Resource-Bounded Measure and Randomness*

Klaus Ambos-Spies[†] Elvira Mayordomo[‡]

Abstract

We survey recent results on resource-bounded measure and randomness in structural complexity theory. In particular, we discuss applications of these concepts to the exponential time complexity classes $\mathbf{E}$ and $\mathbf{E}_2$. Moreover, we treat time-bounded genericity and stochasticity concepts which are weaker than time-bounded randomness but which suffice for many of the applications in complexity theory.

1 Introduction

The first attempt for defining the concept of a random sequence goes back to von Mises [vM19] in 1919. He proposed that an infinite 0-1-sequence S should be considered to be random if, in the limit, the number of the occurrences of the 0s and 1s in S is the same (i.e. the sequence S satisfies the law of large numbers) and if this stability property is inherited by every infinite subsequence of S obtained by an admissible selection rule. A fuzzyness in this concept, due to the lack of a formal definition of admissibility was later eliminated by Church [Ch40] in 1940, who proposed that a selection rule should be admissible if it is given by a recursive, i.e. in a formal sense computable, function, thereby introducing the first concept of algorithmic randomness. As observed by Ville [Vi39] in 1939 already, the von Mises-Church approach to randomness is not satisfying from the point of view of probability theory, however, since random sequences in this sense may fail to satisfy some of the fundamental statistical laws. In particular, Ville constructed such a random sequence which failed to show the typical speed of convergence in the ratio of the 0s and 1s as it is expressed by the law of the iterated logarithm.

The search for more satisfying randomness notions was completed by Martin-Löf [ML66] in 1966 who defined random sequences satisfying all recursive (in fact recursively enumerable) statistical tests. The robustness of this concept

*Supported by the Human Capital and Mobility Program of the European Community under grant CHRX-CT93-0415 (COLORET).

[†]Mathematisches Institut, Universität Heidelberg, D-69120 Heidelberg, Germany

[‡]Universidad de Zaragoza, Dept. Informática, CPS, María del Luna 3, E-50015 Zaragoza, Spain

was demonstrated by alternative characterizations in terms of the descriptional (Kolmogorov) complexity of the finite initial segments of a random sequence (see Li and Vitányi [LV93] for details) and in terms of betting strategies, called martingales (Schnorr [Sch71a], [Sch71b]).

Schnorr also used the martingale characterization of Martin-Löfs randomness concept to point out that, being a notion of recursively enumerable randomness, this concept is too restrictive and he proposed two notions of recursive randomness which he considered to be more adequate. Though it seems that his criticism was not widely accepted, his martingale approach led in a very natural way to resource-bounded measure and randomness concepts in complexity theory. Unfortunately, his notions of time-bounded randomness did not find the attention in complexity theory they deserved, and only recent attempts of Lutz ([Lu90], [Lu92]) for defining measures on the fundamental complexity classes like exponential time led to the rediscovery of Schnorr's concept. Though Lutz's and Schnorr's approach have somewhat different motivations they are equivalent in the sense that each one can be defined in terms of the other one. Lutz's goal was to define a measure on complexity classes sharing the fundamental properties of the classical Lebesgue measure thereby producing a powerful tool for analyzing quantitative, structural aspects of these complexity classes. Since complexity classes are countable and any countable class has measure 0 in the classical sense, this approach had to be based on resource-bounded measure concepts, which are also the basis for the definition of resource-bounded randomness concepts.

In this survey we present the fundamental results of Lutz's resource-bounded measure theory and Schnorr's resource-bounded randomness and their applications in structural complexity theory. We restrict ourselves to the case of deterministic-time complexity, which has been mainly treated in the literature so far. Most of the results are given with complete proofs. We emphasize the relations between Lutz's and Schnorr's approach by focusing on randomness and by proving numerous measure results via randomness. Moreover, we emphasize some concepts, strictly weaker than resource-bounded randomness but sufficient for many applications in complexity theory: the resource-bounded genericity concept of Ambos-Spies, Fleischhack and Huwig [AFH88] and resource-bounded stochasticity, which is the resource-bounded variant of the von Mises-Church-randomness concept recently introduced in [AMWZ96].

The outline of the paper is as follows. In Section 2 we introduce the fragment of Lebesgue measure theory needed in the following and we describe this theory in terms of martingales. Resource-bounded martingales and resource-bounded measure and randomness based on this concept are introduced in Section 3, where also some of the fundamental results on these notions are proven. In Section 4 the aspects of resource-bounded randomness captured by the weaker genericity concept of [AFH88] are discussed and a series of applications in structural complexity is given. Resource-bounded stochasticity and some of its applications are presented in Section 5. In Sections 6 and 7 Lutz's measure on the exponential time classes $\mathbf{E}$ and $\mathbf{E}_2$ is discussed in some detail. In Section 8 the limitations of resource-bounded genericity and stochasticity compared with randomness are discussed and some applications of resource-bounded randomness in complexity theory which seem to require the full strength of this concept are given. In Section 9 we investigate the internal structure of the class **NP** under some measure hypothesis and other strong hypotheses. In Section 10 we shortly summarize further work related to this survey.

The basic objects of structural complexity theory are sets of binary strings, whereas the basic objects of measure theory are infinite 0-1-sequences. By identifying sets with their characteristic sequence, however, we can bridge this gap. Since there are $2^n - 1$ binary strings of length less than n, the length of initial segment $A\restriction x$ of the characteristic sequence of a set A will be exponential in the length of x. Since martingales will have initial segments of sets as their inputs and since the complexity of a set or function is measured in the input length, this will imply that $t(n)$-randomness based on martingales computable in time $t(n)$ will be randomness for the deterministic time class $\mathbf{DTIME}(t(2^n-1))$, not for $\mathbf{DTIME}(t(n))$. This fact is also responsible for problems in defining randomness for subexponential complexity classes. Here we will not discuss this problem, which has not been completely solved yet. For partial solutions we refer the reader to Allender and Strauss ([AS94], [AS95]) and Mayordomo [Ma94c].

We conclude this section by introducing some basic notation.

Let $\Sigma^* = \{0,1\}^*$ denote the set of finite binary strings. For a string x, $x(m)$ denotes the $(m+1)$th bit in x, i.e., $x = x(0)...x(n-1)$, where $n = |x|$ is the length of x. λ is the empty string. $x \sqsubseteq y$ denotes that the string x is extended by y and $x \sqsubset y$ denotes that this extension is proper. We identify strings with numbers, by letting n be the $(n+1)$th string under the canonical length-lexicographical ordering. Since there are 2^m strings of length m, $|n| \approx \log(n)$. N, Q, R denote the sets of natural, rational, and real numbers, respectively. $[0,1]$ is the unit interval in R. Lower case letters $..., x, y, z$ from the end of the alphabet will be used to denote strings, while the other letters denote numbers, with the exception of d, f, g, h and s, t which also denote functions. Lower case Greek letters denote reals.

A set of strings is called a *problem* or shortly a *set*, while sets of sets are called *classes*. Capital letters denote sets, boldface capital letters classes.
$\| A \|$ is the cardinality of the set A. We let $A^{\leq n} = \{x \in A : |x| \leq n\}$ and $A^{=n} = \{x \in A : |x| = n\}$. A set A is called *sparse* if there is a polynomial p such that $\| A^{\leq n} \| \leq p(n)$ for each n, and A is *exponentially dense* if there is a real number $\alpha > 0$ such that $\| A^{\leq n} \| > 2^{n^\alpha}$ almost everywhere. For sets A and B, $A \oplus B = \{0x : x \in A\} \cup \{1x : x \in B\}$ is the join (effective disjoint union) and $A \Delta B = (A - B) \cup (B - A)$ is the symmetric difference of A and B.

We identify a set with its infinite characteristic sequence, i.e., $x \in A$ iff $A(x) = 1$ and $x \notin A$ iff $A(x) = 0$, so that $2^\omega = \{0,1\}^\infty$, the set of infinite binary sequences, is identified with the power class $\mathcal{P}(\{0,1\}^*)$ of $\{0,1\}^*$. We let $A\restriction n$ denote the initial segment $A(0)...A(n-1) \in \{0,1\}^*$ of A of length n. We write $x \sqsubset A$ and say that A *extends* x if x is a finite initial segment of A. The class of all sets extending a string x is denoted by $\mathbf{B}_x = \{A : x \sqsubset A\}$.

We will use strings in two different meanings: as elements of sets and as finite initial segments of sets. In an attempt to avoid confusion, usually we will use the notation $X \upharpoonright x$ for strings intended to denote initial segments. Then $X \upharpoonright x$ denotes a string of length x and, for $y < x$, $X(y)$ or $(X \upharpoonright x)(y)$ will denote the $(y+1)$th bit of $X \upharpoonright x$.

For the following it will be important to note the difference in the length of an initial segment $A \upharpoonright x$ and the length of its bound x, namely

(1.1) $\quad 2^{|x|} - 1 \leq |A \upharpoonright x| \leq 2^{|x|+1} - 1,$

whence, for any number $k \geq 1$, $|A \upharpoonright x|^k \approx 2^{k \cdot |x|}$. (These inequalities will be responsible for the fact that the $\mathbf{DTIME}(t(n))$-measure will be a measure for $\mathbf{DTIME}(t(2^n))$.)

Our complexity theoretic notation is mainly standard. For the fundamental complexity theoretic concepts used but not explained in this paper we refer the reader to [HU79] and [BDG95]. In particular we assume the reader to be familiar with the basic concepts and results of structural complexity theory. We will consider the deterministic time classes

$$\begin{aligned}
&\mathbf{P} = \mathbf{DTIME}(poly) = \textstyle\bigcup_{k \geq 1} \mathbf{DTIME}\left(n^k\right), \\
&\mathbf{E} = \mathbf{DTIME}\left(2^{lin}\right) = \textstyle\bigcup_{k \geq 1} \mathbf{DTIME}\left(2^{kn}\right), \textit{and} \\
&\mathbf{E}_2 = \mathbf{DTIME}\left(2^{poly}\right) = \textstyle\bigcup_{k \geq 1} \mathbf{DTIME}\left(2^{n^k}\right).
\end{aligned}$$

Moreover, in our notation we will not distinguish between complexity classes for sets and functions. For any reducibility r (like 1 (= one-one), m (= many-one), $btt(k)$ (= k-query truth-table), btt (= bounded truth-table), tt (= truth-table) and T (= Turing)), we let $\mathbf{P}_r^{\leq}(A)$ or shortly $\mathbf{P}_r(A)$ be the class $\{B : B \leq_r^p A\}$ of sets which can be reduced to A by an r-reduction in polynomial time. (For the definition of these reducibilities, see [LLS75].) Note that $\mathbf{P}_T(A) = \mathbf{P}(A)$. Also note that $\mathbf{E}_2$ is the downward closure of $\mathbf{E}$ under any of the polynomial reducibilities, whence a set A is $\mathbf{P}$-r-complete for $\mathbf{E}$ iff $A \in \mathbf{E}$ and A is $\mathbf{P}$-r-complete for $\mathbf{E}_2$.

Throughout this article, we assume that all time bounds $t(n)$ are nondecreasing, time-constructible functions satisfying $t(n) \geq n$ for all n and $\mathbf{DTIME}(t(n)) = \mathbf{DTIME}(O(t(n)))$.

2 Measure and Martingales

In the first part of this section we introduce the fragment of the Lebesgue measure concept needed in the following. Then we give a characterization of the measure-0 classes due to Ville [Vi39] which is based on certain betting strategies, called martingales. By giving some examples, we will illustrate this concept, which will be the basis for the randomness concepts discussed in this paper.

For a more complete treatment of Lebesgue measure we refer the reader to Halmos [Ha50] or Oxtoby [Ox80].

The Lebesgue measure μ on the Cantor space is the product measure induced by the equiprobable measure μ_0 on $\{0,1\}$ which assigns to both 0 and 1 the probability $\frac{1}{2}$. A model for this measure is the (independent) tossing of a fair coin. In particular, for the basic open class $\mathbf{B}_x = \{A : x \sqsubseteq A\}$, $\mu(\mathbf{B}_x) = 2^{-|x|}$ is the probability that a randomly chosen sequence of coin tosses begins with the $|x|$ events $x(0), \ldots, x(|x|-1)$. For our goals it will not be necessary to define the Lebesgue measure μ completely but it suffices to define the "small" and "large" classes with respect to this measure, namely the measure-0 and measure-1 classes.

Definition 2.1. An infinite sequence $\mathcal{B} = \{\mathbf{B}_{x_n} : n \geq 0\}$ of basic open sets is an *α-cover* of a class $\mathbf{C}$ if

(i) $\mathbf{C} \subseteq \bigcup_{n\geq 0} \mathbf{B}_{x_n}$ and (ii) $\sum_{n\geq 0} \mu(\mathbf{B}_{x_n}) \leq \alpha$.

Example 2.2. For any set A, the sequence $\mathcal{B}_A = \{\mathbf{B}_{A\restriction n} : n > k\}$ is a 2^{-k}-cover of $\{A\}$.

Definition 2.3. A class $\mathbf{C}$ has *measure* 0 ($\mu(\mathbf{C}) = 0$) if, for all $n \geq 0$, there is a 2^{-n}-cover of $\mathbf{C}$. A class $\mathbf{C}$ has *measure* 1 ($\mu(\mathbf{C}) = 1$) if the complement $\overline{\mathbf{C}}$ of $\mathbf{C}$ has measure 0.

We write $\mu(\mathbf{C}) \neq i$ ($i = 0,1$) to abbreviate that $\mathbf{C}$ does not have measure i. Note that, for any cover $\mathcal{B} = \{\mathbf{B}_{x_n} : n \geq 0\}$ of the power class of $\{0,1\}^*$, $\sum_{n\geq 0} \mu(\mathbf{B}_{x_n}) \geq 1$. Hence, there is no class $\mathbf{C}$ such that $\mu(\mathbf{C}) = 0$ and $\mu(\mathbf{C}) = 1$. This consistency property can be also expressed by

Proposition 2.4. For any measure-0 class $\mathbf{C}$, $\mu(\mathbf{C}) \neq 1$.

In the next lemma we summarize the fundamental closure properties of the family of measure-0 classes.

Lemma 2.5.

(i) For every set A, $\mu(\{A\}) = 0$.

(ii) If $\mathbf{C} \subseteq \mathbf{D}$ and $\mu(\mathbf{D}) = 0$ then $\mu(\mathbf{C}) = 0$.

(iii) Let $\mathbf{C} = \bigcup_{n\geq 0} \mathbf{C}_n$ be the union of the measure-0 classes $\mathbf{C}_n$, $n \geq 0$. Then $\mu(\mathbf{C}) = 0$.

Proof. (i) follows from Example 2.2 while (ii) is immediate by definition. For a proof of (iii), fix $m \geq 0$. To show that $\mathbf{C}$ possesses a 2^{-m}-cover, by assumption choose $2^{-(m+k+1)}$-covers $\mathcal{B}_k = \{\mathbf{B}_{x_{k,n}} : n \geq 0\}$ of $\mathbf{C}_k$. Then, for $\hat{x}_{\langle k,n \rangle} = x_{k,n}$, $\mathcal{B} = \{\mathbf{B}_{\hat{x}_e} : e \geq 0\}$ is a 2^{-m}-cover of $\mathbf{C}$. □

Corollary 2.6. For any countable class $\mathbf{C}$, $\mu(\mathbf{C}) = 0$. □

(Examples of uncountable measure-0 classes can be found below.) By duality, we obtain the following closure properties of measure-1 classes.

Corollary 2.7.

(i) For any class $\mathbf{C}$ with countable complement, $\mu(\mathbf{C}) = 1$.

(ii) If $\mathbf{C} \subseteq \mathbf{D}$ and $\mu(\mathbf{C}) = 1$ then $\mu(\mathbf{D}) = 1$.

(iii) Let $\mathbf{C} = \bigcap_{n \geq 0} \mathbf{C}_n$ be the intersection of the measure-1 classes $\mathbf{C}_n$, $n \geq 0$. Then $\mu(\mathbf{C}) = 1$. □

We next give a characterization of the measure-0 classes in terms of certain betting strategies, called martingales.

Definition 2.8.

(a) A *martingale* is a function $d : \{0,1\}^* \to [0, \infty)$ such that $d(\lambda) > 0$ and, for every $x \in \{0,1\}^*$, the following equality holds:

$$\text{(2.1)} \qquad \frac{d(x0) + d(x1)}{2} = d(x)$$

$d(\lambda)$ is called the *norm* of d. d is *normed* if $d(\lambda) = 1$.

(b) A martingale d *succeeds* on a set A if

$$\limsup_{n \geq 0} d(A \restriction n) = \infty.$$

$S^\infty[d]$ denotes the class of sets on which the martingale d succeeds.

A martingale d *succeeds* on a class $\mathbf{C}$ if $\mathbf{C} \subseteq S^\infty[d]$.

The definitions of martingale and success can be interpreted in relation with a fair betting game on the successive bits of a hidden sequence in $\{0,1\}^\infty$. The gambler starts with capital $d(\lambda)$ and in every round, depending on the previous outcomes x, he bets a certain fraction $\alpha \cdot d(x)$ ($\alpha \in [0,1]$) of his current capital $d(x)$ on the event 0, and he bets the remaining capital $(1-\alpha)d(x)$ on the event 1. The amount put on the correct guess of the event will be doubled while the amount put on the wrong guess will be lost. So for the outcomes 0 and 1 his capital in the next round will be $d(x0) = 2\alpha d(x)$ and $d(x1) = 2(1-\alpha)d(x)$, respectively. (This corresponds to the martingale property (2.1).)

We call the function, which determines the fraction of the capital put onto the 0 event in every round, the strategy underlying the martingale d.

Definition 2.9. A *(betting) strategy* s is a function $s : \{0,1\}^* \to [0,1]$. The *strategy* s_d *underlying the martingale* d is the function

$$(2.2) \qquad s_d(x) = \begin{cases} \frac{d(x0)}{2d(x)} & \text{if } d(x) \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Conversely, for every strategy s and every real $\alpha > 0$, the *martingale* $d[s,\alpha]$ with start capital α *induced* by s is defined by $d(\lambda) = \alpha$ and, for any string $X\restriction(n+1)$ where $n \geq 0$,

$$(2.3) \qquad d(X\restriction(n+1)) = \begin{cases} 2 \cdot s(X\restriction n) \cdot d(X\restriction n) & \text{if} \quad X(n) = 0 \\ 2 \cdot (1 - s(X\restriction n)) \cdot d(X\restriction n) & \text{if} \quad X(n) = 1. \end{cases}$$

We write $d[s]$ in place of $d[s,1]$ for the normed martingale induced by the strategy s. Note that the strategy s_d underlying a martingale d is uniquely determined by d, and the normed martingale $d[s]$ induced by a strategy s is uniquely determined by s. Moreover, $d[s] = d[s']$ if and only if the strategies s and s' differ only on strings x with $d[s](x) = d[s'](x) = 0$.

Example 2.10.

1. For any set A, consider the strategy s defined by

   $$s(X\restriction n) = 1 - A(n).$$

   (I.e., given any string $X\restriction n$, the strategy s bets the whole capital on the guess $i = A(n)$ for the next bit i.) Then, for the normed martingale $d[s]$ induced by s, $S^\infty[d[s]] = \{A\}$. Namely, for every n, $d[s](A\restriction(n+1)) = 2 \cdot d[s](A\restriction n)$, whence $\lim_{n\geq 0} d[s](A\restriction n) = \infty$, whereas for $B \neq A$, say $B(n_0) \neq A(n_0)$, $d[s](B\restriction n) = 0$ for all $n > n_0$.

2. For any infinite set A, let s be the strategy defined by

   $$s(X\restriction n) = \begin{cases} 0 & \text{if } A(n) = 1 \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

   Then $d[s]$ succeeds on the supersets of A: $S^\infty[d[s]] = \{B : A \subseteq B\}$.

3. Recall that a set A is sparse if there is a polynomial p such that $\| A^{\leq n} \| \leq p(n)$ for all n. The strategy s with $s(X\restriction x) = \frac{3}{4}$, which always gives a $3:1$ preference to the outcome 0, succeeds on all sparse sets. Namely, for A and p as above and for $e(n) = \| (\Sigma^*)^{\leq n} \| = 2^{n+1} - 1$,

   $$d[s](A\restriction 0^{n+1}) = \left(\frac{3}{2}\right)^{\|(\Sigma^* - A)^{\leq n}\|} \cdot \left(\frac{1}{2}\right)^{\|A^{\leq n}\|} = \frac{3^{e(n)-p(n)}}{2^{e(n)}}$$

   Hence $\lim_{n\to\infty} d[s](A\restriction 0^n) = \infty$.

4. A set A has *exponential gaps* if $A^{=n} = \emptyset$ for infinitely many n. A martingale that succeeds on all sets with exponential gaps can be defined as follows. For any string $X \restriction x$ such that $X(y) = 0$ for all $y < x$ with $|y| = |x|$, the strategy s gives a $3 : 1$ preference to the outcome 0 and it is unbiased otherwise (i.e. $s((X \restriction 0^n)0^m) = \frac{3}{4}$ for n, m with $m \leq 2^n$ and $s(X \restriction x) = \frac{1}{2}$ otherwise). Then, for any set A and any number n, $d[s](A \restriction 0^{n+1}) \geq \frac{1}{2} d[s](A \restriction 0^n)$ whence $d[s](A \restriction 0^n) \geq (\frac{1}{2})^n$. Moreover, if $A^{=n} = \emptyset$ then $d[s](A \restriction 0^{n+1}) = (\frac{3}{2})^{2^n} \cdot d[s](A \restriction 0^n)$, whence $d[s](A \restriction 0^{n+1}) \geq (\frac{3}{2})^{2^n} \cdot (\frac{1}{2})^n \geq (\frac{3}{2})^{2n} \cdot (\frac{1}{2})^n = (\frac{9}{8})^n$. Since $\lim_{n \to \infty} (\frac{9}{8})^n = \infty$ this implies the claim.

To show that a class $\mathbf{C}$ has measure 0 iff there is a martingale d which succeeds on $\mathbf{C}$, we first describe covers in terms of martingales. We say that a martingale d *covers* a set X if

$$\text{(2.4)} \qquad \liminf_{n \geq 0} d(X \restriction n) \geq 1$$

and d *covers* a class $\mathbf{C}$ if d covers every set $X \in \mathbf{C}$.

Lemma 2.11. Let $\mathcal{B} = \{\mathbf{B}_{x_n} : n \geq 0\}$ be an α-cover of $\mathbf{C}$. There is a martingale d such that $d(\lambda) \leq \alpha$ and d covers $\mathbf{C}$.

Proof. For any string x, the martingale d_x defined by

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

covers $\mathbf{B}_x$ and $d_x(\lambda) = 2^{-|x|} = \mu(\mathbf{B}_x)$. Since $\mathcal{B}$ is an α-cover of $\mathbf{C}$, it follows that d defined by

$$d(y) = \Sigma_{n \geq 0}\ d_{x_n}(y)$$

is a martingale with $d(\lambda) \leq \alpha$ and d covers $\mathbf{C}$. □

Lemma 2.12. Let $\mathbf{C}$ be a measure-0 class. There is a martingale d which succeeds on $\mathbf{C}$.

Proof. By Definition 2.3 and Lemma 2.11, for each $n \geq 0$ there is a martingale d_n such that $d_n(\lambda) \leq 2^{-n}$ and d_n covers $\mathbf{C}$. So, for d defined by $d(y) = \Sigma_{n \geq 0}\ d_n(y)$, d is a martingale which succeeds on $\mathbf{C}$. □

Lemma 2.13. Let d be a martingale and let $\mathbf{C} = \{X : \exists n(d(X \restriction n) \geq 1)\}$. There is a $d(\lambda)$-cover of $\mathbf{C}$.

Proof. We only sketch the proof. Let C_d be the set of minimal strings covered by d, i.e., $C_d = \{x : d(x) \geq 1 \text{ and } \forall y \sqsubset x(d(y) < 1)\}$. Then $\mathbf{C} = \bigcup_{x \in C_d} \mathbf{B}_x$. Moreover, C_d is prefix free, i.e., for $x, y \in C_d$, $x \sqsubseteq y$ implies that $x = y$. By the latter property of C_d it easily follows from the martingale property (2.1) that

$$\Sigma_{x \in C_d}\, d(x) \cdot 2^{-|x|} \leq d(\lambda).$$

Since $d(x) \geq 1$ for $x \in C_d$ it follows that

$$\Sigma_{x \in C_d}\, \mu(\mathbf{B}_x) = \Sigma_{x \in C_d}\, 2^{-|x|} \leq d(\lambda),$$

whence $\mathcal{B} = \{\mathbf{B}_x : x \in C_d\}$ is a $d(\lambda)$-cover of $\mathbf{C}$. □

Lemma 2.14. Let $\mathbf{C}$ be a class and let d be a martingale which succeeds on $\mathbf{C}$. Then $\mu(\mathbf{C}) = 0$.

Proof. Given $m \geq 0$, it suffices to show that there is a 2^{-m}-cover of $\mathbf{C}$. For the constant $c = 2^{-m} \cdot d(\lambda)^{-1}$, let $d'(y) = c \cdot d(y)$. Then $d'(\lambda) = 2^{-m}$, d' is a martingale and $\mathbf{C} \subseteq \{X : \exists n(d'(X \restriction n) \geq 1)\}$. So the required cover exists by Lemma 2.13. □

Theorem 2.15. Let $\mathbf{C}$ be a class. Then $\mu(\mathbf{C}) = 0$ iff there is a martingale which succeeds on $\mathbf{C}$.

Proof. By Lemmas 2.12 and 2.14. □

3 Resource-Bounded Martingales and Randomness

We next introduce Schnorr's resource-bounded randomness concept ([Sch71a], [Sch71b]) and Lutz's resource-bounded measure ([Lu92]). Both concepts, which are closely related to each other, are based on Ville's martingale characterization of the measure-0 classes.

Note that for any countable sequence $D = \{d_n : n \geq 0\}$ of martingales, the class $\mathbf{S} = \bigcup_{n \geq 0} S^{\infty}[d_n]$ has measure 0 (by Theorem 2.15 and Lemma 2.5). So, for every set X in the measure-1 class $\overline{\mathbf{S}}$, no martingale in D succeeds on X. Hence we may call such a set X *random* for D. Schnorr proposed that a set X should be called *recursively random* if no recursive martingale succeeds on X, i.e. if X is random for the class D of recursive martingales. Moreover, by additionally imposing resource bounds, Schnorr introduced resource-bounded randomness concepts. Later Lutz extended these concepts by considering notions of resource-bounded measure. Here we introduce these concepts for the deterministic time complexity classes. By admitting only rational valued strategies and martingales, the time complexity of these functions can be defined in the usual way. To be more precise, we represent nonnegative rational numbers by triples $\langle p, q, r\rangle$ where p, q, r are (binary strings representing) nonnegative integers and $\langle p, q, r\rangle$ denotes the rational number $\frac{p}{q} \cdot 2^{-r}$. With this codification the sum of two rational numbers of length n can be done in time $O(n)$, whereas multiplication and division can be both done in time $O(n(log\ n)^2)$, using the best known integer multiplication algorithms.

Definition 3.1. Let $t : N \to N$ be a nondecreasing recursive function.

1. A $t(n)$-*strategy* is a function $s : \{0,1\}^* \to [0,1] \cap \mathrm{Q}$ such that $s \in \mathbf{DTIME}(t(n))$.

2. A $t(n)$-*martingale* is a martingale $d = d[s, \alpha]$ induced by a $t(n)$-strategy s and a rational number $\alpha > 0$.

Schnorr [Sch71b] and Ambos-Spies, Terwijn and Zheng [ATZ94] call a martingale d a $t(n)$-martingale if $d \in \mathbf{DTIME}(t(n))$, while our definition follows [AMWZ96] (It is chosen in order to simplify the comparison of $t(n)$-randomness with $t(n)$-genericity and $t(n)$-stochasticity in the next two sections). Lutz [Lu92] introduced still another notion of $t(n)$-martingale based on $\mathbf{DTIME}(t(n))$-approximations of real valued martingales. As shown in part by the following proposition, all these concepts are more or less equivalent though the correspondence does not preserve the exact time bounds.

Proposition 3.2. 1. For any $t(n)$-martingale d, $d \in \mathbf{DTIME}(n \cdot t(n) \cdot log(t(n))^2)$.
2. Any martingale $d \in \mathbf{DTIME}(t(n))$ is a $(t(n) \cdot log(t(n))^2)$-martingale.

Proof. By the above mentioned time bounds on multiplication and division of rationals, this follows from (2.3) and (2.2), respectively. $\square$

Example 3.3. The complexity of the martingales in Example 2.10 is as follows:

1. and 2. If $A \in \mathbf{DTIME}(t(2^n - 1))$, then $d[s]$ is a $t(n)$-martingale. Note that for any string x, $2^{|x|} - 1 \le |X \restriction x| \le 2^{|x|+1} - 1$. So $A(x)$, hence $s(X \restriction x)$, can be computed in $t(2^{|x|} - 1) \le t(|X \restriction x|)$ steps.

3. and 4. $d[s]$ is an $O(1)$-martingale and an n^2-martingale, respectively.

Definition 3.4 (Schnorr [Sch71b], Lutz [Lu92]).

1. A class $\mathbf{C}$ has $t(n)$-*measure* 0 ($\mu_t(\mathbf{C}) = 0$) if there is a $t(n)$-martingale d that succeeds on $\mathbf{C}$.

2. A class $\mathbf{C}$ has $t(n)$-*measure* 1 ($\mu_t(\mathbf{C}) = 1$) if $\overline{\mathbf{C}}$ has $t(n)$-measure 0.

3. A set A is $t(n)$-*random* if no $t(n)$-martingale succeeds on it.
   Let $\mathbf{RAND}(t(n))$ denote the class of $t(n)$-random sets.

Note that the $t(n)$-measure μ_t is consistent with the classical measure μ, but due to the presence of resource-bounds, certain classes which in the classical sense are small (large) cannot be classified here. Examples are the singletons $\{A\}$, where A is $t(n)$-random.

Proposition 3.5. Let t, t' be recursive functions such that $t(n) \leq t'(n)$ a.e.

(i) For any class $\mathbf{C}$ and $i \in \{0,1\}$, $\mu_t(\mathbf{C}) = i \Rightarrow \mu_{t'}(\mathbf{C}) = i \Rightarrow \mu(\mathbf{C}) = i$.

(ii) $\mathbf{RAND}(t(n)) \supseteq \mathbf{RAND}(t'(n))$. □

Proposition 3.6. For any set A, the following are equivalent.

(i) A is $t(n)$-random.

(ii) $\mu_t(\{A\}) \neq 0$.

(iii) For every $t(n)$-measure-1 class $\mathbf{C}$, $A \in \mathbf{C}$. □

Another simple but useful observation is that the closure of the deterministic time classes under complement caries over to $t(n)$-measure and $t(n)$-randomness as follows.

Proposition 3.7. Let $\mathbf{C}$ be a class with $\mu_t(\mathbf{C}) = i$ $(i \in \{0,1\})$. Then, for co-$\mathbf{C} = \{\overline{A} : A \in \mathbf{C}\}$, $\mu_t(\text{co-}\mathbf{C}) = i$ too. In particular, for any $t(n)$-random set A, $\overline{A}$ is $t(n)$-random too.

Proof. This follows from the fact that a $t(n)$-martingale d succeeds on a set A iff the $t(n)$-martingale $\overline{d}$ succeeds on $\overline{A}$, where: $\overline{d}(X\upharpoonright n) = d(\overline{X}\upharpoonright n)$ for all strings $X\upharpoonright n$, where $\overline{X}\upharpoonright n$ is defined by $\overline{X}(m) = 1 - X(m)$ for $m < n$. □

By Proposition 3.6, Lemma 2.5 does not hold for the resource-bounded-measure, since the first part fails for any $t(n)$-random set A. The second part obviously holds in this setting too.

Proposition 3.8. If $\mathbf{C} \subseteq \mathbf{D}$ and $\mu_t(\mathbf{D}) = 0$ then $\mu_t(\mathbf{C}) = 0$. □

The closure under countable unions, however, fails too. The countable union of classes of $t(n)$-measure 0 has $t'(n)$-measure 0, however, if $t'(n)$ is chosen big enough so that in particular $\mathbf{DTIME}(t'(n))$ contains a universal function for $\mathbf{DTIME}(t(n))$. This observation also yields a $t(n)$-random set of almost minimum complexity. Similar union lemmas can be found in [Sch71b], [Lu92], [Ma94b], [ATZ94].

Lemma 3.9. Let $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ a.e.. There is a $t'(n)$-martingale d which succeeds on all $t(n)$-measure-0 classes, i.e. $\mu_{t'}(\bigcup\{\mathbf{C} : \mu_t(\mathbf{C}) = 0\}) = 0$. Moreover, there is a $t(n)$-random set $A \in \mathbf{DTIME}(2^n \cdot t'(2^{n+1}))$.

Proof. Let $\{s_k : k \geq 0\}$ be a recursive enumeration of the $t(n)$-strategies. By the standard construction of a universal machine, we may assume that, for $|x| = n > k$, $s_k(x)$ can be uniformly computed in $O(t(n) \cdot log(t(n)))$ steps. For each k define a martingale d_k by $d_k(X \restriction n) = 2^{-k}$ for $n \leq k$ and by (2.3) with d_k in place of d otherwise and combine the martingales d_k to a "universal" martingale d by letting

$$d(X \restriction n) = \sum_{k=0}^{\infty} d_k(X \restriction n) = \sum_{k=0}^{n} d_k(X \restriction n) + \sum_{k=n+1}^{\infty} 2^{-k}.$$

Note that $S^{\infty}[d[s_k]] = S^{\infty}[d_k] \subseteq S^{\infty}[d]$ whence d succeeds on all $t(n)$-measure-0 classes. So it suffices to show that d is a $t'(n)$-martingale. By (2.3), d_k can be inductively defined from s_k in $O(n \cdot t(n) \cdot log(t(n))^3)$ steps whence $d \in$ **DTIME**$(n^2 \cdot t(n) \cdot log(t(n))^3)$. So, by Proposition 3.2.2, d is an $(n^3 \cdot t(n) \cdot log(t(n))^4)$-martingale. For a proof of the second part of the lemma, inductively define A by letting $A(n) = 0$ if $d((A \restriction n)0) \leq d((A \restriction n)1)$ and $A(n) = 1$ otherwise. Then, by (2.1), $d(A \restriction n) \leq d(\lambda)$ for all n whence d does not succeed on A. So A is $t(n)$-random. Moreover, by $d \in$ **DTIME**$(t'(n))$ and by (1.1), $A \in$ **DTIME**$(2^{n+1} \cdot t'(2^{n+1}))$. □

By combining Proposition 3.6 and Lemma 3.9, we obtain the following relations between resource-bounded measure and randomness.

Corollary 3.10. Let t, t' be recursive functions such that $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$ and let $\mathbf{C}$ be any class.

(i) $\mu_t(\mathbf{C}) = \mathbf{0} \Rightarrow \mathbf{RAND}(t(n)) \cap \mathbf{C} = \emptyset \;\Rightarrow \mu_{t'}(\mathbf{C}) = 0$

(ii) $\mu_t(\mathbf{C}) = 1 \;\Rightarrow \mathbf{RAND}(t(n)) \subseteq \mathbf{C} \;\Rightarrow \mu_{t'}(\mathbf{C}) = 1$

Proof. By symmetry, it suffices to prove (i). The first implication is immediate by definition. For the second implication note that $\mathbf{RAND}(t(n)) \cap \mathbf{C} = \emptyset$ implies that $\mu_t(\{A\}) = 0$ for all $A \in \mathbf{C}$. So the claim follows from Lemma 3.9 □

Corollary 3.11. For any function t' such that $t'(n) \geq n^3 \cdot t(n) \cdot \log(t(n))^4$, $\mu_{t'}\ (\mathbf{RAND}(t(n))) = 1$. □

These close relations between measure and randomness allow the choice of which concept to work with. Due to the lack of closure properties of the $t(n)$-measure, the randomness approach sometimes is somewhat simpler, whence we will stress this concept here.

¿From the above examples we obtain the following properties of $t(n)$-random sets.

Lemma 3.12. Let A be $t(n)$-random where $t(n) \geq n^2$. Then A is not sparse and A does not have exponential gaps.

Proof. This follows from the third and fourth parts of Examples 2.10 and 3.3. □

For strengthenings of Lemma 3.12 see Corollaries 5.7 and 8.5. Recall that a set A is **C**-*immune* if A does not contain any infinite set $B \in \mathbf{C}$ as a subset, and A is **C**-*bi-immune* if A and $\overline{A}$ are **C**-immune. (In the following we will write p-(bi-)immune instead of **P**-(bi-)immune.)

Lemma 3.13. Let A be $t(n)$-random. Then $A \notin \mathbf{DTIME}(t(2^n - 1))$. In fact, A is $\mathbf{DTIME}(t(2^n - 1))$-bi-immune.

Proof. By the first parts of Examples 2.10 and 3.3, no $t(n)$-random set can be in $\mathbf{DTIME}(t(2^n-1))$. Similarly, by the second parts of these examples, any $t(n)$-random set is $\mathbf{DTIME}(t(2^n - 1))$-immune, hence, by Proposition 3.7, $\mathbf{DTIME}(t(2^n - 1))$-bi-immune. □

Bi-immunity is a fundamental property in structural complexity theory. Note that a set A is $\mathbf{DTIME}(t(n))$-bi-immune iff, for every infinite set $B \in \mathbf{DTIME}(t(n))$, $A \cap B \notin \mathbf{DTIME}(t(n))$, i.e., iff $t(n)$ is an almost everywhere lower time bound for A (see e.g. [GHS87] for more details). Many natural problems have easy parts, so that the second part of Lemma 3.13 is a quite powerful tool for showing that certain classes have $t(n)$-measure 0. For later use we give the characterization of bi-immunity in terms of complexity cores due to Balcazar and Schöning [BaS85]. Lynch [Ly75] defined that a set B is a $\mathbf{DTIME}(t(n))$-*complexity core* of a set A if, for every Turing machine M which is consistent with A (i.e. whenever $M(x)\downarrow$ then $M(x) = A(x)$), there are only finitely many $x \in B$ such that $M(x)$ is defined in less than $t(|x|)$ steps. (And B is a p-*complexity core* of A if B is a $\mathbf{DTIME}(n^k)$-complexity core of A for all $k \geq 1$.) Note that this is equivalent to saying that, for every infinite set $C \in \mathbf{DTIME}(t(n))$ with $C \subseteq B$, $A \cap C \neq \emptyset$ and $\overline{A} \cap C \neq \emptyset$. So A is $\mathbf{DTIME}(t(n))$-bi-immune iff $\{0,1\}^*$ is a $\mathbf{DTIME}(t(n))$-complexity core of A.

Corollary 3.14. Let A be $t(n)$-random. Then $\{0,1\}^*$ is a $\mathbf{DTIME}(t(2^n - 1))$-complexity core of A. □

4 Genericity versus Randomness

In Section 3 we have seen that random sets have certain properties which are commonly ensured by diagonalization. So, intuitively speaking, a random set has built in certain diagonalizations. For analyzing which types of diagonalizations are subsumed by randomness, it is instructive to compare randomness with genericity. As the random sets are the typical sets with respect to measure, the generic sets are typical with respect to Baire category. Baire category is an alternative topological classification scheme for the Cantor space, in which the meager (comeager) classes correspond to the measure-0 (measure-1) classes. In contrast to measure, however, category is directly related to diagonalization, and various resource-bounded category concepts capturing the most fundamental types of diagonalization arguments in structural complexity have been recently introduced (see [Am96]).

Here we will not consider all of these concepts but we will restrict ourselves to the general $t(n)$-genericity concept of Ambos-Spies [Am96] and a special case of it, $t(n)$-genericity, due to Ambos-Spies, Fleischhack and Huwig [AFH88].

Corresponding to the classical case, where we can find comeager measure-0 classes, general $t(n)$-genericity and $t(n)$-randomness are incompatible too. In contrast, however, all $t(n)$-random sets are $t(n)$-generic, so that the diagonalizations formalized by this genericity notion are captured by $t(n)$-randomness.

We use this observation to establish further properties of the $t(n)$-random sets. Finally we discuss two aspects relative to which $t(n)$-randomness strengthens $t(n)$-genericity.

A *classical extension function* is a function $f : \{0,1\}^* \to \{0,1\}^*$. A set A *meets* the extension function f at n if $(A\upharpoonright n)\, f(A\upharpoonright n) \sqsubseteq A$. Intuitively, if we inductively define the set A by determining longer and longer initial segments of its characteristic sequence and if A meets f at n, then the finite initial segment $A\upharpoonright n$ is extended as required by f. Extension functions correspond to the requirements in a diagonalization construction. E.g. if we want to diagonalize over an infinite countable class $\mathbf{C}$, then any set $C \in \mathbf{C}$ is associated with the extension function $f_c(X\upharpoonright n) = 1 - C(n)$. Then, for any set A, $A \notin \mathbf{C}$ iff A meets all the extension functions associated with the members of $\mathbf{C}$.

We say that a set A *avoids* the extension function f if there is no n such that A meets f at n. A class $\mathbf{C}$ is *nowhere dense* if there is an extension function avoided by all members of $\mathbf{C}$. A countable union of nowhere dense classes is called *meager*, the complement of a meager class is *comeager*. Meager and comeager classes may be viewed as small and large, respectively, and if we replace measure-0 and measure-1 by meager and comeager, respectively, then the fundamental properties of the Lebesgue measure stated in Lemma 2.5 and Corollary 2.7 remain valid. Here we will not pursue these Baire category concepts in detail but we will only consider the typical objects of it. (For a more complete account of classical Baire category, we refer to Oxtoby [Ox80].)

For a countable class $F = \{f_n : n \geq 0\}$ of extension functions, there will be a comeager (hence nonempty) class of sets meeting all members of F. Such sets are called *generic for F*. Resource-bounded genericity concepts can be obtained by considering the class F of extension functions computable within a certain time bound. This approach has been taken by Lutz in [Lu90]. The genericity concept obtained in this way is rather weak, however, whence stronger notions have been introduced. The concept we study here is obtained by considering more flexible extension functions. The first amendment (due to Fenner [Fe91]) is to consider functions, which do not completely specify the extension. The second amendment (due to Ambos-Spies, Fleischhack, and Huwig [AFH84], [AFH87], [AFH88]) is to admit extension functions which are not total but defined infinitely often along the constructed sequence.

Definition 4.1.

(i) An *extension function* is a partial function $f : \{0,1\}^* \to (\{0,1\}^* \times \{0,1\})^*$, such that, for any string $X\restriction x$ on which f is defined,

$$(4.1) \qquad f(X\restriction x) = (x_0, i_0), \ldots, (x_m, i_m)$$

where $m \geq 0$, $x_0, \ldots x_m$ are strings such that $x \leq x_0 < x_1 < \ldots < x_m$ and $i_0, \ldots, i_m \in \{0,1\}$. A $t(n)$-*extension function* is an extension function $f \in \mathbf{DTIME}(t(n))$.

(ii) An extension function f is *dense along* a set A if $f(A\restriction x)$ is defined for infinitely many strings x.

(iii) A set A *meets* an extension function f *at* a string x if $f(A\restriction x)$ is defined, say $f(A\restriction x) = (x_0, i_0), \ldots, (x_m, i_m)$, and $A(x_l) = i_l$ for $0 \leq l \leq m$. A *meets* f if A meets f at some x, and A *avoids* f otherwise.

(iv) A is *general* $t(n)$-*generic* if A meets all $t(n)$-extension functions which are dense along A.

Classical Baire category can be defined in terms of this extension function concept too: A class $\mathbf{C}$ is nowhere dense if there is an extension function f which is dense along all members of $\mathbf{C}$ and avoided by all of them. So, for any recursive function $t(n)$, the class of the general $t(n)$-generic sets is comeager, hence nonempty.

We next give some examples to illustrate the above concepts. These should be compared with Example 2.10.

Examples 4.2.

1. For any set A, let f be the extension function defined by

$$f(X\restriction x) = (x, 1 - A(x)).$$

Then f is dense along all sets and a set B meets f iff $B \neq A$. Moreover, for $A \in \mathbf{DTIME}(t(2^n - 1))$, f is a $t(n)$-extension function.

2. For any infinite set A, let f be the following extension function. For $x \in A$, $f(X\restriction x) = (x, 0)$, and $f(X\restriction x)$ is undefined otherwise. Then, by infinity of A, f is dense along all sets and a set B meets f iff $A \not\subseteq B$. Again, for $A \in \mathbf{DTIME}(t(2^n - 1))$, f is a $t(n)$-extension function.

3. For $m \geq 0$ define the n^2-extension function f_m by

$$f_m(X \restriction 0^n) = (0^n, 0), \ldots, (1^n, 0)$$

if $m \leq n$ and $f_m(X \restriction x) \uparrow$ otherwise. (Since there are 2^n strings x of length n and, for each such x, $|(x, 0)| = O(n)$, $f_m(X \restriction 0^n)$ can be computed in $O(n \cdot 2^n)$ steps, whence f_m is an n^2-martingale by (1.1).) Then f_m is dense along all sets and a set A meets f_m iff $A^{=n} = \emptyset$ for some $n \geq m$. So A has exponential gaps iff A meets f_m for all m.

By the first two examples, for any general $t(n)$-generic set G, $G \notin \mathbf{DTIME}(t(2^n - 1))$, in fact G is $\mathbf{DTIME}(t(2^n - 1))$-bi-immune. So general $t(n)$-generic and $t(n)$-random sets share some interesting properties (cf. Lemma 3.13). By the third example and by Lemma 3.12, however, $t(n)$-randomness and general $t(n)$-genericity are incompatible.

Theorem 4.3 (Ambos-Spies [Am96]). For $t(n) \geq n^2$ there is no set which is general $t(n)$-generic and $t(n)$-random. Namely every general n^2-generic set has exponential gaps whereas no n^2-random set has exponential gaps. □

Theorem 4.3 is based on the observation that, in general, if a set A meets an extension function at some string x, this does not only determine the value of A on some single strings but on intervals of growing length (in $|x|$). By admitting only short extensions, in particular extensions which only determine the value of A on the next string, we obtain a genericity concept compatible with randomness.

Definition 4.4.

(i) An extension function f is *simple* if $f(X \restriction x) \in \{(x, 0), (x, 1)\}$ whenever $f(X \restriction x)$ is defined.

(ii) A set A is $t(n)$-*generic* if A meets every simple $t(n)$-extension function which is dense along A.

Note that the extension functions in Examples 4.2.1 and 4.2.2 are simple. To simplify notation, for a simple extension function f we write $f(X \restriction x) = i$ instead of $f(X \restriction x) = (x, i)$. Definition 4.4 is due to Ambos-Spies et al. [AFH88], though there $t(n)$-genericity is defined in terms of conditions, not extension functions. It can be easily shown, however, that $t(n)$-genericity as defined there coincides with $t(n + 1)$-genericity as defined above (see [Am96] or [AMWZ96]).

Obviously every general $t(n)$-generic set is $t(n)$-generic but the converse in general fails: In contrast to Theorem 4.3, $t(n)$-genericity is compatible with $t(n)$-randomness.

Theorem 4.5 ([ANT94],[ATZ94]). Every $t(n)$-random set is $t(n)$-generic.

Proof. Let A be $t(n)$-random and let f be a simple $t(n)$-extension function which is dense along A. For a contradiction assume that A avoids f. Define a $t(n)$-strategy s by letting

$$s(X\restriction x) = \begin{cases} f(X\restriction x) & \text{if } f(X\restriction x)\downarrow \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Informally, given $X\restriction x$, the strategy s makes a bet iff $f(X\restriction x)\downarrow$, and if so then s bets the whole capital on the outcome $1 - f(X\restriction x)$, i.e. the outcome that X avoids f at x. We will show that the normed $t(n)$-martingale $d[s]$ induced by s succeeds on A contrary to the assumption that A is $t(n)$-random. First observe that, by A avoiding f, $f(A\restriction x) = 1 - A(x)$ for all x such that $f(A\restriction x)\downarrow$, whence $d[s](A\restriction x)$ is nondecreasing in x. Moreover, by density of f along A, $d[s]((A\restriction x)A(x)) = 2\cdot d[s](A\restriction x)$ for infinitely many x, whence $A \in S^\infty[d[s]]$. □

Theorem 4.5 provides a new approach for establishing properties of $t(n)$-random sets, by showing these properties for the $t(n)$-generic sets. E.g., by the second part of Example 4.2, every $t(n)$-generic set is $\mathbf{DTIME}(t(2^n-1))$-bi-immune, which gives an alternative proof of Lemma 3.13.

Lemma 4.6 (Ambos-Spies, Neis and Terwijn [ANT94]). Let A be $t(n)$-generic. Then A is $\mathbf{DTIME}(t(2^n-1))$-bi-immune. □.

Similarly we can show that a $t(n)$-generic set, hence a $t(n)$-random set, is incompressible under $\mathbf{DTIME}(t(2^n-1))$ many-one reductions. Recall that a set A is $\mathbf{DTIME}(t(n))$-*m-incompressible* if, for any set B and for any function $g \in \mathbf{DTIME}(t(n))$ such that $A \leq_m B$ via g, g is almost one-to-one (i.e., for some string x, $g(y) \neq g(z)$ for all strings $x < y < z$). A set A is *p-m-incompressible* if A is $\mathbf{DTIME}(n^k)$-m-incompressible for all $k \geq 1$.

Lemma 4.7 (Ambos-Spies, Neis and Terwijn [ANT94]). Let A be $n\cdot t(n)$-generic. Then A is $\mathbf{DTIME}(t(2^n-1))$-m-incompressible.

Proof. Fix $g \in \mathbf{DTIME}(t(2^n-1))$ and B such that $A(x) = B(g(x))$ for all x. Then g is *consistent* with A, i.e.,

$$\forall\, x, y\ (g(x) = g(y) \Rightarrow A(x) = A(y)).$$

Define the simple $n\cdot t(n)$-extension function f by letting $f(X\restriction x) = 1 - X(y)$ for the least $y < x$ such that $g(y) = g(x)$ if such a y exists, and by letting $f(X\restriction x)\uparrow$ otherwise.

Then, for any set X which meets f, g is not consistent with X. So, by $n\cdot t(n)$-genericity of A, f is not dense along A. Since $f(A\restriction x)\downarrow$ if x witnesses a violation of the injectivity of g, it follows that g is almost one-to-one. □

Note that any $t(n)$-m-incompressible set is $t(n)$-bi-immune (Ko and Moore [KoM75]). Incompressibility is frequently used in the following form.

Proposition 4.8. Let A be p-m-incompressible and let $A \leq_m^p B$ via g. There is a number n_0 such that

$$\forall n \geq n_0 \, \exists x \, (|x| = n \,\&\, |g(x)| \geq n).$$

Moreover, for $G = \{x : |g(x)| \geq |x| - 1\}$, $||G^{\leq n+1}|| \geq 2^n$ a.e.

Proof. There are 2^n strings of length n but only $2^n - 1$ strings of length less than n. □

For obtaining more properties of the $t(n)$-generic, hence the $t(n)$-random sets, it is useful to note that a $t(n)$-generic set does not only meet 1-bit extension functions but also those extension functions for which the extension is specified by a constant number of strings, and that it meets the extension functions not just once but infinitely often.

Proposition 4.9 (Ambos-Spies et al. [AFH87]). Let A be $t(n)$-generic and let f be a simple $t(n)$-extension function which is dense along A. Then A meets f at x for infinitely many strings x.

Proof. Given y, it suffices to show that A meets f at x for some $x \geq y$. Define the simple $t(n)$-extension function f_y by letting $f_y(X \restriction x) = f(X \restriction x)$ for strings $X \restriction x$ where $x \geq y$ and by letting $f_y(X \restriction x)$ be undefined otherwise. Then f_y is dense along A, whence A meets f_y. By definition of f_y this implies that A meets f for some $x \geq y$. □

Definition 4.10. A $t(n)$-extension function f is *k-bounded* ($k \geq 1$) if whenever $f(X \restriction x)$ is defined then $f(X \restriction x) = (x_0, i_0), \ldots, (x_l, i_l)$ for some $l < k$ (and for some $x_0, \ldots, x_l, i_0, \ldots, i_l$). If, moreover, $x_m = x + m$ for $m \leq l$ then f is *strongly k-bounded.*

Lemma 4.11. Let A be $n \cdot t(n)$-generic. Then A meets every k-bounded $t(n)$-extension function f which is dense along A at infinitely many strings x ($k \geq 1$).

Lemma 4.11 has been shown for strongly k-bounded extensions in [AFH87] and in its general form in [Am96].

Proof. Fix a k-bounded extension function f which is dense along A. W.l.o.g. we may assume that, for $X \restriction x$ in the domain of f, $f(X \restriction x)$ is of the form (4.1) with $m = k-1$. Define simple $n \cdot t(n)$-extension functions f_l ($l < k$) as follows. If there is no string $x < y$ such that, for some $x_0, \ldots, x_{k-1}, i_0, \ldots, i_{k-1}$, $f(X \restriction x) = (x_0, i_0), \ldots, (x_{k-1}, i_{k-1})$, $y = x_l$, and $X(x_j) = i_j$ for $j < l$, then let $f_l(X \restriction y)$ be undefined. Otherwise choose the least such x and let $f(X \restriction y) = i_l$. Then, by induction on l, f_l is dense along A and (by Proposition 4.9) A meets f_l infinitely often. By definition, however, if A meets f_{k-1} infinitely often then A meets f infinitely often too. □

We now apply Lemma 4.11 to give some properties of the n^3-generic (hence n^3-random) sets related to the polynomial time reducibilities. We observe that the n^3-generic sets separate the standard bounded query reductions. Here we consider the 1 (one-one), m (many-one), $btt(k)$ (bounded truth-table of norm k), btt (bounded truth-table) and tt (truth-table) reducibilities. (For definitions and more details, see e.g. Ladner et al. [LLS75].) For any polynomial reducibility p-r from above we let

$$\text{(4.2)}\quad \begin{array}{ll} \mathbf{P}_r(A) = \mathbf{P}_r^{\leq}(A) = \{B : B \leq_r^p A\} & (\textit{lower p-r-span} \text{ of } A) \\ \mathbf{P}_r^{-1}(A) = \mathbf{P}_r^{\geq}(A) = \{B : A \leq_r^p B\} & (\textit{upper p-r-span} \text{ of } A) \\ \mathbf{P}_r^{=}(A) = \{B : A =_r^p B\} & (\textit{p-r-degree} \text{ of } A) \end{array}$$

Theorem 4.12 ([AFH87],[ANT94]). Let A be n^3-generic. Then, for any $k \geq 1$,

$$\text{(4.3)}\quad \mathbf{P}_1(A) \subset \mathbf{P}_m(A) \subset \mathbf{P}_{btt(k)}(A) \subset \mathbf{P}_{btt(k+1)}(A) \subset \mathbf{P}_{btt}(A) \subset \mathbf{P}_{tt}(A).$$

Proof. As one can easily check,

$$\begin{array}{lll} A \oplus A \leq_m^p A, & & \\ \overline{A} \leq_{btt(1)}^p A, & & \\ A_k \leq_{btt(k+1)}^p A, & \text{where} & A_k = \{x : \{x, \ldots, x+k\} \cap A \neq \emptyset\} \\ A_\omega \leq_{tt}^p A, & \text{where} & A_\omega = \{0^k 1x : x \in A_k\} \end{array}$$

Hence it suffices to show that

$$\text{(4.4)}\quad A \oplus A \not\leq_1^p A$$

$$\text{(4.5)}\quad \overline{A} \not\leq_m^p A$$

$$\text{(4.6)}\quad A_k \not\leq_{btt(k)}^p A$$

$$\text{(4.7)}\quad A_\omega \not\leq_{btt}^p A$$

Now (4.7) is an easy consequence of (4.6). The other claims are proved by contradiction. For a fixed reduction refuting the claim, we define a simple or bounded n^2-extension function f such that f is dense along A but A does not meet f. By Lemma 4.11 this will contradict n^3-genericity of A. In the first two parts we use p-m-incompressibility of the n^2-generic sets to avoid case distinctions in the definition of the extension function.
1. Assume that $A \oplus A \leq_1^p A$ via the one-to-one function $g \in \mathbf{P}$. Then, for all strings x,

$$\text{(4.8)}\quad A(g(0x)) = A(g(1x)) \text{ and } g(0x) \neq g(1x).$$

Moreover, by injectivity of g, as in the proof of Proposition 4.8 we can argue that for all $n \geq 1$ there is a string x of length n such that $|g(0x)| \geq n$ and $|g(1x)| \geq n$. For each n let x_n be the least such string. Then f, defined by

$f(X\lceil 0^n) = (g(0x_n),0),(g(1x_n),1)$ and $f(X\lceil x)\uparrow$ otherwise, is a 2-bounded n^2-extension function which is dense along all sets. By (4.8), however, A does not meet f.
2. Assume that $\overline{A} \leq^p_m A$ via $g \in \mathbf{P}$. Then, for all strings x,

$$(4.9) \quad A(x) \neq A(g(x))$$

and, by Lemma 4.7 and Proposition 4.8, we may fix n_0 such that, for $n \geq n_0$, $|g(x)| \geq n$ for some string x of length n. Let x_n be the first such string. Then f, defined by $f(X\lceil 0^n) = (x_n,0),(g(x_n),0)$ and $f(X\lceil x)\uparrow$ otherwise, is a 2-bounded n^2-extension function which is dense along all sets but, by (4.9), A does not meet f.
3. Assume that $A_k \leq^p_{btt(k)} A$ via $g_0,\ldots,g_{k-1},h \in \mathbf{P}$ where $g_i : \{0,1\}^* \to \{0,1\}^*$ are selectors and $h : \{0,1\}^* \times \{0,1\}^k \to \{0,1\}$ is an evaluator so that

$$(4.10) \quad A_k(x) = h(x, A(g_0(x)),\ldots,A(g_{k-1}(x)))$$

for all strings x. Moreover, w.l.o.g., $g_0(x) < g_1(x) < \ldots < g_{k-1}(x)$ for all x. Define a total $(2k+1)$-bounded n^2-extension function f as follows. Given $X\lceil x$, let l be the least m such that $g_m(x) \geq x$ or $m = k$, let $i = h(x, X(g_0(x)),\ldots,X(g_{l-1}(x)),0,\ldots,0)$, and let $z_0,\ldots,z_n$ be the elements of

$$\{x,\ldots,x+k\} - \{g_0(x),\ldots,g_{k-1}(x)\}$$

in order. (Note that this difference is nonempty whence z_0 is defined.) Then

$$f(X\lceil x) = (z_0,1-i),(z_1,0),\ldots,(z_n,0),(g_l(x),0),\ldots,(g_{k-1}(x),0).$$

It remains to show that A does not meet f at x. Otherwise, $A(g_m(x)) = 0$ for $l \leq m < k$, whence $h(x,A(g_0(x)),\ldots,A(g_{k-1}(x))) = i$, while on the other side $A \cap \{x,\ldots x+k\} = A \cap \{z_0\}$ and $\| A \cap \{z_0\} \| = 1-i$, whence $A_k(x) = 1-i$. So (4.10) fails contrary to assumption. □

In the remainder of this section we will address some limitations of $t(n)$-genericity and the resulting differences between $t(n)$-genericity and $t(n)$-randomness. These limitations are illustrated by the following technical result, which we state without proof.

Theorem 4.13 (Ambos-Spies et al. [ANT94]). For any recursive function t, any recursive set B, and any recursive nondecreasing and unbounded function $s : N \to N$ there is a recursive $t(n)$-generic set G such that $\|(G\Delta B)^{=n}\| \leq s(n)$ for all n.

The first limitation of $t(n)$-genericity, which is typical for genericity in general, is that genericity alone does not suffice to control the frequency with which an extension function is met. By Proposition 4.9 we know that a $t(n)$-generic set G meets every simple $t(n)$-extension function which is dense along G infinitely often and, similarly, by symmetry, G avoids f at infinitely many strings. The relative frequency of these events, however, is not determined by G. E.g., for the extension function $f(X\restriction x) = 0$ requiring the next bit to be a 0, balanced occurrences of the events of A meeting and avoiding f at some string x will result in a set A satisfying the *law of large numbers*:

$$\text{(4.11)} \qquad \lim_{n\to\infty} \frac{\| \{x < n : A(x) = 0\} \|}{\| \{x < n : A(x) = 1\} \|} = 1$$

In particular such a set is exponentially dense. There are $t(n)$-generic sets, however, which are sparse.

Corollary 4.14 ([AFH88], [ANT94]). There is a sparse $t(n)$-generic set G.

Proof. In Theorem 4.13 let $B = \emptyset$ and $s(n) = n$. Then $\| G^{\leq n} \| \leq n^2$. □

In [AMWZ96] the concept of balanced $t(n)$-genericity is introduced which overcomes this shortcoming.

Definition 4.15 (Ambos-Spies, Mayordomo, Wang, Zheng [AMWZ96]). A set A is *balancedly $t(n)$-generic* if A *balancedly* meets every simple $t(n)$-extension function f which is dense along A, i.e., if

$$\text{(4.12)} \qquad \lim_{n\to\infty} \frac{\| \{x < n : A \text{ meets } f \text{ at } x\} \|}{\| \{x < n : f(A\restriction x)\downarrow\} \|} = \frac{1}{2}.$$

We will discuss this concept, which coincides with the resource-bounded version of the recursive randomness concept proposed by Church [Ch40], in the next section. There, in particular, we will show that any $t(n)$-random set is balancedly $t(n)$-generic.

Balancing $t(n)$-genericity, however, is not sufficient for completely subsuming $t(n)$-randomness. As shown in Lemma 4.11, $t(n)$-genericity does not only capture diagonalization steps of length 1 but also those of constant length. If the length of the diagonalization grows with the length of the string at which we (start to) diagonalize, however, then $t(n)$-genericity in general will fail. We will illustrate this phenomenon by considering necessary gaps in the $t(n)$-generic sets.

We say that a set A has *$s(n)$-gaps* ($s(n) \leq 2^n$) if, for infinitely many n, the first $s(n)$ strings of length n do not belong to A, i.e., if $A \cap \{0^n, 0^n + 1, \ldots, 0^n + s(n) - 1\} = \emptyset$. Note that A has 2^n-gaps iff A has exponential gaps in the sense of Example 2.10.4.

Lemma 4.16.

(a) For $t(n) \geq n^3$ and $k \geq 1$, every $t(n)$-generic set A has k-gaps.

(b) Let $l : N \to N$ be a recursive, nondecreasing, unbounded function. There is a recursive $t(n)$-generic set G without $l(n)$-gaps.

Proof. Part (a) follows from Lemma 4.11 by considering the k-bounded n^2-extension function $f(X\upharpoonright 0^n) = (0^n, 0), \ldots, (0^n + k - 1, 0)$. For a proof of part (b) apply Theorem 4.13 to $B = \{0,1\}^*$ and $s(n) = l(n) \dot{-} 1$. □

Though this limitation of $t(n)$-genericity extends to balanced $t(n)$-genericity, $t(n)$-randomness captures certain diagonalizations of non-constant length. In Section 8 we will discuss this in more detail.

5 Stochasticity

The first notion of randomness was proposed by von Mises [vM19] in 1919. He called a sequence $A \in \{0,1\}^\infty$ random if the sequence satisfies the law of large numbers (4.11) and if this property is inherited by every infinite subsequence of A obtained by an "admissible selection rule". In 1940 Church [Ch40] formalized this concept by interpreting "admissible selection" by recursive selection functions thereby introducing the first algorithmic randomness concept. Following Kolmogorov (see [USS90]) we call randomness based on the uniform distribution of 0*s* and 1*s* *stochasticity.*

Ambos-Spies, Mayordomo, Wang, and Zheng [AMWZ96] recently introduced $t(n)$-stochasticity, a resource-bounded version of Church's stochasticity concept, and they analyzed the relations between $t(n)$-stochasticity, $t(n)$-genericity, and $t(n)$-randomness. By giving characterizations of $t(n)$-stochasticity in terms of prediction functions, which are just simple extension functions, and in terms of martingales, they showed that $t(n)$-stochasticity and balanced $t(n)$-genericity coincide and that the following implications hold:

(5.1) $t(n)$-random $\Rightarrow$ $t(n)$-stochastic $\Rightarrow$ $t(n)$-generic

Here we summarize these results and give a few properties of the $t(n)$-stochastic sets.

Definition 5.1 (Church [Ch40] , Ambos-Spies et al. [AMWZ96]). A *selection function* is a total recursive function $f : \{0,1\}^* \to \{0,1\}$. A $t(n)$-*selection function* is a selection function $f \in \mathbf{DTIME}(t(n))$. The selection function f is *dense along* a set A if $f(A\upharpoonright x) = 1$ for infinitely many x. For f dense along A, the *subsequence* of A *selected* by f is the sequence

$$S[A, f] = i_0 i_1 i_2 \ldots \quad (i_n \in \{0, 1, \lambda\})$$

where $i_n = A(n)$ if $f(A\upharpoonright n) = 1$ and $i_n = \lambda$ otherwise. A set A is $t(n)$-*stochastic* if, for every $t(n)$-selection function f which is dense along A, the selected subsequence $S[A, f]$ satisfies the law of large numbers, i.e.,

$$\text{(5.2)} \quad \lim_{n\to\infty} \frac{\| \{x < n : f(A\upharpoonright x) = 1 \,\&\, x \in A\} \|}{\| \{x < n : f(A\upharpoonright x) = 1\} \|} = \frac{1}{2}.$$

Di Paola [Pa69] studied subrecursive versions of Church stochasticity corresponding to the Ritchie and Grzegorczyk hierarchies. Time-bounded stochasticity concepts, which are weaker than the one introduced above, were proposed by Wilber [Wi83] and Ko [Ko86]. For the relations among these resource-bounded stochasticity concepts see [AMWZ96].

To illustrate Definition 5.1, let $B \in \mathbf{DTIME}(t(2^n-1))$. Then f defined by $f(X\restriction n) = B(n)$ is a $t(n)$-selection function which selects the places x which are elements of B. So, for infinite B, f is dense along all sets A, and $A \cap B \neq \emptyset$ iff the sequence $S[A, f]$ contains at least one 1. So, for $t(n)$-stochastic A, $A \cap B \neq \emptyset$. By symmetry, it follows that every $t(n)$-stochastic set is $\mathbf{DTIME}(t(2^n-1))$-bi-immune.

By taking the n-selection function f selecting all places, i.e. $f(X\restriction x) = 1$ everywhere, $S[A, f] = A$, whence, by (5.2) every $t(n)$-stochastic set A satisfies the law of large numbers (4.11).

Proposition 5.2 ([AMWZ96]). Let A be $t(n)$-stochastic. Then A satisfies the law of large numbers, hence is exponentially dense.

Proof. By the above, it suffices to observe that (4.11) implies that $\|A^{\leq n}\| \geq 2^{n-1}$ for almost all n. □

For comparing $t(n)$-stochasticity with $t(n)$-genericity and $t(n)$-randomness it is convenient to characterize this concept in terms of *prediction* functions.

Definition 5.3 ([AMWZ96]). A *prediction function* f is a partial recursive function $f : \{0,1\}^* \to \{0,1\}$ with recursive domain. A $t(n)$-*prediction function* is a prediction function $f \in \mathbf{DTIME}(t(n))$. A prediction function f is *dense* along a set A if $f(A\restriction x)\downarrow$ for infinitely many x. f *predicts* A if f is dense along A and

$$(5.3) \qquad \limsup_{n\to\infty} \frac{\|\{x < n : f(A\restriction x)\downarrow = A(x)\}\|}{\|\{x < n : f(A\restriction x)\downarrow\}\|} > \frac{1}{2}.$$

A set A is $t(n)$-*predictable* if there is a $t(n)$-prediction function which predicts A, and A is $t(n)$-*unpredictable* otherwise.

Just like a martingale, a prediction function f can be interpreted as a strategy in a fair betting game on the successive bits of a hidden sequence $X \in \{0,1\}^\infty$. A player using this strategy who has seen the first n bits $X\restriction n$ of this sequence will predict that the next bit will be i if $f(X\restriction n) = i$ and he will not make any prediction for the next bit if $f(X\restriction n)\uparrow$. The player will win if he makes infinitely many predictions (i.e. if f is dense along X) and, for some $\epsilon > 0$, the ratio of the correct vs. the false predictions will be greater than or equal to $1+\epsilon$ infinitely often (i.e. f predicts X).

Note that making no prediction corresponds to splitting the capital in equal parts on the 0 and 1 outcomes in the martingale game. As we will see below, the martingale game is more flexible in allowing the player to express different degrees of confidence in the prediction, by allocating smaller or larger sums on the predicted bit. If we eliminate this option, however, both concepts are equivalent (see Theorem 5.6 below).

Note that a $t(n)$-prediction function is just a simple $t(n)$-extension function: Density along a set is defined in the same way for both concepts, and f correctly predicts a value $A(x)$ iff A meets f at x. So unpredictability and balanced genericity coincide. Moreover, selection and prediction functions can be expressed by each other whence we obtain the following equivalence.

Theorem 5.4 ([AMWZ96]). For any recursive function t and any set A, the following are equivalent.

(i) A is $t(n)$-stochastic

(ii) A is $t(n)$-unpredictable

(iii) A is balancedly $t(n)$-generic

Proof. We will prove the implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).
(i) $\Rightarrow$ (ii). Let A be $t(n)$-stochastic and let f be a $t(n)$-prediction function which is dense along A. We have to show that (5.3) fails. For a contradiction assume (5.3). Then, for some $i \in \{0, 1\}$, $f(A\restriction x) = i$ for infinitely many x and

$$\limsup_{n\to\infty} \frac{\|\{x < n : f(A\restriction x) = i = A(x)\}\|}{\|\{x < n : f(A\restriction x) = i\}\|} > \frac{1}{2}.$$

So, for the $t(n)$-selection function $\hat{f}$ defined by $\hat{f}(X\restriction x) = 1$ if $f(X\restriction x) = i$ and $\hat{f}(X\restriction x) = 0$ otherwise, $\hat{f}$ is dense along A and (5.2) fails for $\hat{f}$ (in place of f). So A is not $t(n)$-stochastic contrary to assumption.
(ii) $\Rightarrow$ (iii). Let A be $t(n)$-unpredictable and let f be a simple $t(n)$-extension function which is dense along A. We have to show that (4.12) holds. For a contradiction assume that (4.12) fails. Then

$$\limsup_{n\to\infty} \frac{\|\{x < n : f(A\restriction x)\downarrow = A(x)\}\|}{\|\{x < n : f(A\restriction x)\downarrow\}\|} > \frac{1}{2} \quad \text{or}$$

$$\liminf_{n\to\infty} \frac{\|\{x < n : f(A\restriction x)\downarrow = A(x)\}\|}{\|\{x < n : f(A\restriction x)\downarrow\}\|} < \frac{1}{2}.$$

Since f is a $t(n)$-prediction function the former is impossible by $t(n)$-unpredictability of A. Hence the latter must hold. So, for the $t(n)$-prediction function $\hat{f}$ defined by $\hat{f}(X\restriction x) = 1 - f(X\restriction x)$ if $f(X\restriction x)\downarrow$ and $\hat{f}(X\restriction x)\uparrow$ otherwise, $\hat{f}$ is dense along A and $\hat{f}$ satisfies (5.3). But this contradicts $t(n)$-unpredictability of A.
(iii) $\Rightarrow$ (i). Let A be balancedly $t(n)$-generic and let f be a $t(n)$-selection

function which is dense along A. We have to show that (5.2) holds. Define the simple $t(n)$-extension function $\hat{f}$ by letting $\hat{f}(X\restriction x) = 1$ if $f(X\restriction x) = 1$ and $\hat{f}(X\restriction x)\uparrow$ if $f(X\restriction x) = 0$. Then $\hat{f}$ is dense along A whence, by balanced $t(n)$-genericity, (4.12) holds for $\hat{f}$. Obviously this implies (5.2) for f.

$\square$

The proof that every $t(n)$-random set is $t(n)$-generic can be easily modified to show that every $t(n)$-random set is $t(n)$-stochastic too. In fact we can characterize $t(n)$-stochasticity in terms of a particular type of $t(n)$-martingales.

Definition 5.5 ([AMWZ96]). A martingale d is *simple* if it is induced by a strategy s with $range(s) \subseteq \{\frac{1}{2}, \alpha, 1-\alpha\}$ for some rational number $\alpha \in [0,1]$.

Theorem 5.6 ([AMWZ96]). A set A is $t(n)$-stochastic iff no simple $t(n)$-martingale succeeds on A. In particular, every $t(n)$-random set is $t(n)$-stochastic.

Proof. (Sketch). First assume that A is $t(n)$-stochastic and let d be a simple $t(n)$-martingale. We have to show that d does not succeed on A. Fix $\alpha > \frac{1}{2}$ such that $range(s) \subseteq \{\frac{1}{2}, \alpha, 1-\alpha\}$ for the strategy s underlying d and, for a contradiction, assume that d succeeds on A. Then

$$\limsup_{n\to\infty} \frac{\| \{x < n : \ d(A\restriction(x+1)) = 2\cdot\alpha\cdot d(A\restriction x)\} \|}{\| \{x < n : \ d(A\restriction(x+1)) = 2\cdot(1-\alpha)\cdot d(A\restriction x)\} \|} > 1$$

So, for the $t(n)$-prediction function f defined by $f(X\restriction x) = 0$ if $s(X\restriction x) = \alpha$, $f(X\restriction x) = 1$ if $s(X\restriction x) = 1-\alpha$, and $f(X\restriction x)\uparrow$ if $s(X\restriction x) = \frac{1}{2}$, f predicts A. By Theorem 5.4 this implies that A is not $t(n)$-stochastic contrary to assumption.

For a proof of the other direction, assume that no simple $t(n)$-martingale succeeds on A. We have to show that A is $t(n)$-stochastic. For a contradiction assume that A is not $t(n)$-stochastic. Then, by Theorem 5.4, there is a $t(n)$-prediction function f which predicts A. So we may fix $\epsilon > 0$ such that

$$(5.4) \qquad \frac{\| \{x < n : \ f(A\restriction x)\downarrow \neq A(x)\} \|}{\| \{x < n : \ f(A\restriction x)\downarrow = A(x)\} \|} < 1-\epsilon$$

for infinitely many n. Choose $\alpha \in (0,1)\cap Q$ such that

$$(5.5) \qquad (1+\alpha) \geq \left(\frac{1}{1-\alpha}\right)^{1-\frac{\epsilon}{2}}$$

and let d be the normed $t(n)$-martingale induced by the strategy s where

$$s(X\restriction x) = \begin{cases} (1+\alpha)/2 & \text{if } f(X\restriction x) = 0 \\ (1-\alpha)/2 & \text{if } f(X\restriction x) = 1 \\ 1/2 & \text{otherwise.} \end{cases}$$

Then it follows from (5.4) and (5.5) that d succeeds on A contrary to assumption.

$\square$

Like the weaker $t(n)$-genericity property, by Theorem 5.6, $t(n)$-stochasticity can be used to prove properties of $t(n)$-random sets. E.g., by Proposition 5.2, we have:

Corollary 5.7 ([AMWZ96]). Every $t(n)$-random set A satisfies the law of large numbers. Hence $||A^{\leq n}|| \geq 2^{n-1}$ a.e., whence A is exponentially dense. $\square$

As a second example we show that the $t(n)$-stochastic, hence the $t(n)$-random sets, are *normal* in the sense of Borel, where normality extends the law of large numbers from bits to finite sequences. For this we first observe that, as in the case of genericity, predictability of the next bit is equivalent to predictability of the next k bits.

Lemma 5.8. Let A be $n \cdot t(n)$-stochastic and let f be a $t(n)$-extension function such that $f(X \restriction x) = (x, i_0), \ldots, (x+k-1, i_{k-1})$ (for some $i_0, \ldots, i_{k-1} \in \{0, 1\}$) whenever $f(X \restriction x)$ is defined and such that f is dense along A. Then

$$\lim_{n \to \infty} \frac{||\{x < n : f(A \restriction x) = (x, A(x)), \ldots, (x+k-1, A(x+k-1))\}||}{||\{x < n : f(A \restriction x)\downarrow\}||} = \frac{1}{2^k}.$$

Proof. By a straightforward modification of the proof of Lemma 4.11. $\square$

Corollary 5.9 (Wang [Wa96], Schnorr [Sch71b]). Let A be n^2-stochastic or n^2-random. Then A is normal: For any string $x \neq \lambda$, the relative frequency of the occurrences of x in (the characteristic sequence of) A is $2^{-|x|}$, i.e.,

$$\lim_{n \to \infty} \frac{||\ \{m < n : (A \restriction m)x \sqsubseteq A\}\ ||}{n} = 2^{-|x|}.$$

Proof. Given a string x of length k, apply Lemma 5.8 to the total n-extension function $f(X \restriction y) = (y, x(0)), \ldots, (y+k-1, x(k-1))$. $\square$

6 Measure on Exponential Time

In this section we consider resource-bounded measure for the classes of linear-exponential time ($\mathbf{E}$) and polynomial-exponential time ($\mathbf{E}_2$). By considering families of time-classes in place of single time classes a measure with better closure properties can be obtained. Based on this observation, Lutz [Lu92] introduced measures for $\mathbf{E}$ and $\mathbf{E}_2$ which share some of the basic properties with the classical measure and which proved to be useful tools for the quantitative analysis of these important complexity classes. Since $(2^n)^k = 2^{nk}$, it follows from (1.1) that the n^k-measure corresponds to the class $\mathbf{DTIME}(2^{kn})$, whence the polynomial measure is adequate for $\mathbf{E}$. Similarly, the $2^{(log\ n)^k}$-measure, for $k \geq 1$, will correspond to $\mathbf{E}_2$.

Also note that, though $\mathbf{E} \subset \mathbf{E}_2$, $\mathbf{E}_2$ is the closure of $\mathbf{E}$ under p-m-equivalence: For any set $A \in \mathbf{DTIME}(2^{n^k})$ the set $\hat{A} = \{0^{n^k}1x : x \in A\}$ is p-m-equivalent to A and in $\mathbf{DTIME}(2^n)$.

Definition 6.1 (Lutz [Lu92]).

1. A class $\mathbf{C} \subseteq \{0,1\}^\infty$ has p-(p_2-)*measure* $0\,(1)$ if there is a $k \in \mathbf{N}$ such that $\mu_{n^k}(\mathbf{C}) = 0\,(1)$ $(\mu_{2^{(\log n)^k}}(\mathbf{C}) = 0\ (1))$.
2. A class $\mathbf{C} \subseteq \{0,1\}^\infty$ has *measure* 0 *in* $\mathbf{E}$ ($\mathbf{E}_2$) if $\mathbf{C} \cap \mathbf{E}$ ($\mathbf{C} \cap \mathbf{E}_2$) has p-(p_2-)*measure* 0, and we write $\mu(\mathbf{C} \mid \mathbf{E}) = 0$ $(\mu(\mathbf{C} \mid \mathbf{E}_2) = 0)$.
3. A class $\mathbf{C} \subseteq \{0,1\}^\infty$ has *measure* 1 *in* $\mathbf{E}$ ($\mathbf{E}_2$) if $\overline{\mathbf{C}}$ has measure 0 in $\mathbf{E}$ ($\mathbf{E}_2$), and we write $\mu(\mathbf{C} \mid \mathbf{E}) = 1$ $(\mu(\mathbf{C} \mid \mathbf{E}_2) = 1)$.
4. A set A is p-(p_2-)*random* if A is n^k-($2^{(log\ n)^k}$-)random for all $k \in N$.

Note that, by definition, the following relations hold among these measure concepts ($i \in \{0,1\}$, $\mathbf{C}$ any class):

$$\text{(6.1)}\qquad \begin{array}{ccccc} \mu_p(\mathbf{C}) = i & \Rightarrow & \mu_{p_2}(\mathbf{C}) = i & \Rightarrow & \mu(\mathbf{C}) = i \\ \Downarrow & & \Downarrow & & \\ \mu(\mathbf{C}|\mathbf{E}) = i & & \mu(\mathbf{C}|\mathbf{E}_2) = i & & \end{array}$$

(It will follow from results below that no other implications hold.)

The following union lemma for the p- and p_2-measure is a special case of the general union lemma in Section 3.

Lemma 6.2 (Union Lemma, [Lu92]). Let $\mathbf{C}_m, m \geq 0$, be classes such that $\mu_{n^k}(\mathbf{C}_m) = 0$ $(\mu_{2^{log(n)^k}}(\mathbf{C}_m) = 0)$ for some k and all m. Then $\mu_p(\mathbf{C}) = 0$ $(\mu_{p_2}(\mathbf{C}) = 0)$ for $\mathbf{C} = \bigcup_{m \geq 0} \mathbf{C}_m$. In particular, the finite union of p-(p_2-)measure-0 classes has p-(p_2-)measure 0 again.

Proof. Since $n^{k+4} \geq n^3 \cdot n^k \cdot log(n^k)^4$ a.e., $\mu_{n^{k+4}}(\mathbf{C}) = 0$ by Lemma 3.9 $\square$

To express the above measure concepts in terms of $t(n)$-randomness we use the close relations between resource-bounded measure and randomness pointed out in Section 3.

Lemma 6.3 ([ATZ94]). For any class $\mathbf{C}$ the following hold:

$$\text{(6.2)}\qquad \begin{array}{lcl} \mu_p(\mathbf{C}) = 0 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(n^k) \cap \mathbf{C} = \emptyset) \\ \mu_{p_2}(\mathbf{C}) = 0 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(2^{(log\ n)^k}) \cap \mathbf{C} = \emptyset) \\ \mu(\mathbf{C}|\mathbf{E}) = 0 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(n^k) \cap \mathbf{E} \cap \mathbf{C} = \emptyset) \\ \mu(\mathbf{C}|\mathbf{E}_2) = 0 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(2^{(log\ n)^k}) \cap \mathbf{E}_2 \cap \mathbf{C} = \emptyset) \end{array}$$

$$
(6.3)\quad
\begin{array}{rcl}
\mu_p(\mathbf{C}) \neq 0 & \Leftrightarrow & \forall\, k \in N(\mathbf{RAND}(n^k) \cap \mathbf{C} \neq \emptyset) \\
\mu_{p_2}(\mathbf{C}) \neq 0 & \Leftrightarrow & \forall\, k \in N(\mathbf{RAND}(2^{(log\ n)^k}) \cap \mathbf{C} \neq \emptyset) \\
\mu(\mathbf{C}|\mathbf{E}) \neq 0 & \Leftrightarrow & \forall\, k \in N(\mathbf{RAND}(n^k) \cap \mathbf{E} \cap \mathbf{C} \neq \emptyset) \\
\mu(\mathbf{C}|\mathbf{E}_2) \neq 0 & \Leftrightarrow & \forall\, k \in N(\mathbf{RAND}(2^{(log\ n)^k}) \cap \mathbf{E}_2 \cap \mathbf{C} \neq \emptyset)
\end{array}
$$

$$
(6.4)\quad
\begin{array}{rcl}
\mu_p(\mathbf{C}) = 1 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(n^k) \subseteq \mathbf{C}) \\
\mu_{p_2}(\mathbf{C}) = 1 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(2^{(log\ n)^k}) \subseteq \mathbf{C}) \\
\mu(\mathbf{C}|\mathbf{E}) = 1 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(n^k) \cap \mathbf{E} \subseteq \mathbf{C}) \\
\mu(\mathbf{C}|\mathbf{E}_2) = 1 & \Leftrightarrow & \exists\, k \in N(\mathbf{RAND}(2^{(log\ n)^k}) \cap \mathbf{E}_2 \subseteq \mathbf{C})
\end{array}
$$

Proof. Note that (6.3) and (6.4) follow from (6.2) by definition of the measure concepts. We prove the first equivalence in (6.2). (The proofs of the other equivalences are similar.) If $\mu_p(\mathbf{C}) = 0$ then $\mu_{n^k}(\mathbf{C}) = 0$ for some k, whence $\mathbf{RAND}(n^k) \cap \mathbf{C} = 0$ by Corollary 3.10. Conversely, if $\mathbf{RAND}(n^k) \cap \mathbf{C} = \emptyset$ then $\mu_{n^{k+4}}(\mathbf{C}) = 0$ by Corollary 3.10, whence $\mu_p(\mathbf{C}) = 0$. □

Corollary 6.4 ([ATZ94]). For $k \geq 1$ the class $\mathbf{RAND}(n^k)$ of the n^k-random sets has p-measure 1, and $\mathbf{RAND}(2^{(log\ n)^k})$ has p_2-measure 1. □

Moreover, the general results of Section 3 provide the following lower and upper bounds on the mimimum complexity of n^k-($2^{(log\ n)^k}$-)random sets.

Lemma 6.5 ([ATZ94]). For $k \geq 1$, there is an n^k-random set A in $\mathbf{DTIME}(2^{(k+5)n})$ but there is no such set in $\mathbf{DTIME}(2^{kn})$. Similarly, there is a $2^{(log\ n)^k}$-random set A in $\mathbf{DTIME}(2^{n^{k+1}})$ but there is no such set in $\mathbf{DTIME}(2^{n^k})$.

Proof. By the second part of Lemma 3.9 and the first part of Lemma 3.13 □

Using the above characterizations of the measure concepts for the exponential time classes we can show that these concepts are consistent and preserve essential properties of the classical measure in this setting.

Theorem 6.6 ([Lu92]).

(a) For any k, $\mu_p(\mathbf{DTIME}(2^{kn})) = 0$ and $\mu_{p_2}(\mathbf{DTIME}(2^{n^k})) = 0$, whence $\mu(\mathbf{DTIME}(2^{kn})|\mathbf{E}) = 0$ and $\mu(\mathbf{DTIME}(2^{n^k})|\mathbf{E}_2) = 0$.

(b) $\mathbf{E}$, $\mu(\mathbf{C}|\mathbf{E}) = 1$ ($\mu(\mathbf{C}|\mathbf{E}_2) \neq 0$)). For any class $\mathbf{C}$ such that $\mu(\mathbf{C}|\mathbf{E}) = 1$ ($\mu(\mathbf{C}|\mathbf{E}_2) = 1$), $\mu(\mathbf{C}|\mathbf{E}) \neq 0$ ($\mu(\mathbf{C}|\mathbf{E}_2) \neq 0$). In particular, $\mu(\mathbf{E}|\mathbf{E}) \neq 0$ and $\mu(\mathbf{E}_2|\mathbf{E}_2) \neq 0$ (whence $\mu_p(\mathbf{E}) \neq 0$ and $\mu_{p_2}(\mathbf{E}_2) \neq 0$).

Proof. We consider only the linear exponential case.
(a) By Lemma 6.5, $\mathbf{DTIME}(2^{kn}) \cap \mathbf{RAND}(n^k) = \emptyset$ whence the claim follows from (6.2).
(b) Assume that $\mu(\mathbf{C}|\mathbf{E}) = 1$. By (6.4) there is a number k such that $\mathbf{RAND}(n^k)$

$\cap \mathbf{E} \subseteq \mathbf{C}$. Since, for $k' \geq k$, any $n^{k'}$-random set is n^k-random too, it follows with Lemma 6.5, that, for all k', there is an $n^{k'}$-random set in $\mathbf{E} \cap \mathbf{C}$. By (6.3) this implies $\mu(\mathbf{C}|\mathbf{E}) \neq 0$. □

While the second part of the theorem shows the consistency of the measure on $\mathbf{E}$ and $\mathbf{E}_2$, the first part implies that, for any set A of the corresponding universe ($\mathbf{E}$ or $\mathbf{E}_2$), the singleton $\{A\}$ has measure 0 as in the classical case. Moreover, as there, subclasses of measure-0 classes have measure 0 again.

Lutz and others used the measures on $\mathbf{E}$ and $\mathbf{E}_2$ for a quantitative analysis of structural properties of the exponential time sets. In the following we give some examples, where we restrict ourselves to the measure on $\mathbf{E}$.

We start with some properties which can be obtained from the genericity concept of Section 4 by the following observation.

Lemma 6.7 ([ANT94]). For any $k \geq 1$, the class of the n^k-generic sets has p-measure 1.

Proof. By Theorem 4.5 and by (6.4). □

Theorem 6.8. The following classes have p-measure 1 hence measure 1 in $\mathbf{E}$:

(i) the $\mathbf{DTIME}(2^{kn})$-bi-immune sets (for any fixed $k \geq 1$; Mayordomo [Ma94a])

(ii) the $\mathbf{DTIME}(2^{kn})$-m-incompressible sets (for any fixed $k \geq 1$; Juedes and Lutz [JL95a])

(iii) the p-btt-incomplete sets for $\mathbf{E}$ (Ambos-Spies et al. [ANT94])

Proof. By Lemma 6.7, parts (i) and (ii) are immediate by Lemmas 4.6 and 4.7, respectively. For a proof of part (iii) assume that A is p-btt-complete for $\mathbf{E}$ and let B be a p-m-complete set for $\mathbf{E}$. Then, for some $k \in N$, $B \leq^p_{btt(k)} A$, whence, by p-m-completeness of B, $C \leq^p_{btt(k)} A$ for all $C \in \mathbf{E}_2$ (recall that every complete set for $\mathbf{E}$ is complete for $\mathbf{E}_2$ too). Since $\mathbf{E}_2$ is closed under p-T-reductions, hence p-btt-reductions, it follows that $\mathbf{E}_2 = \mathbf{P}^{\leq}_{btt(k)}(A) = \mathbf{P}^{\leq}_{btt}(A)$. So, by Theorem 4.12, A is not n^3-generic. By Lemma 6.7 this completes the proof. □

By using the same approach we can classify the measure in $\mathbf{E}$ of another interesting property which plays an important role in the structural analysis of the class $\mathbf{NP}$. Selman [Se79] calls a set A *p-selective* if there is a function $g \in \mathbf{P}$, $g : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ such that, for all strings x and y, $g(x,y) \in \{x,y\}$ and, if $x \in A$ or $y \in A$ then $g(x,y) \in A$. The function g is called a *selector* for A.

Lemma 6.9 ([AFH87]). If A is n^2-generic then A is not p-selective. Hence the class of p-selective sets has p-measure 0.

Proof. Assume that A is n^2-generic and fix $g \in \mathbf{P}$ such that $g(x,y) \in \{x,y\}$ for all strings $x, y \in \{0,1\}^*$. Define the total 2-bounded n-extension function f by

$$f(X \upharpoonright x) = \begin{cases} (x,0),(x+1,1) & \text{if} \quad g(x,x+1) = x \\ (x,1),(x+1,0) & \text{if} \quad g(x,x+1) = x+1 \end{cases}$$

Then, by Lemma 4.11, A meets f. Obviously this implies that g is not a selector for A. □

We will discuss some concepts related to p-selectivity in Section 8.

The above genericity approach is limited to properties not requiring any "balanced" actions. In such cases, however, stochasticity can be used in place of genericity.

Lemma 6.10. For $k \geq 1$, the class of the n^k-stochastic sets has p-measure 1.

Proof. By Theorem 5.6 and by (6.4). □

Lemma 6.11 ([Lu92]). The class of the exponentially dense sets has p-measure 1. In particular, the class of sparse sets has p-measure 0.

Proof. By Proposition 5.2 and Lemma 6.10. □

In the remainder of this section we discuss the question to what extent the $\leq^p_m$-successors and predecessors of a random set A can be random again. (The reader may observe that we will obtain corresponding results if we replace $t(n)$-randomness by $t(n)$-genericity or $t(n)$-stochasticity.) First we show that randomness of the successors is bounded by the complexity of A. This follows from the following fact.

Lemma 6.12 (Juedes and Lutz [JL95a], Lindner [Li93]). Let $A \in \mathbf{DTIME}(2^{kn})$ be p-m-incompressible and let $A \leq^p_m B$. Then B is not $\mathbf{DTIME}(2^{(k+1)n})$-bi-immune.

Proof. Fix g such that $A \leq^p_m B$ via g. By p-m-incompressibility of A there are infinitely many strings x such that $|g(x)| \geq |x|$ (cf. Proposition 4.8). Moreover, by symmetry, we may assume that $x \in A$ for infinitely many such strings x. So, for $C = \{y : \exists x(|x| \leq |y| \;\&\; g(x) = y \;\&\; x \in A)\}$, $C \in \mathbf{DTIME}(2^{(k+1)n})$, C is infinite and $C \subseteq B$. □

Theorem 6.13 ([ANT94], [ATZ94]). Let $A \in \mathbf{DTIME}(2^{kn})$ be n^2-random and assume that $A \leq^p_m B$. Then B is not n^{k+1}-random.

Proof. By Lemma 6.12, this follows from Theorem 4.5 and Lemmas 4.6 and 4.7. □

For the other direction, Ambos-Spies et al. [ATZ94] also proved the following expansion of randomness below a random set.

Theorem 6.14 ([ATZ94]). Let A be an n^2-random set. For any $k \geq 1$ there is an n^k-random set $A_k \leq_m^p A$. In fact, there is a p-random set A_∞ with $A_\infty \leq_m^p A$ and, for any $k \geq 1$, there is a $2^{(log\ n)^k}$-random set B_k with $B_k \leq_m^p A$. If, moreover, $A \in \mathbf{E}$ then A_k and A_∞ can be chosen so that $A_k \in \mathbf{E}$ and $A_\infty \in \mathbf{DTIME}(2^{n^2})$, and if $A \in \mathbf{E}_2$ then B_k can be chosen to be in $\mathbf{E}_2$.

Proof. We sketch the proof of the part related to the sets A_k. Let $A_k = \{x : 0^{k \cdot |x|}x \in A\}$. Then $A_k \leq_m^p A$ via $g(x) = 0^{k \cdot |x|}x$ and, for $A \in \mathbf{DTIME}(2^{cn})$, $A_k \in \mathbf{DTIME}(2^{(k+1)cn})$. So it suffices to show that A_k is n^k-random.

Let d be a normed n^k-martingale. To show that d does not succeed on A_k, from d we construct an n^2-martingale $\hat{d}$ such that $\hat{d}$ will succeed on A if d succeeds on A_k. So, by n^2-randomness of A, d can not succeed on A_k.

For the definition of $\hat{d}$, use the following notation: For a string $X \restriction 0^{k \cdot |x|}x$ let $\tilde{X} \restriction x$ be defined by $\tilde{X}(y) = X(0^{k \cdot |y|}y)$ for $y < x$. Then, for the strategy $s \in \mathbf{DTIME}(n^k)$ underlying d, let $\hat{s}(X \restriction 0^{k \cdot |x|}x) = s(\tilde{X} \restriction x)$ and, for any string $X \restriction y$ not of this form let $\hat{s}(X \restriction y) = \frac{1}{2}$. As one can easily check, $\hat{s} \in \mathbf{DTIME}(n^2)$ and, for $\hat{d} = d[\hat{s}]$, $\hat{d}(A \restriction 0^{k \cdot |x|}x) = d(A_k \restriction x)$ for all strings x.

The other parts of the theorem are proved similarly by letting $A_\infty = \{x : 0^{(|x|+1)(log(|x|+1))}x \in A\}$ and $B_k = \{x : 0^{|x|^{k+1}}x \in A\}$. □

Theorem 6.14 implies that, for complexity classes which are downward closed under $\leq_m^p$, the p-measure and the p_2-measure coincide. So interesting complexity classes as **NP**, **PSPACE**, **BPP** have the same measure in $\mathbf{E}$ and $\mathbf{E}_2$. Moreover, Theorem 6.14 yields further characterizations of the measure of such classes in terms of $t(n)$-randomness.

Corollary 6.15 ([JL95b], [ATZ94]). Let $\mathbf{C}$ be downward closed under $\leq_m^p$. The following are equivalent:

(i) For some $k \geq 2$, $\mathbf{C}$ contains an n^k-random set.

(ii) For all $k \geq 2$, $\mathbf{C}$ contains an n^k-random set.

(iii) For all $k \geq 2$, $\mathbf{C}$ contains a $2^{(\log n)^k}$-random set.

(iv) $\mu_p(\mathbf{C}) \neq 0$.

(v) $\mu_{p_2}(\mathbf{C}) \neq 0$.

Proof. Obviously, (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i) and, by (6.3), (ii) $\Leftrightarrow$ (iv) and (iii) $\Leftrightarrow$ (v). So it suffices to show that (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). But this holds by Theorem 6.14. $\Box$

Corollary 6.16 ([JL95b]). Let $\mathbf{C}$ be closed under $\leq^p_m$-reducibility. Then the following hold.

(i) $\mu_p(\mathbf{C}) = 0 \Leftrightarrow \mu_{p_2}(\mathbf{C}) = 0$

(ii) $\mu(\mathbf{C}|\mathbf{E}_2) = 0 \Rightarrow \mu(\mathbf{C}|\mathbf{E}) = 0$

Proof. By Corollary 6.15 and Lemma 6.3. $\Box$

Remark 6.17 ([JL95b]). Note that the implication in Corollary 6.16(ii) cannot be reversed. For a p-random set $A \in \mathbf{E}_2$, let $\mathbf{C} = \mathbf{P}^{\leq}_m(A)$. Then, by Theorem 6.14, $\mathbf{C} = \mathbf{C} \cap \mathbf{E}_2$ contains $2^{(log\ n)^k}$-random sets for all $k \geq 1$, whence $\mu(\mathbf{C}|\mathbf{E}_2) \neq 0$ by (6.3). By Theorem 6.13, however, $\mathbf{P}^{\leq}_m(A) \cap \mathbf{E}$ does not contain any n^2-random set, whence $\mu(\mathbf{C}|\mathbf{E}) = 0$ by (6.2).

As Theorem 6.14 shows, the class of n^k-random sets is invariant under certain selection functions. This observation has been generalized by Wang [Wa96] who proved a general invariance lemma for prediction functions.

Definition 6.18 (Wang [Wa96]). Let A be a set and let f be a prediction function. Then the set $A\Delta f$ is defined by its characteristic sequence $A\Delta f = i_0 i_1 i_2 \ldots$ ($i_n \in \{0, 1, \lambda\}$) where

$$i_n = \begin{cases} 1 & \text{if} \quad f(A{\restriction}n){\downarrow} \neq A(n) \\ 0 & \text{if} \quad f(A{\restriction}n){\downarrow} = A(n) \\ \lambda & \text{if} \quad f(A{\restriction}n){\uparrow} \end{cases}$$

Note that $A\Delta f$ is the sequence of the results of the prediction function f on A, where 0 (1) indicates that the prediction is correct (false).

Lemma 6.19 (Wang [Wa96]). Let A be $n \cdot t(n)$-generic/stochastic/random and let f be a $t(n)$-prediction function which is dense along A. Then $A\Delta f$ is $t(n)$-generic/stochastic/random.

Proof. We describe the case of random A. Let d be a $t(n)$-martingale. As in the proof of Theorem 6.14, it suffices to define an $n \cdot t(n)$-martingale $\hat{d}$ such that $\hat{d}$ succeeds on A if d succeeds on $A\Delta f$. For any string $X{\restriction}m$ let $(X{\restriction}m)\Delta f = i_0 \ldots i_{m-1}$ where $i_n = 0$ if $f(X{\restriction}n){\downarrow} = X(n)$, $i_n = 1$ if $f(X{\restriction}n){\downarrow} \neq X(n)$, and $i_n = \lambda$ otherwise ($n < m$). Then the martingale $\hat{d}$ with $\hat{d}(X{\restriction}n) = d((X{\restriction}n)\Delta f)$ will have the required properties. $\Box$

In the following we give some applications of this invariance lemma.

Example 6.20. Let A be n^{k+1}-random (generic, stochastic).

1. For any string x let $A_x = \{y : xy \in A\}$. Then $A_x = A\Delta f$ for the n-prediction function f defined by $f(X\restriction z) = 0$ if $z = xy$ for some string y and $f(X\restriction z)\uparrow$ otherwise. So A_x is n^k-random (generic, stochastic).

2. Let $B \in \mathbf{DTIME}(2^{kn})$ and let $A\Delta B$ be the symmetric difference of A and B. Then $A\Delta B = A\Delta f$ for the total n^k-prediction function $f(X\restriction n) = B(n)$, whence $A\Delta B$ is n^k-random (generic, stochastic). In particular (for $B = \Sigma^*$), $\overline{A}$ is n^k-random (generic, stochastic).

The second example implies that a proper subclass $\mathbf{C}$ of $\mathbf{E}$ ($\mathbf{E}_2$) which is closed under symmetric difference or union and intersection does not have measure 1 in $\mathbf{E}$ ($\mathbf{E}_2$).

Lemma 6.21 (Regan, Sivakumar, and Cai [RSC95]). Let $\mathbf{C}$ be a class such that $\mu(\mathbf{C}|\mathbf{E}) = 1$ ($\mu(\mathbf{C}|\mathbf{E}_2) = 1$) and $\mathbf{C}$ is either closed under symmetric difference or closed under union and intersection. Then $\mathbf{E} \subseteq \mathbf{C}$ ($\mathbf{E}_2 \subseteq \mathbf{C}$).

Proof. We only consider the case of $\mathbf{E}$. By (6.4), fix k such that

(6.5) $\quad \mathbf{RAND}(n^k) \cap \mathbf{E} \subseteq \mathbf{C}$

and let A be any set in $\mathbf{E}$, say $A \in \mathbf{DTIME}(2^{k'n})$ where w.l.o.g. $k' > k$. To show that $A \in \mathbf{C}$, let R be any $n^{k'+2}$-random set in $\mathbf{E}$. Then $R, \overline{R}, R\Delta A, \overline{R}\Delta A \in \mathbf{E}$, and, by Example 6.20.2, these sets are n^k-random. So $R, \overline{R}, R\Delta A, \overline{R}\Delta A \in \mathbf{C}$ by (6.5). Since $A = (R\Delta A)\Delta R$ and $A = [(R\Delta A) \cap \overline{R}] \cup [(\overline{R}\Delta A) \cap R]$, $A \in \mathbf{C}$ follows by the closure properties of $\mathbf{C}$. □

Corollary 6.22. The following are equivalent.

(i) $\mathbf{E}_2 = \mathbf{NP}$

(ii) $\mu(\mathbf{NP}|\mathbf{E}) = 1$

(iii) $\mu(\mathbf{NP}|\mathbf{E}_2) = 1$.

Proof. Since $\mathbf{NP} \subseteq \mathbf{E}_2$ and $\mathbf{NP}$ is closed under $\leq^p_m$, union and intersection, this follows from Lemma 6.21. □

7 Polynomial Reducibilities and Weak Completeness

In this section we present one of the applications of the measure on $\mathbf{E}$ (and $\mathbf{E}_2$) in detail. In classical recursion theory, Sacks (see [Ro67]) has shown that for the standard recursive reducibilities like $\leq_m$ and $\leq_T$, the upper and the lower span of any nonrecursive set A have measure 0:

$$\mu(\{B:\ B \leq_r A\}) = \mu(\{B:\ A \leq_r B\}) = 0$$

(since $\{B : B \leq_r A\}$ is countable, the first part is trivial). Corresponding results for the polynomial time reducibilities in part depend on the still unresolved question of how **BPP** is related to **P**: For $r \in \{tt, T\}$,

$$\text{(7.1)} \quad \mu(\mathbf{P}_r^{\geq}(A)) = 0 \Leftrightarrow A \notin \mathbf{BPP}$$

whereas for $r \in \{1, m, btt\}$,

$$\text{(7.2)} \quad \mu(\mathbf{P}_r^{\geq}(A)) = 0 \Leftrightarrow A \notin \mathbf{P}$$

(see [BG81], [Am86a], [Am86b], [TB91]). In any case, by countability, $\mu(\mathbf{P}_r^{\leq}(A)) = 0$.

Here we study the question to what extent these results carry over to the measure on $\mathbf{E}$ and $\mathbf{E}_2$. We concentrate on the case of $\leq_m^p$ and $\mathbf{E}$ and summarize the known results for the other reducibilities and for $\mathbf{E}_2$ at the end of this section. The following result, known as *small-span-theorem*, shows that, for any set in $\mathbf{E}$, at least one of its spans has to be small in $\mathbf{E}$.

Theorem 7.1 (Juedes and Lutz [JL95a]). For every set $A \in \mathbf{E}$,

$$\text{(7.3)} \quad \mu(\mathbf{P}_m^{\leq}(A)|\mathbf{E}) = 0$$

or

$$\text{(7.4)} \quad \mu_p(\mathbf{P}_m^{\geq}(A)) = \mu(\mathbf{P}_m^{\geq}(A)|\mathbf{E}) = 0$$

Proof. W.l.o.g. assume that (7.3) fails. Then, by (6.3), there is an n^2-random set $B \in \mathbf{P}_m^{\leq}(A) \cap \mathbf{E}$, say $\mathbf{B} \in \mathbf{DTIME}(2^{kn})$. By Theorem 6.13, B does not have any n^{k+1}-random successor under $\leq_m^p$, whence, by $B \leq_m^p A$, $\mathbf{P}_m^{\geq}(A) \cap \mathbf{RAND}(n^{k+1}) = \emptyset$. So (7.4) follows from (6.2). □

Corollary 7.2. For every set $A \in \mathbf{E}$, the p-m-degree of A has measure 0 in $\mathbf{E}$: $\mu_p(\mathbf{P}_m^{=}(A) \cap \mathbf{E}) = \mu(\mathbf{P}_m^{=}(A)|\mathbf{E}) = 0$. □

Corollary 7.3 (Mayordomo [Ma94a]). The class of p-m-complete sets for $\mathbf{E}$ has measure 0 in $\mathbf{E}$. □

Note that the restriction to $\mathbf{E}$ in (7.3) and in Corollary 7.2 is necessary: For a p-random set $B \in \mathbf{E}_2$, by padding we obtain a set $A \in \mathbf{E}$ with $A =_m^p B$. So $\mu_p(\mathbf{P}_m^{=}(A)) = \mu_p(\mathbf{P}_m^{=}(B)) \neq 0$ by (6.3).

Theorem 7.1 leaves the following three possible cases for the size of the p-m-spans of a set $A \in \mathbf{E}$:

(SS) $\mathbf{P}_m^{\leq}(A)$ and $\mathbf{P}_m^{\geq}(A)$ are small in $\mathbf{E}$, i.e.,
$\mu(\mathbf{P}_m^{\leq}(A)|\mathbf{E}) = \mu(\mathbf{P}_m^{\geq}(A)|\mathbf{E}) = 0$

(SN) $\mathbf{P}_m^{\leq}(A)$ is small but $\mathbf{P}_m^{\geq}(A)$ is not small in $\mathbf{E}$, i.e.,
$\mu(\mathbf{P}_m^{\leq}(A)|\mathbf{E}) = 0$ and $\mu(\mathbf{P}_m^{\geq}(A)|\mathbf{E}) \neq 0$

(NS) $\mathbf{P}_m^{\leq}(A)$ is not small but $\mathbf{P}_m^{\geq}(A)$ is small in $\mathbf{E}$, i.e.,
$\mu(\mathbf{P}_m^{\leq}(A)|\mathbf{E}) \neq 0$ and $\mu(\mathbf{P}_m^{\geq}(A)|\mathbf{E}) = 0$

In the following we will show that these possibilities actually occur and we will give some examples. Natural but trivial examples for the cases (SN) and (NS) are the sets in $\mathbf{P}$ and the p-m-complete sets for $\mathbf{E}$, respectively (by Theorem 6.6). By structural properties we get examples of sets of type (SS):

Lemma 7.4. Let $A \in \mathbf{E}$ be sparse and p-m-incompressible. Then $\mu_p(\mathbf{P}_m^{\leq}(A)) = \mu_p(\mathbf{P}_m^{\geq}(A)) = 0$.

Proof. Since A is p-m-incompressible, by Lemma 6.12, A does not have any $\mathbf{DTIME}(2^{kn})$-bi-immune successors (for some k), whence $\mu_p(\mathbf{P}_m^{\geq}(A)) = 0$ by Theorem 6.8 (i). On the other hand, as one can easily check, any p-m-incompressible predecessor of a sparse set is sparse too, whence, by sparseness of A,

$$\mathbf{P}_m^{\leq}(A) \subseteq \{B : B \text{ sparse }\} \cup \{B : B \ p\text{-}m\text{-compressible}\}$$

So $\mu_p(\mathbf{P}_m^{\leq}(A)) = 0$ by Lemma 6.11 and Theorem 6.8 (ii). □

In Buhrman and Mayordomo [BuM95] a natural example of a set of type (SS) is given: For any time constructible $t(n)$ such that $t(n) \in \mathbf{DTIME}(2^{O(1)\cdot n})$ and $2^{3n} \leq t(n)$ a.e., the set $R_{t(n)}$ of the strings which are incompressible in the sense of $t(n)$-time-bounded Kolmogorov complexity, i.e., $R_{t(n)} = \{x : K^{t(n)}(x) \geq |x|\}$, has small upper and lower span in $\mathbf{E}$. (In fact, $\mu_p(\mathbf{P}_{tt}^{\leq}(A)) = 0$ and, for each $k \in N$, $\mu_p(\mathbf{P}_{btt(k)}^{\geq}(A)) = 0$.)

As we shall show next, the sets of type (NS) are typical for $\mathbf{E}$. They are called weakly complete.

Definition 7.5 (Lutz [Lu95]). A set A is *weakly p-m-hard* for $\mathbf{E}$ if $\mu(\mathbf{P}_m^{\leq}(A)|\mathbf{E}) \neq 0$. A set A is *weakly p-m-complete* for $\mathbf{E}$ if $A \in \mathbf{E}$ and A is weakly p-m-hard for $\mathbf{E}$.

Lutz [Lu95] has shown that there are weakly p-m-complete sets which are not p-m-complete. Stronger existence results are implied by the following characterization of weak completeness.

Lemma 7.6 (Ambos-Spies, Terwijn and Zheng [ATZ94]). For any set $A \in \mathbf{E}$ the following are equivalent

(i) A is weakly p-m-complete for $\mathbf{E}$.

(ii) For every $k \geq 1$, there is an n^k-random set in $\mathbf{P}_m^{\leq}(A) \cap \mathbf{E}$.

(iii) There is an n^2-random set in $\mathbf{P}_m^{\leq}(A) \cap \mathbf{E}$.

Proof. The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) are immediate by definition and by (6.3), while the implication (iii) $\Rightarrow$ (i) follows from Theorem 6.14 and from (6.3). □

In particular, any n^2-random set in $\mathbf{E}$ is weakly p-m-complete. It follows with (6.4):

Theorem 7.7 ([ATZ94]). The class of weakly p-m-complete sets has measure 1 in $\mathbf{E}$.

Corollary 7.8 ([Lu95], [ATZ94]). There is a weakly p-m-complete set which is not p-m-complete, in fact not p-btt-complete, for $\mathbf{E}$.

Proof. By Theorem 7.7 this follows from Corollary 7.3 and Theorem 6.8 (iii), respectively. □

Since n^2-random sets in $\mathbf{E}$ are weakly p-m-complete, p-m-complete and weakly p-m-complete sets can have rather different properties (e.g. no complete set is p-bi-immune (Berman [Be76])). Still, certain properties of the complete sets extend to the weakly complete sets. As an example we consider the complexity cores of the weakly p-m-complete sets (c.f. Corollary 3.14). Orponen and Schöning [OS86] have shown that every p-m-hard set for $\mathbf{E}$ has an exponentially dense p-complexity core. In the following theorem, this observation, in a slightly stronger form, is extended to weakly hard sets. Call B an *exponential complexity core* of A if B is a $\mathbf{DTIME}(2^{n^\alpha})$-complexity core of A for some real $\alpha > 0$.

Theorem 7.9 (Juedes and Lutz [JL95a]). Every weakly p-m-hard set for $\mathbf{E}$ has an exponentially dense exponential complexity core.

Proof. The proof is a variation of the proof of Lemma 6.12. Let A be weakly p-m-hard for $\mathbf{E}$, choose $B \in \mathbf{RAND}(n^2) \cap \mathbf{E}$ and $g \in \mathbf{P}$ such that $B \leq_m^p A$ via g, and fix k such that $|g(x)| \leq |x|^k$ a.e. We claim that, for $C = \{x : |g(x)| \geq |x| - 2\}$, $g(C)$ is an exponentially dense $\mathbf{DTIME}(2^{n^\alpha})$-complexity core of A where $\alpha = 1/(k+1)$. Note that, by p-m-incompressibility of B and by Proposition 4.8, $\| g(C)^{\leq n^k} \| \geq \| C^{\leq n} \| - c$ a.e. for some constant c and $\| C^{\leq n} \| \geq 2^{n-1}$ a.e. Obviously this implies that $g(C)$ is exponentially dense. Finally, for a contradiction assume that $g(C)$ is not a $\mathbf{DTIME}(2^{n^\alpha})$-complexity core of A. Fix a Turing machine M which is consistent with A such that $M(x)\downarrow$ converges in less than $2^{|x|^\alpha}$ steps for infinitely many $x \in g(C)$. Then the Turing machine M' which on input x simulates $M(g(x))$ is consistent with B and infinitely often terminates in less than 2^n steps. So $\{0,1\}^*$ is not a $\mathbf{DTIME}(2^{2n})$-complexity core of B contrary to Corollary 3.14. $\square$

We close our discussion of the small-span theorem by observing that there are also nontrivial examples of sets of type (SN), though we do not know of any natural nontrivial examples.

Lemma 7.10. There is a set $C \in \mathbf{E} - \mathbf{P}$ such that $\mu(\mathbf{P}_m^{\geq}(C)|\mathbf{E}) \neq 0$.

Proof. We sketch the proof which duplicates the argument of the corresponding result in the category setting in [Am96]. Let $A \in \mathbf{E}$ be n^2-random. Fix the n^k-random sets $A_k = \{x : 0^{k\cdot|x|}x \in A\} \in \mathbf{E}$ from (the proof of) Theorem 6.14, let B be the set $\{0^{n!} : n \geq 0\} \in \mathbf{P}$, and define C by letting $C = A \cap B$. By $B \in \mathbf{P}$, $C \in \mathbf{E}$ while, by p-bi-immunity of A, $C \notin \mathbf{P}$. Moreover, for n with $k+1 \leq n$, $0^{n!} \in C$ iff $0^{n!} \in A$ iff $0^{n!/(k+1)} \in A_k$, whence $C \leq_m^p A_k$ for all k. So $\mu(\mathbf{P}_m^{\geq}(C)|\mathbf{E}) \neq 0$ by (6.3). $\square$

Essentially all of the above results hold for $\mathbf{E}_2$ in place of $\mathbf{E}$ too. Since $\mathbf{E}_2$ is closed under $\leq_m^p$-reducibility, however, in the corresponding small span theorem, (7.3) may be replaced by

$$\mu_{p_2}(\mathbf{P}_m^{\leq}(A)) = \mu(\mathbf{P}_m^{\leq}(A)|\mathbf{E}_2) = 0.$$

Ambos-Spies et al. [ANT94] have extended the small-span-theorem to p-$btt(k)$-reducibility (for all k) on $\mathbf{E}$ and thereby to p-btt-reducibility on $\mathbf{E}_2$. Whether the small-span-theorem can be extended to p-btt-reducibility on $\mathbf{E}$ too is still open. The possibility of a further extension to p-tt- or even p-T-reducibility, is related to the still open question about the relation between $\mathbf{BPP}$ and $\mathbf{E}_2$. If $\mathbf{BPP} = \mathbf{E}_2$ (an oracle relative to which these classes coincide can be found in Heller [He86]) then, by (7.1), $\mu(\mathbf{P}_{tt}^{\geq}(A)) \neq 0$, hence $\mu_p(\mathbf{P}_{tt}^{\geq}(A)) \neq 0$, for all sets $A \in \mathbf{E}_2$. So, in this case, any complete set for $\mathbf{E}$ has nonsmall upper and lower p-tt-spans, whence the small-span-theorem for p-tt- and p-T-reducibility would fail.

The weak completeness notions (for $\mathbf{E}$ and $\mathbf{E}_2$) for the standard polynomial reducibilities were recently compared by Ambos-Spies et al. [AMZ96]. Their results correspond to the results for the classical completeness notions (Berman [Be76], Homer et al. [HKR93], Watanabe [Wa87]). E.g. weak completeness for $\leq_1^p$, $\leq_m^p$ and $\leq_{btt(1)}^p$ coincides, whereas $\leq_{btt(k)}^p$, $\leq_{btt(k+1)}^p$, $\leq_{btt}^p$, $\leq_{tt}^p$, $\leq_T^p$ yield pairwise different weak completeness notions. The separation of weak p-tt-completeness and weak p-T-completeness for $\mathbf{E}_2$ was independently shown by Schuler [Sch96]. He showed that $\mathbf{E}_2$ is contained in the p-T-closure of the class of the average polynomial time sets whereas the p-tt-closure of this class has measure 0 in $\mathbf{E}_2$.

The concept of weak p-r-completeness for $\mathbf{E}$ can be strengthened by requiring that $A \in \mathbf{E}$ and

$$(7.5) \qquad \mu(\mathbf{P}_r^{\leq}(A)|\mathbf{E}) = 1$$

(and similarly for $\mathbf{E}_2$). Obviously any p-r-complete set A for $\mathbf{E}$ satisfies (7.5). Moreover, for $r \in \{btt, tt, T\}$, $\mathbf{P}_r^{\leq}(A)$ is closed under union and intersection, whence for these reducibilities (7.5) already implies p-r-completeness of A by Lemma 6.21. For $r = m$, however, an application of Lemma 6.21 only shows that a set $A \in \mathbf{E}$ satisfying (7.5) is p-$btt(2)$-complete for $\mathbf{E}$. The question whether or not A will be p-m-complete, however, is still open.

8 Beyond Stochasticity

For the examples of applications of $t(n)$-randomness in structural complexity given so far, $t(n)$-stochasticity or even $t(n)$-genericity was sufficient. It seems that the full power of $t(n)$-randomness is required for properties involving reducibilities not of the bounded-query-type (btt). Here we will give some examples of such applications. Historically, Ville [Vi39] was the first who pointed out the inadequacy of stochasticity for modelling randomness. Though stochasticity guarantees, in all admissible subsequences, the typical distribution of $0s$ and $1s$ in the limit (the law of large numbers), it does not determine the way this limit is reached. In contrast, as shown by Schnorr [Sch71b], any recursively random set A shows the typical rate of convergence expressed by the *law of the iterated logarithm*:

$$(8.1) \qquad \limsup_{n\to\infty} \frac{(2 \cdot \Sigma_{m<n} A(m)) - n}{\sqrt{2n\ \log(\log(n))}} = 1 \text{ and}$$

$$\liminf_{n\to\infty} \frac{(2 \cdot \Sigma_{m<n} A(m)) - n}{\sqrt{2n\ \log(\log(n))}} = -1.$$

Recently, Wang ([Wa96], [Wa96a]) has shown that, for sufficiently large k, any n^k-random set satisfies this law, whence the class of sets satisfying the law of the iterated logarithm has p-measure 1. Note that (8.1) implies that, for $i \in \{0, 1\}$, there are infinitely many n such that $||\{x \leq n : A(x) = i\}|| < ||\{x \leq n : A(x) = 1 - i\}||$, whereas Ville [Vi39] constructed a stochastic sequence A such that $||\{x \leq n : A(x) = 1\}|| > ||\{x \leq n : A(x) = 0\}||$ for all n. The difference between stochasticity and randomness can be also illustrated by the gaps in these sets. Ville's construction can be easily modified to show that, for any unbounded, nondecreasing function $s : N \to N$, there is a $t(n)$-stochastic set without $s(n)$-gaps. The sizes of necessary and possible gaps in typical sets, however, are as follows.

Lemma 8.1. (a) Let $s : N \to N$ be a function such that $\sum_{n=0}^{\infty} 2^{-s(n)} = \infty$. Then $\mu(\{A : A \text{ has } s(n)\text{-gaps}\}) = 1$.
(b) Let $s : N \to N$ be a function such that $\sum_{n=0}^{\infty} 2^{-s(n)} < \infty$. Then $\mu(\{A : A \text{ has } s(n)\text{-gaps}\}) = 0$.

Proof. For a proof of (a) fix $m \geq 1$. By Lemma 2.5 it suffices to show that, for $\mathbf{C} = \{A : \forall n \geq m\ (A \cap \{0^n, \ldots, 0^n + s(n) - 1\} \neq \emptyset)\}$, $\mu(\mathbf{C}) = 0$. A normed martingale d which succeeds on $\mathbf{C}$ is defined as follows: For $X\restriction x$ with $x < 0^m$, $d(X\restriction x) = 1$; for $X\restriction x$ where $X\restriction x = (X\restriction 0^n)0^k$ for $n \geq m$, $k < s(n)$, and $X \cap \{0^p, \ldots, 0^p + s(p) - 1\} \neq \emptyset$ for all p with $m \leq p < n$,

$$d((X\restriction x)i) = \begin{cases} d(X\restriction x) - 2^{k-s(n)} & \text{if} \quad i = 0 \\ d(X\restriction x) + 2^{k-s(n)} & \text{if} \quad i = 1 \end{cases};$$

and, for $i \in \{0,1\}$, $d((X\restriction x)i) = d(X\restriction x)$ in all other cases. Then, for $A \in \mathbf{C}$ and $n \geq m$,

$$d(A\restriction 0^{n+1}) = d((A\restriction 0^n)A(0^n)\ldots A(0^n + s(n) - 1)) = d(A\restriction 0^n) + \frac{1}{2^{s(n)}},$$

whence, by assumption, $\lim_{n\to\infty} d(A\restriction 0^n) = \infty$.

For a proof of (b) fix $c \in N$ such that $\sum_{n=0}^{\infty} 2^{-s(n)} < c$ and let $\mathbf{C} = \{A : A$ has $s(n)$-gaps$\}$. A martingale d which succeeds on $\mathbf{C}$ is defined as follows: $d(\lambda) = c$; for $X\restriction x$ such that $X\restriction x = (X\restriction 0^n)0^k$ for $k < s(n)$,

$$d((X\restriction x)i) = \begin{cases} d(X\restriction x) + 2^{k-s(n)} & \text{if} \quad i = 0 \\ d(X\restriction x) - 2^{k-s(n)} & \text{if} \quad i = 1; \end{cases}$$

and, for $i \in \{0,1\}$, $d((X\restriction x)i) = d(X\restriction x)$ in all other cases. Then

$$d(X\restriction 0^{n+1}) = \begin{cases} d(X\restriction 0^n) + 1 - 2^{-s(n)} & \text{if } X \cap \{0^n, \ldots, 0^n + s(n) - 1\} = \emptyset \\ d(X\restriction 0^n) - 2^{-s(n)} & \text{if } X \cap \{0^n, \ldots, 0^n + s(n) - 1\} \neq \emptyset \end{cases}$$

whence, for a set A having p $s(n)$-gaps in $A\restriction 0^m$, $d(A\restriction 0^m) = c + p - \sum_{n=0}^{m} 2^{-s(n)} \geq p$. $\square$

The two parts of Lemma 8.1 are special instances of the Borel-Cantelli Lemma which says that for an infinite sequence $\mathbf{C}_n$, $n \geq 0$, of measurable classes, $\mathbf{C}_\infty = \{A : \exists^\infty n(A \in \mathbf{C}_n)\}$ has measure 0 if $\sum_{n=0}^{\infty} \mu(\mathbf{C})$ converges and $\mu(\mathbf{C}_\infty) = 1$ if the classes $\mathbf{C}_n$ are independent and $\sum_{n=0}^{\infty} \mu(\mathbf{C}_n)$ diverges (see [Ha50]). For resource-bounded versions of this lemma, see Lutz and Mayordomo [LM94] and Regan and Sivakumar [RS95].

In the following we will only give a resource bounded version of the first part of Lemma 8.1 as an example. Since the strategies underlying the martingales in the proof of this lemma are *absolute*, i.e., the amount bet on the next string does not depend on the current capital as in the case of the *proportional* strategies used so far, we first have to express the former in terms of the latter.

Definition 8.2. An *absolute* (betting) *strategy* s is a function $s : \{0,1\}^* \to R$. An absolute $t(n)$-strategy is an absolute strategy $s : \{0,1\}^* \to Q$ such that $s \in \mathbf{DTIME}(t(n))$. The *(pseudo) martingale* $d_a[s,\alpha]$ of norm $\alpha > 0$ *induced* by s is inductively defined by $d_a[s,\alpha](\lambda) = \alpha$ and

$$d_a[s,\alpha]((X\restriction x)i) = d_a[s,\alpha](X\restriction x) + (1-2i)s(X\restriction x).$$

The absolute strategy s is α*-correct* if $d_a[s,\alpha](X\restriction x) \geq 0$ for all strings $X\restriction x$.

Note that, for α-correct s, $d_a[s,\alpha]$ is a martingale.

Proposition 8.3. Let s be an α-correct absolute $t(n)$-strategy where $\alpha \in Q$ and let $t'(n) \geq n \cdot t(n) \cdot \log(t(n))^2$. Then $d_a[s,\alpha]$ is a $t'(n)$-martingale

Proof. Since $d_a[s,\alpha](X\restriction x) = \alpha + \sum_{y<x}(1 - 2\cdot X(y)) \cdot s(X\restriction y)$, $d_a[s,\alpha] \in \mathbf{DTIME}(n \cdot t(n))$. So the claim follows from Proposition 3.2 (Note that, by $n \leq t(n), O(\log(n\cdot t(n))^2) = O(\log(t(n))^2)$). □

We are now ready to state a resource-bounded variant of Lemma 8.1.

Lemma 8.4. Let $s : N \to N$ be a function such that $s \in \mathbf{P}$ and $\sum_{n=0}^{\infty} 2^{-s(n)} = \infty$, let $X = \{x_n : n \geq 0\}$ be a set such that $X \in \mathbf{P}$ and $x_n + s(n) < x_{n+1}$ for all $n \in N$, and let $f : X \to \{0,1\}^*$ be a function such that $f \in \mathbf{DTIME}(2^n)$ and $|f(x_n)| = s(n)$ for all $n \in N$. For any n^4-random set A there are infinitely many numbers n such that $(A\restriction x_n)f(x_n) \sqsubset A$.

Proof. The proof is a variant of the proof of the first part of Lemma 8.1. Given $m \geq 1$, consider the absolute strategy s defined as follows: For $X\restriction x$ such that $X\restriction x = (X\restriction x_n)(f(x_n)\restriction k)$ for some $n \geq m$ and $k < s(n)$, and $(X\restriction x_p)f(x_p)$ is not extended by $X\restriction x$ for all p with $m \leq p < n$ let

$$s(X\restriction x) = \begin{cases} -2^{k-s(n)} & \text{if} \quad f(x_n)(k) = 0 \\ 2^{k-s(n)} & \text{if} \quad f(x_n)(k) = 1; \end{cases}$$

and let $s(X\restriction x) = 0$ in all other cases. Then s is 1-correct and the martingale $d_a[s,1]$ succeeds on all sets X such that $(X\restriction x_n)f(x_n)$ is not extended by X for all n. Moreover, as one can easily check, s is an absolute n^2-strategy, whence $d_a[s,1]$ is an n^4-martingale by Proposition 8.3. So $d_a[s,1]$ does not succeed on A, whence $(A\restriction x_n)f(x_n) \sqsubseteq A$ for some $n \geq m$. □

By letting $x_n = 0^n$ and $f(0^n) = 0^{s(n)}$, Lemma 8.4 implies

Corollary 8.5. Let $s : N \to N$ be a function $s \in \mathbf{P}$ such that $\sum_{n=0}^{\infty} 2^{-s(n)} = \infty$. Then any n^4-random set has $s(n)$-gaps. □

We next use Lemma 8.4 to give an application of $t(n)$-randomness in complexity theory related to p-selectivity (defined in Section 6) which is due to Wang [Wa96]. If f is a selector for a set A and $f(x,y) = x$ then $A(x)A(y) \neq 01$, whence one possibility for the value of $A(x)A(y) \in \{0,1\}^2$ can be ruled out. Beigel suggested the following generalization of p-selectivity: A set A is (p,k)-*approximable* if there is a function $f \in \mathbf{P}$, $f : (\{0,1\}^*)^k \to \{0,1\}^k$ such that $f(x_0,\ldots,x_{k-1}) \neq A(x_0)\ldots A(x_{k-1})$ for all strings $x_0,\ldots,x_{k-1}$, and a set A is p-*approximable* if A is (p,k)-approximable for some k. This notion was further extended by Ogihara [Og95], who replaced the constant k by an arbitrary function $g: N \to N$: A set A is $(p, g(n))$-*approximable* if there is a partial function $f \in \mathbf{P}$, $f : (\{0,1\}^*)^* \to \{0,1\}^*$, such that, for any number $k \geq 1$ and any strings $x_0,\ldots,x_{k-1}$ satisfying $g(max\{|x_0|,\ldots,|x_{k-1}|\}) \leq k$, $f(x_0,\ldots,x_{k-1})$ is defined, $f(x_0,\ldots,x_{k-1}) \in \{0,1\}^k$, and $f(x_0,\ldots,x_{k-1}) \neq A(x_0)\ldots A(x_{k-1})$. ($f$ is called a (p,g)-approximation function of A. Ogihara calls $(p,g(n))$-approximable sets p-$g(n)$-membership comparable.) Obviously, for any number $k \geq 2$ and any unbounded nondecreasing function g,

$$
\text{(8.2)} \qquad
\begin{array}{rcl}
p\text{-selective} & \Rightarrow & (p,2)\text{-approximable} \\
 & \Rightarrow & (p,k)\text{-approximable} \\
 & \Rightarrow & p\text{-approximable} \\
 & \Rightarrow & (p,g(n))\text{-approximable.}
\end{array}
$$

The observation that no n^2-generic set (hence no n^2-random set) is p-selective (Lemma 6.9) can be easily extended to show that no n^2-generic set is p-approximable (Gasarch). By Theorem 4.13, however, $t(n)$-genericity fails to capture non-$(p,g(n))$-approximability for unbounded and nondecreasing g, and, by the above mentioned variant of Ville's theorem, so does $t(n)$-stochasticity. ¿From Lemma 8.4 we can deduce, however, that n^4-randomness rules out $(p,g(n))$-approximability if g is not growing too fast.

Theorem 8.6 (Wang [Wa96]). Let A be n^4-random. Then A is not (p,n)-approximable.

Proof. Let $\hat{f} \in \mathbf{P}$ be a partial function such that, for all $k \geq 1$ and all strings $y_0 < \ldots < y_{k-1}$ with $|y_{k-1}| \leq k$, $\hat{f}(y_0,\ldots,y_{k-1})\downarrow \in \{0,1\}^k$. We have to show that $\hat{f}(y_0,\ldots,y_{k-1})\downarrow = A(y_0)\ldots A(y_{k-1})$ for some strings $y_0,\ldots,y_{k-1}$. In the hypothesis of Lemma 8.4 let $s(n) = log(n) + log(log(n)) + 4$, $x_n = 2 \cdot n \cdot s(n)$ and $f(x_n) = \hat{f}(x_n, x_n+1, \ldots, x_n + s(n) - 1)$. Note that $|x_n + s(n) - 1| = log((2n+1)\cdot s(n)) \leq log(n) + log(s(n)) + 2 \leq log(n) + log(2log(n)) + 2 \leq log(n) + log(log(n)) + 4 = s(n)$ for all sufficiently large n. So f is well defined and $(A\restriction x_n)f(x_n) \sqsubseteq A$ for some n, which completes the proof. □

Ogihara [Og95] has shown that any set which is p-tt-reducible to a p-selective set is $(p, log(n))$-approximable and Wang [Wa96] has shown that any set which is p-tt-reducible to a p-approximable set is (p,n)-approximable. Together with Theorem 8.6 this implies:

Corollary 8.7 (Wang [Wa96], Buhrman and Longpré [BuL96]). Let A be weakly p-tt-hard for $\mathbf{E}$. Then A is not p-selective, in fact not p-approximable.$\square$

This corollary extends Toda's result that no p-tt-hard set for $\mathbf{E}$ is p-selective ([To91]).

Another recent measure result, which does not seem to follow by the stochasticity approach, deals with the density of (weakly) hard sets for $\mathbf{E}$ under non-adaptive reductions with quasi-linear number of queries. For any function $s : N \to N$, we say that A is p-$tt(s(n))$-reducible to B if $A \leq_{tt}^{p} B$ via a reduction in which the number of queries on input x is bounded by $s(|x|)$.

Theorem 8.8 (Lutz and Mayordomo [LM94]). Let $\alpha \in (0, 1)$. Then

$$\mu_p(\{A : \exists B(A \leq_{tt(n^\alpha)}^{p} B \ \& \ B \text{ is not exponentially dense})\}) = 0.$$

Hence, any weakly p-$tt(n^\alpha)$-hard set for $\mathbf{E}$ is exponentially dense.

We omit the proof of this theorem. Recently Fu [Fu95] has independently proven a related result for Turing reducibility.

9 Largeness Axioms for NP

Lutz [Lu90] proposed to study the internal structure of $\mathbf{NP}$ under the hypothesis that $\mathbf{NP}$ does not have p-measure 0 and under related measure assumptions like $\mathbf{NP}$ not having measure 0 in $\mathbf{E}$. There are many properties which can be shown under these assumptions but which so far could not be obtained from the weaker assumption that $\mathbf{P} \neq \mathbf{NP}$ (see Lutz and Mayordomo [LM96]). On the other hand, these measure assumptions are *consistent* in the sense that they hold for some relativizations. In fact Kautz and Miltersen [KaM94] have shown that the class of oracles A such that $\mu_{p^A}(\mathbf{NP}^A) \neq 0$ has measure 1. Though there is no evidence that this relativization to a random oracle describes the unrelativized case, working with strong hypotheses might be of interest by pointing out the relations between possible structural properties of $\mathbf{NP}$. The plausibility of such a hypothesis may then be judged by its consequences. So Ambos-Spies [Am94] proposed to consider not only Lutz's measure axiom for $\mathbf{NP}$ but also weaker hypotheses. Here we shortly discuss some of the hypotheses proposed there. All of these axioms require the existence of sets with certain structural properties in $\mathbf{NP}$:

(N)	$\exists A \in \mathbf{NP}(A \notin \mathbf{P})$	(Nontriviality Hypothesis)
(S)	$\exists A \in \mathbf{NP}(A \notin \mathbf{P} \ \& \ A \text{ is sparse})$	(Sparseness Hypothesis)
(B)	$\exists A \in \mathbf{NP}(A \ p\text{-bi-immune})$	(Bi-immunity Hypothesis)
(G)	$\exists A \in \mathbf{NP}(A \ p\text{-generic})$	(Genericity Hypothesis)
(R)	$\exists A \in \mathbf{NP}(A \ p\text{-random})$	(Randomness Hypothesis)
(C)	$\exists A \in \mathbf{NP}(A \ p\text{-}m\text{-complete for } \mathbf{E}_2)$	(Completeness Hypothesis)

Note that

(9.1) (C) $\Rightarrow$ (R) $\Rightarrow$ (G) $\Rightarrow$ (B) $\Rightarrow$ (S) $\Rightarrow$ (N)

Namely, by the obvious relations between deterministic and nondeterministic time, $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{E}_2$ whence (N) is the weakest largeness axiom saying that $\mathbf{P} \subset \mathbf{NP}$ and (C) is the strongest largeness axiom saying that $\mathbf{NP} = \mathbf{E}_2$. The other nontrivial implications follow from the fact that every p-random set is p-generic (Theorem 4.5), every p-generic set is p-bi-immune (Lemma 4.6), and, for every p-bi-immune set A, the tally set $A \cap \{0\}^*$ is not in $\mathbf{P}$ (and, for $A \in \mathbf{NP}$, $A \cap \{0\}^* \in \mathbf{NP}$ too).

Moreover, these hypotheses are consistent in the sense that there are oracles relative to which they hold (see Heller [He86] for an oracle satisfying the strongest hypothesis (C)), and the implications are strict in the sense, that (9.1) relativizes and for any implication we can find an oracle relative to which the implication cannot be reversed.

By Corollary 6.15, the randomness hypothesis (R) is equivalent to Lutz's measure hypothesis.

Lemma 9.1. The following are equivalent

(i) $\mathbf{NP}$ contains a p-random set.

(ii) $\mathbf{NP}$ contains an n^k-random set for some $k \geq 2$.

(iii) $\mathbf{NP}$ contains $2^{(\log n)^k}$-random sets for all $k \geq 1$.

(iv) $\mu_p(\mathbf{NP}) \neq 0$.

(v) $\mu_{p_2}(\mathbf{NP}) \neq 0$. □

By the analog of Corollary 6.15 for genericity (see [Am96]), a similar robustness lemma for the genericity hypothesis follows.

Lemma 9.2. The following are equivalent

(i) $\mathbf{NP}$ contains a p-generic set.

(ii) $\mathbf{NP}$ contains an n^k-generic set for some $k \geq 2$.

(iii) $\mathbf{NP}$ contains $2^{(\log n)^k}$-generic sets for all $k \geq 1$. □

In the following we list some consequences of the different hypotheses.

The probably most spectacular consequence of the Nontriviality Hypothesis was Mahaney's theorem that the p-m-hard sets for $\mathbf{NP}$ are not sparse [Ma82]. Later this was extended to the p-btt-hard sets by Ogiwara and Watanabe [OW91]. Another consequence of (N) is the existence of sets in $\mathbf{NP}$ which are neither complete (for any of the standard polynomial reducibilities) nor in $\mathbf{P}$ (Ladner [La75]). In fact, the degree structure of $\mathbf{NP}$ is very rich; e.g. it contains so called minimal pairs (see Ambos-Spies [Am87] for a survey). Moreover, the honest and nonhonest polynomial reducibilities differ on **NP** (Ambos-Spies [Am89]).

The stronger Sparseness Hypothesis is equivalent to the existence of a tally set in **NP**-**P** which in term is equivalent to the hypothesis that $\mathbf{E} \neq \mathbf{NE}$, i.e., that deterministic and nondeterministic exponential time disagree. Among the consequences of (S) is the existence of sets in **NP**-**P** which are not disjunctively self-reducible and which are p-selective (Selman [Se79]).

The Bi-immunity Hypothesis implies the existence of arbitrarily sparse sets in $\mathbf{NP} - \mathbf{P}$: For p-bi-immune $A \in \mathbf{NP}$ and infinite $B \in \mathbf{P}$, $A \cap B \in \mathbf{NP} - \mathbf{P}$. So, e.g. for $B = \{0^{\delta(n)} : n \geq 0\}$ where $\delta(0) = 0$ and $\delta(n+1) = 2^{\delta(n)}$, $A \cap B$ will be super sparse in the sense of Hartmanis [Ha83] and in the (stronger) sense of Ambos-Spies [Am86]. The latter e.g. implies that there are sets in **NP** which are not p-T-autoreducible (in the sense of [Am84]) while the former implies that $\mathbf{EE} \neq \mathbf{NEE}$, i.e., that deterministic and nondeterministic double exponential time disagree (and, by using still sparser sets in **NP**, similar separations for larger time classes can be obtained). The hypothesis $\mathbf{EE} \neq \mathbf{NEE}$ in term implies the existence of an **NP** search problem which does not reduce to the corresponding decision problem (Bellare and Goldwasser [BeG94]).

The Genericity Hypothesis suffices to distinguish many of the standard polynomial time reducibilities on **NP**: For n^3-generic $A \in \mathbf{NP}$, the separations in (4.3) - with the possible exception of $\mathbf{P}_m(A) \neq \mathbf{P}_{btt(1)}(A)$ - are witnessed by sets in **NP**. So, by (the proof of) Theorem 4.12, $\leq_1^p$, $\leq_m^p$, $\leq_{btt(k)}^p$ for $k \geq 2$, $\leq_{btt}^p$ and $\leq_{tt}^p$ are mutually different on **NP**. (The relations between $\leq_m^p$ and $\leq_{btt(1)}^p$ and between $\leq_{tt}^p$ and $\leq_T^p$ on **NP** under the hypothesis (G) are not known.)

One of the most beautiful implications of Lutz's measure axiom is the separation of p-m-completeness and p-T-completeness (Lutz and Mayordomo [LM96]). As Ambos-Spies [Am94] has shown, in fact the Genericity Hypothesis is sufficient for this separation.

Theorem 9.3. Assuming (G), there is an **NP**-set A which is p-T-complete (in fact, p-$btt(3)$-complete) but not p-m-complete for **NP**.

Proof. Let C be p-m-complete for **NP**, let $G \in \mathbf{NP}$ be n^3-generic, and let $A = G_0 \oplus [(G_0 \cap C) \oplus (G_0 \cup C)]$ (where $G_0 = \{x : 0x \in G\}$; see Example 6.20.1). Obviously $A \in \mathbf{NP}$. Moreover, for any set $B \in \mathbf{NP}$, $B \leq_{btt(3)}^p A$ by the following reduction: Given the p-m-reduction g from B to C, for any string x,

$$\begin{aligned} x \in B \quad & \Leftrightarrow g(x) \in C \\ & \Leftrightarrow (g(x) \in G_0 \;\&\; g(x) \in G_0 \cap C) \vee (g(x) \notin G_0 \;\&\; g(x) \in G_0 \cup C). \end{aligned}$$

So it suffices to show that A is not p-m-complete for **NP**.

For a contradiction assume that A is p-m-complete. Then $G_1 \leq_m^p A$, say via h. Split G_1 into the 3 parts reducible to the components of A: For $z \in \{0, 10, 11\}$ and a fixed string $x_0 \notin G_0 \cup C$ (w.l.o.g. we may choose C and G so that $\lambda \notin G_0 \cup C$) let $B_z = \{x : h(x) = zy \text{ for some string } y\}$ and define h_z by requiring $h(x) = zh_z(x)$ for $x \in B_z$ and by letting $h_z(x) = x_0$ otherwise. Then the sets B_z are pairwise disjoint, $B_z \in \mathbf{P}$ and

$$G_1 \cap B_0 \leq_m^p G_0 \text{ via } h_0$$
$$G_1 \cap B_{10} \leq_m^p G_0 \cap C \text{ via } h_{10}$$
$$G_1 \cap B_{11} \leq_m^p G_0 \cup C \text{ via } h_{11}$$

Moreover, for $x \notin B_0 \cup B_{10} \cup B_{11}$, $h(x) \notin A$ whence w.l.o.g. we may assume that $h(x) = 0x_0$. So $B_0 \cup B_{10} \cup B_{11} = \{0,1\}^*$.

Now, by n^3-genericity of G, G_1 is n^2-generic (Example 6.20.1), hence p-m-incompressible (Lemma 4.7). So, by Proposition 4.8 and by definition of the functions h_z, for some $z \in \{0, 10, 11\}$,

$$\text{(9.2)} \quad \exists^\infty x \in B_z(|h_z(x)| \geq |x| - 2)$$

holds. Also note that, for $z \in \{0, 10\}$,

$$\text{(9.3)} \quad \forall x \in B_z(G_1(x) \leq G_0(h_z(x)))$$

and, for $z = 11$,

$$\text{(9.4)} \quad \forall x \in B_z(G_1(x) \geq G_0(h_z(x))).$$

So we may fix z such that (9.2) and (by symmetry) w.l.o.g. (9.3) hold.

Then the desired contradiction is obtained as follows: Define a 2-bounded n^2-extension function f by letting $f(X{\restriction}0^n) = (1x, 0), (0h_z(x), 1)$ for the least $x \in B_z$ such that $|x| = n+2$ and $|h_z(x)| \geq n$, if such an x exists, and by letting $f(X{\restriction}x)\uparrow$ otherwise. Now, by (9.2), f is dense along all sets, whence, by Lemma 4.11, G meets f. It follows that, for some $x \in B_z$,

$$G_1(x) = G(1x) = 0 < 1 = G(0h_z(x)) = G_0(h_z(x)).$$

So (9.3) fails contrary to the assumption. □

Examples of properties of **NP** which have been proven from the Randomness Hypothesis and which are not known to follow from the Genericity Hypothesis include those involving reducibilities which are not of the bounded query type (*btt*). E.g., (R) implies the following extension of the Ogiwara-Watanabe Theorem on the density of the p-*btt*-hard sets.

Theorem 9.4 (Lutz and Mayordomo [LM96]). Assume (R). Then, for any real number $\alpha < 1$, every p-$tt(n^\alpha)$-hard set for **NP** is exponentially dense.

Proof. By (R), every hard set for **NP** is weakly hard for **E**. So the claim follows from Theorem 8.8. □

Similarly, Wang's result on (p, n)-approximability (Section 8) implies:

Theorem 9.5 (Wang [Wa96]). Assume (R). No p-tt-hard set for **NP** is p-selective or p-approximable.

Proof. By Corollary 8.7 □

Under the weaker assumption (N), it is only known that no p-$tt(n^\alpha)$-hard set for **NP** is p-selective ($\alpha \in (0,1)$; see [Og95]).

Largeness Hypotheses for other polynomial complexity classes have been considered too. E.g. the result of Lautemann [La83] and Sipser and Gacs [Si83] that $\mathbf{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$ has been modified by Allender and Strauss [AS94] as follows: If $\mu_p(\Delta_2^p) \neq 0$ then $\mathbf{BPP} \subseteq \Delta_2^p$. For a survey of other recent results in this direction, see Lutz [Lu96].

10 Further Results

Due to lack of space our survey on resource-bounded measure and randomness and their applications in complexity theory cannot be complete. In particular some interesting recent developments and topics could not be treated.

Relations between measure and circuit size complexity, nonuniform complexity and Kolmogorov complexity have been investigated e.g. by Lutz [Lu92], Lutz and Mayordomo [LM94], and Buhrman and Mayordomo [BuM95]. Moreover, Regan et al. [RSC95] recently related resource-bounded measure to the natural proofs of Razborov and Rudich [RR94] and pseudorandom generators. For a survey of these results we refer to Lutz [Lu96].

An interesting characterization of the p-measure in terms of incompressibility was recently given by Buhrman and Longpré [BuL96].

Acknowledgements

We thank Levke Bentzien, Gunther Mainhardt and Frank Stephan for their comments and corrections.

References

[Am84] K. Ambos-Spies. P-mitotic sets. In *Logic and Machines: Decision Problems and Complexity*, Lecture Notes in Computer Science 171 (1984) 1-23, Springer Verlag.

[Am86] K. Ambos-Spies. Inhomogenities in the polynomial time degrees: the degrees of super sparse sets. *Information Processing Letters* 22 (1986) 113-117.

[Am86a] K. Ambos-Spies. Randomness, relativizations, and polynomial reducibilities. In *Proceedings of the First Structure in Complexity Theory Conference*, Lecture Notes in Computer Science 223 (1986) 23-34, Springer Verlag.

[Am86b] K. Ambos-Spies. Randomness, relativizations, and polynomial reducibilities. (Extended version of [Am86a].) Unpublished typescript, August 1986.

[Am87] K. Ambos-Spies. Polynomial time degrees of NP-sets. In *Trends in Theoretical Computer Science* (E. Börger, Ed.), 95-142, Computer Science Press, 1987.

[Am89] K. Ambos-Spies. Honest polynomial time reducibilities and the P=?NP problem. *Journal of Computer and System Sciences* 39 (1989) 250-281.

[Am94] K. Ambos-Spies. Largeness axioms for NP. Lecture at the *Annual Meeting of the Special Interest Group "Logik in der Informatik" of the Gesellschaft für Informatik (GI)*, Paderborn (Germany), May 1994 (Unpublished lecture notes).

[Am96] K. Ambos-Spies. Resource-bounded genericity. In *Computability, Enumerability, Unsolvability* (S.B. Cooper et al., Eds.), London Math. Soc. Lect. Notes Series 224 (1996) 1-59, Cambridge University Press.

[AFH84] K. Ambos-Spies, H. Fleischhack and H. Huwig. P-generic sets. In *Proceedings of the 11th Colloquium on Automata, Languages and Programming, ICALP '84*, Lecture Notes in Computer Science 172 (1984) 58-68, Springer Verlag.

[AFH87] K. Ambos-Spies, H. Fleischhack and H. Huwig. Diagonalizations over polynomial time computable sets. *Theoretical Computer Science* 51 (1987) 177-204.

[AFH88] K. Ambos-Spies, H. Fleischhack and H. Huwig. Diagonalizations over deterministic polynomial time. In *Proceedings of the First Workshop on Computer Science Logic, CSL '87*, Lecture Notes in Computer Science 329 (1988) 1-16, Springer Verlag.

[AMWZ96] K. Ambos-Spies, E. Mayordomo, Y. Wang and X. Zheng. Resource-bounded balanced genericity, stochasticity, and weak randomnesss. In *Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science, STACS 96*, Lecture Notes in Computer Science 1046 (1996) 63-74, Springer Verlag.

[AMZ96] K. Ambos-Spies, E. Mayordomo and X. Zheng. A comparison of weak completeness notions. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)*, 171-178, IEEE Computer Society Press, 1996.

[ANT94] K. Ambos-Spies, H.-C. Neis and S. A. Terwijn. Genericity and measure for exponential time. *Theoretical Computer Science* (to appear). Extended abstract in *Proceedings of the 19th International Symposium on Mathematical Foundations of Computer Science, MFCS '94*, Lecture Notes in Computer Science 841 (1994) 221-232, Springer Verlag.

[AS94] E. Allender and M. Strauss. Measure on small complexity classes with applications for BPP. In *Proceedings of the 35th Symposium on Foundations of Computer Science*, 807-818, IEEE Computer Society Press, 1994.

[AS95] E. Allender and M. Strauss. Measure on P: Robustness of the notion. In *Proceedings of the 20th International Symposium on Mathematical Foundations of Computer Science, MFCS '95*, Lecture Notes in Computer Science 969 (1995) 129-138, Springer Verlag.

[ATZ94] K. Ambos-Spies, S. A. Terwijn and X. Zheng. Resource bounded randomness and weakly complete problems. *Theoretical Computer Science* (to appear). Extended abstract in *Proceedings of the 5th International Symposium on Algorithms and Computation, ISAAC '94*, Lecture Notes in Computer Science 834 (1994) 369-377, Springer Verlag.

[BaS85] J. L. Balcázar and U. Schöning. Bi-immune sets for complexity classes. *Mathematical Systems Theory* 18 (1985) 1-10.

[Be76] L. Berman. On the structure of complete sets: Almost everywhere complexity and infinitely often speedup. In *Proceedings of the Seventeenth Annual Conference on Foundations of Computer Science*, 76-80, IEEE Computer Society Press, 1976.

[BeG94] M. Bellare and S. Goldwasser. The complexity of decision versus search. *SIAM Journal on Computing* 23 (1994) 97-119.

[BuL96] H. Buhrman and L. Longpré. Compressibility and resource bounded measure. In *Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science, STACS 96*, Lecture Notes in Computer Science 1046 (1996) 13-24, Springer Verlag.

[BuM95] H. Buhrman and E. Mayordomo. An excursion to the Kolmogorov random strings. In *Proceedings of the Tenth Annual Structure in Complexity Theory Conference*, 197-203, IEEE Computer Society Press, 1995.

[BDG95] J. L. Balcázar, J. Díaz and J. Gabarró. *Structural Complexity I.* Second edition. Springer Verlag, 1995.

[BG81] C. H. Benett and J. Gill. Relative to a random oracle $A, P^A \neq NP^A \neq co\text{-}NP^A$ with probability 1. *SIAM Journal on Computing* 10 (1981) 96-113.

[Ch40] A. Church. On the concept of a random sequence. *Bulletin of the American Mathematical Society* 46 (1940) 130-135.

[Fe91] S. A. Fenner. Notions of resource-bounded category and genericity. In *Proceedings of the Sixth Annual Structure in Complexity Theory Conference*, 196-212, IEEE Computer Society Press, 1991. 1985.

[Fu95] B. Fu. With quasi-linear queries, EXP is not polynomial time Turing reducible to sparse sets. *SIAM Journal on Computing* 24 (1995) 1082-1090.

[GHS87] J. Geske, D. Huyn and A. Selman. A hierarchy theorem for almost everywhere complex sets with applications to polynomial complexity degrees. In *Proceedings of the 4th Symposium on Theoretical Aspects of Computer Science, STACS 87*, Lecture Notes in Computer Science 247 (1987) 125-135, Springer Verlag.

[Ha50] P. R. Halmos. *Measure Theory.* Springer Verlag, 1950.

[Ha83] J. Hartmanis. On sparse sets in NP-P. *Information Processing Letters* 16 (1983) 55-60.

[He86] H. Heller. On relativized exponential and probabilistic complexity classes. *Information and Control* 71 (1986) 231-243.

[HKR93] S. Homer, S. Kurtz and J. Royer. A note on 1-truth-table complete sets. *Theoretical Computer Science* 115 (1993) 383-389.

[HU79] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison-Wesley, 1979.

[JL95a] D. W. Juedes and J. H. Lutz. The complexity and distribution of hard problems. *SIAM Journal on Computing* 24 (1995) 279-295.

[JL95b] D. W. Juedes and J. H. Lutz. Weak completeness in E and E_2. *Theoretical Computer Science* 143 (1995) 149-158.

[KaM94] S. M. Kautz and P. B. Miltersen. Relative to a random oracle, NP is not small. In *Proceedings of the Ninth Annual Stucture in Complexity Theory Conference*, 162-174, IEEE Computer Society Press, 1994.

[Ko86] K. Ko. On the notion of infinite pseudorandom sequences. *Theoretical Computer Science* 48 (1986) 9-33.

[KoM75] K. Ko and D. Moore. Completeness, approximation and density. *Journal of the ACM* 22 (1975) 787-796.

[La75] R. E. Ladner. On the structure of polynomial time reducibility. *Journal of the ACM* 22 (1975) 155-171.

[La83] C. Lautemann. BPP and the polynomial hierarchy. *Information Processing Letters* 14 (1983) 215-217.

[Li93] W. Lindner. *On the polynomial time bounded measure of one-truth-table degrees and p-selectivity.* Diplomarbeit, Technische Universität Berlin, 1993.

[Lu90] J. H. Lutz. Category and measure in complexity classes. *SIAM Journal on Computing* 19 (1990) 1100-1131.

[Lu92] J. H. Lutz. Almost everywhere high nonuniform complexity. *Journal of Computer and System Sciences* 44 (1992) 220-258.

[Lu95] J. H. Lutz. Weakly hard problems. *SIAM Journal on Computing* 24 (1995) 1170-1189.

[Lu96] J. H. Lutz. The quantitative structure of exponential time. In *Complexity Theory Retrospective, II* (to appear).

[Ly75] N. Lynch. On reducibility to complex or sparse sets. *Journal of the ACM* 22 (1975) 341-345.

[LLS75] R. Ladner, N. Lynch and A. Selman. A comparison of poynomial-time reducibilities. *Theoretical Computer Science* 1 (1975) 103-123.

[LM94] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal of Computing* 23 (1994) 762-779.

[LM96] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science* 164 (1996) 141-163.

[LV93] M. Li and P. M. B. Vitányi. An Introduction to Kolmogorov Complexity and its Applications. Springer Verlag, 1993.

[Ma82] S. R. Mahaney. Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis. *Journal of Computer and System Sciences* 25 (1982) 130-143.

[Ma94a] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science* 136 (1994) 487-506.

[Ma94b] E. Mayordomo. *Contributions to the Study of Resource-Bounded Measure*. PhD Thesis, Universitat Politècnica de Catalunya, Barcelona, Spain, 1994.

[Ma94c] E. Mayordomo. Measuring in PSPACE. In *Proceedings of the International Meeting of Young Computer Scientists '92*, 93-100, Gordon and Breach, 1994.

[ML66] P. Martin-Löf. The definition of random sequences. *Information and Control* 9 (1966) 602-619.

[Og95] M. Ogihara. Polynomial-time membership comparable sets. *SIAM Journal on Computing* 24 (1995) 1068-1081.

[Ox80] J. C. Oxtoby. *Measure and Category.* Second edition. Springer Verlag, 1980.

[OS86] P. Orponen and U. Schöning. The density and complexity of polynomial cores for intractable sets. *Information and Control* 70 (1986) 54-68.

[OW91] M. Ogiwara and O.Watanabe. On polynomial bounded truth-table reducibility of NP sets to sparse sets. *SIAM Journal on Computing* 20 (1991) 471-483.

[Pa69] R. A. Di Paola. Random sets in subrecursive hierarchies. *Journal of the ACM* 16 (1969) 621-630.

[Ro67] H. Rogers.*Theory of Recursive Functions and Effective Computability.* McGraw Hill, 1967.

[RR94] A. Razborov and S. Rudich. Natural proofs. In *Proceedings of the 26th ACM Symposium on Theory of Computing*, 204-213, 1994.

[RS95] K. Regan and D. Sivakumar. Improved resource-bounded Borel-Cantelli and stochasticity theorems. Technical report UB-CS-TR 95-08, Computer Science Department, University of Buffalo, 1995.

[RSC95] K. W. Regan, D. Sivakumar and J.Cai. Pseudorandom generators, measure theory, and natural proofs. In *36th IEEE Symposium on Foundations of Computer Science*, 26-35, IEEE Computer Society Press, 1995.

[Sch71a] C. P. Schnorr. A unified approach to the definition of random sequences. *Mathematical Systems Theory* 5 (1971) 246-258.

[Sch71b] C. P. Schnorr. *Zufälligkeit und Wahrscheinlichkeit.* Lecture Notes in Mathematics 218, 1971.

[Sch96] R. Schuler. Truth-table closure and Turing closure of Average Polynomial Time have different measures in EXP. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)*, 190-195, IEEE Computer Society Press, 1996.

[Se79] A. L. Selman. P-selective sets, tally languages, and the behaviour of polynomial time reducibilities on NP. *Mathematical Systems Theory* 13 (1979) 55-65.

[Si83] M. Sipser. A complexity-theoretic approach to randomness. In *Proceedings of the 15th ACM Symposium on Theory of Computing*, 330-335, 1983.

[To91] S. Toda. On polynomial time truth-table reducibilities of intractable sets to **P**-selective sets. *Mathematical System Theory* 24 (1991) 69-82.

[TB91] S. Tang and R. Book. Polynomial-time reducibilities and "almost all" oracle sets. *Theoretical Computer Science* 18 (1991) 35-47.

[USS90] V. A. Uspenskii, A. L. Semenov and A. Kh. Shen. Can an individual sequence of zeros and ones be random? *Russian Mathematical Surveys* 45 (1990) 121-189.

[vM19] R. von Mises. Grundlagen der Wahrscheinlichkeitsrechnung. Mathematische Zeitschrift 5 (1919) 52-89.

[Vi39] J. Ville. Etude Critique de la Notion de Collectif. Gauthiers-Villars, 1939.

[Wa87] O. Watanabe. A comparison of polynomial time completeness notions. *Theoretical Computer Science* 54 (1987) 249-256.

[Wa96] Y. Wang. *Randomness and Complexity.* Doctoral Dissertation, Universität Heidelberg, 1996.

[Wa96a] Y. Wang. The law of the iterated logarithm for p-random sequences. In *Proceedings of the 11th Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference)*, 180-189, IEEE Computer Society Press, 1996.

[Wi83] R. Wilber. Randomness and the density of hard problems. In *Proceedings of the 24th IEEE Symposium on Foundations of Computer Science*, 335-342, IEEE Computer Society Press, 1983.