,h)}$ *denotes the set of sequences that do not withstand the sw-test* (F, h).

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

The Solovay style characterization of Kurtz's randomness concept can be given as follows.

Definition 3.1.26 *A* So-w-test *is a pair* (F, h) *of recursive functions* $F : N \times \Sigma^* \to R^+$ *and* $h : N \to N$ *such that the following hold.*

1. $\sum_{i=0}^{\infty} F(i, \lambda) < \infty$ *is computable, that is, we can recursively find a number* n_k *for each* k *such that* $\sum_{i=n_k}^{\infty} F(i, \lambda) < 2^{-k}$.

2. *For each* i, $F_i(x) = F(i, x)$ *is a martingale.*

A sequence $\xi \in \Sigma^{\infty}$ *is* covered *by* F_i *with respect to* h *if* $F_i(\xi[0..n-1]) \geq 1$ *for all* $n > h(i)$. *A sequence* ξ does not withstand *the So-w-test* (F, h) *if* ξ *is covered by almost all* F_i *w.r.t.* h. *A sequence* ξ *is* So-w-random *if it withstands all So-w-tests.* **So-W-NULL**$_{(F,h)}$ *denotes the set of sequences that do not withstand the So-w-test* (F, h).

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

The following theorem shows that the notions of randomness defined above coincide.

Theorem 3.1.27 W-RAND $=$ **MW-RAND** $=$ **SW-RAND** $=$ **So-W-RAND**.

Proof. It suffices to prove the following implications.

SW-NULL$\subseteq$**MW-NULL**$\subseteq$**W-NULL** $\subseteq$**MW-NULL**$\subseteq$**So-W-NULL** $\subseteq$**MW-NULL**$\subseteq$**SW-NULL**.

(1). **SW-NULL** $\subseteq$ **MW-NULL**

Let (F, f) be an sw-test. W.l.o.g., assume that $F(\lambda) = 1$. Let

$$h(n) = \mu m(f(m) \geq 2^{n+1})$$

and

$$U^{[k]} = \{x \in \Sigma^{\leq h(k)} : F(x) > 2^k\}.$$

Then, for each k, the following hold.

1. $U^{[k]} \subseteq \Sigma^{\leq h(k)}$.

2. $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.

Hence (U, h) is an mw-test. Moreover, for each $\xi \in \textbf{SW-NULL}_{(F,h)}$, we have $\xi \in U^{[n]} \cdot \Sigma^\infty$ a.e., that is, ξ does not withstand the mw-test (U, h).

(2). **MW-NULL** $\subseteq$ **W-NULL**

Given an mw-test (U, g), let $V_s \subseteq \Sigma^{\leq g(s)}$ be a set satisfying

1. $U^{[s]} \cdot \Sigma^\infty \cup V_s \cdot \Sigma^\infty = \Sigma^\infty$.

2. $U^{[s]} \cdot \Sigma^\infty \cap V_s \cdot \Sigma^\infty = \emptyset$.

For a sequence ξ that does not withstand the mw-test (U, g), there is a $k_0 \in N$ such that $\xi \in U^{[n]} \cdot \Sigma^\infty$ for all $n > k_0$. Let $V = \cup_{s>k_0} V_s$. Then V is a Kurtz test and $\xi \notin V \cdot \Sigma^\infty$.

(3). **W-NULL** $\subseteq$ **MW-NULL**

Given a Kurtz test V, let V_s be the set of elements which have been enumerated into V at the end of the sth step, $g(s) = \max\{|x| : x \in V_s\}$ and $U^{[s]} \subseteq \Sigma^{\leq g(s)}$ be a set satisfying

1. $U^{[s]} \cdot \Sigma^\infty \cup V_s \cdot \Sigma^\infty = \Sigma^\infty$.

2. $U^{[s]} \cdot \Sigma^\infty \cap V_s \cdot \Sigma^\infty = \emptyset$.

Then (U, g) is an mw-test. It is straightforward that the sequences that do not withstand the Kurtz test V do not withstand the mw-test (U, g).

(4). **MW-NULL** $\subseteq$ **So-W-NULL**

Let (U, h) be an mw-test. W.l.o.g., assume that for each i, $U^{[i]}$ is prefix-free. Define a function F by

$$F(i, x) = \sum_{xy \in U^{[i]}} 2^{-|y|} + \sum_{\substack{x[0..n-1] \in U^{[i]} \\ n < |x|}} 1.$$

It is straightforward that (F, h) is a So-w-test and, for each sequence ξ that does not withstand the mw-test (U, h), $\xi \in \textbf{So-W-NULL}_{(F,h)}$.

(5). **So-W-NULL** $\subseteq$ **MW-NULL**

Let (F, h) be a So-w-test and $n_0, n_1, \cdots$ be a sequence of numbers such that, for each k,

$$\sum_{i=n_k}^{\infty} F(i, \lambda) \leq 2^{-k}.$$

For each i, let $U^{[i]} = \{x \in \Sigma^{\leq h(n_i)} : F(n_i, x) \geq 1\}$. Obviously, (U, h) is an mw-test and, for each sequence ξ, if ξ is covered by F_{n_i} w.r.t. h, then $\xi \in U^{[i]} \cdot \Sigma^\infty$. Hence, for each $\xi \in \textbf{So-W-NULL}_{(F,h)}$, ξ does not withstand the mw-test (U, h).

(6). **MW-NULL** $\subseteq$ **SW-NULL**

Let (U, h) be an mw-test. W.l.o.g., assume that h is nondecreasing. Let

$$F(x) = \sum_{k \in N} \left(\sum_{xy \in U^{[k]}} 2^{-|y|} + \sum_{\substack{x[0..n-1] \in U^{[k]} \\ n < |x|}} 1 \right)$$

and

$$g_i(x) = \sum_{k=0}^{i+|x|} \left(\sum_{xy \in U^{[k]}} 2^{-|y|} + \sum_{\substack{x[0..n-1] \in U^{[k]} \\ n < |x|}} 1 \right).$$

Then F is approximable as witnessed by g_i. By Lemma 3.1.12, there is a recursive martingale F' such that $F'(x) \geq F(x)$ for all $x \in \Sigma^*$. For each sequence ξ that does not withstand the mw-test (U, h), there exists $k_1 \in N$ such that $\xi \in U^{[n]} \cdot \Sigma^\infty$ for all $n \geq k_1$. Hence $F(\xi[0..h_1(n) - 1]) \geq n - k_1$ and $F'(\xi[0..h_1(n) - 1]) \geq n - k_1$ for all $n \geq k_1$. That is, ξ does not withstand the sw-test (F', h_2), where $h_2 = \frac{1}{2} h_1^{-1}$. ■

3.2 Relations among Notions of Typicalness

In this section, we show the relationship among these notions of randomness we have discussed in the previous section.

Theorem 3.2.1 *(Schnorr [88, 89])* **M-RAND**$\subset$**rec-RAND**.

Remark. Theorem 3.2.1 has already been proved by Schnorr in [88, Theorem 3.2] and [89, Satz 7.2]. In the following, we will present another proof which will be useful for our discussions.

Proof. It is straightforward that **M-RAND**$\subseteq$**rec-RAND**. So it suffices to construct a sequence $\xi \in$ **rec-RAND** $-$ **M-RAND**.

Later in this proof, we call a rec-test F *standard* if $F(\lambda) = 1$.

Let $G_0, G_1, \cdots$ be an enumeration of all standard rec-tests. The standard method to construct a rec-random sequence η is to minimize the value of the weighted sum of these martingales on η. For example, let $\eta[0] = 0$ and, for $n > 0$, let $\eta[n] = 1 \Leftrightarrow g(\eta[0..n-1]0) \geq g(\eta[0..n-1]1)$, where

$$g(x) = \sum_{i=0}^{|x|} 2^{-2i} G_i(x).$$

Then the sequence η is rec-random.

If we had a recursive enumeration $G_0, G_1, \cdots$ of all standard rec-tests, then the above construction yielded a recursive sequence which is rec-random. Since there is no recursive rec-random sequence, we have to take a recursive enumeration of all partial recursive functions from Σ^* to Q^+ and have to guess which of these functions are standard rec-tests. So let $\{F_e : e \geq 0\}$ be a recursive enumeration of all partial recursive functions from Σ^* to Q^+. We use strings x to denote the possible guesses which of them are standard rec-tests. That is, x encodes the guess

$$\forall e < |x| \ (F_e \text{ is a standard rec-test } \Leftrightarrow x[e] = 1).$$

Now the basic idea for defining a sequence $\xi \in$ **rec-RAND** $-$ **M-RAND** is as follows.

We define a partial recursive function $u : \Sigma^* \to \Sigma^*$ such that

1. If x is a correct guess, then $u(x)$ is defined.
2. If $x \sqsubset y$ and y is a correct guess, then $u(x) \sqsubset u(y)$.

So, for the "correct infinite guess" $\gamma \in \Sigma^\infty$, i.e.,

$$\forall e \ (F_e \text{ is a standard rec-test } \Leftrightarrow \gamma[e] = 1),$$

the sequence

$$\xi = \lim_{n\to\infty} u(\gamma[0..n-1])$$

is a well defined infinite sequence.

To make ξ rec-random, we minimize the weighted sum of the standard rec-tests guessed by $\gamma[0..n-1]$ on the part of $u(\gamma[0..n])$ extending $u(\gamma[0..n-1])$. In order to ensure that ξ is not Martin-Löf random, we ensure that $|u(\gamma[0..n-1])| = 2n$. Then, for

$$U^{[k]} = \{u(x) : |x| = k \text{ and } u(x) \text{ is defined }\},$$

U is recursively enumerable, $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$, and $\xi \in U^{[k]} \cdot \Sigma^\infty$ for all k. So ξ will not withstand the Martin-Löf test U.

Now we give the formal construction of u and the "universal" functions $\Phi_{(x,u(x))}$ with respect to the guess x.

Stage 0.
Let $u(\lambda) = \lambda$ and let $\Phi_{(\lambda,u(\lambda))}(z) = 0$ for all $z \in \Sigma^*$.

Stage $s+1$ $(s \geq 0)$.
In this stage, we define $u(xb)$ and $\Phi_{(xb,u(xb))}$ for all $x \in \Sigma^s$ and $b \in \Sigma$.

Given $x \in \Sigma^s$ such that $u(x)$ is defined, we say that a string y_x is *optimal* with respect to the pair $(x, u(x))$ if

1. $y_x \in \Sigma^2$.
2. For $i < 2$, $y_x[i] = 1$ iff $\Phi_{(x,u(x))}(u(x)y_x[0..i-1]1) < \Phi_{(x,u(x))}(u(x)y_x[0..i-1]0)$.

For each $x \in \Sigma^s$ such that $u(x)$ is defined, we distinguish the following two cases.

Case 1. There exists a string y_x which is optimal with respect to the pair $(x, u(x))$. Let $u(x0) = u(x1) = u(x)y_x$ and, for all $z \in \Sigma^*$, let

$$\Phi_{(x0,u(x0))}(u(x0)z) = \Phi_{(x,u(x))}(u(x0)z)$$

and

$$\Phi_{(x1,u(x1))}(u(x1)z) = \Phi_{(x,u(x))}(u(x1)z) + \frac{1}{2^{|x|}F_{|x|}(u(x1))}F_{|x|}(u(x1)z)$$

where we assume that $F_{|x|}(u(x1)) \neq 0$ (otherwise, let $\Phi_{(x1,u(x1))}(u(x1)z) = \Phi_{(x,u(x))}(u(x1)z)$).

Case 2. There is no string y_x which is optimal with respect to the pair $(x, u(x))$.

Let $u(xb)$ and $\Phi_{(xb,u(xb))}$ be undefined for $b \in \Sigma$.

End of construction.

It remains to verify that the above constructed g and ξ satisfy the requirements, we establish this by proving a sequence of claims.

Claim 1 *For the correct infinite guess γ, $g(\gamma[0..n-1])$ is defined and $|g(\gamma[0..n-1])| = 2n$ for all n. Moreover, $g(\gamma[0..n-1]) \sqsubset g(\gamma[0..n])$.*

Proof. Straightforward from the construction. □

Claim 2 *Let $U^{[k]} = \{u(x) : |x| = k$ and $u(x)$ is defined $\}$. Then $\xi \in U^{[k]} \cdot \Sigma^\infty$ and $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$ for all k.*

Proof. It is obvious from the definition of ξ that $\xi \in U^{[k]} \cdot \Sigma^\infty$ for all k.

$$\begin{aligned} Prob[U^{[k]} \cdot \Sigma^\infty] &= \textstyle\sum_{|x|=k\&u(x)\downarrow} 2^{-|u(x)|} \\ &= \textstyle\sum_{|x|=k\&u(x)\downarrow} 2^{-2k} \\ &\leq 2^{-k}. \end{aligned}$$

□

Claim 3 *Let F_e be a standard rec-test. Then $\limsup_{n\to\infty} F_e(\xi[0..n-1]) < \infty$.*

Proof. Let γ be the correct infinite guess. By Claim 1, $u(\gamma[0..e])$ is defined. For $n \geq |u(\gamma[0..e])|$, by the construction,

$$\begin{aligned} F_e(u(\gamma[0..n-1])) &\leq 2^e F_e(u(\gamma[0..e])) \left(\Phi_{(\gamma[0..e],u(\gamma[0..e]))}(u(\gamma[0..e])) + \textstyle\sum_{j=e+1}^{n-1} \frac{1}{2^j}\right) \\ &\leq 2^e F_e(u(\gamma[0..e]))(\Phi_{(\gamma[0..e],u(\gamma[0..e]))}(u(\gamma[0..e])) + 2). \end{aligned}$$

I.e.,

$$\begin{aligned} F_e(\xi[0..2n-1]) &= F_e(u(\gamma[0..n-1])) \\ &\leq 2^e F_e(u(\gamma[0..e]))(\Phi_{(\gamma[0..n-1],u(\gamma[0..e]))}(u(\gamma[0..e])) + 2). \end{aligned}$$

Hence $\limsup_{n\to\infty} F_e(\xi[0..n-1]) < \infty$. □

All of these claims complete the proof of Theorem 3.2.1. ■

Theorem 3.2.2 rec-RAND $\subset$ S-RAND.

Proof. Obviously, we have **rec-RAND** $\subseteq$ **S-RAND**. So it suffices to construct a sequence $\xi \in$ **S-RAND** $-$ **rec-RAND**.

We start with some notation. Call a Schnorr test (F, h) *standard* if $F(\lambda) = 1$ and $h(0) = 0$.

Let $(F_0, h_0), (F_1, h_1), \cdots$ be an effective enumeration of all pairs of partial recursive functions satisfying, for each $e \in N$,

$$F_e : \Sigma^* \to Q^+ \text{ and } h_e : N \to N,$$

and let $(M_0', M_0''), (M_1', M_1''), \cdots$ be the corresponding Turing machines computing those functions.

Let $n_0, n_1, \cdots$ be a sequence of numbers such that

(1). For each i, (F_{n_i}, h_{n_i}) is a standard Schnorr test.

(2). For each i, if (F_i, h_i) is a standard Schnorr test, then there exists j such that $i = n_j$. That is, $(F_{n_0}, h_{n_0}), (F_{n_1}, h_{n_1}), \cdots$ is an enumeration (note that this enumeration is not effective) of all standard Schnorr tests.

For the sequence $n_0, n_1, \cdots$, define a "universal" martingale Φ by

$$\Phi(x) = \sum_{i=0}^{\infty} 2^{-n_i} F_{n_i}(x).$$

In the following we construct a recursive martingale F and a sequence ξ such that F succeeds on ξ and, for each e, the following requirement is satisfied.

N_e : If (F_e, h_e) is a standard Schnorr test, then there exists $c \in N$ such that, for all $n > c$, $F_e(\xi[0..n-1]) < h_e(n)$.

These requirements ensure that ξ is Schnorr random. Namely, if ξ is not Schnorr random, then there exists a standard Schnorr test (F_{e_1}, h_{e_1}) such that $F_{e_1}(\xi[0..n-1]) \geq h_{e_1}(n)$ *i.o.*, which contradicts the requirement N_{e_1}.

In the process of construction, we will construct F recursively and construct ξ using the oracle Φ (the "universal" martingale defined above).

We cannot effectively decide whether (F_e, h_e) is a standard Schnorr test or not. In order to construct $F(x)$ recursively, we will use some bits of x to code assumptions whether certain (F_e, h_e)s are standard Schnorr tests or not. That is, in the construction, we define a partial recursive function $d : \Sigma^* \to \Sigma^*$ such that, for a string x on which d is defined, $d(x)$ denotes the following assumptions: For $e < |d(x)|$, we assume that (F_e, h_e) is a standard Schnorr test if and only if $d(x)[e] = 1$.

The strategy for making F succeed on ξ is as follows: At some stages, let $F(x1) = 2F(x)$ if $x1$ has the potential possibility of becoming an initial segment of ξ. The strategy for meeting requirements N_e is as follows: At some stage s, let $d(\xi[0..s])[e] = 1$, and, for each $y \in \xi[0..s] \cdot \Sigma^*$, do not increase the value of $F(y)$ until $h_e(|y|)$ is large enough such that $F_e(\xi[0..|y|-1]) < h_e(|y|)$, where ξ is defined by induction on i satisfying,

$$\Phi(\xi[0..i-1]) \leq 2^{|d(\xi[0..i-1])|} F(\xi[0..i-1]) \Phi(\lambda).$$

Construction of ξ, F and d.

Stage 0.
$F(\lambda) = 1$ and $d(\lambda) = \lambda$.

Stage 1.
$F(0) = F(1) = 1$, $d(0) = 0$ and $d(1) = 1$.
If (F_0, h_0) is a standard Schnorr test then $\xi[0] = 1$ else $\xi[0] = 0$.

Stage $s + 1 (s > 0)$.
For each string $x \in \Sigma^s$ such that neither $F(x0)$ nor $F(x1)$ has been defined before stage $s + 1$, we distinguish the following two cases.

Case 1. $d(x)$ is not defined.
$F(x0) = F(x1) = F(x)$.

Case 2. $d(x) = b_0 \cdots b_k$ is defined.
For each $j \le k$ satisfying $b_j = 1$, and for each $m \le |x|$, simulate $M''_j(m)$ for $s + 1$ steps. If, for each $j \le k$ satisfying $b_j = 1$, there exists $m_j \le |x|$ such that $M''_j(m_j)$ stops in $s + 1$ steps and

$$2^{j+|d(x)|+3} F(x) < h_j(m_j), \tag{3.1}$$

then go to Process 1, else go to Process 2.

Process 1. $F(x0) = 0, F(x10) = F(x11) = F(x1) = 2F(x)$, $d(x1) = d(x)$, $d(x10) = d(x)0$, $d(x11) = d(x)1$.

If $\xi[0..s-1] = x$, then $\xi[0..s+1] = \xi[0..s-1]1b$, where $b = 1$ if (F_{k+1}, h_{k+1}) is a standard Schnorr test and $b = 0$ otherwise.

Process 2. $F(x0) = F(x1) = F(x)$, $d(x0) = d(x1) = d(x)$.

If $\xi[0..s-1] = x$, then $\xi[0..s] = \xi[0..s-1]b$, where $b = 1$ if $\Phi(x1) \le \Phi(x0)$ and $b = 0$ otherwise.

End of construction.

It remains to verify that the above constructed F and ξ satisfy the requirements, we establish this by proving a sequence of claims.

Claim 1 $\lim_n F(\xi[0..n-1]) = \infty$.

Proof. First, we prove by induction that $d(\xi[0..s])$ is defined for all $s \in N$. Hence, at each stage s, $F(\xi[0..s])$ is defined in Case 2 of the construction. Assume that $d(\xi[0..s-1])$ is defined. At stage $s + 1$, for $x = \xi[0..s-1] \in \Sigma^s$, if Process 1 of Case 2 happens, then $\xi[0..s] = \xi[0..s-1]1$, $d(\xi[0..s]) = d(\xi[0..s-1])$ and $d(\xi[0..s+1]) = d(\xi[0..s])\xi[s+1]$; Otherwise, Process 2 of Case 2 happens and $d(\xi[0..s]) = d(\xi[0..s-1])$.

At stage $s + 1$, if $F(\xi[0..s])$ is defined in the Process 1 of Case 2, then $F(\xi[0..s]) = 2F(\xi[0..s-1])$; Otherwise $F(\xi[0..s]) = F(\xi[0..s-1])$. So it suffices to show that there are infinitely many stages s such that $F(\xi[0..s-1])$ is defined in the Process 1 of Case 2. We prove this by induction. Given s_0, we have to show that there exists a stage $s > s_0$ such that $F(\xi[0..s-1])$ is defined in the Process 1 of Case 2. For each $i < |d(\xi[0..s_0])|$ satisfying $d(\xi[0..s_0])[i] = 1$, (F_i, h_i) is a standard Schnorr test, hence h_i is an unbounded, nondecreasing, recursive function, which implies that there exists some $s > s_0$ such that, at stage $s+1$, the condition (3.1) holds for $x = \xi[0..s-1]$. Let s_1 be the least such s. Then $F(\xi[0..s_1])$ is defined in the Process 1 of Case 2. This completes the proof. □

Claim 2 *For each $s \in N$, $\Phi(\xi[0..s-1]) \leq 2^{|d(\xi[0..s-1])|+1} F(\xi[0..s-1])$.*

Proof. We prove the claim by induction on s. For $s = 0$, because $\Phi(\lambda) \leq 2$, it is straightforward that $\Phi(\lambda) \leq 2^{0+1} F(\lambda)$.

For the inductive step, we distinguish the following two cases.

Case 1. At stage $s+1$, $\xi[0..s]$ is defined in the Process 1. Then

$$\begin{aligned}\Phi(\xi[0..s]) &\leq 2\Phi(\xi[0..s-1]) \\ &\leq 2^{|d(\xi[0..s-1])|+1} 2 \cdot F(\xi[0..s-1]) \\ &= 2^{|d(\xi[0..s])|+1} F(\xi[0..s])\end{aligned}$$

and

$$\begin{aligned}\Phi(\xi[0..s+1]) &\leq 2\Phi(\xi[0..s]) \\ &\leq 2^{|d(\xi[0..s])|+2} F(\xi[0..s]) \\ &\leq 2^{|d(\xi[0..s+1])|+1} F(\xi[0..s+1]).\end{aligned}$$

Case 2. At stage $s+1$, $\xi[0..s]$ is defined in the Process 2. Then

$$\begin{aligned}\Phi(\xi[0..s]) &\leq \Phi(\xi[0..s-1]) \\ &\leq 2^{|d(\xi[0..s-1])|+1} F(\xi[0..s-1]) \\ &= 2^{|d(\xi[0..s])|+1} F(\xi[0..s]).\end{aligned}$$

□

Claim 3 *For each e, if (F_e, h_e) is a standard Schnorr test, then*

$$2^{e+|d(\xi[0..n-1])|+1} F(\xi[0..n-1]) < h_e(n) \quad a.e.$$

Proof. Let c_1 be large enough such that $|d(\xi[0..c_1-1])| > e$. By the construction, there exist $c_0 > m_e > c_1$ such that

$$2^{e+|d(\xi[0..c_0-1])|+3} F(\xi[0..c_0-1]) < h_e(m_e) \leq h_e(c_0).$$

For each $s+1 > c_0$, we distinguish the following two cases.

Case 1. At stage $s+1$, $\xi[0..s]$ is defined in the Process 1. Then, by the construction, there exists $s_e < s+1$ such that

$$2^{e+|d(\xi[0..s-1])|+3} F(\xi[0..s-1]) < h_e(s_e).$$

So

$$\begin{aligned}2^{e+|d(\xi[0..s])|+1}F(\xi[0..s]) &= 2^{e+|d(\xi[0..s-1])|+2}F(\xi[0..s-1]) \\ &< h_e(s_e) \\ &\leq h_e(s+1)\end{aligned}$$

and

$$\begin{aligned}2^{e+|d(\xi[0..s+1])|+1}F(\xi[0..s+1]) &= 2^{e+|d(\xi[0..s-1])|+3}F(\xi[0..s-1]) \\ &< h_e(s_e) \\ &\leq h_e(s+2).\end{aligned}$$

Case 2. At stage $s+1$, $\xi[0..s]$ is defined in the Process 2. Then

$$\begin{aligned}2^{e+|d(\xi[0..s])|+1}F(\xi[0..s]) &= 2^{e+|d(\xi[0..s-1])|+1}F(\xi[0..s-1]) \\ &< h_e(s) \\ &\leq h_e(s+1).\end{aligned}$$

□

Claim 4 *For each e, the requirement N_e is met.*

Proof. If (F_e, h_e) is not a standard Schnorr test, then N_e is met trivially. Otherwise let c_0 be large enough so that $2^{e+|d(\xi[0..n-1])|+1}F(\xi[0..n-1]) < h_e(n)$ for all $n \geq c_0$.

It suffices to show that, for all $s \geq c_0$,

$$\begin{aligned}F_e(\xi[0..s-1]) &\leq 2^e\Phi(\xi[0..s-1]) \\ &\leq 2^{e+|d(\xi[0..s-1])|+1}F(\xi[0..s-1]) \\ &< h_e(s).\end{aligned}$$

□

All of these claims complete the proof of Theorem 3.2.2. ■

Theorem 3.2.3 S-RAND $\subset$ W-RAND.

Proof. (1). **S-RAND $\subseteq$ W-RAND** follows from Theorem 3.1.22 and Theorem 3.1.27.

(2). There is a Kurtz random sequence which does not satisfy the law of large numbers (see, e.g., Kautz [44] or Kurtz [54]), whereas all Schnorr random sequences satisfy the law of large numbers (see, e.g., Schnorr [89] or van Lambalgen [57]). ■

3.3 Chaoticness and Stochasticity

3.3.1 Chaoticness

In this section we give an exposition of the complexity approach to random sequences based on the natural idea that randomness is an absence of regularities. It became possible to make this idea precise when Chaitin [29] and, independently, Kolmogorov [51] introduced a notion of complexity of finite objects. However, this plan encountered some difficulties (see Martin-Löf [74]). These difficulties were overcome by Levin [59] and Schnorr [90], independently. Levin [59] introduced the following notion of monotonic Kolmogorov complexity.

Let $f : \Sigma^* \to \Sigma^*$ be a partial recursive function and let $y \in \Sigma^*$. If y is a prefix of $f(x)$ for some x, then x is called a *description* of y. The *complexity* of y with respect to f is defined by

$$KM_f(y) = \inf\{|x| : x \text{ is a description of } y\}.$$

As the following theorem shows, there is a universal description system.

Theorem 3.3.1 *(Chaitin and Kolmogorov) There exists a universal function, that is, there exists a partial recursive function g such that, for any partial recursive function f, there is a constant c satisfying $KM_g(x) \leq KM_f(x) + c$ for all x.*

In the rest of the thesis, unless otherwise stated, we will use a fixed universal partial recursive function g in the sense of Theorem 3.3.1 and omit the subscript g. A sequence ξ is *chaotic* if and only if ξ is a member of **CHAOT** $= \cup_{c \in N}\{\xi : KM(\xi[0..n-1]) \geq n - c \text{ a.e.}\}$.

Theorem 3.3.2 *(Levin and Schnorr)* **CHAOT** = **M-RAND**.

Theorem 3.3.2 shows that, for a Martin-Löf random sequence ξ, ξ has the maximal monotonic Kolmogorov complexity. However, as the following theorem shows, some rec-random sequences have arbitrary small monotonic Kolmogorov complexity.

Theorem 3.3.3 *Let $f : N \to N$ be a strictly increasing, total recursive function. Then there is a rec-random sequence ξ and a constant c such that $f(KM(\xi[0..n-1]) - c) \leq n$ for all n.*

Proof. In the proof of Theorem 3.2.1, we constructed a partial recursive function $u : \Sigma^* \to \Sigma^*$ such that if $u(x)$ is defined, then $|u(x)| = 2|x|$. In fact, we can define u in such a way that if $u(x)$ is defined, then $|u(x)| = f(|x|)$. Let $\xi = \lim_{n\to\infty} u(\gamma[0..n-1])$, where γ is the correct infinite guess. Then, for each n, $\gamma[0..n-1]$ is a description of $u(\gamma[0..n-1])$. This completes the proof of the theorem. ■

3.3.2 Stochasticity

As we have mentioned in the introduction, the stochasticity of a sequence means that the property of frequency stability holds for this sequence and for its subsequences obtained by "legal choices". Von Mises was the first to suggest defining the notion of randomness in terms of stochasticity. But von Mises' "legal selection rule" was not formally given. In the past, work in this area mainly concentrated on the definition of "legal selection rules". For example, Church suggested that a "legal selection rule" should be some recursive processes and proposed the following definition.

For a sequence $\xi \in \Sigma^* \cup \Sigma^\infty$ such that $|\xi| \geq n$, let $s_n(\xi) = \sum_{i=0}^{n-1} \xi[i]$. A *Church selection rule* is a total recursive function $\varphi : \Sigma^* \to \Sigma$. A Church selection rule φ *induces* a partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$, where $\Phi(\xi)$ is defined if $\varphi(\xi[0..n-1]) = 1$ for infinitely many $n \in N$ and $\Phi(\xi) = b_0 b_1 \cdots$ where

$$b_n = \begin{cases} \lambda & \varphi(\xi[0..n-1]) = 0 \\ \xi[n] & \varphi(\xi[0..n-1]) = 1 \end{cases}$$

A sequence ξ is *Church stochastic* if and only if, for each Church selection rule φ such that $\Phi(\xi)$ is defined, $\lim_n \frac{s_n(\Phi(\xi))}{n} = \frac{1}{2}$. Let **C-STOCH** be the set of Church stochastic sequences.

Later, Kolmogorov [51] and, independently, Loveland [61] generalized the notion of selection rules and got a narrower set of stochastic sequences.

A *Kolmogorov-Loveland selection rule* is a pair (φ_1, φ_2) of partial recursive functions, where $\varphi_1 : \Sigma^* \to N$ and $\varphi_2 : \Sigma^* \to \Sigma$. Given a sequence $\xi = b_0 b_1 \cdots$, first we define a sequence of natural numbers $n_0 = \varphi_1(\lambda)$, $n_1 = \varphi_1(b_{n_0}), n_2 = \varphi_1(b_{n_0} b_{n_1})$, and so on. The construction terminates if at least one of the values $\varphi_1(b_{n_0} b_{n_1} \cdots b_{n_k})$ and $\varphi_2(b_{n_0} b_{n_1} \cdots b_{n_k})$ turns out to be undefined or the value $\varphi_1(b_{n_0} b_{n_1} \cdots b_{n_k})$ coincides with one of $n_0, n_1, \cdots, n_k$. Each Kolmogorov-Loveland selection rule (φ_1, φ_2) *induces* a partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$, where $\Phi(\xi) = b'_0 b'_1 \cdots$ satisfies

$$b'_k = \begin{cases} \lambda & \varphi_2(b_{n_0} b_{n_1} \cdots b_{n_{k-1}}) = 0 \\ b_{n_k} & \varphi_2(b_{n_0} b_{n_1} \cdots b_{n_{k-1}}) = 1 \end{cases}$$

where we assume that $b_{-1} = \lambda$. A sequence ξ is *Kolmogorov-Loveland stochastic* if and only if, for each Kolmogorov-Loveland selection rule (φ_1, φ_2) such that $\Phi(\xi) \in \Sigma^\infty$, $\lim_n \frac{s_n(\Phi(\xi))}{n} = \frac{1}{2}$. Let **KL-STOCH** be the set of Kolmogorov-Loveland stochastic sequences.

Theorem 3.3.4 *(Muchnik [80])* **KL-STOCH** $\subset$ **C-STOCH**.

Proof. (Idea) By the definition, **KL-STOCH** $\subseteq$ **C-STOCH**. We can construct a Church stochastic sequence which has monotonic Kolmogorov complexity $O(\log n)$ for each initial segment of length n, whereas Muchnik [80] has shown that, for $c < 1$, any sequence which has monotonic Kolmogorov complexity less than cn is not Kolmogorov-Loveland stochastic. ■

The following theorem summarizes the relations between the notions of typicalness and the notions of stochasticity.

Theorem 3.3.5 *1. (Shen [92])* **M-RAND** $\subset$ **KL-STOCH**.

2. **C-STOCH** $\not\subseteq$ **S-RAND**.

3. **rec-RAND** $\subset$ **C-STOCH**.

4. **rec-RAND** $\not\subseteq$ **KL-STOCH**.

5. **S-RAND** $\not\subseteq$ **C-STOCH**.

Proof. (Idea) 1. The proof of **M-RAND** $\subseteq$ **KL-STOCH** is just an effective modification of the classical proof (see, e.g. [97]) for the law of large numbers. **KL-STOCH** $\not\subseteq$ **M-RAND** is proved by Shen [92]: There is a probability distribution $p = (p_0, p_1, \cdots)$ on Σ^∞ such that each Martin-Löf typical sequence with respect to this distribution p is Kolmogorov-Loveland stochastic with respect to the uniform Bernoulli distribution, and no Martin-Löf typical sequence with respect to this distribution p is Martin-Löf typical with respect to the uniform Bernoulli distribution.

2. By the construction of Ville [98], there is a Church stochastic sequence which does not satisfy the law of the iterated logarithm, whereas all Schnorr random sequences satisfy the law of the iterated logarithm (see Schnorr [89]). (See also Chapter 5).

3. See Chapter 5.

4. In Theorem 3.3.3, we showed that there exists a rec-random sequence which has arbitrary small monotonic Kolmogorov complexity. So the claim follows from the result of Muchnik [80].

5. In the proof of Theorem 3.2.2, we constructed a recursive martingale F and a Schnorr random sequence ξ which have the following properties.

(1). F succeeds on ξ.

(2). For all $x \in \Sigma^*$ and $b \in \Sigma$, $F(xb) = 2bF(x)$ or $F(xb) = F(x)$.

(3). If $F(\xi[0..n]) = 2\xi[n] \cdot F(\xi[0..n-1])$, then $\xi[n] = 1$.

Define a Church selection rule φ by

$$\varphi(x) = \begin{cases} 1 & \text{if } F(xb) = 2bF(x) \\ 0 & \text{if } F(xb) = F(x) \end{cases}$$

Then, obviously, φ induces a partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ such that $\Phi(\xi) = 111\cdots$. Hence, ξ is not Church stochastic. ■

The item 5 of Theorem 3.3.5 shows that the notion of Schnorr randomness seems to us less adequate to our intuition than the notions of Martin-Löf and rec-randomness.

3.4 Invariance Properties of Typical Sequences

In the previous sections, we have shown that basically there are three different notions of randomness: stochasticity, chaoticness and typicalness. It is interesting to get the same notion from the three different approaches. For example, we have pointed out in section 3.3 that a sequence is monotonic Kolmogorov random if and only if it is Martin-Löf random. Hence we have the same meaning when we say that a sequence is chaotic or typical. But it is still open whether we can define a concrete set of place selection rules so that the notion of stochasticity and the notion of typicalness coincide. Some partial results have been got in this line for abstract selection rules.

In this section we give a summary of Schnorr's characterization of Martin-Löf's randomness concept (resp. Schnorr's randomness concept) in terms of invariance properties. We also give a similar characterization of Kurtz's randomness concept.

Definition 3.4.1 *(Schnorr [89])*

1. *A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is* measure-nondecreasing *(note that Schnorr used a different word: massverkleinernd) if, for each Lebesgue measurable set $\mathbf{C} \subseteq \Sigma^\infty$,*

$$Prob[\Phi^{-1}(\mathbf{C})] \leq Prob[\mathbf{C}].$$

2. *A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is* measure-invariant *if, for each Lebesgue measurable set $\mathbf{C} \subseteq \Sigma^\infty$,*

$$Prob[\Phi^{-1}(\mathbf{C})] = Prob[\mathbf{C}].$$

3. *A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is* measure bounded *if, for each Lebesgue measurable set $\mathbf{C} \subseteq \Sigma^\infty$, there exists a constant c such that*

$$Prob[\Phi^{-1}(\mathbf{C})] \leq c \cdot Prob[\mathbf{C}].$$

Definition 3.4.2 *(Schnorr [89])*

1. *A partial function $\varphi : \Sigma^* \to \Sigma^*$ is* monotonic *if $\varphi(xy) \in \varphi(x) \cdot \Sigma^*$ for all $x, xy \in dom(\varphi)$.*

2. *A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is* continuous *if, for each set $A \subseteq \Sigma^*$, there exists a set $B \subseteq \Sigma^*$ such that $\Phi^{-1}(A \cdot \Sigma^\infty) = (B \cdot \Sigma^\infty) \cap dom(\Phi)$, where $dom(\Phi)$ is the domain of Φ.*

Definition 3.4.3 *A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is* induced *by a partial function $\varphi : \Sigma^* \to \Sigma^*$ if, for each $\xi \in dom(\Phi)$ and $n \in N$, $\Phi(\xi) \in \varphi(\xi[0..n-1]) \cdot \Sigma^\infty$.*

Lemma 3.4.4 *(Schnorr [89]) A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is continuous if and only if there is a partial, monotonic function $\varphi : \Sigma^* \to \Sigma^*$ such that, on the domain of Φ, Φ is induced by φ.*

Definition 3.4.5 *(Schnorr [89])*

1. *A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is* sub-computably continuous *if it is induced by some partial recursive, monotonic function $\varphi : \Sigma^* \to \Sigma^*$.*

2. *A partial function $\Phi : \Sigma^\infty \to \Sigma^\infty$ is* computably continuous *if it is induced by some total recursive, monotonic function $\varphi : \Sigma^* \to \Sigma^*$, and there is a total recursive function $h : N \to N$ such that $dom(\Phi) = \{\xi \in \Sigma^\infty : |\varphi(\xi[0..h(n)-1])| \geq n, n \in N\}$.*

After these preliminary definitions, we can introduce von Mises style characterizations of the notions of Martin-Löf randomness and Schnorr randomness now.

Theorem 3.4.6 *(Schnorr [89]) Let $\Phi : \Sigma^\infty \to \Sigma^\infty$ be a total, sub-computably continuous, measure-bounded function. Then $\Phi(\mathbf{M\text{-}RAND}) \subseteq \mathbf{M\text{-}RAND}$.*

Theorem 3.4.7 *(Schnorr [89]) Given a recursive sequence $\eta \in \Sigma^\infty$, a sequence $\xi \in \Sigma^\infty$ is Martin-Löf random if and only if there is no total, sub-computably continuous, measure-nondecreasing function $\Phi : \Sigma^\infty \to \Sigma^\infty$ such that $\Phi(\xi) = \eta$.*

Theorem 3.4.8 *(Schnorr [89]) Let $\Phi : \Sigma^\infty \to \Sigma^\infty$ be a partial, sub-computably continuous, measure-invariant function. Then $\Phi(\mathbf{S\text{-}RAND} \cap dom(\Phi)) \subseteq \mathbf{S\text{-}RAND}$.*

Theorem 3.4.9 *(Schnorr [89]) Let $\Phi : \Sigma^\infty \to \Sigma^\infty$ be a total, computably continuous, measure-bounded function. Then $\Phi(\mathbf{S\text{-}RAND}) \subseteq \mathbf{S\text{-}RAND}$.*

Let $\mathbf{C}_1$ be the set of total, computably continuous, measure-bounded functions $\Phi : \Sigma^\infty \to \Sigma^\infty$, $\mathbf{C}_2$ be the set of total, computably continuous, measure-nondecreasing functions $\Phi : \Sigma^\infty \to \Sigma^\infty$, $\mathbf{C}_3$ be the set of partial, sub-computably continuous, measure-invariant functions $\Phi : \Sigma^\infty \to \Sigma^\infty$, and $\mathbf{C}_4$ be the set of computably continuous, measure-invariant functions $\Phi : \Sigma^\infty \to \Sigma^\infty$.

Theorem 3.4.10 *(Schnorr [89]) For $i = 1, 2, 3, 4$, a sequence $\xi \in \Sigma^\infty$ is Schnorr random if and only if, for all $\Phi \in \mathbf{C}_i$ with $\xi \in dom(\Phi)$, $\Phi(\xi)$ satisfies the law of large numbers.*

By our characterization of Kurtz's randomness concept in previous sections, a similar characterization as Theorem 3.4.10 can be given for Kurtz's concept. The proofs of the following theorems are a minor modification of the proofs of Theorem 3.4.8, Theorem 3.4.9 and Theorem 3.4.10.

Theorem 3.4.11 *Let $\Phi : \Sigma^\infty \to \Sigma^\infty$ be a partial, sub-computably continuous, measure-invariant function. Then $\Phi(\mathbf{W\text{-}RAND} \cap dom(\Phi)) \subseteq \mathbf{W\text{-}RAND}$.*

Proof. It suffices to show that, for each mw-test (U, g), there is another mw-test (V, f) such that

$$\Phi^{-1}(\mathbf{NULL}_{(U,g)}) \subseteq \mathbf{NULL}_{(V,f)} \tag{3.2}$$

where $\mathbf{NULL}_{(U,g)}$ (resp. $\mathbf{NULL}_{(V,f)}$) is the set of sequences that do not withstand the mw-test (U, g) (resp. (V, f)).

W.l.o.g., we may assume that Φ is induced by a total recursive, monotonic function $\varphi : \Sigma^* \to \Sigma^*$. Let $V^{[k]} = \{x : \varphi(x) \in U^{[k]}\}$ and $f(n) = g(n)$ for all $k, n \in N$. Then, by the measure-invariance property of Φ, $Prob[V^{[k]} \cdot \Sigma^\infty] = Prob[U^{[k]} \cdot \Sigma^\infty]$ and $V^{[k]} \subseteq \Sigma^{\leq f(k)}$.

Obviously, (3.2) holds. This completes the proof of the theorem. ■

Theorem 3.4.12 *Let $\Phi : \Sigma^\infty \to \Sigma^\infty$ be a total, computably continuous, measure-bounded function. Then $\Phi(\mathbf{W\text{-}RAND}) \subseteq \mathbf{W\text{-}RAND}$.*

Proof. It suffices to show that, for each mw-test (U, g), there is another mw-test (V, f) such that (3.2) holds.

Let $\varphi : \Sigma^* \to \Sigma^*$ and $h : N \to N$ be a pair of total functions which witness that Φ is computably continuous. Fix the number c such that, for all Lebesgue measurable set $\mathbf{C} \subseteq \Sigma^\infty$, $Prob[\Phi^{-1}(\mathbf{C})] \leq c \cdot Prob[\mathbf{C}]$.

Let $V^{[k]} = \{x : \varphi(x) \in U^{[k+c]}\}$ and $f(k) = h(g(k+c))$ for all k. W.l.o.g., we may assume that $U^{[k]}$ is prefix-free for all k. Then

$$Prob[V^{[k]} \cdot \Sigma^\infty] \leq c \cdot Prob[U^{[k+c]} \cdot \Sigma^\infty] \leq 2^{-k}$$

and $V^{[k]} \subseteq \Sigma^{\leq f(k)}$ for all $k \in N$.

Obviously, (3.2) holds. This completes the proof of the theorem. ■

Theorem 3.4.13 *Let (U, g) be an mw-test and $\eta \in \Sigma^\infty$ be a recursive sequence. Then there exists a computably continuous, measure-invariant function $\Phi : \Sigma^\infty \to \Sigma^\infty$ such that $\Phi(\xi) = \eta$ for all $\xi \in \mathbf{NULL}_{(U,g)}$.*

Proof. W.l.o.g., we may assume that, for all k, the following hold.

1. g is strictly increasing.
2. $U^{[k]} \subseteq \Sigma^{g(k)}$.
3. For all $x \in U^{[k+1]}$, there is a prefix y of x such that $y \in U^{[k]}$.
4. $Prob[U^{[k]} \cdot \Sigma^\infty] = 2^{-k}$.

In the following we define a total recursive, monotonic function $\varphi : \Sigma^* \to \Sigma^*$ such that the induced function $\Phi : \Sigma^\infty \to \Sigma^\infty$ satisfies our requirements.

At first, we define sequences $C_{(k,0)}, \cdots, C_{(k,2^k-1)}$ of sets and sequences $x_{(k,0)}, \cdots, x_{(k,2^k-1)}$ of strings by induction on k.

Let $C_{(0,0)} = \{\lambda\}$ and $x_{(0,0)} = \{\lambda\}$.

Let $C_{(k+1,0)}, \cdots, C_{(k+1,2^{k+1}-1)}$ be a sequence of subsets of $\Sigma^{g(k+1)}$ such that

1. $(C_{(k+1,2i)} \cup C_{(k+1,2i+1)}) \cdot \Sigma^\infty = C_{(k,i)} \cdot \Sigma^\infty$ for $i < 2^k$.
2. $C_{(k+1,0)} = U^{[k+1]}$.
3. $C_{(k+1,i)} \cap C_{(k+1,j)} = \emptyset$ for $i \neq j$.
4. $Prob[C_{(k+1,i)} \cdot \Sigma^\infty] = 2^{-(k+1)}$ for $i < 2^{k+1}$.

and let $x_{(k+1,0)}, \cdots, x_{(k+1,2^{k+1}-1)}$ be an enumeration of all strings in Σ^{k+1} such that

1. $x_{(k+1,0)} = \eta[0..k]$.
2. $x_{(k,i)} \cdot \Sigma^\infty = \{x_{(k+1,2i)}, x_{(k+1,2i+1)}\} \cdot \Sigma^\infty$ for all $i < 2^k$.

Now the function φ is defined by

$$\varphi(xb) = \begin{cases} x_{(k,i)} & \text{if } xb \in C_{(k,i)} \text{ for some } k, i \in N \\ \varphi(x) & \text{otherwise} \end{cases}$$

where $b \in \Sigma$.

It is straightforward to check that the induced function $\Phi : \Sigma^\infty \to \Sigma^\infty$ by φ is computably continuous and measure-invariant. Moreover, for all $\xi \in \mathbf{NULL}_{(U,g)}$, $\Phi(\xi) = \eta$. ■

Now we are ready to characterize the notion of Kurtz randomness in terms of invariance properties.

Theorem 3.4.14 *Given a recursive sequence $\eta \in \Sigma^\infty$, a sequence $\xi \in \Sigma^\infty$ is Kurtz random if and only if, for all computably continuous, measure-invariant function $\Phi : \Sigma^\infty \to \Sigma^\infty$, $\Phi(\xi) \neq \eta$.*

Proof. This follows from Theorem 3.4.13. ■

By combining the previous theorems, we get the following theorem.

Theorem 3.4.15 *For $i = 1, 2, 3, 4$ and a recursive sequence $\eta \in \Sigma^\infty$, a sequence $\xi \in \Sigma^\infty$ is Kurtz random if and only if $\Phi(\xi) \neq \eta$ for all $\Phi \in \mathbf{C}_i$ with $\xi \in dom(\Phi)$.*

Proof. This follows from Theorem 3.4.11, Theorem 3.4.12 and Theorem 3.4.13. ■

The topic of this section is related to the independence properties of subsequences of a random sequence and is also related to the independent random sequences. A number of general independence properties for subsequences of a random sequence are established by Kautz [46] and van Lambalgen [58, 57] et al. There are various applications of independence properties and independent random sequences. For example, Book [20] and Lutz [66] used the independent random oracles to characterize complexity classes, and Kautz and Miltersen [46] used independence properties of Martin-Löf random sequences to show that relative to a random oracle, **NP** is not small in the sense of p-measure.

Chapter 4

n-Randomness

In this chapter, we study the notions of n-randomness, which are the refinements of the notions of effective randomness corresponding to the levels of the arithmetical hierarchy. The notion of n-randomness (resp. weak n-randomness) corresponding to the notion of Martin-Löf randomness (resp. Kurtz randomness) was first introduced by Kurtz [54]. We introduce notions of n-randomness corresponding to all notions of randomness we have discussed in Chapter 3, that is, Martin-Löf n-randomness, n-rec-randomness, Schnorr n-randomness and Kurtz n-randomness. We will characterize these n-randomness concepts in different terms as we have done for 1-randomness concepts in Chapter 3.

4.1 Different Kinds of n-Randomness

At first we introduce the Kleene hierarchy of sets. The Kleene hierarchy classifies the "arithmetical" sets in classes Σ_n, Π_n $(n = 0, 1, \cdots)$ defined as follows. Σ_n is the class of all sets A of the form $A = \{x : (Q_1 x_1)(Q_2 x_2) \cdots (Q_n x_n) R(x, x_1, x_2, \cdots, x_n)\}$, where R is a recursive predicate, the Q_{2k+1} are existential quantifiers and the Q_{2k} are universal quantifiers. Π_n is the class of all sets as above, except that the Q_{2k+1} are universal quantifiers and the Q_{2k} are existential quantifiers. The class $\Sigma_n \cap \Pi_n$ is usually denoted as Δ_n. The following facts are known (see Soare [93]):

1. $\Delta_0 = \Sigma_0 = \Pi_0 = \Delta_1$ is the collection of all recursive sets.

2. $A \in \Sigma_n \iff \bar{A} \in \Pi_n$ ($\bar{A}$ is the complement of A).

3. $\Sigma_n \cup \Pi_n \subseteq \Delta_{n+1}$ for all $n \geq 0$ and the containment is proper for $n > 0$.

4. $A \in \Sigma_{n+1}$ if and only if A is recursively enumerable relative to a set $B \in \Pi_n$.

5. $A \in \Delta_{n+1}$ if and only if A is recursive relative to a set $B \in \Pi_n$.

Afterwards, we say that a function $f : \Sigma^* \to Q$ is *Δ_n-computable* if it is computable relative to a set in Δ_n.

4.1.1 Martin-Löf n-randomness

Definition 4.1.1 *(Kurtz [54]) A* Martin-Löf n-test *is a Δ_n-recursively enumerable set U with the property that $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$ for all $k \in N$. An infinite sequence ξ* does not withstand *the Martin-Löf n-test U if $\xi \in U^{[k]} \cdot \Sigma^\infty$ for all $k \in N$. A sequence ξ is* Martin-Löf n-random *if it withstands all Martin-Löf n-tests.*

Let n-**M-NULL** be the set of sequences which do not withstand some Martin-Löf n-test, and let n-**M-RAND** $= \Sigma^\infty - n$-**M-NULL** be the set of Martin-Löf n-random sequences.

The notion of Martin-Löf n-randomness can also be characterized in terms of martingales.

Definition 4.1.2 *A total function $F : \Sigma^* \rightarrow R$ is* weakly Δ_n-approximable *if there is a Δ_n-computable function $h : N \times \Sigma^* \rightarrow Q$ such that*

1. *For each $n \in N$ and $x \in \Sigma^*$, $h(n, x) \leq h(n + 1, x) \leq F(x)$.*
2. *For each $x \in \Sigma^*$, $\lim_n h(n, x) = F(x)$.*

Definition 4.1.3 *An* n-m-1-test *is a weakly Δ_n-approximable martingale F. An infinite sequence ξ* does not withstand *the n-m-1-test F if F succeeds on ξ. A sequence ξ is* n-m-1-random *if it withstands all n-m-1-tests.*

Let n-**M-1-NULL** be the set of sequences which do not withstand some n-m-1-test, and let n-**M-1-RAND** $= \Sigma^\infty - n$-**M-1-NULL** be the set of n-m-1-random sequences.

Theorem 4.1.4 n-**M-1-RAND** $= n$-**M-RAND**.

Proof. The proof is a relativization of the proof of Theorem 3.1.6. ■

There is also a similar theorem for Martin-Löf n-randomness like Theorem 3.1.7 for Martin-Löf randomness.

Theorem 4.1.5 *There exists a universal n-m-1-test, that is, there is a weakly Δ_n-approximable martingale F such that* $\mathbf{NULL}_F = n$-**M-1-NULL**.

Proof. The proof is a relativization of the proof of Theorem 3.1.7. ■

4.1.2 n-rec-randomness

Definition 4.1.6 *A* n-rec-test *is a Δ_n-computable martingale $F : \Sigma^* \rightarrow Q^+$. An infinite sequence ξ* does not withstand *the n-rec-test F if F succeeds on ξ. A sequence ξ is* n-rec-random *if it withstands all n-rec-tests.*

Let n-**rec-NULL** be the set of sequences which do not withstand some n-rec-test, and let n-**rec-RAND** $= \Sigma^\infty - n$-**rec-NULL** be the set of n-rec-random sequences.

4.1.3 Schnorr n-randomness

Definition 4.1.7 *A* Schnorr n-test *is a pair* (F, h) *of functions with the properties that* F *is a* Δ_n*-computable martingale and* $h : N \to N$ *is an unbounded, nondecreasing,* Δ_n*-computable function. A sequence* ξ does not withstand *the Schnorr* n*-test* (F, h) *if* $\limsup_n(F(\xi[0..n-1]) - h(n)) \geq 0$*, i.e., if* $F(\xi[0..n-1]) \geq h(n)$ *i.o. A sequence* ξ *is* Schnorr n-random *if it withstands all Schnorr* n*-tests.*

Let n-**S-NULL** be the set of sequences which do not withstand some Schnorr n-test, and let n-**S-RAND** $= \Sigma^\infty - n$-**S-NULL** be the set of Schnorr n-random sequences.

The following is a Martin-Löf style characterization of the notion of Schnorr n-randomness.

Definition 4.1.8 *An* n-s-1-test *is a pair* (U, g) *consisting of a* Δ_n*-recursively enumerable set* U *and a* Δ_n*-computable function* g*, together with a* Δ_n*-recursive enumeration* $\{U_s\}_{s\in N}$ *of* U *such that, for each* k *and* j*,*

1. $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.
2. $Prob[(U^{[k]} - U^{[k]}_{g(k,j)}) \cdot \Sigma^\infty] \leq 2^{-j}$.

An infinite sequence ξ does not withstand *the* n*-s-1-test* (U, g) *if* $\xi \in U^{[k]} \cdot \Sigma^\infty$ *for all* $k \in N$*. A sequence* ξ *is* n-s-1-random *if it withstands all* n*-s-1-tests.*

Let n-**S-1-NULL** be the set of sequences which do not withstand some n-s-1-test, and let n-**S-1-RAND** $= \Sigma^\infty - n$-**S-1-NULL** be the set of n-s-1-random sequences.

Theorem 4.1.9 n-**S-1-RAND** $= n$-**S-RAND**.

Proof. The proof is a relativization of the proof of Theorem 3.1.22. ■

4.1.4 Weak n-randomness

Kurtz [54] defined a notion of weak n-randomness.

Definition 4.1.10 *(Kurtz [54]) A* Kurtz n-test *is a* Δ_n*-recursively enumerable set* U *with the property that* $Prob[U \cdot \Sigma^\infty] = 1$*. A sequence* ξ does not withstand *the Kurtz* n*-test* U *if* $\xi \notin U \cdot \Sigma^\infty$*. A sequence* ξ *is* Kurtz n-random *if it withstands all Kurtz* n*-tests.*

Let n-**W-NULL** be the set of sequences that do not withstand some Kurtz n-test, and let n-**W-RAND** $= \Sigma^\infty - n$-**W-NULL** be the set of Kurtz n-random sequences.

Now we give a martingale characterization of the notion of Kurtz n-randomness.

Definition 4.1.11 *An* n-sw-test *is a pair* (F, h) *of functions with the properties that* F *is a* Δ_n*-computable martingale and* $h : N \to N$ *is an unbounded, nondecreasing,* Δ_n*-computable function. A sequence* ξ does not withstand *the* n*-sw-test* (F, h) *if* $\liminf_n(F(\xi[0..n-1]) - h(n)) \geq 0$*, i.e., if* $F(\xi[0..n-1]) \geq h(n)$ *a.e. A sequence* ξ *is* n-sw-random *if it withstands all* n*-sw-tests.*

Let n-**SW-NULL** be the set of sequences which do not withstand some n-sw-test, and let n-**SW-RAND** $= \Sigma^\infty - n$-**SW-NULL** be the set of n-sw-random sequences.

Theorem 4.1.12 n-**SW-RAND** $=$ n-**W-RAND**.

Proof. The proof is a relativization of the proof of Theorem 3.1.27. ■

4.2 Relations among Notions of n-Randomness

Theorem 4.2.1 n-**M-RAND**$\subset$ n-**rec-RAND**$\subset$ n-**S-RAND**.

Proof. The proof is a relativization of the proofs of Theorem 3.2.1 and Theorem 3.2.2. ■

Theorem 4.2.2 *(Kautz [44])* n-**S-RAND** $\subset$ n-**W-RAND**.

Proof. See Kautz [44]. ■

Remark. Theorem 4.2.2 is open until Kautz [44]. Kurtz [54] showed that **1-M-RAND** is a proper subset of **1-W-RAND**, and conjectured that this situation holds for n-randomness also, that is, n-**M-RAND** is a proper subset of n-**W-RAND**. Kautz used finitary injury argument to answer this conjecture affirmatively, in fact, he proved that n-**S-RAND** is a proper subset of n-**W-RAND**.

Now we establish the relations between the notion of n-randomness and the notion of $n+1$-randomness.

Lemma 4.2.3 *There exists a set A in Δ_{n+1} which is Martin-Löf n-random.*

Proof. Let $F : \Sigma^* \to R^+$ be a universal n-m-1-test (see Theorem 4.1.5) which is given by a Δ_n-computable function $h : N \times \Sigma^* \to Q^+$. W.l.o.g., assume that $F(\lambda) < 1$. Let ξ be defined inductively by

$$\xi[i] = 1 \text{ iff } \forall j \in N \ (h(j, \xi[0..i]) < 1).$$

Let A be the set which is represented by the characteristic sequence ξ. Then A is in Δ_{n+1}. The construction implies that A is Martin-Löf n-random. ■

Lemma 4.2.4 *No set in Δ_n is Kurtz n-random.*

Proof. Let $A \in \Delta_n$ and ξ be its characteristic sequence. Define a Δ_n-computable martingale F by

$$F(x1) = 2F(x) \text{ iff } \xi[|x|] = 1.$$

Then $F(\xi[0..i]) \geq 2^{i-2}$ for all $i \in N$. Hence A is not Kurtz n-random. ■

Each infinite set in Σ_{n+1} has an infinite subset in Δ_n, so a similar proof can be given for a strengthening of Lemma 4.2.4.

Theorem 4.2.5 *No set in $\Sigma_{n+1} \cup \Pi_{n+1}$ is Kurtz $n+1$-random.*

Proof. Straightforward. ■

Remark. Schnorr [88] introduced a kind of (0)-randomness concept which coincides with our 2-rec-randomness concept, and he has already observed that there is no 2-rec-random set in $\Sigma_2 \cup \Pi_2$ (see [88, Theorem 3.6] and [89, Satz 7.7]), hence 2-rec-randomness is a proper refinement of Martin-Löf randomness. But his proof is not correct, his proof only works for the fact that no set in Δ_2 is 2-rec-random.

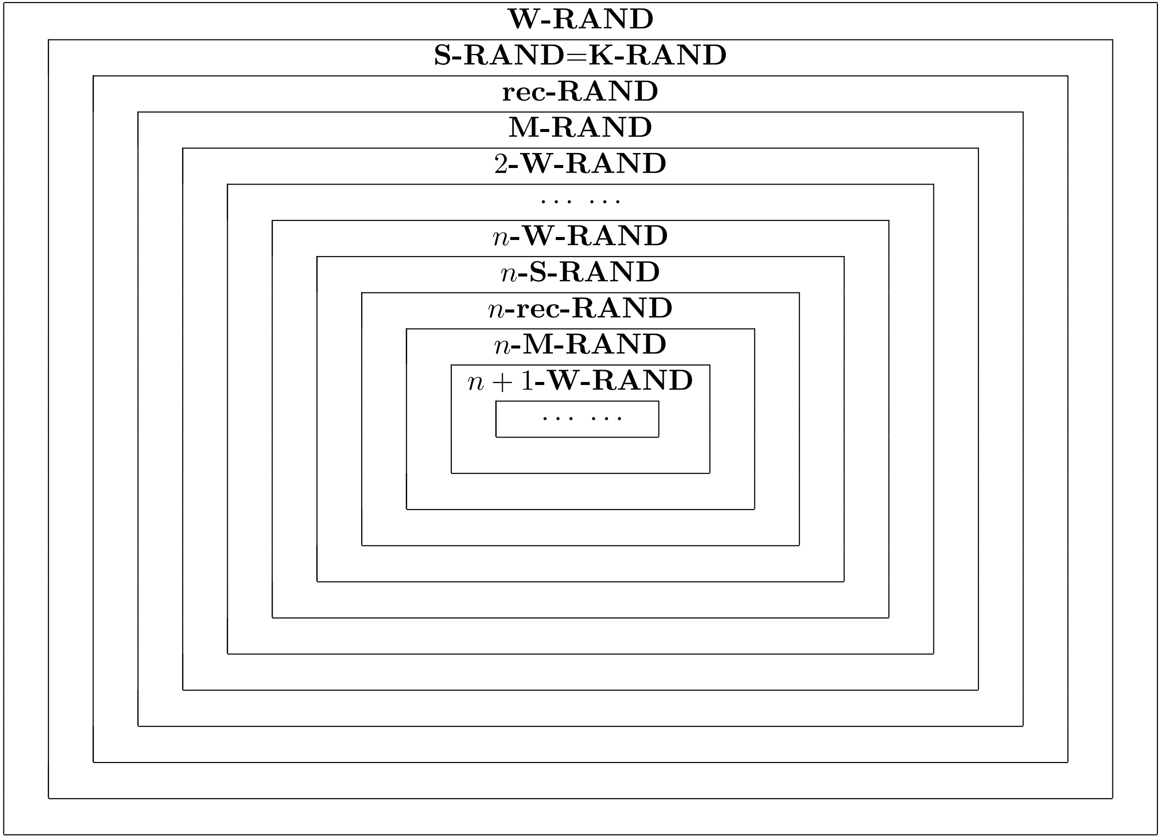
By combining the previous theorems, we get the following theorem.

Theorem 4.2.6 *(Kurtz [54])* $n+1$-**W-RAND** $\subset$ n-**M-RAND**.

Proof. Follows from Lemma 4.2.3 and Lemma 4.2.4. ■

By combining these theorems in this chapter and in Chapter 3, we get the table 4.1 that describes the relations among these notions of randomness we have discussed.

Table 4.1: The relation among the notions of randomness



Chapter 5

Resource Bounded Randomness

This chapter is devoted to the study of resource bounded randomness concepts. In section 5.1, we 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 rec-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 [65]. We also show, however, that if we consider only recursive sets, then these randomness concepts coincide.

2. For polynomial time bounds, the notion of Ko randomness is independent of the notions of rec-randomness, Schnorr randomness and Kurtz randomness.

In section 5.2 and section 5.3, we discuss notions of resource bounded stochasticity. Here we concentrate our attention on the stochastic properties of p-random sequences, and we show that many important laws in probability theory hold for 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 randomness), play a central role in the study of probability theory (see e.g., [33]) and in the study of classical randomness concepts (see e.g., [44, 74, 89, 98]). We will show that these two laws hold for p-random sequences also. In fact, we can show that all the standard laws 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 thesis. 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 is obvious that all p-random sets have stochastic distributions on their elements, hence the density of most intractable set is just "one half". When combined with an invariance property of p-random sequences, these laws are also useful in proving that some complexity classes have p-measure 0. We will give an application of these laws in Chapter 6.

It is difficult to find the relationship between $\mathbf{P}$/poly and $\mathbf{E}$ at present. Wilson [114] has shown that there are oracles A and B such that $\mathbf{E}^A \subseteq \mathbf{P}^A$/poly and $\mathbf{E}^B \not\subseteq \mathbf{P}^B$/poly, which means that this question is unrelativizable. If $\mathbf{E} \subseteq \mathbf{P}/\text{poly}$, then, for every set $A \in \mathbf{E}$, the initial segments of its characteristic sequence have polynomial time bounded Kolmogorov complexity $(\log)^k$. Hence it is difficult to introduce notions of resource bounded randomness in $\mathbf{E}$ in terms of chaoticness, that is to say, in terms of resource bounded Kolmogorov complexity. In this thesis we do not consider the question of introducing resource bounded chaoticness concepts.

5.1 Resource Bounded Typicalness

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

5.1.1 Resource bounded randomness, resource bounded Schnorr and Kurtz randomness

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

Definition 5.1.1 *(Schnorr [89] and Lutz [65]) A $\mathcal{C}$-*test *is a martingale $F \in \mathcal{C}$. An infinite sequence ξ* does not withstand *the $\mathcal{C}$-test F if F succeeds on ξ. A sequence ξ is $\mathcal{C}$-*random *if it withstands all $\mathcal{C}$-tests.*

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

Definition 5.1.2 *A* Schnorr $(\mathcal{C}_1, \mathcal{C}_2)$-test *is a pair (F, h) of functions such that $F \in \mathcal{C}_1$ is a martingale and $h \in \mathcal{C}_2$ is an unbounded, nondecreasing function from N to N. An infinite sequence ξ* does not withstand *the Schnorr $(\mathcal{C}_1, \mathcal{C}_2)$-test (F, h) if $\limsup_n(F(\xi[0..n-1]) - h(n)) \geq 0$, i.e., if $F(\xi[0..n-1]) \geq h(n)$ i.o. A sequence ξ is* Schnorr $(\mathcal{C}_1, \mathcal{C}_2)$-random *if it withstands all Schnorr $(\mathcal{C}_1, \mathcal{C}_2)$-tests.*

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

Definition 5.1.3 *A* Kurtz $(\mathcal{C}_1, \mathcal{C}_2)$-test *is a pair (F, h) of functions such that $F \in \mathcal{C}_1$ is a martingale and $h \in \mathcal{C}_2$ is an unbounded, nondecreasing function from N to N. An infinite sequence ξ* does not withstand *the Kurtz $(\mathcal{C}_1, \mathcal{C}_2)$-test (F, h) if $\liminf_n(F(\xi[0..n-1]) - h(n)) \geq 0$, i.e., if $F(\xi[0..n-1]) \geq h(n)$ a.e. A sequence ξ is* Kurtz $(\mathcal{C}_1, \mathcal{C}_2)$-random *if it withstands all Kurtz $(\mathcal{C}_1, \mathcal{C}_2)$-tests.*

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

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

Lemma 5.1.4 *For any function classes $\mathcal{C}_1$ and $\mathcal{C}_2$,*

$$\mathcal{C}_1\textbf{-RAND} \subseteq (\mathcal{C}_1, \mathcal{C}_2)\textbf{-S-RAND} \subseteq (\mathcal{C}_1, \mathcal{C}_2)\textbf{-W-RAND}$$

Moreover,

$$\mathcal{C}_1\textbf{-RAND} = (\mathcal{C}_1, \textbf{all})\textbf{-S-RAND}$$

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

Proof. Straightforward. ■

Lemma 5.1.5 *For any function classes $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_1'$ and $\mathcal{C}_2'$ such that $\mathcal{C}_1 \subseteq \mathcal{C}_1'$ and $\mathcal{C}_2 \subseteq \mathcal{C}_2'$,*

$$(\mathcal{C}_1', \mathcal{C}_2')\textbf{-S-RAND} \subseteq (\mathcal{C}_1, \mathcal{C}_2)\textbf{-S-RAND}$$

and

$$(\mathcal{C}_1', \mathcal{C}_2')\textbf{-W-RAND} \subseteq (\mathcal{C}_1, \mathcal{C}_2)\textbf{-W-RAND}$$

Proof. Straightforward. ■

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

Theorem 5.1.6 *Let $f_1, f_2 \in \mathbf{P}$ be two functions such that $\frac{f_1}{f_2}$ converges to 0 monotonically. Then $(\mathbf{P}, OL(f_1))$*-**S-RAND** $\subset$ *$(\mathbf{P}, OL(f_2))$*-**S-RAND**, *where $OL(f_i) = \{cf_i : c \in N\}$.*

Proof. Schnorr [89, Satz 16.2] proved that

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

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

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

Theorem 5.1.7 *Let $\mathcal{C}$ be a class of recursive functions such that $DTIME(n^3) \subseteq \mathcal{C}$. Then $\mathcal{C}$*-**RAND** $\subset$ *$(\mathcal{C}, \mathbf{REC})$*-**S-RAND** $\subseteq$ *$(\mathcal{C}, \mathcal{C})$*-**S-RAND**.

Theorem 5.1.8 $(\mathbf{P},\mathbf{P})$**-S-RAND** $\subset$ $(\mathbf{P},\mathbf{P})$**-W-RAND**.

Proof. By Lemma 5.1.4, $(\mathbf{P},\mathbf{P})$**-S-RAND** $\subseteq$ $(\mathbf{P},\mathbf{P})$**-W-RAND**. It was observed by Kurtz [54] that there exists a Kurtz random sequence ξ which does not satisfy the law of large numbers, whereas all Schnorr $(\mathbf{P},\mathbf{P})$-random sequences satisfy the law of large numbers (cf. the proof of Theorem 5.2.12). ∎

The above theorems show that, in general, the notion of resource bounded randomness is stronger than the notion of resource bounded Schnorr randomness and the notion of resource bounded Schnorr randomness is stronger than the notion of resource bounded Kurtz randomness.

5.1.2 Resource bounded measure

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

1. Let n^k-**RAND**, n^k-**S-RAND** and n^k-**W-RAND** denote $DTIME(n^k)$-**RAND**, $(DTIME(n^k),\mathcal{C}_k)$-**S-RAND** and $(DTIME(n^k),\mathcal{C}_k)$-**W-RAND**, respectively, where $\mathcal{C}_k$ 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 with time bound in $O(n^k)$.
3. We will say that a sequence ξ is p-random if it is **P**-random.

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

Definition 5.1.9 *(Lutz [65]) 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 [65] introduced his p-measure in terms of approximable martingales. However, the following lemma shows that it is equivalent to the above definition.

Definition 5.1.10 *(Lutz [65]) 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 thesis, unless otherwise stated, we will use $h(n,x)$ to denote $h(0^n,x)$.

Lemma 5.1.11 *For each p-approximable martingale F, 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. [10], Juedes and Lutz [43] or Mayordomo [76]. ■

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

Theorem 5.1.12 *Let $\mathcal{C}$ be a class of languages. Then $\mathcal{C}$ has p-measure* 0 *if and only if there exists a number $k \in N$ such that there is no n^k-random set in $\mathcal{C}$.*

Proof. Straightforward. ■

It was proved by Ambos-Spies et al. [10] that, for each $k \in N$, there exist n^k-random sets in **E**. Hence we have the following theorem.

Theorem 5.1.13 *(Lutz [65])* **E** *does not have p-measure* 0.

Proof. This follows from Theorem 5.1.12. ■

It has been shown that p-measure (whence n^k-randomness concepts) 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 complexity classes, the p-measures based on Schnorr and Kurtz randomness concepts coincide with the above p-measure based on rec-randomness concepts.

5.1.3 Resource bounded randomness and complexity

In this section we will show that n^k-**RAND** and n^k-**S-RAND** coincide within **E**. We will also show that a recursive set is polynomial time 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 p-randonmess, polynomial time bounded Schnorr and Kurtz randomness coincide in the recursive sets, we need the following lemma which is essentially due to Allender and Strauss [3]. It should be noted that our results and proof is a little different from that of Allender and Strauss [3].

Lemma 5.1.14 *(cf. Allender and Strauss [3]) Let F be an n^k-martingale. Then there exists an n^{k+1}-martingale F' and an n^{k+1}-time computable function $d : \Sigma^* \to N$ such that,*

1. *For all $x \sqsubseteq y$, $d(x) \leq d(y)$.*
2. *For all x, $F'(x) \geq d(x)$.*
3. *For any sequence $\xi \in \Sigma^\infty$, if $\limsup_n F(\xi[0..n-1]) = \infty$, then $\lim_n d(\xi[0..n-1]) = \infty$.*

Proof. We construct d and F' in stages, where at stage s we define $F'(x)$ and $d(x)$ 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 $d(\lambda) = F(\lambda) - 1 = 0$.

Stage $s+1$.

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

Case 1. $d(x) + 1 \geq F'(x)$.

Let $F'(xb) = d(x) + (F'(x) - d(x))l(xb)$ and $d(xb) = d(x)$.

Case 2. $d(x) + 1 < F'(x)$.

Let $F'(xb) = d(x) + 1 + (F'(x) - d(x) - 1)l(xb)$ and $d(xb) = d(x) + 1$.

End of construction.

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

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

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

Claim 2 *For all $x \sqsubseteq y$, $d(x) \leq d(y)$.*

Proof. Straightforward from the construction. □

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

Proof. A simple induction. □

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

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

Proof. If $y \in \Sigma$, then the claim follows from the construction. Assume that

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

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

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

where $b = 0, 1$. □

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

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

By the construction, $d(\lambda) \geq 0$.

Assume that $k+1 \geq F'(\xi[0..n_1-1]) > d(\xi[0..n_1-1]) = k$ for some $n_1 \in N$. Then, by Claim 4,

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

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

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

Hence there exists $n_3 \leq n_2$ such that $F'(\xi[0..n_3-1]) > d(\xi[0..n_1-1]) + 1 = k+1$ and $d(\xi[0..n_3]) \geq k+1$. ■

Theorem 5.1.15 *Let $k \geq 2$ and let ξ be an infinite recursive sequence which is Kurtz n^k-random. Then ξ is n^{k-1}-random.*

Proof. For a contradiction assume that ξ is not 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 d be the n^k-martingale and the n^k-time computable function corresponding to F according to Lemma 5.1.14. Define a function h as follows.

Stage 0

Let $h(0) = 0$.

Stage $s+1$.

For at most $s+1$ steps search for a string $x \sqsubseteq \xi[0..s]$ (using the Turing machine M) such that $d(x) \geq h(|x|) + 1 = h(s) + 1$. 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 obvious that h is an n^2-time computable (with respect to the unary representation of numbers), unbounded, nondecreasing function and $F'(\xi[0..n-1]) \geq h(n)$ a.e. Hence ξ is not Kurtz n^k-random contrary to assumption. ■

Corollary 5.1.16 *For any recursive sequence ξ, ξ is p-random if and only if ξ is Schnorr p-random, if and only if ξ is Kurtz p-random. That is to say,*

$$\mathbf{P\text{-}RAND} \cap \mathbf{REC} = (\mathbf{P}, \mathbf{P})\text{-}\mathbf{S\text{-}RAND} \cap \mathbf{REC} = (\mathbf{P}, \mathbf{P})\text{-}\mathbf{W\text{-}RAND} \cap \mathbf{REC}$$

Corollary 5.1.16 shows that it suffices to study resource bounded randomness in the context of complexity classes. In the rest of the thesis, unless otherwise stated, we will study resource bounded randomness and omit the prefix name of person.

5.1.4 Resource bounded Ko randomness

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

Definition 5.1.17 *(Ko [48]) A* Ko $(\mathcal{C}_1, \mathcal{C}_2)$-test *is a pair (U, g) where $U \in \mathcal{C}_1$ is a subset of Σ^* (notice that we identify a set with its characteristic function) and $g \in \mathcal{C}_2$ is an unbounded, nondecreasing function from N to N such that the following hold.*

1. $U^{[0]} = \Sigma^*$.
2. $U^{[k+1]} \subseteq U^{[k]}$.
3. $Prob[U^{[k]} \cdot \Sigma^\infty] \leq 2^{-k}$.

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

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

Lemma 5.1.18 *(Ko [48]) 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 (cf. Chapter 3). Then $\xi \in$* $(\mathbf{P}, \log)$-**K-RAND**.

Proof. See the proof of Ko [48, Corollary 3.9]. ■

Lemma 5.1.19 $(\mathbf{P}, \log)$-**K-RAND** $\not\subseteq$ $(\mathbf{P}, \log)$-**W-RAND**.

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

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

Then

$$\begin{aligned} KM^{2^{2n}}(\xi[0..n-1]) &\geq KM(\xi[0..n-1]) \\ &\geq KM(\xi_1[0..n - [\log n] - 1]) - c_1 \\ &\geq n - [\log n] - c \quad \text{(By Theorem 3.3.2)} \\ &> n - [4\log n] \quad a.e. \end{aligned}$$

Hence, by Lemma 5.1.18, $\xi \in (\mathbf{P}, \log)$**-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 $F(\xi[0..n-1]) \geq \frac{n}{2}$ for all $n \in N$, so $\xi \notin (\mathbf{P}, \log)$**-W-RAND**. ■

As a corollary of the proof of Lemma 5.1.19, we have

Corollary 5.1.20 *There exists a Ko* $(\mathbf{P}, \log)$*-random set which is not* $\mathbf{P}$*-immune.*

Remark. Using Meyer and McCreight's weighted priority diagonalization, Ko [48] 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 5.1.21 *Let* $A \in \mathbf{E}_2$*. Then* $A \notin (\mathbf{P}, \log)$**-K-RAND**.

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

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, $\max\{m : \xi[0..n-1] \in U^{[m]}\} \geq [\log n]$ for almost all n.

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

Lemma 5.1.22 P-RAND $\not\subseteq (\mathbf{P}, \log)$**-K-RAND**.

Proof. Lutz [65] has shown that there is a p-random set A in $DTIME(2^{n^2})$. So the lemma follows from Lemma 5.1.21. ■

By Lemma 5.1.19 and Lemma 5.1.22, we get the following independence results.

Theorem 5.1.23 *1.* **P-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.*

5.2 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, work in this area mainly concentrated on the definition of "legal selection rules". For example, Church [31] 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., [97]). Di Paola [85] considered notions of stochasticity in subrecursive hierarchies. Based on these works, Wilber [113] and Ko [48] introduced two notions of polynomial time pseudostochasticity. Huynh [39] showed that the notion of Wilber's pseudostochasticity is independent of the notion of **P**-immunity. Especially, there exists a Wilber pseudostochastic set which is not **P**-immune. Since a random set must not contain any infinite easy parts, this shows that Wilber's concept is not an acceptable randomness notion. Lutz and Mayordomo [76] defined a notion of weak stochasticity to prove that, for $\alpha < 1$, all $\leq^p_{n^\alpha-tt}$-hard sets for **E** are exponentially dense. And it is also easy to show that there exists a weakly stochastic set of Lutz and Mayordomo which is not **P**-immune. The reason why these concepts do not guarantee **P**-immunity is that they select too many elements from Σ^n for each n. In [8], Ambos-Spies, Mayordomo, Wang and Zheng removed this restraint and got a stronger, more satisfactory notion of p-stochasticity. They showed that this notion of p-stochasticity is weaker than the notion of p-randomness, and all p-stochastic sets are **P**-immune. Moreover, all p-stochastic sequences, hence p-random sequences, satisfy the strong law of large numbers. Furthermore, we show that p-stochastic sequences are normal in the sense of Borel. (The fact that p-random sequences are normal was proved by Schnorr in [89]).

Definition 5.2.1 *(Ko [48]) Let $\mathcal{C}$ be a class of total functions from Σ^* to Σ. A sequence $\xi \in \Sigma^\infty$ is* Ko $\mathcal{C}$-stochastic *if, for all $f \in \mathcal{C}$,*

$$\lim_{n\to\infty} \frac{\|\{k < n : f(\xi[0..k-1]) = \xi[k]\}\|}{n} = \frac{1}{2}. \tag{5.1}$$

The function f in Definition 5.2.1 can be considered as a *prediction function*, that is, given a finite initial segment $\xi[0..n-1]$ of a sequence ξ, f predicts the next bit $\xi[n]$ of the sequence. Intuitively, a sequence ξ is Ko $\mathcal{C}$-stochastic if and only if, for each prediction function $f \in \mathcal{C}$, the probability of success is not better than tossing an unbiased coin.

For the reason of convenience, in the rest of the thesis, we use the notation p-stochastic instead of **P**-stochastic.

Theorem 5.2.2 *(Ambos-Spies et al. [8]) There exists a Ko p-stochastic set A which is not* **P***-immune.*

Proof. Let ξ be a Ko p-stochastic sequence. Define a sequence η by

$$\eta[n] = \begin{cases} 0 & n = 2^i \text{ for some } i \in N \\ \xi[n] & \text{otherwise} \end{cases}$$

Let A be the set with the characteristic sequence η. Then A is not **P**-immune. So it suffices to show that η is Ko p-stochastic.

Let $f : \Sigma^* \to \Sigma$ be a total function in **P**. We have to show that (5.1) holds with η in place of ξ.

Define a total function f' by letting $f'(x) = f(x_\eta)$, where x_η is defined by

$$x_\eta[n] = \begin{cases} 0 & n = 2^i \text{ for some } i \in N \\ x[n] & \text{otherwise} \end{cases}$$

for $n < |x|$. Then $f' \in \mathbf{P}$ and $f'(\xi[0..n-1]) = f(\eta[0..n-1])$ for all $n \geq 1$. Since

$$\lim_{n\to\infty} \frac{\|\{k \leq n : \xi[k] \neq \eta[k]\}\|}{n} = 0$$

this implies

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

Now, by Ko p-stochasticity of ξ, the limit on the right side equals to $\frac{1}{2}$. This completes the proof. ■

For a better understanding of Ko p-stochasticity, we next give a characterization of Ko's concepts in terms of martingales.

Definition 5.2.3 *A* Schnorr $\mathcal{C}$-exp-test *is a pair (F, c), where $F \in \mathcal{C}$ is a martingale and $c > 1$ is a real number. A sequence ξ* does not withstand *the Schnorr $\mathcal{C}$-exp-test (F, c) if* $\limsup_n(F(\xi[0..n-1]) - c^n) > 0$. *A sequence ξ is* Schnorr $\mathcal{C}$-exp-random *if it withstands all Schnorr $\mathcal{C}$-exp-tests.*

Theorem 5.2.4 *For any infinite sequence $\xi \in \Sigma^\infty$, ξ is Ko p-stochastic if and only if ξ is Schnorr p-exp-random.*

Proof. The proof technique is the same as that in the proof of Schnorr's Satz 18.4 in [89]. We omit the details here. ■

By Theorem 5.2.4, the notion of Ko p-stochasticity is just a little stronger than the notion of non-p-computability. Namely, a sequence $\xi \in \Sigma^\infty$ is polynomial time computable (that is to say, $\xi[0..n-1]$ 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

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

In [8], Ambos-Spies, Mayordomo, Wang and Zheng introduced an even stronger notion of stochasticity based on partial prediction functions that implies **P**-immunity.

Definition 5.2.5 *(Ambos-Spies et al. [8]) Let $\mathcal{C}$ be a class of partial functions from Σ^* to Σ. A sequence $\xi \in \Sigma^\infty$ is* $\mathcal{C}$-stochastic *if, for each $f \in \mathcal{C}$ such that $\{n : f(\xi[0..n-1])$ is defined $\}$ is infinite,*

$$\lim_{n\to\infty} \frac{\|\{k \le n : f(\xi[0..k-1]) = \xi[k]\}\|}{\|\{k \le n : f(\xi[0..k-1]) \textit{is defined}\}\|} = \frac{1}{2}. \tag{5.2}$$

*The set of $\mathcal{C}$-stochastic sequences is denoted by $\mathcal{C}$-***STOCH**.

Definition 5.2.5 is based on prediction functions. While the notion of stochasticity was originally introduced in terms of selection functions (cf. Chapter 3). Next we characterize $\mathcal{C}$-stochasticity in these terms.

Definition 5.2.6 *(Ambos-Spies et al. [8]) Let $\mathcal{C}$ be a class of total functions from Σ^* to Σ. A sequence $\xi \in \Sigma^\infty$ is* $\mathcal{C}$-1-stochastic *if, for each $f \in \mathcal{C}$ such that $\{n : f(\xi[0..n-1]) = 1\}$ is infinite,*

$$\lim_{n\to\infty} \frac{\|\{k \le n : f(\xi[0..k-1]) = \xi[k] = 1\}\|}{\|\{k \le n : f(\xi[0..k-1]) = 1\}\|} = \frac{1}{2}. \tag{5.3}$$

*The set of $\mathcal{C}$-1-stochastic sequences is denoted by $\mathcal{C}$-1-***STOCH**.

The function f in Definition 5.2.6 can be considered as a *selection function* (cf. Church [31]), that is, a function which select a subsequence η of ξ. Intuitively, a sequence ξ is $\mathcal{C}$-1-stochastic if and only if, for each selection function $f \in \mathcal{C}$, the numbers of 0s and 1s in the selected subsequence η are asymptotically the same.

Theorem 5.2.7 *(Ambos-Spies et al. [8]) Let $\mathbf{P}_1$ (resp. $\mathbf{P}_2$) be the class of polynomial time computable total (resp. partial) functions from Σ^* to Σ. Then*

$$\mathbf{P}_2\textbf{-STOCH} = \mathbf{P}_1\textbf{-1-STOCH}.$$

Proof. (1). $\mathbf{P}_1$-1-**STOCH** $\subseteq$ $\mathbf{P}_2$-**STOCH**.

Given a sequence $\xi \notin \mathbf{P}_2$-**STOCH**, there exists a prediction function $f \in \mathbf{P}_2$ such that $\{n : f(\xi[0..n-1])$ is defined$\}$ is infinite and (5.2) does not hold. Then one of the following two conditions holds:

$$\|\{k : f(\xi[0..k-1]) = 1\}\| = \infty \quad \text{and} \quad \lim_{n\to\infty} \frac{\|\{k \le n : f(\xi[0..k-1]) = \xi[k] = 1\}\|}{\|\{k \le n : f(\xi[0..k-1]) = 1\}\|} \ne \frac{1}{2} \tag{5.4}$$

$$\|\{k : f(\xi[0..k-1]) = 0\}\| = \infty \quad \text{and} \quad \lim_{n\to\infty} \frac{\|\{k \le n : f(\xi[0..k-1]) = \xi[k] = 0\}\|}{\|\{k \le n : f(\xi[0..k-1]) = 0\}\|} \ne \frac{1}{2} \tag{5.5}$$

W.l.o.g., we may assume that (5.4) holds. Define a selection function f_1 by

$$f_1(x) = \begin{cases} 1 & \text{if } f(x) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then obviously $\{n : f_1(\xi[0..n-1]) = 1\}$ is infinite, and

$$\frac{\|\{k \leq n : f_1(\xi[0..k-1]) = \xi[k] = 1\}\|}{\|\{k \leq n : f_1(\xi[0..k-1]) = 1\}\|} = \frac{\|\{k \leq n : f(\xi[0..k-1]) = \xi[k] = 1\}\|}{\|\{k \leq n : f(\xi[0..k-1]) = 1\}\|}$$

So (5.3) does not hold with f_1 in place of f. I.e., $\xi \notin \mathbf{P}_1$-1-**STOCH**.

(2). $\mathbf{P}_2$-**STOCH** $\subseteq \mathbf{P}_1$-1-**STOCH**.

Given a sequence $\xi \notin \mathbf{P}_1$-1-**STOCH**, there exists a selection function $f \in \mathbf{P}_1$ such that $\{n : f(\xi[0..n-1]) = 1\}$ is infinite and (5.3) does not hold. Define a prediction function f_1 by

$$f_1(x) = \begin{cases} 1 & \text{if } f(x) = 1 \\ \text{undefined} & \text{otherwise} \end{cases}$$

Then obviously $\{k : f_1(\xi[0..k-1]) \text{ is defined}\}$ is infinite, and

$$\frac{\|\{k \leq n : f_1(\xi[0..k-1]) = \xi[k]\}\|}{\|\{k \leq n : f_1(\xi[0..k-1]) \text{ is defined}\}\|} = \frac{\|\{k \leq n : f(\xi[0..k-1]) = \xi[k] = 1\}\|}{\|\{k \leq n : f(\xi[0..k-1]) = 1\}\|}$$

So (5.2) does not hold with f_1 in place of f. I.e., $\xi \notin \mathbf{P}_2$-**STOCH**. ■

Theorem 5.2.8 *(Ambos-Spies et al. [8]) Let A be a p-stochastic set. Then A is $\mathbf{E}$-immune.*

Proof. For a contradiction assume that A has an infinite subset $B \in \mathbf{E}$. Define a prediction function f by

$$f(x) = \begin{cases} 1 & \text{if } z_{|x|} \in B \\ \text{undefined} & \text{otherwise} \end{cases}$$

Then $f \in \mathbf{P}$, $\{n : f(A\restriction z_n) \text{ is defined}\}$ is infinite, and

$$\lim_{n\to\infty} \frac{\|\{k \leq n : f(A\restriction z_k) = A(z_k)\}\|}{\|\{k \leq n : f(A\restriction z_k) \text{ is defined}\}\|} = 1$$

Hence A is not p-stochastic contrary to the assumption. ■

In the following, we show that resource bounded stochasticity is weaker than resource bounded typicalness. This coincides with the relationship between the corresponding classical (recursive) notions. At first, we show the invariance property of p-random sequences. This property is implicit in Ambos-Spies et al. [10].

Theorem 5.2.9 *Let ξ be an n^k-random sequence and let $f : \Sigma^* \to \Sigma$ be an n^{k-1}-time computable selection function such that $\{n : f(\xi[0..n-1]) = 1\}$ is infinite. Then the selected subsequence ξ_f of ξ by f is n^{k-1}-random, where $\xi_f = b_0 b_1 \cdots$ is defined by*

$$b_i = \begin{cases} \lambda & \textit{if } f(\xi[0..i-1]) = 0 \\ \xi[i] & \textit{if } f(\xi[0..i-1]) = 1 \end{cases}$$

Proof. For a contradiction, assume that ξ_f is not n^{k-1}-random. Then there is an n^{k-1}-martingale F which succeeds on ξ_f. Define an n^k-martingale G by $G(x) = F(x_f)$, where x_f is defined in the same way as ξ_f. It is straightforward to check that $\limsup_{n\to\infty} G(\xi[0..n-1]) = \limsup_{n\to\infty} F(\xi_f[0..n-1]) = \infty$. Hence G succeeds on ξ, which is contrary to the assumption. ■

Corollary 5.2.10 *Let $\xi \in \Sigma^\infty$ be a p-random sequence and $f : \Sigma^* \to \Sigma$ be a polynomial time computable selection function such that $\{n : f(\xi[0..n-1]) = 1\}$ is infinite. Then the selected subsequence ξ_f of ξ by f is p-random.*

Definition 5.2.11 *An infinite sequence $\xi \in \Sigma^\infty$ satisfies the law of large numbers if*

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

Schnorr has already shown that the law of large numbers holds for p-random sequences.

Theorem 5.2.12 *(The law of large numbers, Schnorr [89]) Let $\xi \in \Sigma^\infty$ be an n^2-random sequence. Then ξ satisfies the law of large numbers.*

Proof. The following proof is taken from Schnorr [89]. We include it here only for the sake of completeness.

For a contradiction assume that ξ does not satisfy the law of large numbers. W.l.o.g., we may assume that

$$\limsup_n \frac{s_n}{n} > \frac{1}{2}$$

where $s_n = \sum_{i=0}^{n-1} \xi[i]$. We will construct an n^2-martingale F which succeeds on ξ.

Let $0 < q < 1$ be small enough such that

$$\frac{1}{2}(\log(1+q) + \log(1-q)) + a(\log(1+q) - \log(1-q)) = c > 0$$

where $a = \limsup_{n\to\infty} \frac{s_n}{n} - \frac{1}{2}$. Note that this q exists since $\log(1+q) + \log(1-q)$ converges to 0 very quickly as $q \to 0$ and $\log(1+q) - \log(1-q)$ is positive for $q > 0$.

Define an n^2-martingale $F : \Sigma^* \to Q^+$ by letting $F(\lambda) = 1$ and letting

$$F(xb) = \begin{cases} (1+q)F(x) & \text{if } b = 1 \\ (1-q)F(x) & \text{if } b = 0 \end{cases}$$

Then, for $n \in N$,

$$F(\xi[0..n-1]) = (1-q)^{n-s_n}(1+q)^{s_n}.$$

Hence

$$\log F(\xi[0..n-1]) = \frac{n}{2}(\log(1+q) + \log(1-q)) + (s_n - \frac{1}{2})(\log(1+q) - \log(1-q))$$

and

$$\begin{aligned}\limsup_{n\to\infty}\tfrac{1}{n}\log F(\xi[0..n-1]) &\geq \tfrac{1}{2}(\log(1+q)+\log(1-q))+a(\log(1+q)-\log(1-q))\\ &= c>0.\end{aligned}$$

I.e.,

$$\limsup_{n\to\infty} F(\xi[0..n-1]) \geq \limsup_{n\to\infty} 2^{c\cdot n} = \infty.$$

So ξ is not n^2-random, contrary to assumption. ■

Theorem 5.2.13 *(Ambos-Spies et al. [8])* **P-RAND** $\subset$ **P**$_1$**-1-STOCH**, *where* **P**$_1$ *is defined in Theorem 5.2.7.*

Proof. Let $\xi \in \Sigma^\infty$ be a p-random sequence, and $f : \Sigma^* \to \Sigma$ be a polynomial time computable selection function such that $\{n : f(\xi[0..n-1]) = 1\}$ is infinite. Then, by Corollary 5.2.10, the selected subsequence ξ_f of ξ by f is p-random. Hence, by Theorem 5.2.12, (5.3) holds. That is to say, ξ is p-stochastic.

Ville [98] constructed a Church stochastic sequence ξ satisfying the property

$$0 \leq \frac{1}{2} - \frac{1}{n}\sum_{i=0}^{n-1}\xi[i] \leq \frac{f(n)}{n}$$

where $f(n)$ is a given unbounded, nondecreasing, time constructible function. That is to say, ξ does not satisfy the law of the iterated logarithm. Obviously ξ is p-stochastic too. In Theorem 5.3.6, we will show that p-random sequences satisfy the law of the iterated logarithm, hence ξ is not p-random. ■

In order to study the property of stochastic sequences, the concept of normal sequences has been introduced and has been studied extensively. Recently Strauss [94] used the concept of normal sequences to show that almost all sets in **PSPACE** are sources for **BPP** (the concept of sources for **BPP** was introduced by Lutz in [64]). In the following, we show that all p-stochastic sequences are normal.

Definition 5.2.14 *For $\xi \in \Sigma^\infty$, $w \in \Sigma^+$ and $n \in N^+$, let*

$$freq^w(\xi[0..n-1]) = \frac{\|\{i \leq n-|w| : \xi[i..i+|w|-1] = w\}\|}{n}$$

and

$$freq^w(\xi) = \lim_{n\to\infty} freq^w(\xi[0..n-1])$$

provided that this limit exists.

Definition 5.2.15 *Let $m \in N^+$. A sequence $\xi \in \Sigma^\infty$ is* m-normal*, and we write $\xi \in$* **NORM**$_m$*, if, for all $w \in \Sigma^m$,*

$$freq^w(\xi) = 2^{-m}.$$

A sequence $\xi \in \Sigma^\infty$ is normal*, and we write $\xi \in$* **NORM***, if ξ is m-normal for all $m \in N^+$, i.e.,*

$$\mathbf{NORM} = \bigcap_{m=1}^{\infty} \mathbf{NORM}_m.$$

Theorem 5.2.16 n^2_{part}-**STOCH** $\subseteq$ **NORM**, *where* n^2_{part} *is the class of* n^2*-time computable partial functions.*

Proof. Assume that $\xi \in n^2_{part}$-**STOCH**. We show $\xi \in \mathbf{NORM}_m$ by induction on m.

Basic Step

For $w \in \Sigma$, define the total prediction function f by letting $f(x) = w$ for all $x \in \Sigma^*$. Then, by n^2_{part}-stochasticity of ξ,

$$\begin{aligned}
freq^w(\xi) &= \lim_{n\to\infty} freq^w(\xi[0..n-1]) \\
&= \lim_{n\to\infty} \frac{\|\{i < n : \xi[i] = w\}\|}{n} \\
&= \lim_{n\to\infty} \frac{\|\{i < n : f(\xi[0..i-1]) = \xi[i]\}\|}{n} \\
&= \frac{1}{2}.
\end{aligned}$$

Inductive Step

Let $w \in \Sigma^*$ and $b \in \Sigma$ be given, where, by inductive hypothesis, $freq^w(\xi) = 2^{-|w|}$. To show that $freq^{wb}(\xi) = 2^{-(|w|+1)}$, define the n^2-computable partial prediction function f by

$$f(x) = \begin{cases} b & \text{if } x = yw \text{ for some } y \in \Sigma^*, \\ \text{undefined} & \text{otherwise.} \end{cases}$$

Then, by the n^2_{part}-stochasticity of ξ,

$$\begin{aligned}
freq^{wb}(\xi) &= \lim_{n\to\infty} freq^{wb}(\xi[0..n-1]) \\
&= \lim_{n\to\infty} \frac{\|\{i < n - |w| : \xi[i..i+|w|] = wb\}\|}{n} \\
&= \lim_{n\to\infty} \frac{\|\{i < n : f(\xi[0..i-1]) = \xi[i]\}\|}{n} \\
&= \lim_{n\to\infty} \frac{\|\{i < n : f(\xi[0..i-1]) \text{ is defined}\}\|}{n} \cdot \\
&\qquad \frac{\|\{i < n : f(\xi[0..i-1]) = \xi[i]\}\|}{\|\{i < n : f(\xi[0..i-1]) \text{ is defined}\}\|} \\
&= freq^w(\xi) \cdot \frac{1}{2} = 2^{-|w|-1}.
\end{aligned}$$

This completes the proof. ■

Corollary 5.2.17 *(Schnorr [89])* n^2-**RAND** $\subseteq$ **NORM**.

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

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

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

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

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

denote the *reduced number* of 1s in x. Note that $S^*(x)$ amounts to measuring the deviations of $S(x)$ from $\frac{|x|}{2}$ 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 $\frac{S(\xi[0..n-1])}{n}$ 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 5.3.1 *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 the next chapter, we will use 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.

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 [63] 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 5.3.2 *(Lutz [63]) 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 5.3.3 *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 $\cup_{i=0}^{\infty} \mathbf{NULL}_{F_i}$ 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 5.3.3 still holds.

Proof. By the p-union lemma of Lutz [65], 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

$$\bigcup_{i=0}^{\infty} \mathbf{NULL}_{F_i} \subseteq \bigcup_{i=0}^{\infty} \mathbf{NULL}_{F'_i}. \tag{5.6}$$

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

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

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

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

Hence (5.6) holds. ■

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

Theorem 5.3.4 *[33, p144] 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 $u(n) > c_0$,

$$u^{-2}e^{-u^2/2} \leq Prob\left[\{\xi \in \Sigma^\infty : S^*(\xi[0..n-1]) > u(n)\}\right] \leq e^{-u^2/2}.$$

We will also use the following lemma from Feller [33, p158].

Lemma 5.3.5 *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*

$$\mathbf{C} = \left\{\xi \in \Sigma^\infty : S(\xi[0..k-1]) - \frac{1}{2}k > u(n) \text{ for some } k \leq n\right\},$$

then

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

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

Theorem 5.3.6 *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

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

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 to say, $\mathbf{Y} = \cup_{k=1}^\infty \mathbf{Y}_k$ 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 5.3.6.

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

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

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

and

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

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

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

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 5.3.3, 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 $|x| > v(k)$,

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

Let

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

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

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

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

If $i\leq\left\lceil\frac{4\ln|x|}{\ln\beta}\right\rceil$, then $n_i\leq|x|^4+1$. 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 $n_{i+1}\leq\beta\cdot(|x|^4+1)$. 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 5.3.4, c_1 be the constant in Lemma 5.3.5, $c=\frac{c_1}{3}>0$ and $u_1(k)=[6e^{2c_0^2}k^2]$. Then the following conditions hold for all k.*

1. *For all $i>u_1(k)$,*
$$Prob[\mathbf{Y}_{k,i}]\leq\int_i^{i+1}\frac{dx}{c\cdot((x-1)\ln\beta)^\alpha}.$$

2. *For all $i>\max\{u_1(k),\left\lceil\frac{4\ln|x|}{\ln\beta}\right\rceil\}$,*
$$Prob[\mathbf{Y}_{k,i}|\mathbf{C}_x]\leq\int_i^{i+1}\frac{dx}{c\cdot((x-1)\ln\beta)^\alpha}.$$

Proof. 1. By Lemma 5.3.5,

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

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

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

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 5.3.4) we get, therefore, for $i>u_1(k)=[6e^{c_0^2}k^2]$,

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

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

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

where

$$\mathbf{Y}_{k,i,j} = \left\{ \xi \in \Sigma^\infty \ : \ S(\xi[0..n-1]) - \frac{1}{2}n + j > \alpha\sqrt{\frac{1}{2}n_i \ln\ln n_i}, n_i \leq n < n_{i+1} \right\}$$

for $i, j \in N$.

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

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

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

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

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, we have

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

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

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

□

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 $\alpha = 1 - \frac{1}{k}$ $(k > 5)$, $\beta = k^4$, $\gamma = 1 - \frac{1}{k^3}$ and $n_i = \beta^i$ $(i = 1, 2, \cdots)$. 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

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

We first show that if $i > e^{c_0^2}$ (where c_0 is the constant in Theorem 5.3.4), then $Prob[\mathbf{X}_{k,i}] \geq i^{-1}$.

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

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

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

If $i > e^{c_0^2}$, then $\sqrt{2\gamma\ln\ln n_i} > c_0$. So, by the DeMoivre-Laplace limit theorem (Theorem 5.3.4), for $i > e^{c_0^2}$,

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

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

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

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

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 all $k \in N$ 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 5.3.3, $\mathbf{Z}_{k,0}$ has p-measure 0.

Next, 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 $\sum_i Prob[\mathbf{X}_{k,i}^{(1,1)}] = \infty$ and $\sum_i Prob[\mathbf{X}_{k,i}^{(1,2)}] = \infty$. Let

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

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 5.3.3, $\mathbf{Z}$ 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

$$S(\xi[0..n_{i-1}-1]) - \frac{1}{2}n_{i-1} > -(\gamma-\alpha)\sqrt{\frac{1}{2}n_i \ln\ln n_i}. \tag{5.7}$$

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

$$D_i(\xi) - \frac{1}{2}(n_i - n_{i-1}) > \gamma\sqrt{\frac{1}{2}n_i \ln\ln n_i} \text{ i.o.} \tag{5.8}$$

Adding (5.7) to (5.8), 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. ■

Corollary 5.3.7 *There exists a number $k \in N$ such that every n^k-random sequence satisfies the law of the iterated logarithm.*

5.4 Some Remarks on Statistical Laws

In the previous two sections, we showed that the two most important statistical laws hold for p-random sequences. Actually, almost all standard stochastic properties of Schnorr random sequences can be carried over to p-random sequences. Especially, for those laws which only depend on the 0-1 distributions of the sequences.

Theorem 5.4.1 *(the "gap" law, see [58] or [33]) For each Schnorr random sequence ξ and each real $\alpha < 1$, there are infinitely many $n \in N$ such that*

$$\xi[0..n + [\alpha \ln n] - 1] = \xi[0..n-1]1^{[\alpha \ln n]}.$$

Using a variation of the proof of Theorem 5.4.1, we can show that this law holds for p-random sequences also (we will not prove it here).

Our work shows that, on the one hand, the pure statistical laws can not characterize classical randomness concepts very well (because all p-random sets in $\mathbf{E}_2$ satisfies these laws also), on the other hand, we can design low-complexity (using some p-random sets in $\mathbf{E}_2$) systems which can be used for statistical interest.

Chapter 6

Resource Bounded Category, Resource Bounded Measure and Polynomial Time Approximations

The notion of polynomial time safe approximations was introduced by Meyer and Paterson in [78] (see also [49]). A safe approximation algorithm for a set A is a polynomial time algorithm M that on each input x outputs either 1 (accept), 0 (reject) or ? (do not know) such that all inputs accepted by M are members of A and no member of A is rejected by M. An approximation algorithm is optimal if no other polynomial time algorithm correctly decides infinitely many more inputs, that is, outputs infinitely many more correct 1s or 0s. In Orponen et al. [83], the existence of optimal approximations was phrased in terms of **P**-levelability: A set A is **P**-levelable if for any deterministic Turing machine M accepting A and for any polynomial p there is another machine M' accepting A and a polynomial p' such that for infinitely many elements x of A, M does not accept x within $p(|x|)$ steps while M' accepts x within $p'(|x|)$ steps. It is easy to show that A has an optimal polynomial time safe approximation if and only if neither A nor $\bar{A}$ is **P**-levelable.

The notion of unsafe approximations was introduced by Yesha in [116]: An unsafe approximation algorithm for a set A is just a standard polynomial time bounded deterministic Turing machine M with outputs 1 and 0. Duris and Rolim [32] further investigated unsafe approximations and introduced a levelability concept, Δ-levelability, which implies the nonexistence of optimal polynomial time unsafe approximations. They showed that complete sets for **E** are Δ-levelable and there exists an intractable set in **E** which has an optimal safe approximation but no optimal unsafe approximation. But they did not succeed to produce an intractable set with optimal unsafe approximations. Ambos-Spies [4] defined a concept of weak Δ-levelability and showed that there exists an intractable set in **E** which is not weakly Δ-levelable (hence it has an optimal unsafe approximation). In this thesis, we study a little different notion of unsafe approximations.

Like resource bounded measure and resource bounded randomness concepts, different kinds of resource bounded categories and resource bounded genericity concepts were introduced by Ambos-Spies et al. [5, 6, 7], Fenner [34] and Lutz [63] to determine whether a complexity class is large or small in a topological sense. It has been proved that resource bounded generic sets are useful in providing a coherent picture of complexity classes. They embody the method of diagonalization construction, that is, requirements which can always be satisfied by finite extensions are automatically satisfied by generic sets.

It was shown in Ambos-Spies et al. [9] that the generic sets of Ambos-Spies are **P**-immune, and that the class of sets which have optimal safe approximations is large in the sense of resource bounded Ambos-Spies category. Mayordomo [75] has shown that the class of **P**-immune sets is neither meager nor comeager both in the sense of resource bounded Lutz category and in the sense of resource bounded Fenner category. We extend this result by showing that the class of sets which have optimal safe approximations is neither meager nor comeager both in the sense of resource bounded Lutz category and in the sense of resource bounded Fenner category. Moreover, we will show the following relations between unsafe approximations and resource bounded categories.

1. The class of weakly Δ-levelable sets is neither meager nor comeager in the sense of resource bounded Ambos-Spies category [9].

2. The class of weakly Δ-levelable sets is comeager (so is large) in the sense of resource bounded general Ambos-Spies [5], Fenner [34] and Lutz [63] categories.

3. The class of Δ-levelable sets is neither meager nor comeager in the sense of resource bounded general Ambos-Spies [5], Fenner [34] and Lutz [63] categories.

In the last section of this chapter, we will show the relations between polynomial time approximations and the p-measure. Mayordomo [76] has shown that the class of **P**-bi-immune sets has p-measure 1. It follows that the class of sets which have optimal polynomial time safe approximations has p-measure 1. Using the law of the iterated logarithm for p-random sequences which we have proved in Chapter 5, we will show that:

1. The class of Δ-levelable sets has p-measure 0.

2. The class of sets which have optimal polynomial time unsafe approximations has p-measure 0.

3. p-Random sets are weakly Δ-levelable but not Δ-levelable.

Hence typical sets in the sense of resource bounded measure do not have optimal polynomial time unsafe approximations.

It should be noted that the above results show that the class of weakly Δ-levelable sets is large both in the sense of resource bounded categories and in the sense of resource bounded measure. That is to say, typical sets in $\mathbf{E}_2$ (in the sense of resource bounded categories or in the sense of resource bounded measure) are weakly Δ-levelable.

We will use some special notation for this chapter. We define a *finite function* to be a partial function from Σ^* to Σ whose domain is finite. For a finite function σ and a string $x \in \Sigma^*$, we write $\sigma(x)\downarrow$ if $x \in dom(\sigma)$, and $\sigma(x)\uparrow$ otherwise. For two finite functions σ, τ, we say σ and τ are compatible if $\sigma(x) = \tau(x)$ for all $x \in dom(\sigma) \cap dom(\tau)$. The concatenation $\sigma\tau$

of two finite functions σ and τ is defined as: $\sigma\tau = \sigma \cup \{(z_{n_\sigma+i+1}, b) : z_i \in dom(\tau)\ \&\ \tau(z_i) = b\}$ where $n_\sigma = \max\{n : z_n \in dom(\sigma)\}$. For a set A and a string x, we identify the characteristic string $A\restriction x$ with the finite function $\{(y, A(y)) : y < x\}$. For a finite function σ and a set A, σ is extended by A if $\sigma(x) = A(x)$ for all $x \in dom(\sigma)$.

6.1 Genericity versus Polynomial Time Safe Approximations

In this section, we summarize some known results on the relations between the notions of resource bounded genericity and the notion of polynomial time safe approximations.

At first, we introduce some concepts of resource bounded genericity.

Definition 6.1.1 *A partial function f from Σ^* to $\{\sigma : \sigma$ is a finite function $\}$ is* dense along *a set A if there are infinitely many strings x such that $f(A\restriction x)$ is defined. A set A* meets *f if, for some x, the finite function $(A\restriction x)f(A\restriction x)$ is extended by A. Otherwise, A* avoids *f.*

Definition 6.1.2 *A class $\mathbf{C}$ of sets is* nowhere dense *via f if f is dense along all sets in $\mathbf{C}$ and for every set $A \in \mathbf{C}$, A avoids f.*

Definition 6.1.3 *Let $\mathbf{F}$ be a class of (partial) functions from Σ^* to $\{\sigma : \sigma$ is a finite function$\}$. A class $\mathbf{C}$ of sets is $\mathbf{F}$-*meager *if there exists a function $f \in \mathbf{F}$ such that $\mathbf{C} = \cup_{i \in N}\mathbf{C}_i$ and $\mathbf{C}_i$ is nowhere dense via $f_i(x) = f(< i, x >)$. A class $\mathbf{C}$ of sets is $\mathbf{F}$-*comeager *if $\bar{\mathbf{C}}$ is $\mathbf{F}$-meager.*

Definition 6.1.4 *A set G is $\mathbf{F}$-*generic *if G is an element of all $\mathbf{F}$-comeager classes.*

Lemma 6.1.5 *(See [5]) A set G is $\mathbf{F}$-generic if and only if G meets all functions $f \in \mathbf{F}$ which are dense along G.*

For a class $\mathbf{F}$ of functions, each function $f \in \mathbf{F}$ can be considered as a finitary property $\mathcal{P}$ of sets. If $f(A\restriction x)$ is defined, then all sets extending $(A\restriction x)f(A\restriction x)$ have the property $\mathcal{P}$. So a set A has the property $\mathcal{P}$ if and only if A meets f. f is dense along A if and only if in a construction of A along the ordering $<$, where at stage s of the construction we decide whether or not the string z_s belongs to A, there are infinitely many stages s such that, by appropriately defining $A(z_s) \cdots A(z_{s+k-1})$ where $k = |f(A\restriction z_s)|$, we can ensure that A has the property $\mathcal{P}$ (that is to say, for some string x, $(A\restriction x)f(A\restriction x)$ is extended by A).

For different function classes $\mathbf{F}$, we have different notions of $\mathbf{F}$-genericity. In this thesis, we will concentrate on the following four kinds of function classes which have been investigated by Ambos-Spies et al. [5, 9], Fenner [34] and Lutz [63], respectively. $\mathbf{F}_1$ is the class of polynomial time computable partial functions from Σ^* to Σ; $\mathbf{F}_2$ is the class of polynomial time computable partial functions from Σ^* to $\{\sigma : \sigma$ is a finite function$\}$; $\mathbf{F}_3$ is the class of polynomial time computable total functions from Σ^* to $\{\sigma : \sigma$ is a finite function$\}$; $\mathbf{F}_4$ is the class of polynomial time computable total functions from Σ^* to Σ^*.

Definition 6.1.6 1. *(Ambos-Spies et al. [9]) A set G is* A-generic *if G is $\mathbf{F}_1$-generic.*

2. *(Ambos-Spies [5]) A set G is* general A-generic *if G is $\mathbf{F}_2$-generic.*

3. *(Fenner [34]) A set G is* F-generic *if G is $\mathbf{F}_3$-generic.*

4. *(Lutz [63]) A set G is* L-generic *if G is $\mathbf{F}_4$-generic.*

Obviously, we have the following implications.

Theorem 6.1.7 *1. If a set G is general A-generic, then G is A-generic, F-generic and L-generic.*

2. If a set G is F-generic, then G is L-generic.

Proof. Straightforward. ■

In this thesis, we will also study the following n^k-time ($k > 1$) bounded genericity concepts: A set G is Ambos-Spies n^k-generic (resp. general Ambos-Spies n^k-generic, Fenner n^k-generic, Lutz n^k-generic) if G meets all n^k-time computable functions $f \in \mathbf{F}_1$ (resp. $\mathbf{F}_2$, $\mathbf{F}_3$, $\mathbf{F}_4$) which are dense along G.

Theorem 6.1.8 *(see Ambos-Spies [5]) A class $\mathbf{C}$ of sets is meager in the sense of Ambos-Spies category (resp. general Ambos-Spies category, Fenner category, Lutz Category) if and only if there exists a number $k \in N$ such that there is no Ambos-Spies n^k-generic (resp. general Ambos-Spies n^k-generic, Lutz n^k-generic, Fenner n^k-generic) set in $\mathbf{C}$.*

As an example, we show that Ambos-Spies n^2-generic sets are $\mathbf{P}$-immune.

Theorem 6.1.9 *(Ambos-Spies et al. [9]) Let G be an Ambos-Spies n^2-generic set. Then G is $\mathbf{P}$-immune.*

Proof. For a contradiction assume that $A \in \mathbf{P}$ is an infinite subset of G. Then the function $f : \Sigma^* \to \Sigma$ defined by

$$f(x) = \begin{cases} 0 & z_{|x|} \in A \\ \uparrow & z_{|x|} \notin A \end{cases}$$

is computable in time n^2 and is dense along G. So, by the Ambos-Spies n^2-genericity of G, G meets f. By the definition of f, this implies that there exists some string $z_i \in A$ such that $z_i \notin G$, a contradiction. ■

It has been shown (see Mayordomo [76]) that neither F-genericity concept nor L-genericity concept can characterize the property of $\mathbf{P}$-immunity. But still we have the following weaker result which states that any L-generic set cannot have a too "large" subset in $\mathbf{P}$.

Theorem 6.1.10 *Let $B = \{z_{2n} : n \in N\}$ and G be a Lutz n^2-generic set. Then B is not a subset of G.*

Proof. The function $f : \Sigma^* \to \Sigma^*$ defined by $f(x) = 00$ for all $x \in \Sigma^*$ is computable in time n^2. So, by the Lutz n^2-genericity of G, G meets f. By the definition of f, this implies that there exists some string $z_i \in B$ such that $z_i \notin G$. ■

A *partial* set A is defined by a partial characteristic function $f : \Sigma^* \to \Sigma$. A partial set A is polynomial time computable if its partial characteristic function is computable in polynomial time.

Definition 6.1.11 *(Meyer et al. [78]) A* polynomial time safe approximation *of a set A is a polynomial time computable partial set Q which is consistent with A, that is to say, for every string $x \in dom(Q)$, $A(x) = Q(x)$. The approximation Q is* optimal *if, for every polynomial time safe approximation Q' of A, $dom(Q') - dom(Q)$ is finite.*

Definition 6.1.12 *(Orponen et al. [83]) A set A is* **P**-levelable *if, for any subset $B \in \mathbf{P}$ of A, there is another subset $B' \in \mathbf{P}$ of A such that $\|B' - B\| = \infty$.*

Lemma 6.1.13 *(Orponen et al. [83]) A set A possesses an optimal polynomial time safe approximation if and only if neither A nor $\bar{A}$ is **P**-levelable.*

Proof. Straightforward. ■

Lemma 6.1.14 *If a set A is **P**-immune, then A is not **P**-levelable.*

Proof. Straightforward. ■

Theorem 6.1.15 *(Ambos-Spies et al. [5]) Let G be an Ambos-Spies n^2-generic set. Then neither G nor $\bar{G}$ is **P**-levelable. That is to say, G has an optimal polynomial time safe approximation.*

Proof. This follows from Theorem 6.1.9 and Lemma 6.1.14. ■

Theorem 6.1.15 shows that the class of **P**-levelable sets is "small" in the sense of resource bounded (general) Ambos-Spies category.

Corollary 6.1.16 *The class of **P**-levelable sets is meager in the sense of resource bounded (general) Ambos-Spies category.*

Now we show that the class of **P**-levelable sets is neither meager nor comeager in the sense of resource bounded Fenner and Lutz categories.

Theorem 6.1.17 *1. There exists a set G in $\mathbf{E}_2$, which is both F-generic and **P**-levelable.*

*2. There exists a set G in $\mathbf{E}_2$, which is F-generic but not **P**-levelable.*

*3. There exists a set G in $\mathbf{E}_2$, which is **P**-levelable but not L-generic.*

*4. There exists a set G in $\mathbf{E}_2$, which is neither L-generic nor **P**-levelable.*

Proof. 1. Let $\delta(0) = 0, \delta(n+1) = 2^{2^{\delta(n)}}$, $I_1 = \{x : \delta(2n) \leq |x| < \delta(2n+1), n \in N\}$, $I_2 = \Sigma^* - I_1$ and $\{f_i : i \in N\}$ be an enumeration of $\mathbf{F}_3$.

In the following, we construct a set G at stages which is both F-generic and $\mathbf{P}$-levelable. In the construction we will ensure that

$$G \cap \Sigma^{[e]} \cap I_1 =^* \Sigma^{[e]} \cap I_1$$

for $e \geq 0$. Hence $G \cap \Sigma^{[e]} \cap I_1 \in \mathbf{P}$ for $e \geq 0$. In order to ensure that G is $\mathbf{P}$-levelable, it suffices to satisfy for all $e \geq 0$ the following requirements:

$L_e : P_e \subseteq G \cap I_1 \Rightarrow P_e \subseteq^* \Sigma^{[\leq e]} \cap I_1$.

To show that the requirements $L_e (e \geq 0)$ ensure that G is $\mathbf{P}$-levelable, fix a subset $C \in \mathbf{P}$ of G. We have to define a subset $C' \in \mathbf{P}$ of G such that $C' - C$ is infinite. Fix e such that $P_e = C \cap I_1$. Then, by the requirement L_e, $C \cap I_1 \subseteq^* \Sigma^{[\leq e]} \cap I_1$. So, for $C' = G \cap \Sigma^{[e+1]} \cap I_1$, $C' \in \mathbf{P}$ and C' is infinite. Since $C' \cap C$ is finite, C' has the required property.

The strategy for meeting a requirement L_e is as follows: If there is a string $x \in (I_1 \cap P_e) - \Sigma^{[\leq e]}$, then we let $G(x) = 0$ to refute the hypothesis of the requirement L_e (so L_e is trivially met). To ensure that G is F-generic, it suffices to meet for all $e \geq 0$ the following requirements:

G_e: There exists a string x such that G extends $(G \restriction x) f_e(G \restriction x)$.

Because the set I_1 is used to satisfy L_e, we will use I_2 to satisfy G_e. The strategy for meeting a requirement G_e is as follows: For some string $x \in I_2$, let G extend $(G \restriction x) f_e(G \restriction x)$.

Define a priority ordering of the requirements by letting $R_{2n} = G_n$ and $R_{2n+1} = L_n$. Now we give the construction of G formally.

Stage s.

If $G(z_s)$ has been defined before stage s, then go to stage $s+1$.

A requirement L_e *requires* attention if

1. $e < s$.

2. $z_s \in P_e \cap \Sigma^{[>e]} \cap I_1$.

3. For all $y < z_s$, if $y \in P_e$ then $y \in G \cap I_1$.

A requirement G_e *requires* attention if $e < s$, G_e has not received attention yet, and $x \in I_2$ for all $z_s \leq x \leq z_t$ where z_t is the greatest element in $dom((G \restriction z_s) f_e(G \restriction z_s))$.

Fix the minimal n such that R_n requires attention. If there is no such n, then let $G(z_s) = 1$. Otherwise, we say that R_n *receives* attention. Moreover, if $R_n = L_e$ then let $G(z_s) = 0$. If $R_n = G_e$ then let $G \restriction z_{t+1} = fill_1((G \restriction z_s) f_e(G \restriction z_s), t)$, where z_t is the greatest element in $dom((G \restriction z_s) f_e(G \restriction z_s))$ and for a finite function σ and a number k, $fill_1(\sigma, k) = \sigma \cup \{(x, 1) : x \leq z_k \ \& \ x \notin dom(\sigma)\}$.

This completes the construction of G.

It is easy to verify that the set G constructed above is both $\mathbf{P}$-levelable and F-generic, the details are omitted here.

2. For a general A-generic set G, by Theorem 6.1.9, G is $\mathbf{P}$-immune. By Theorem 6.1.7, G is F-generic. Hence, G is F-generic but not $\mathbf{P}$-levelable.

3. Let $A \in \mathbf{E}$ be a $\mathbf{P}$-levelable set and $G = \{z_{2n+1} : z_n \in A\} \cup \{z_{2n} : n \in N\}$. Then G is $\mathbf{P}$-levelable and, by Theorem 6.1.10, G is not L-generic.

4. Let $A \in \mathbf{E}$ be a $\mathbf{P}$-immune set and $G = \{z_{2n+1} : z_n \in A\} \cup \{z_{2n} : n \in N\}$. Then G is not $\mathbf{P}$-levelable and, by Theorem 6.1.10, G is not L-generic. ■

Corollary 6.1.18 *The class of* $\mathbf{P}$*-levelable sets is neither meager nor comeager in the sense of resource bounded Fenner and Lutz categories.*

Proof. This follows from Theorem 6.1.17. ■

6.2 Genericity versus Polynomial Time Unsafe Approximations

Definition 6.2.1 *(Duris and Rolim [32] and Yesha [116]) A* polynomial time unsafe approximation *of a set A is a set $B \in \mathbf{P}$. The set $A\Delta B$ is called the* error *set of the approximation. Let f be an unbounded function on the natural numbers. A set A is* Δ-levelable with density f *if, for any set $B \in \mathbf{P}$, there is another set $B' \in \mathbf{P}$ such that*

$$\|(A\Delta B)\upharpoonright z_n\| - \|(A\Delta B')\upharpoonright z_n\| \geq f(n)$$

for almost all $n \in N$. A set A is Δ-levelable *if A is Δ-levelable with density f for some unbounded function f on the natural numbers.*

Definition 6.2.2 *(Ambos-Spies [4]) A polynomial time unsafe approximation B of a set A is* optimal *if, for any approximation $B' \in \mathbf{P}$ of A,*

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

A set A is weakly Δ-levelable *if, for any polynomial time unsafe approximation B of A, there is another polynomial time unsafe approximation B' of A such that*

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

It should be noted that our above definitions are a little different from the original definitions of Ambos-Spies [4], Duris and Rolim [32], and Yesha [116]. In the original definitions, they considered the errors on strings up to certain length (i.e. $\|(A\Delta B)^{\leq n}\|$) instead of errors on strings up to z_n (i.e. $\|(A\Delta B)\upharpoonright z_n\|$). But it is easy to check that all our results except Theorem 6.3.8 in this thesis hold for the original definitions also.

Lemma 6.2.3 *(Ambos-Spies [4])*

1. *A set A is weakly Δ-levelable if and only if A does not have an optimal polynomial time unsafe approximation.*

2. If a set A is Δ-levelable then it is weakly Δ-levelable.

Lemma 6.2.4 *Let A, B be two sets such that A is Δ-levelable with linear density and $A\Delta B$ is sparse. Then B is Δ-levelable with linear density.*

Proof. Let p be a polynomial such that, for all n, $\|(A\Delta B)^{\leq n}\| \leq p(n)$, and assume that A is Δ-levelable with density αn ($\alpha > 0$). Then there is a real number $\beta > 0$ such that, for large enough n, $\alpha n - 2p(1 + [\log n]) > \beta n$. We will show that B is Δ-levelable with density βn.

Now, given any set $C \in \mathbf{P}$, by Δ-levelability of A, choose $D \in \mathbf{P}$ such that

$$\|(A\Delta C)\restriction z_n\| > \|(A\Delta D)\restriction z_n\| + \alpha n$$

for almost all n. Then

$$\begin{aligned} \|(B\Delta C)\restriction z_n\| &\geq \|(A\Delta C)\restriction z_n\| - p(1 + [\log n]) \\ &> \|(A\Delta D)\restriction z_n\| + \alpha n - p(1 + [\log n]) \\ &\geq \|(B\Delta D)\restriction z_n\| + \alpha n - 2p(1 + [\log n]) \\ &> \|(B\Delta D)\restriction z_n\| + \beta n \end{aligned}$$

for almost all n. Hence, B is Δ-levelable with density βn. ■

Theorem 6.2.5 *1. There exists a set G in $\mathbf{E}_2$, which is both A-generic and Δ-levelable.*

2. There exists a set G in $\mathbf{E}_2$, which is A-generic, but not weakly Δ-levelable.

Proof. 1. Duris and Rolim [32] constructed a set A in $\mathbf{E}$ which is Δ-levelable with linear density and, in [9], Ambos-Spies et al. showed that, for any set $B \in \mathbf{E}$, there is an A-generic set B' in $\mathbf{E}_2$ such that $B\Delta B'$ is sparse. So, for any set A which is Δ-levelable with linear density, there is an A-generic set G in $\mathbf{E}_2$ such that $A\Delta G$ is sparse. It follows from Lemma 6.2.4 that G is Δ-levelable with linear density.

2. Ambos-Spies [4, Theorem 3.3] constructed a $\mathbf{P}$-bi-immune set in $\mathbf{E}$ which is not weakly Δ-levelable. In his proof, he used the requirements

$BI_{2e} : P_e \subseteq G \Rightarrow P_e$ is finite

$BI_{2e+1} : P_e \subseteq \bar{G} \Rightarrow P_e$ is finite

to ensure that the constructed set G is $\mathbf{P}$-bi-immune. In order to guarantee that G is not weakly Δ-levelable, he used the requirements

$R : \forall e \in N\ \forall n \in N\ (\|(G\Delta B)\restriction z_n\| \leq \|(G\Delta P_e)\restriction z_n\| + e + 1)$

to ensure that $B = \cup_{i\geq 0}\Sigma^{[2i]}$ will be an optimal unsafe approximation of G. If we change the requirements BI_{2e} and BI_{2e+1} to the requirements

R_e : If $f_e \in \mathbf{F}_1$ is dense along G, then G meets f_e

then a routine modification of the finite injury argument in the proof of Ambos-Spies [4, Theorem 3.3] can be used to construct an A-generic set G in $\mathbf{E}_2$ which is not weakly Δ-levelable. The details are omitted here. ■

Corollary 6.2.6 *The class of (weakly) Δ-levelable sets is neither meager nor comeager in the sense of resource bounded Ambos-Spies category.*

Corollary 6.2.6 shows that the class of weakly Δ-levelable sets is neither large nor small in the sense of resource bounded Ambos-Spies category. However, as we will show next, it is large in the sense of resource bounded general Ambos-Spies category, resource bounded Fenner category and resource bounded Lutz category.

Theorem 6.2.7 *Let G be a Lutz n^3-generic set. Then G is weakly Δ-levelable.*

Proof. Let $B \in \mathbf{P}$. We show that $\bar{B}$ witnesses that the unsafe approximation B of G is not optimal. For any string x, define $f(x) = y$, where $|y| = |x|^2$ and $y[j] = 0$ if and only if $z_{|x|+j} \in B$. Obviously, f is computable in time n^3. Because G is Lutz n^3-generic, G meets f infinitely often. Hence, for any k and n_0, there exists $n > n_0$ such that $n^2 - 2n > k$ and, for all strings x with $z_n \leq x < z_{n^2}$, $x \in G$ if and only if $x \in \bar{B}$. Hence

$$\begin{aligned} \|(G\Delta B)\restriction z_{n^2}\| &\geq n^2 - n \\ &> n + k \\ &\geq \|(G\Delta \bar{B})\restriction z_{n^2}\| + k, \end{aligned}$$

which implies that G is weakly Δ-levelable. ■

Corollary 6.2.8 *The class of weakly Δ-levelable sets is comeager in the sense of resource bounded Lutz, Fenner and general Ambos-Spies categories.*

Proof. This follows from Theorem 6.1.7, Theorem 6.1.8 and Theorem 6.2.7. ■

Now we show that the class of Δ-levelable sets is neither meager nor comeager in the sense of all these resource bounded categories we have discussed above.

Theorem 6.2.9 *There exists a set G in $\mathbf{E}_2$, which is both general A-generic and Δ-levelable.*

Proof. Let $\delta(0) = 0, \delta(n+1) = 2^{2^{\delta(n)}}$. For each set $P_e \in \mathbf{P}$, let $P_{g(e)}$ be defined in such a way that

$$P_{g(e)}(x) = \begin{cases} 1 - P_e(x) & \text{if } x = 0^{\delta(<e,n>)} \text{ for some } n \in N \\ P_e(x) & \text{otherwise} \end{cases}$$

In the following we construct a general A-generic set G, which is Δ-levelable by keeping $P_{g(e)}$ to witness that the unsafe approximation P_e of G is not optimal. Let $\{f_i : i \in N\}$ be an enumeration of all functions in $\mathbf{F}_2$.

The set G is constructed in stages. To ensure that G is general A-generic, it suffices to meet for all $e \in N$ the following requirements:

G_e : If f_e is dense along G then G meets f_e.

To ensure that G is Δ-levelable, it suffices to meet for all $e, k \in N$ the following requirements

$L_{<e,k>} : \exists n_1 \in N\ \forall n > n_1\ (\|(G \Delta P_e)\restriction z_n\| > \|(G \Delta P_{g(e)})\restriction z_n\| + k)$.

The strategy for meeting a requirement G_e is as follows: At stage s, if G_e has not been satisfied yet and $f_e(G\restriction z_s)$ is defined, then let G extend $(G\restriction z_s)f_e(G\restriction z_s)$. But this action may injure the satisfaction of some requirements $L_{<i,k>}$ and G_m. The conflict is solved by delaying the action until it will not injure the satisfaction of the requirements $L_{<i,k>}$ and G_m which have higher priority than G_e.

The strategy for meeting a requirement $L_{<e,k>}$ is as follows: At stage s, if $L_{<e,k>}$ has not been satisfied yet and $P_e(z_s) \neq P_{g(e)}(z_s)$, then let $G(z_s) = P_{g(e)}(z_s)$. When a requirement G_e becomes satisfied at some stage, it is satisfied forever. So $L_{<e,k>}$ can only be injured finitely often and then it will have chance to become satisfied forever.

Stage s.
In this stage, we define the value of $G(z_s)$.
A requirement G_n *requires* attention if

1. $n < s$.

2. G_n has not been satisfied yet, that is to say, there is no $t < s$ such that $G\restriction z_s$ extends $(G\restriction z_t)f(G\restriction z_t)$.

3. There exists $t \leq s$ such that

   A. $f_n(G\restriction z_t)$ is defined.

   B. $G\restriction z_s$ is consistent with $(G\restriction z_t)f_n(G\restriction z_t)$.

   C. For all $e, k \in N$ such that $< e, k >< n$, there is at most one $m \in N$ such that $0^{\delta(<e,m>)} \in dom((G\restriction z_t)f_n(G\restriction z_t))$.

   D. For all $e, k \in N$ such that $< e, k >< n$,

$$\|(G \Delta P_e)\restriction z_s\| - \|(G \Delta P_{g(e)})\restriction z_s\| > k + n \tag{6.1}$$

Fix the minimal m such that G_m requires attention, and fix the minimal t in the above item 3 corresponding to the requirement G_m. If there is no such m then let $G(z_s) = 1 - P_e(z_s)$ if $z_s = 0^{\delta(<e,n>)}$ for some $e, n \in N$ and let $G(z_s) = 0$ otherwise. Otherwise we say that G_m *receives* attention. Moreover, let

$$G(z_s) = \begin{cases} ((G\restriction z_t)f_m(G\restriction z_t))(z_s) & \text{if } z_s \in dom((G\restriction z_t)f_m(G\restriction z_t)) \\ 1 - P_e(z_s) & \text{if } z_s \notin dom((G\restriction z_t)f_m(G\restriction z_t))\ \&\ z_s = 0^{\delta(<e,n>)} \text{ for some } e, n \\ 0 & \text{otherwise} \end{cases}$$

This completes the construction.

We show that all requirements are met by proving a sequence of claims.

Claim 1 *Every requirement G_n requires attention at most finitely often.*

Proof. The proof is by induction. Fix n and assume that the claim is correct for all numbers less than n. Then there is a stage s_0 such that no requirement G_m with $m < n$ requires attention after stage s_0. So G_n receives attention at any stage $s > s_0$ at which it requires attention. Hence if G_n requires attention infinitely often, then it will be satisfied at some stage and stops requiring attention. □

Claim 2 *Given $n_0 \in N$, if no requirement G_n ($n < n_0$) requires attention after stage s_0 and G_{n_0} requires attention at stage s_0, then for all $< e, k >< n_0$ and $s > s_0$,*

$$\|(G \Delta P_e) \restriction z_s\| - \|(G \Delta P_{g(e)}) \restriction z_s\| > k + n_0 - 1$$

Proof. Straightforward from the construction. □

Claim 3 *Every requirement G_n is met.*

Proof. For a contradiction, fix the minimal n such that G_n is not met. Then f_n is dense along G. We have to show that R_n requires attention infinitely often which is contrary to Claim 1. Since $\|P_e \Delta P_{g(e)}\| = \infty$ for all $e \in N$, by the construction and Claim 2, there will be a stage s_0 such that at all stages $s > s_0$, (6.1) holds for all $e, k \in N$ such that $< e, k >< n$. Hence G_n requires attention at each stage $s > s_0$ at which $f_n(G \restriction z_s)$ is defined. □

Claim 4 *Every requirement $L_{<e,k>}$ is met.*

Proof. This follows from Claim 1 and Claim 2. □

Now we show that G is both A-generic and Δ-levelable. G is A-generic since all requirements G_n are met. For $< e, k >\in N$, let $n_{<e,k>}$ be the least number s_0 such that for all $s > s_0$,

$$\|(G \Delta P_e) \restriction z_s\| > \|(G \Delta P_{g(e)}) \restriction z_s\| + k$$

and let

$$f(n) = \mu k(\forall e \leq k \ (n \geq n_{<e,k>})).$$

Then $f(n)$ is unbounded and, for all $e \in N$,

$$\|(G \Delta P_e) \restriction z_n\| \geq \|(G \Delta P_{g(e)}) \restriction z_n\| + f(n) \ \ a.e.$$

That is to say, G is Δ-levelable with density f. ■

Theorem 6.2.10 *There exists a set G in $\mathbf{E}_2$, which is general A-generic but not Δ-levelable.*

Proof. As in the previous proof, a set G is constructed in stages. To ensure that G is general A-generic, it suffices to meet for all $e \in N$ the following requirements:

G_e : If f_e is dense along G then G meets f_e.

Fix a set $B \in \mathbf{P}$. Then the requirements

$NL_{<e,k>} : P_e \Delta B$ infinite $\Rightarrow \exists n\ (\|(G\Delta P_e)\restriction z_n\| - \|(G\Delta B)\restriction z_n\| \geq k)$

will ensure that B witnesses the failure of Δ-levelability of G.

To meet the requirements G_e, we use the strategy in Theorem 6.2.9. The strategy for meeting a requirement $NL_{<e,k>}$ is as follows: At stage s such that $P_e(z_s) \neq B(z_s)$ and $\|(G\Delta P_e)\restriction z_n\| - \|(G\Delta B)\restriction z_n\| < k$ for all $n < s$, let $G(z_s) = B(z_s)$. If $P_e \neq^* B$, this action can be repeated over and over again. Hence $\|G\Delta P_e\|$ is growing more quickly than $\|G\Delta B\|$ and eventually the requirement $NL_{<e,k>}$ is met at some sufficiently large stage.

Define a priority ordering of the requirements by letting $R_{2n} = G_n$ and $R_{2<e,k>+1} = NL_{<e,k>}$. We now describe the construction of G formally.

Stage s.

In this stage, we define the value of $G(z_s)$.

A requirement $NL_{<e,k>}$ *requires* attention if $< e, k >< s$ and

1. $P_e(z_s) \neq B(z_s)$.
2. $\|(G\Delta P_e)\restriction z_n\| - \|(G\Delta B)\restriction z_n\| < k$ for all $n < s$.

A requirement G_n *requires* attention if

1. $n < s$.
2. G_n has not been satisfied yet, that is to say, there is no $t < s$ such that $G\restriction z_s$ extends $(G\restriction z_t)f_n(G\restriction z_t)$.
3. There exists $t \leq s$ such that

   A. $f_n(G\restriction z_t)$ is defined.

   B. $G\restriction z_s$ is consistent with $(G\restriction z_t)f_n(G\restriction z_t)$.

   C. There is no $e, k \in N$ such that

   (1). $< e, k >< n$.

   (2). $\forall u < s\ (\|(G\Delta P_e)\restriction z_u\| - \|(G\Delta B)\restriction z_u\| < k)$.

   (3). There exists $y \in dom((G\restriction z_t)f_n(G\restriction z_t)) - dom(G\restriction z_t)$ such that $P_e(y) \neq B(y)$.

Fix the minimal m such that R_m requires attention. If there is no such m, let $G(z_s) = B(z_s)$. Otherwise we say that R_m *receives* attention. Moreover, if $R_m = NL_{<e,k>}$ then let $G(z_s) = B(z_s)$. If $R_m = G_n$ then fix the least t in the above item 3 corresponding to the requirement G_n. Let $G(z_s) = ((G\restriction z_t)f_n(G\restriction z_t))(z_s)$ if $z_s \in dom((G\restriction z_t)f_n(G\restriction z_t))$ and let $G(z_s) = B(z_s)$ otherwise.

This completes the construction of G.

It suffices to show that all requirements are met. Note that, by definition of requiring attention, R_m is met if and only if R_m requires attention at most finitely often. So, for a contradiction, fix the minimal m such that R_m requires attention infinitely often. By minimality of m, fix a stage s_0 such that no requirement $R_{m'}$ with $m' < m$ requires attention after stage s_0. Then R_m receives attention at any stage $s > s_0$ at which R_m requires attention. Now, we first assume that $R_m = G_n$. Then at some stage $s > s_0$, G_n receives attention and become satisfied forever. Finally assume that $R_m = NL_{<e,k>}$. Then $B\Delta P_e$ is infinite and, at all stages $s > s_0$ such that $B(z_s) \neq P_e(z_s)$, the requirement $NL_{<e,k>}$ receives attention, hence $G(z_s) = B(z_s)$. Since, for all other stages s with $s > s_0$, $B(z_s) = P_e(z_s)$, $G\Delta P_e$ grows more rapidly than $G\Delta B$, hence

$$\lim_n (\|(G\Delta P_e)\restriction z_n\| - \|(G\Delta B)\restriction z_n\|) = \infty$$

and $NL_{<e,k>}$ is met contrary to assumption. ■

Corollary 6.2.11 *The class of Δ-levelable sets is neither meager nor comeager in the sense of resource bounded general Ambos-Spies, Lutz and Fenner categories.*

Proof. Follows from Theorem 6.1.7, Theorem 6.2.9 and Theorem 6.2.10. ■

6.3 Resource Bounded Measure versus Polynomial Time Approximations

The relation between p-measure and the class of $\mathbf{P}$-levelable sets is characterized by the following theorem.

Theorem 6.3.1 *(Mayordomo [75]) The class of $\mathbf{P}$-bi-immune sets has p-measure 1.*

Corollary 6.3.2 *The class of $\mathbf{P}$-levelable sets has p-measure 0.*

Corollary 6.3.3 *The class of sets which possess optimal polynomial time safe approximations has p-measure 1.*

Corollary 6.3.4 *For each p-random set A, A has an optimal polynomial time safe approximation.*

Now we turn our attention to the relations between p-randomness concept and the concept of polynomial time unsafe approximations. In our following proof, we will use the law of the iterated logarithm for p-random sequences (see Theorem 5.3.6). So it is more convenient to identify a set with its characteristic sequence. The symmetric difference of two sets can be characterized by the parity function on sequences.

Definition 6.3.5 *1. The parity function $\oplus : \Sigma \times \Sigma \to \Sigma$ on bits is defined by*

$$b_1 \oplus b_2 = \begin{cases} 0 & \text{if } b_1 = b_2 \\ 1 & \text{otherwise} \end{cases}$$

where $b_1, b_2 \in \Sigma$.

2. The parity function $\oplus : \Sigma^\infty \times \Sigma^\infty \to \Sigma^\infty$ on sequences is defined by $(\xi \oplus \eta)[n] = \xi[n] \oplus \eta[n]$.

3. *The parity function $\oplus : \Sigma^* \times \{f : f$ is a partial function from Σ^* to $\Sigma\} \to \Sigma^*$ on strings and functions is defined by $x \oplus f = b_0 \cdots b_{|x|-1}$ where $b_i = x[i] \oplus f(x[0..i-1])$ if $f(x[0..i-1])$ is defined and $b_i = \lambda$ otherwise.*

4. *The parity function $\oplus : \Sigma^\infty \times \{f : f$ is a partial function from Σ^* to $\Sigma\} \to \Sigma^* \cup \Sigma^\infty$ on sequences and functions is defined by $\xi \oplus f = b_0 b_1 \cdots$ where $b_i = \xi[i] \oplus f(\xi[0..i-1])$ if $f(\xi[0..i-1])$ is defined and $b_i = \lambda$ otherwise.*

The intuitive meaning of $\xi \oplus f$ is as follows: Given a sequence ξ and a number $n \in N$ such that $f(\xi[0..n-1])$ is defined, we use f to predict the value of $\xi[n]$ from the first n bits $\xi[0..n-1]$. If the prediction is successful, then output 0, else output 1. And $\xi \oplus f$ is the output sequence.

At first, we explain a useful technique which is similar to the invariance property of p-random sequences (see Theorem 5.2.9).

Lemma 6.3.6 *(cf. Theorem 5.2.9) Let $\xi \in \Sigma^\infty$ be n^k-random and $f : \Sigma^* \to \Sigma$ be a partial function computable in time n^k such that $\xi \oplus f$ is an infinite sequence. Then $\xi \oplus f$ is n^{k-1}-random.*

Proof. For a contradiction assume that $\xi \oplus f$ is not n^{k-1}-random and let $F : \Sigma^* \to Q^+$ be an n^{k-1}-martingale that succeeds on $\xi \oplus f$. Define $F' : \Sigma^* \to Q^+$ by letting $F'(x) = F(x \oplus f)$ for all $x \in \Sigma^*$. It is a routine to check that F' is an n^k-martingale. Moreover, since F succeeds on $\xi \oplus f$, F' succeeds on ξ. A contradiction with the hypothesis that ξ is n^k-random. ■

Lemma 6.3.7 *Let k be the number in Corollary 5.3.7, and let $A, B, C \subseteq \Sigma^*$ be three sets such that the following conditions hold.*

1. *$B, C \in \mathbf{P}$.*

2. *$\|B \Delta C\| = \infty$.*

3. *There exists $c \in N$ such that, for almost all n,*

$$\|(A\Delta C)\restriction z_n\| - \|(A\Delta B)\restriction z_n\| \geq -c. \tag{6.2}$$

Then A is not n^{k+1}-random.

Proof. Let α, β and γ be the characteristic sequences of A, B and C, respectively.

By Lemma 6.3.6, it suffices to define an n^2-time computable partial function $f : \Sigma^* \to \Sigma$ such that $\alpha \oplus f$ is an infinite sequence which is not n^k-random. Define the function f by

$$f(x) = \begin{cases} \beta[|x|] & \text{if } \beta[|x|] \neq \gamma[|x|] \\ \text{undefined} & \text{if } \beta[|x|] = \gamma[|x|] \end{cases}$$

Then f is n^2-time computable and, since $\|B\Delta C\| = \infty$, $\alpha \oplus f$ is an infinite sequence. In order to show that $\alpha \oplus f$ is not n^k-random, we show that $\alpha \oplus f$ does not satisfy the law of the iterated logarithm.

At first, we show that, for all $n \in N^+$, the following equation holds.

$$\sum_{i=0}^{n-1}(\alpha \oplus \gamma)[i] - \sum_{i=0}^{n-1}(\alpha \oplus \beta)[i] = l_n - 2\sum_{i=0}^{l_n-1}(\alpha \oplus f)[i] \tag{6.3}$$

where $l_n = |\alpha[0..n-1] \oplus f|$.

Let

$$a(n) = \|\{i < n : \alpha[i] \neq \gamma[i] = \beta[i]\}\|$$

$$b(n) = \|\{i < n : \alpha[i] \neq \gamma[i] \neq \beta[i]\}\|$$

$$c(n) = \|\{i < n : \alpha[i] = \gamma[i] \neq \beta[i]\}\|$$

$$d(n) = \|\{i < n : \alpha[i] = \gamma[i] = \beta[i]\}\|$$

Then

$$\begin{array}{rcl}
\sum_{i=0}^{n-1}(\alpha \oplus \gamma)[i] & = & a(n) + b(n) \\
\sum_{i=0}^{n-1}(\alpha \oplus \beta)[i] & = & a(n) + c(n) \\
l_n & = & b(n) + c(n) \\
\sum_{i=0}^{l_n-1}(\alpha \oplus f)[i] & = & c(n)
\end{array}$$

Obviously, this implies (6.3).

The condition (6.2) is equivalent to

$$\sum_{i=0}^{n-1}(\alpha \oplus \gamma)[i] - \sum_{i=0}^{n-1}(\alpha \oplus \beta)[i] \geq -c$$

So, by (6.3),

$$l_n - 2\sum_{i=0}^{l_n-1}(\alpha \oplus f)[i] \geq -c \tag{6.4}$$

for almost all n, where $l_n = |\alpha[0..n-1] \oplus f|$. By (6.4),

$$\liminf_{n\to\infty} \frac{n - 2\sum_{i=0}^{n-1}(\alpha \oplus f)[i]}{\sqrt{2n \ln \ln n}} \geq 0.$$

Hence, by Corollary 5.3.7, $\alpha \oplus f$ is not n^k-random. This completes the proof. ■

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

Theorem 6.3.8 *The class of* Δ*-levelable sets has p-measure* 0*.*

Proof. Let A be a Δ-levelable set. Then there is an unbounded function $f(n) \geq 0$ and polynomial time computable sets B, C such that for all n,

$$\|(A\Delta C){\restriction}z_n\| - \|(A\Delta B){\restriction}z_n\| \geq f(n).$$

By Lemma 6.3.7, A is not n^{k+1}-random, where k is the number in Corollary 5.3.7. So the theorem follows from Theorem 5.1.12. ■

Theorem 6.3.9 *The class of sets which have optimal polynomial time unsafe approximations has p-measure* 0*.*

Proof. If A has an optimal polynomial time unsafe approximation, then there is a polynomial time computable set B and a number $c \in N$ such that, for all n,

$$\|(A\Delta B){\restriction}z_n\| - \|(A\Delta \bar{B}){\restriction}z_n\| < c$$

I.e.

$$\|(A\Delta \bar{B}){\restriction}z_n\| - \|(A\Delta B){\restriction}z_n\| > -c$$

By Lemma 6.3.7, A is not n^{k+1}-random, where k is the number in Corollary 5.3.7. So the theorem follows from Theorem 5.1.12. ■

Corollary 6.3.10 *The class of sets which are weakly Δ-levelable but not Δ-levelable has p-measure* 1*.*

Corollary 6.3.11 *Every p-random set is weakly Δ-levelable but not Δ-levelable.*

Chapter 7

NP-hard Sets Are Superterse unless NP Is Small

7.1 Introduction

One of the important questions in computational complexity theory is whether every **NP** problem is solvable by polynomial time circuits, i.e., **NP** $\subseteq ?\mathbf{P}/poly$. Furthermore, it has been asked what the deterministic time complexity of **NP** is if **NP** $\subseteq$ **P**$/poly$. That is, if **NP** is easy in the nonuniform complexity measure, how easy is **NP** in the uniform complexity measure? It is well known that $\mathbf{P}_T(\mathbf{SPARSE}) = \mathbf{P}/poly$, where $\mathbf{P}_T(\mathbf{SPARSE})$ is the class of languages that are polynomial time Turing reducible to some sparse sets. Hence the above question is equivalent to the following question.

$$\mathbf{NP} \subseteq ?\mathbf{P}_T(\mathbf{SPARSE}).$$

It has been shown by Wilson [114] that this question is oracle dependent. Hence it seems difficult to give an absolute answer to this question at present. In the past, many efforts have been made to consider the question whether **NP** is not included in some subclasses of $\mathbf{P}_T(\mathbf{SPARSE})$. Since $\mathbf{P}_T(\mathbf{SPARSE})$ is the class of languages that are Turing reducible to some sparse sets, one way of obtaining subclasses of $\mathbf{P}_T(\mathbf{SPARSE})$ is to consider some restrictions on the reducibility. For example, Mahaney [73] showed that if all **NP** sets are many-one reducible to some sparse set, then **P** = **NP**. Subsequently this result was improved by Ogihara and Watanabe [82] to truth-table reducibility with a constant number of queries, i.e.,

$$\mathbf{NP} \neq \mathbf{P} \Rightarrow \mathbf{NP} \not\subseteq \mathbf{P}_{btt}(\mathbf{SPARSE}).$$

Other subclasses of $\mathbf{P}_T(\mathbf{SPARSE})$ are obtained by considering the **P**-selective sets introduced by Selman [91]. A set A is **P**-selective if there exists a polynomial time computable function that selects one of two given input strings such that if any one of the two strings is in A, then so is the selected one. Let **SELECT** denote the class of **P**-selective sets. Then we know the following facts:

1. (Selman and Ko (see [95])) $\mathbf{P}_T(\mathbf{SPARSE}) = \mathbf{P}_T(\mathbf{SELECT})$.

2. (Watanabe [109]) $\mathbf{P}_T(\mathbf{SELECT}) \not\subseteq \mathbf{P}_{tt}(\mathbf{SELECT})$.

Regarding our above question, the following results are known:

1. (Selman [91]) If $\mathbf{P} \neq \mathbf{NP}$, then $\mathbf{NP} \not\subseteq \mathbf{P}_m(\mathbf{SELECT})$.
2. (Agrawal and Arvind [1], Beigel, Kummer and Stephan [15], Ogihara [81]) If $\mathbf{P} \neq \mathbf{NP}$, then $\mathbf{NP} \not\subseteq \mathbf{P}_{n^\alpha\text{-}tt}(\mathbf{SELECT})$ for all $\alpha < 1$.
3. (Beigel [14]) If $\mathbf{P} \neq \mathbf{UP}$ or $\mathbf{R} \neq \mathbf{NP}$, then $\mathbf{NP} \not\subseteq \mathbf{P}_{tt}(\mathbf{SELECT})$

It seems difficult to remove the condition $\alpha < 1$ in the item 2. In the following, however, we will remove this condition under a stronger but reasonable hypothesis. We show that

$$\mu_p(\mathbf{NP}) \neq 0 \Rightarrow \mathbf{NP} \not\subseteq \mathbf{P}_{tt}(\mathbf{SELECT}).$$

Many evidences have been presented by Lutz and Mayordomo [71] and Kautz and Miltersen [46] that this stronger hypothesis is reasonable. For example, the following results are known:

1. (Lutz and Mayordomo [70]) If $\mu_p(\mathbf{NP}) \neq 0$, then there exists an **NP** search problem which is not reducible to the corresponding decision problem.
2. (Lutz and Mayordomo [70]) If $\mu_p(\mathbf{NP}) \neq 0$, then the "Cook versus Karp-Levin" conjecture holds for **NP**.
3. (Lutz and Mayordomo [71]) If $\mu_p(\mathbf{NP}) \neq 0$, then, for every real number $\alpha < 1$, every $\leq^p_{n^\alpha\text{-}tt}$-hard language for **NP** is dense.
4. (Kautz and Miltersen [46]) For a Martin-Löf random language A, $\mu_p^A(\mathbf{NP}^A) \neq 0$.

We also give a partial affirmative answer to a conjecture by Beigel, Kummer and Stephan [15]. They conjectured that every $\leq^p_{tt}$-hard set for **NP** is **P**-superterse unless $\mathbf{P} = \mathbf{NP}$. We will prove that every $\leq^p_{tt}$-hard set for **NP** is **P**-superterse unless **NP** has p-measure 0.

7.2 Resource Bounded Measure and Polynomial Time Membership Comparable Sets

Jockusch [40] defined a set A to be *semirecursive* if there is a recursive function f such that for all x and y,

1. $f(x, y) \in \{x, y\}$.
2. If $\{x, y\} \cap A \neq \emptyset$, then $f(x, y) \in A$.

We call the function f a *selector* for A. Selman [91] considered a polynomial time version of semirecursive sets and defined a set A to be $\mathbf{P}$-*selective* if A has a polynomial time computable selector. $\mathbf{P}$-selective sets have been widely studied, see, e.g., [1, 15, 81].

For a set A, we identify A and its characteristic function. Let f be a selector for A. If f maps a pair (x, y) to y, then we have "$x \in A \rightarrow y \in A$", equivalently, "$A(x)A(y) \neq 10$". Thus we can view a selector for A as a function f that maps every pair (x, y) of strings to a string $z \in \{01, 10\}$ such that $A(x)A(y) \neq z$. By replacing pairs of strings by k-tuples of strings for any number $k \geq 1$, we obtain the concept of an approximable set. A set A is *approximable* if there exists some $k > 0$ and a polynomial time computable function f such that for all $x_0, \cdots, x_{k-1} \in \Sigma^*$, $f(x_0, \cdots, x_{k-1}) \neq A(x_0) \cdots A(x_{k-1})$. A further extension of this concept, namely membership comparability, was introduced by Ogihara [81]. Here the length of the tuples is not fixed but it may vary depending on the maximum length of the strings contained in the tuples.

Definition 7.2.1 *(Beigel [15]) Given a number $k \in N^+$, a set A is* $\mathbf{P}$-approximable via *k if there is a polynomial time computable function $f : \prod_{i=0}^{k-1} \Sigma^* \rightarrow \Sigma^k$ such that for all $x_0, \cdots, x_{k-1} \in \Sigma^*$, $f(x_0, \cdots, x_{k-1}) \neq A(x_0) \cdots A(x_{k-1})$. A set A is* $\mathbf{P}$-approximable *if A is* $\mathbf{P}$-approximable *via some $k \in N^+$. A set A is* $\mathbf{P}$-superterse *if A is not $\mathbf{P}$-approximable.*

Note that the above definition of a $\mathbf{P}$-approximable set is a little different from Beigel's [12] original definition.

Definition 7.2.2 *(Ogihara [81]) Let $g : N \rightarrow N^+$ be a nondecreasing, polynomial time computable and polynomial bounded function.*

1. *A function f is called a* g-membership comparing function *(a* g-mc-function *for short) for A if, for all $m \in N^+$ and all $x_0, \cdots, x_{m-1} \in \Sigma^*$ with $m \geq g(\max\{|x_0|, \cdots, |x_{m-1}|\})$,*

$$f(x_0, \cdots, x_{m-1}) \in \Sigma^m \text{ and } A(x_0) \cdots A(x_{m-1}) \neq f(x_0, \cdots, x_{m-1}).$$

2. *A set A is polynomial time* g-membership comparable *if there exists a polynomial time computable g-mc-function for A.*

3. *$\mathbf{P}$-mc(g) denotes the class of all polynomial time g-membership comparable sets.*

The following proposition is obvious from the definition.

Proposition 7.2.3 1. *If A is $\mathbf{P}$-selective, then A is $\mathbf{P}$-approximable.*

2. *A set A is $\mathbf{P}$-approximable if and only if $A \in \mathbf{P}$-mc(c) for some constant $c \in N$. That is to say,*

$$\mathbf{P}\text{-}appro = \cup_{c \in N} \mathbf{P}\text{-}mc(c),$$

where $\mathbf{P}$-appro is the class of $\mathbf{P}$-approximable sets.

Theorem 7.2.4 *(Ogihara [81]) $\mathbf{P}_{tt}(\mathbf{SELECT}) \subseteq \mathbf{P}$-mc($\mathbf{LOG}$), where $\mathbf{LOG} = \{c \log : c > 0\}$.*

Theorem 7.2.5 *(Ogihara [81])* $\mathbf{P}$-*mc*$(\mathbf{LOG}) \subset \mathbf{P}$-*mc*$(n)$.

The next proposition gives an important property of **P**-approximable sets which we need latter. If A is **P**-approximable then, for strings $x_0, \cdots, x_{s-1} \in \Sigma^*$, we can compute in polynomial time a subset of Σ^s which contains $A(x_0) \cdots A(x_{s-1})$.

Proposition 7.2.6 *(Beigel [12, 13]) If A is* **P**-*approximable via $k \in N^+$, then there is a polynomial time computable function which computes for any s strings $x_0, \cdots x_{s-1}$ a set of at most*

$$S(s,k) = \binom{s}{0} + \binom{s}{1} + \cdots \binom{s}{k-1}$$

elements from Σ^s which contains $A(x_0) \cdots A(x_{s-1})$. (Note that, for a fixed k, $S(s,k)$ is a polynomial in s of degree $k-1$).

Let $\mathbf{P}_{tt}(\mathbf{P}$-*appro*$)$ be the class of sets which can be $\leq^p_{tt}$-reduced to some **P**-approximable sets. Then we have the following theorem.

Theorem 7.2.7 $\mathbf{P}_{tt}(\mathbf{P}$-*appro*$) \subseteq \mathbf{P}$-*mc*$(n)$.

Remark. In fact, Theorem 7.2.7 is a corollary of Corollary 2.7 in Beigel et al. [15]. For the reason of completeness, we will give the proof here. The idea underlying the following proof is the same as that underlying the proof of Theorem 3.3 in Ogihara [81].

Proof. Let A be a **P**-approximable set via $k \in N$, and let $L \leq^p_{tt} A$ via a machine M. Assume that the number of queries in the reduction $L \leq^p_{tt} A$ is bounded by the polynomial f. Now, to show that $L \in \mathbf{P}$-mc(n), fix $n \in N$ and $x_0, \cdots x_{n-1} \in \Sigma^*$ such that $n \geq \max\{|x_0|, \cdots, |x_{n-1}|\}$. We have to compute a string $g(x_0, \cdots, x_{n-1})$ of length n in polynomial time such that $L(x_0) \cdots L(x_{n-1}) \neq g(x_0, \cdots, x_{n-1})$. For each $i < n$, let Q_i denote the set of queries of M on x_i, and $Q = Q_0 \cup \cdots \cup Q_{n-1}$. Since f is nondecreasing, $\|Q_i\| \leq f(n)$. So, for sufficiently large n,

$$\|Q\|^k \leq (nf(n))^k < 2^n.$$

By Lemma 7.2.6, we can compute, in time polynomial in $\sum_{y \in Q} |y|$, and thus, in time polynomial in n, a set $R = \{z : z \in \Sigma^{\|Q\|}\}$ of at most $\|Q\|^k$ elements which contains the characteristic sequence of A on domain Q. Now, for each $z \in R$ and $j < n$, let $b_{z,j} = M^z(x_j)$. Clearly, there is some $z \in R$ such that, for every $j < n$, $L(x_j) = b_{z,j}$. Since $\|R\| < 2^n$, there is some $v \in \Sigma^n$ such that $v \neq b_{z,0} \cdots b_{z,n-1}$ for all $z \in R$. Let $g(x_0, \cdots, x_{n-1}) = v$. This proves the theorem. ■

In order to prove our main theorem, we prove a lemma at first.

Lemma 7.2.8 *Let $1 < n_1, n_2, \cdots$ be an infinite sequence of numbers such that $n_{i+1} \leq n_i + \log n_i$ for all i. Then* $\lim_{m\to\infty} \prod_{i=1}^m (1 + \dfrac{1}{n_i}) = \infty$.

Proof. By a simple induction, it is easy to check that there exists a number $k \geq 5$ such that $n_i \leq i \log i \log\log i$ for $i \geq k$. Hence

$$\lim_{m\to\infty} \prod_{i=1}^{m} \left(1 + \frac{1}{n_i}\right) \geq \lim_{m\to\infty} \prod_{i=k}^{m} \left(1 + \frac{1}{i \log i \log\log i}\right) = \infty.$$

■

Theorem 7.2.9 *Let A be an n^2-random set. Then $A \notin \mathbf{P}$-mc(n).*

Proof. For a contradiction, assume that f witnesses that A is polynomial time n-membership comparable. In the following, we construct an n^2-martingale F which succeeds on A.

Let $n_i = i$ for $i \leq 5$ and $n_{i+1} = n_i + [\log n_i]$ for $i \geq 5$. For $|x| \leq n_5$, let $F(x) = 1$. For $x \in \Sigma^{n_{i+1}}$ $(i \geq 5)$, fix the initial segment $y \in \Sigma^{n_i}$ of x and let

$$F(x) = \begin{cases} \left(1 + \frac{1}{2^{[\log n_i]-1}}\right) F(y) & \text{if } x \neq yf(z_{n_i}, \cdots, z_{n_{i+1}-1}) \\ 0 & \text{if } x = yf(z_{n_i}, \cdots, z_{n_{i+1}-1}) \end{cases}$$

And, for other $x \in \Sigma^*$ such that $|x| \neq n_i$ $(i \in N)$, we define the value of $F(x)$ as follows.

$$F(x) = \frac{1}{2^k} \sum_{y \in \Sigma^k} F(xy)$$

where k is the least number such that $|x| + k = n_i$ for some $i \in N$.

It is easily verified that the above defined function F is an n^2-martingale. So it suffices to show that F succeeds on A. Obviously, for $i \geq 5$,

$$F(A\restriction z_{n_{i+1}}) = \left(1 + \frac{1}{2^{[\log n_5]} - 1}\right) \cdots \left(1 + \frac{1}{2^{[\log n_i]} - 1}\right) \geq \left(1 + \frac{1}{n_5}\right) \cdots \left(1 + \frac{1}{n_i}\right).$$

By Lemma 7.2.8, $\limsup_i F(A\restriction z_{n_i}) = \infty$, that is to say, F succeeds on A. ■

Corollary 7.2.10 $\mathbf{P}$-*mc*(n) *has p-measure* 0*, i.e.,* $\mu_p(\mathbf{P}\text{-}mc(n)) = 0$.

By combining Theorem 5.1.13 and Corollary 7.2.10, we get

Theorem 7.2.11 $\mathbf{E} \not\subseteq \mathbf{P}_{tt}(\mathbf{P}\text{-}appro)$.

Corollary 7.2.12 *(Toda [96])* $\mathbf{E} \not\subseteq \mathbf{P}_{tt}(\mathbf{SELECT})$.

Note that Toda proved Corollary 7.2.12 using a direct diagonalization. The importance of our Theorem 7.2.9 is that it also has implications on the structure of **NP**. By combining Corollary 7.2.10 and Theorem 7.2.7, we get the following theorem.

Theorem 7.2.13 *If* **NP** *does not have p-measure* 0*, then no* **P***-approximable set is* $\leq_{tt}^{p}$*-hard for* **NP***. That is to say, every* $\leq_{tt}^{p}$*-hard set for* **NP** *is* **P***-superterse unless* $\mu_p(\mathbf{NP}) = 0$.

Corollary 7.2.14 *If* **NP** *does not have p-measure* 0*, then no* **P***-selective set is* $\leq_{tt}^{p}$*-hard for* **NP**.

Remark 1. Recently Buhrman and Longpré [26] independently proved that $\mathbf{P}_{tt}(\mathbf{SELECT})$ has p-measure 0.

Remark 2. Recently Beigel (personal communication) has observed that actually our results can be strengthed as follows:

Observation. If **NP** does not have p-measure 0, then no set in **P**-mc($\sqrt{n}$) is $\leq_{tt}^{p}$-hard for **NP**.

Bibliography

[1] M. Agrawal and V. Arvind. Polynomial time truth-table reductions to **P**-selective sets. In *Proc. 9th Conf. on Structure in Complexity Theory*, pages 24–30. IEEE Computer Society Press, 1994.

[2] E. Allender and M. Strauss. Measure on small complexity classes, with applications for **BPP**. In *Proc. 35th Symp. FOCS*, pages 807–818. IEEE Computer Society Press, 1994.

[3] E. Allender and M. Strauss. Measure on **P**: Robustness of the notion. In *Proc. 20th MFCS 95*, Lecture Notes in Comput. Sci., 969, pages 129–138. Springer Verlag, 1995.

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

[5] K. Ambos-Spies. Resource-bounded genericity. In *Proc. 10th Conf. on Structure in Complexity Theory*, pages 162–181. IEEE Computer Society Press, 1995.

[6] K. Ambos-Spies, H. Fleischhack, and H. Huwig. **P**-generic sets. In *Proc. 11th ICALP*, pages 58–68. Springer Verlag, 1984.

[7] K. Ambos-Spies, H. Fleischhack, and H. Huwig. Diagonalizations over polynomial time computable sets. *Theoret. Comput. Sci.*, 51:177–204, 1987.

[8] K. Ambos-Spies, E. Mayordomo, Y. Wang, and X. Zheng. Resource-bounded balanced genericity, stochasticity and weak randomness. In *Proc. 13rd STACS*, Lecture Notes in Comput. Sci., 1046, pages 63-74. Springer Verlag, 1996.

[9] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn. Genericity and measure for exponential time. In *Proc. 19th MFCS*, Lecture Notes in Comput. Sci., 841, pages 221–232. Springer Verlag, 1994.

[10] 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.

[11] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* Springer Verlag. 1988.

[12] R. Beigel. *Query-limited Reducibilities.* PhD thesis, Stanford University, 1987.

[13] R. Beigel. A structural theorem that depends quantitatively on the complexity of **SAT**. In *Proc. 2nd Conf. on Structure in Complexity Theory*, pages 28–32. IEEE Computer Society Press, 1987.

[14] R. Beigel. **NP**-*hard sets are* **P**-*superterse unless* **R**=**NP**, Tech. Rep. 88-04, Department of Computer Science, The John Hopkins University, 1988.

[15] R. Beigel, M. Kummer, and F. Stephan. Approximable sets. In *Proc. 9th Conf. on Structure in Complexity Theory*, pages 12–23. IEEE Computer Society Press, 1994.

[16] M. Bellare and S. Goldwasser. The complexity of decision versus search. *SIAM J. Comput.*, 23:97–119, 1994.

[17] L. Berman. On the structure of complete sets. In *Proc. 17th Symp. FOCS*, pages 76–80, 1976.

[18] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput.*, 13:850–864, 1984.

[19] R. Book. On sets with small information content. In O. Watanabe, editor, *Kolmogorov Complexity and Computational Complexity*, pages 23–42. Springer Verlag, 1992.

[20] R. Book. On languages reducible to algorithmically random languages. *SIAM J. Comput.*, 23:1275–1282, 1994.

[21] R. Book and D. Du. The existence and density of generalized complexity cores. *J. Assoc. Comput. Math.*, 34:718–730, 1987.

[22] R. Book, D. Du, and D. Russo. On polynomial and generalized complexity cores. In *Proc. 3rd Conf. on Structure in Complexity Theory*, pages 236–250. IEEE Computer Society Press, 1988.

[23] R. Book and K. Ko. On sets truth-table reducible to sparse sets. *SIAM J. Comput.*, 17:903–919, 1988.

[24] R. Book, J. Lutz, and K. Wagner. An observation on probability versus randomness with applications to complexity classes. *Math. System Theory*, 27:201–209, 1994.

[25] R. Book and O. Watanabe. On random hard sets for **NP**. In *Proc. ISAAC 94*, Lecture Notes in Comput. Sci., 834, pages 47–55. Springer Verlag, 1994.

[26] H. Buhrman and L. Longpré. Compressibility and Resource Bounded Measure. In *Proc. 13rd STACS*, Lecture Notes in Comput. Sci., 1046, pages 13-24. Springer Verlag, 1996.

[27] H. Buhrman and E. Mayordomo. An excursion to the Kolmogorov random strings. In *Proc. 10th Conf. on Structure in Complexity Theory*, pages 197–203. IEEE Computer Society Press, 1995.

[28] H. Buhrman and L. Torenvliet. On the structure of complete sets. In *Proc. 9th Conf. on Structure in Complexity Theory*, pages 118–133. IEEE Computer Society Press, 1994.

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

[30] G. J. Chaitin. Incompleteness theorems for random reals. *Adv. in Appl. Math.*, 8:119–146, 1987.

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

[32] P. Duris and J. D. P. Rolim. **E**-complete sets do not have optimal polynomial time approximations. In *Proc. 19th MFCS*, Lecture Notes in Comput. Sci., 841, pages 38–51. Springer Verlag, 1994.

[33] W. Feller. *Introduction to Probability Theory and Its Applications.* Volume I. John Wiley & Sons, Inc., 1968.

[34] S. Fenner. Notions of resource-bounded category and genericity. In *Proc. 6th Conf. on Structure in Complexity Theory*, pages 196–212. IEEE Computer Society Press, 1991.

[35] S. Fenner. Resource-bounded Baire category: A stronger approach. In *Proc. 10th Conf. on Structure in Complexity Theory*, pages 182–192. IEEE Computer Society Press, 1995.

[36] B. Fu. With quasi-linear queries **EXP** is not polynomial time Turing reducible to sparse sets. In *Proc. 8th Conf. on Structure in Complexity Theory*, pages 185–191. IEEE Computer Society Press, 1993.

[37] P. Gács. Every sequence is reducible to a random one. *Inform. and Control*, 70:186–192, 1986.

[38] H. Gaifman and M. Snir. Probabilities over rich languages, testing and randomness. *J. Symbolic Logic*, 47:495–548, 1982.

[39] 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.

[40] C. Jockusch. Semirecursive sets and positive reducibility. *Trans. Amer. Math. Soc.*, 131:420–436, 1968.

[41] D. Juedes, J. Lathrop, and J. H. Lutz. Computational depth and reducibility. *Theoret. Comput. Sci.*, 132:37–70, 1994.

[42] D. Juedes and J. H. Lutz. The complexity and distribution of hard problem. *SIAM J. Comput.*, 24:279–295, 1995.

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

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

[45] S. Kautz. *Independence properties of algorithmically random sequences.* Manuscript, 1995.

[46] S. Kautz and P. Miltersen. Relative to a random oracle, **NP** is not small. In *Proc. 9th Conf. on Structure in Complexity Theory*, pages 162–174. IEEE Computer Society Press, 1994.

[47] S. Kleene. General recursive functions of natural numbers. *Math. Ann.*, 112:727–742, 1936.

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

[49] K. Ko and D. Moore. Completeness, approximation and density. *SIAM J. Comput.*, 10:787–796, 1981.

[50] K. Ko, P. Orponen, U. Schöning, and O. Watanabe. What is a hard instance of a computational problem? In *Proc. 1st Conf. on Structure in Complexity Theory*, Lecture Notes in Comput. Sci., 223, pages 197–217. Springer Verlag, 1986.

[51] A. N. Kolmogorov. On tables of random numbers. *Sankhya Ser. A*, 25:369–376, 1963.

[52] A. N. Kolmogorov. Three approaches to the definition of the concept “quantity of information”. *Problemy Inform. Transmission*, 1:3–7, 1965.

[53] A. N. Kolmogorov and V. A. Uspenskii. Algorithms and randomness. *Theory Probab. Appl.*, 32:389–412, 1987.

[54] S. Kurtz. *Randomness and Genericity in the Degrees of Unsolvability.* PhD thesis, University of Illinois at Urbana-Champaign, 1981.

[55] R. E. Ladner. On the structure of polynomial time reducibility. *J. Assoc. Comput. Math.*, 22:155–171, 1975.

[56] R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial time reducibilities. *Theoret. Comput. Sci.*, 1:103–123, 1975.

[57] M. van Lambalgen. *Random Sequences.* PhD thesis, University of Amsterdam, 1987.

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

[59] L. A. Levin. The concept of a random sequence. *Soviet Math. Dokl.*, 14:1413–1416, 1974.

[60] M. Li and P. M. B. Vitányi. Applications of Kolmogorov complexity in the theory of computation. In A. L. Selman, editor, *Complexity Theory Retrospective*, pages 147–203. Springer Verlag, 1988.

[61] D. Loveland. The Kleene hierarchy classification of recursively random sequences. *Trans. Amer. Math. Soc.*, 125:497–510, 1966.

[62] D. Loveland. A new interpretation of the von Mises concept of a random sequence. *Z. Math. Logik Grundlag. Math.*, 12:279–294, 1966.

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

[64] J. H. Lutz. Pseudorandom sources for **BPP**. *J. Comput. System Sci.*, 41:307–320, 1990.

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

[66] J. H. Lutz. On independent random oracles. *Theoret. Comput. Sci.*, 92:301–307, 1992.

[67] J. H. Lutz. A pseudorandom characterization of **BPP**. *SIAM J. Comput.*, 22:1075–1086, 1993.

[68] J. H. Lutz. The quantitative structure of exponential time. In *Proc. 8th Conf. on Structure in Complexity Theory*, pages 158–175. IEEE Computer Society Press, 1993.

[69] J. H. Lutz. Weakly hard problems. In *Proc. 9th Conf. on Structure in Complexity Theory*, pages 146–161. IEEE Computer Society Press, 1994.

[70] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: separating completeness notions if **NP** is not small. In *Proc. 11th STACS*, Lecture Notes in Comput. Sci., 775, pages 415–426. Springer Verlag, 1994.

[71] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM J. Comput.*, 23:762–779, 1994.

[72] J. H. Lutz and W. Schmidt. Circuit size relative to pseudorandom oracles. *Theoret. Comput. Sci.*, 107:95–120, 1993.

[73] S. R. Mahaney. Sparse complete sets for **NP**: Solution of a conjecture of Berman and Hartmanis. *J. Comput. System Sci.*, 25:130–143, 1982.

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

[75] E. Mayordomo. Almost every set in exponential time is **P**-bi-immune. *Theoret. Comput. Sci.*, 136:487–506, 1994.

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

[77] W. Merkle and Y. Wang. Separations by random oracles and "almost" classes for the generalized reducibilities. In *Proc. 20th MFCS*, Lecture Notes in Comput. Sci., 969, pages 179–190. Springer-Verlag, 1995.

[78] 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.

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

[80] A. A. Muchnik. reported in [97].

[81] M. Ogihara. Polynomial-time membership comparable sets. *SIAM J. Comput.*, 24:1068–1081, 1995.

[82] M. Ogihara and O. Watanabe. On polynomial bounded truth-table reducibility of **NP** sets to sparse sets. *SIAM J. Comput.*, 20:471–483, 1991.

[83] P. Orponen, A. Russo, and U. Schöning. Optimal approximations and polynomially levelable sets. *SIAM J. Comput.*, 15:399–408, 1986.

[84] J. O. Oxtoby. *Measure and Category.* Springer Verlag, 1971.

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

[86] K. Regan, D. Sivakumar, and J. Cai. Pseudorandom generators, measure theory, and natural proofs. Technical Report TR95-006, Electronic Colloquium on Computational Complexity, 1995.

[87] D. A. Russo. Optimal approximations of complete sets. In *Proc. 1st Conf. on Structure in Complexity Theory*, Lecture Notes in Computer Science, pages 311–324. Springer-Verlag, 1986.

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

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

[90] C. P. Schnorr. Process complexity and effective random tests. *J. Comput. System Sci.*, 7:376–388, 1973.

[91] A. Selman. **P**-selective sets, tally languages, and the behavior of polynomial time reducibilities on **NP**. *Math. System Theory*, 13:55–65, 1979.

[92] A. Kh. Shen. On relations between different algorithmic definitions of randomness. *Soviet Math. Dokl.*, 38:316–319, 1989.

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

[94] M. Strauss. Normal Numbers and Sources for **BPP**, *Proc. 12th STACS*, Lecture Notes in Comput. Sci., 900, pages 515–526, 1995.

[95] T. Thierauf, S. Toda, and O. Watanabe. On sets bounded truth-table reducible to **P**-selective sets. In *Proc. 11th STACS*, Lecture Notes in Comput. Sci., 775, pages 427–438. Springer Verlag, 1994.

[96] S. Toda. On polynomial time truth-table reducibilities of intractable sets to **P**-selective sets. *Math. System Theory*, 24:69–82, 1991.

[97] 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.

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

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

[100] Y. Wang. *A comparison of some randomness concepts.* Submitted.

[101] 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*), pages 180-189. IEEE Computer Society Press, 1996.

[102] Y. Wang. ***NP**-hard sets are superterse unless **NP** is small.* Information Processing Letters, 1997.

[103] Y. Wang. *Resource bounded genericity, resource bounded randomness and polynomial time approximations.* SIAM Journal on Computing, 1997.

[104] Y. Wang. Stochasticity, Randomness and Approximations. Submitted. Max-Planck-Institut fuer Informatik, 1996.

[105] Y. Wang. *The computing power of ordered Petri nets* (in Chinese). Journal of Software, 3(4):35–41, 1993.

[106] Y. Wang and G. Hu. *The fundamental theory for object-oriented languages* (in Chinese). Journal of Computer Science, 20(4):1–6, 1993.

[107] Y. Wang and G. Hu. *An algorithm and its data structure from sequential US MMCM to parallel machines.* In: Computer Mathematics (TianJin,1991) pages 58-65, World Sci. Publishing, River Edge, NJ, 1993.

[108] Y. Wang and S. Xu. *The Blum's speedup theorem and the hierarchy of recursive functions* (in Chinese). Journal of Software, 4(4):38–43, 1993.

[109] O. Watanabe. reported in [95].

[110] O. Watanabe. A comparison of polynomial time completeness notions. *Theoret. Comput. Sci.*, 54:249–265, 1987.

[111] O. Watanabe. *On the Structure of Intractable Complexity Classes*. PhD thesis, Tokyo Institute of Technology, 1987.

[112] O. Watanabe. Polynomial time reducibility to a set of small density. In *Proc. 2nd Conf. on Structure in Complexity Theory*, pages 138–146. IEEE Computer Society Press, 1987.

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

[114] C. B. Wilson. Relativized circuit complexity. *J. Comput. System Sci.*, 31:169–181, 1985.

[115] A. C. Yao. Theory and applications of trapdoor functions. In *Proc. 23rd Symp. FOCS*, pages 80–91, 1982.

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