Resource Bounded Randomness and Weakly Complete Problems[1]

Klaus Ambos-Spies
Universität Heidelberg
Mathematisches Institut
Im Neuenheimer Feld 294
D-69120 Heidelberg, Germany
Email: ambos@math.uni-heidelberg.de

Sebastiaan A. Terwijn[2]
Universiteit van Amsterdam
FWI, Plantage Muidergracht 24
NL-1018 TV Amsterdam
The Netherlands
Email: terwijn@fwi.uva.nl

Xizhong Zheng[3]
Nanjing University
Department of Mathematics
Nanjing 210008, P.R. China

Abstract

We introduce and study resource bounded random sets based on Lutz's concept of resource bounded measure ([7, 8]). We concentrate on n^c-randomness ($c \geq 2$) which corresponds to the polynomial time bounded (p-) measure of Lutz, and which is adequate for studying the internal and quantitative structure of $\mathbf{E} = \mathrm{DTIME}(2^{lin})$. However we will also comment on $\mathbf{E}_2 = \mathrm{DTIME}(2^{pol})$ and its corresponding (p_2-) measure. First we show that the class of n^c-random sets has p-measure 1. This provides a new, simplified approach to p-measure 1-results. Next we compare randomness with genericity (in the sense of [2, 3]) and we show that n^{c+1}-random sets are n^c-generic, whereas the converse fails. From the former we conclude that n^c-random sets are not p-btt-complete for $\mathbf{E}$. Our technical main results describe the distribution of the n^c-random sets under p-m-reducibility. We show that every n^c-random set in $\mathbf{E}$ has n^k-random predecessors in $\mathbf{E}$ for any $k \geq 1$, whereas the amount of randomness of the successors is bounded. We apply this result to answer a question raised by Lutz [10]: We show that the class of weakly complete sets has measure 1 in $\mathbf{E}$ and that there are weakly complete problems which are not p-btt-complete for $\mathbf{E}$.

[1]This research was done while the second and third author visited the University of Heidelberg in 1993/94 and was supported in part by the Human Capital and Mobility program of the European Community under grant CHRX-CT93-0415. It was presented at the ISAAC '94 conference held in Beijing, China, August 1994.

[2]The second author was also supported by the Dutch VSB foundation and by the Nederlandse Organisatie voor Wetenschappelijk Onderzoek under grant SIR 13-2694.

[3]The third author was also supported by the Chinese State Education Commission.

1 Introduction

Recently, Lutz [7, 8] introduced resource bounded versions of the classical Lebesgue measure. He proposed these concepts as natural tools for the quantitative analysis of complexity classes. In particular he suggested to use the polynomial time bounded (p-) measure for the study of the class $\mathbf{E} = \mathrm{DTIME}(2^{linear})$, of exponential time computable sets, and he and others already obtained interesting results along these lines (see [9] for a survey). Juedes and Lutz [5] used this new measure approach to prove new and reprove old results on the strong intractability of p-m-complete sets for $\mathbf{E}$, like the result of Orponen and Schöning [13] that any p-m-complete set A for $\mathbf{E}$ has a dense polynomial complexity core. As Lutz observed, the measure approach does not require p-m-completeness (or hardness) but only a weaker property of the complete sets: It suffices that the class $P_m(A) \cap \mathbf{E}$ of the predecessors of A in $\mathbf{E}$ does not have p-measure 0. Lutz calls a set $A \in \mathbf{E}$ with this property *weakly complete* (for $\mathbf{E}$), and in [10] he constructed a weakly complete set which is not p-m-complete for $\mathbf{E}$. His construction required a new sophisticated diagonalization technique which he calls *martingale diagonalization*. The combinatorial complexity of the argument, however, makes it difficult to combine it with other techniques. So Lutz raised the question what properties the weakly complete sets might have and how they are distributed in $\mathbf{E}$. In particular, he asked about the p-measure of this class and whether there are weakly complete sets in $\mathbf{E}$ which are incomplete under the weaker polynomial time reducibilities.

Here, by using a very different (and technically much simpler) approach, we answer some of Lutz's questions. To obtain our results we introduce and study resource bounded random sets. This concept is of fundamental interest for the investigation of resource bounded measure. Our application of this concept to investigate the weakly complete problems should be viewed as just one example illustrating the power of this concept. Hence we will also mention some fundamental properties of the random sets not required for the study of the weakly complete sets. In particular we relate randomness to genericity.

In Section 2 we introduce the randomness concept. Following Schnorr [14] and Lutz [9] we say that a set A is $t(n)$-random if A does not belong to any class of $t(n)$-measure 0. So a $t(n)$-random set has all properties which occur with $t(n)$-measure 1. It is easy to show that, for any recursive time bound t, there is a recursive $t(n)$-random set. Here we will concentrate on n^c-randomness ($c \geq 1$), which corresponds to the p-measure of Lutz and is appropriate for the analysis of $\mathbf{E}$. We show that the class of n^c-random sets has p-measure 1. It follows that the n^c-random sets have measure 1 in $\mathbf{E}$, which in turn implies the existence of such sets in $\mathbf{E}$. Similar results hold for the class $\mathbf{E}_2 = \mathrm{DTIME}(2^{polynomial})$ and the corresponding p_2-measure.

Next, in Section 3, we relate randomness to the resource bounded genericity concepts introduced by Ambos-Spies, Fleischhack, and Huwig in [2, 3]. These genericity concepts were recently used by Ambos-Spies, Neis, and Terwijn [4] to investigate the p-measure on $\mathbf{E}$. In particular they observed that the class of n^c-generic sets has p-measure 1, so that the properties shared by all generic sets occur with p-measure 1. By studying properties of the n^c-generic sets, Ambos-Spies et al. [4] obtained various new p-measure 1-results. Here we show that any n^{c+1}-random set is n^c-generic. So the results on n^c-generic sets obtained in [4] carry over to the n^c-random sets. For instance we obtain that n^c-random sets are not p-btt-complete for $\mathbf{E}$ and that the amount of randomness of the successors (under p-m-reducibility) of an n^c-random set is limited.

In Section 4 we contrast the result on the successors of random sets by a theorem on the predecessors: We show that any n^c-random set in $\mathbf{E}$ ($c \geq 2$) has n^k-random predecessors in $\mathbf{E}$ for any $k \geq 1$ and, in fact, has a p-random predecessor in DTIME(2^{n^2}). Furthermore, it has $2^{(\log n)^k}$-random predecessors in $\mathbf{E}_2$, for any $k \geq 1$.

Finally, in Section 5, we apply some of our results on random sets to weak completeness. Our result on the predecessors of n^c-random sets immediately implies that any n^c-random set in $\mathbf{E}$ is weakly complete for $\mathbf{E}$ ($c \geq 2$). So, by the results on n^c-random sets from Section 2, we may conclude that the class of weakly complete problems does not have p-measure 0, in fact, has measure 1 in $\mathbf{E}$, and that there are weakly complete problems which are not p-btt-complete. Moreover, the question whether the latter result can be extended to the weaker polynomial time reducibilities like p-tt (polynomial truth-table) or p-T (polynomial Turing) reducibility can be reduced to the problem of showing that the corresponding incomplete sets for $\mathbf{E}$ do not have p-measure 0. Again, similar results hold for the p_2-measure on $\mathbf{E}_2$.

We conclude this section by introducing some notation. Let $\Sigma = \{0,1\}$ and let Σ^* be the set of binary strings. A subset of Σ^* is called a *problem* or simply a *set*. Strings are denoted by lower case letters from the end of the alphabet (u, v, w, x, y, z), problems are denoted by capital letters A, B, C,... and classes of problems are denoted by boldface capital letters $\mathbf{A}$, $\mathbf{B}$, $\mathbf{C}$,... The concatenation of two strings x and y is denoted by xy and the n^{th} iteration of x by x^n; λ is the empty string; $|x|$ denotes the length of the string x; $<$ is the length-lexicographical ordering on Σ^*; z_n is the n^{th} string under this ordering, and $x+1$ is the $<$-successor of x. The i^{th} bit of the string x is denoted by $x(i)$, so $x = x(0)\dots x(|x|-1)$. We identify a problem A with its characteristic function, i.e. $x \in A$ iff $A(x) = 1$. For $A \subseteq \Sigma^*$ and $x \in \Sigma^*$ we let $A \restriction x$ denote the finite initial segment of A below x, i.e. $A \restriction x = \{y : y < x \wedge y \in A\}$, and we identify this initial segment with its characteristic string, i.e. $A \restriction z_n = A(z_0)\dots A(z_{n-1}) \in \Sigma^*$. For the calculations below it is crucial to note that

$$2^{|x|} - 1 \leq |A \restriction x| < 2^{|x|+1} - 1, \tag{1}$$

whence $O(|A \restriction x|^c) = O(2^{c|x|})$ for any $c \geq 1$. In particular, since the concepts of n^c-measure, n^c-randomness, and n^c-genericity introduced below refer to initial segments of length n, these concepts are intimately related to (diagonalizations over) DTIME(2^{cn}). We let $\mathcal{N}$, $\mathcal{Q}^+$, and $[0,\infty)$ denote the sets of nonnegative integers, rationals, and reals, respectively. The lower case letters c, k, n always denote elements of $\mathcal{N}$.

2 Resource Bounded Measure and Randomness

Lutz's resource bounded measure theory is inspired by earlier effectivizations of Lebesgue measure by Martin-Löf [12] and Schnorr [14]. It is based on the concept of a computable martingale. For technical convenience our definition of a martingale slightly differs from the one of Lutz (our martingales are called density functions by Lutz, and supermartingales by Schnorr and others). Though for a fixed time bound $t(n)$ the corresponding measure concepts may differ by a linear factor, both definitions lead to the same notion of p-measure and measure in $\mathbf{E}$. Throughout, $t(n) : \mathcal{N} \to \mathcal{N}$ will be a recursive, time constructible function satisfying $t(n) \geq n$ for almost every n.

Definition. A *martingale* is a function $d : \Sigma^* \to [0,\infty)$ such that, for all $w \in \Sigma^*$, $d(w0) + d(w1) \leq 2d(w)$. A martingale d *succeeds on* a problem $A \subseteq \Sigma^*$ if $\limsup_n d(A \restriction z_n) = \infty$. To define computability of a martingale d we consider approximations $\hat{d}_k : \Sigma^* \to \mathcal{Q}^+$ satisfying $|d(w) - \hat{d}_k(w)| \leq 2^{-k}$. If such a sequence $\hat{d}_k$ is uniformly computable in time $O(t(n))$, we say that d is a $t(n)$-*martingale* and that the function $\hat{d} : \mathcal{N} \times \Sigma^* \to \mathcal{Q}^+$ defined by $\hat{d}(k,w) = \hat{d}_k(w)$ is a $t(n)$-*computation* of d. (The complexity of $\hat{d} : \mathcal{N} \times \Sigma^* \to \mathcal{Q}^+$ on argument (k,w) is measured in $\max\{k, |w|\}$.) We say that d is a *p-martingale* if it is an n^c-martingale, for some c.

Definition. A class $\mathbf{C}$ of problems has $t(n)$-*measure 0* ($\mu_{t(n)}(\mathbf{C}) = 0$) if there is a $t(n)$-martingale which succeeds on every problem in $\mathbf{C}$. The class $\mathbf{C}$ has $t(n)$-*measure 1* ($\mu_{t(n)}(\mathbf{C}) = 1$) if $\mu_{t(n)}(\mathbf{C}^c) = 0$ for the complement $\mathbf{C}^c = \{A \subseteq \Sigma^* : A \notin \mathbf{C}\}$ of $\mathbf{C}$.

Definition. A set A is $t(n)$-*random* if, for every $t(n)$-martingale $d : \Sigma^* \to [0,\infty)$, $\limsup_n d(A \restriction z_n) < \infty$, i.e. d does not succeed on A. A set is *p-random* if it is n^c-random for every c.

Note that a set A is $t(n)$-random if and only if A does not belong to any class of $t(n)$-measure 0, i.e. if and only if the singleton $\{A\}$ does not have $t(n)$-measure 0. As the following technical lemma shows, for the definition of measure and randomness it suffices to consider martingales with rational values, which are not just approximable but *exactly* computable within the given time bound. This observation simplifies the construction of random sets.

Lemma 2.1 *If, for a class $\mathbf{C}$ of problems, $\mu_{t(n)}(\mathbf{C}) = 0$, then there is a martingale $\tilde{d} : \Sigma^* \to \mathcal{Q}^+$ computable in time $O(t(n))$ which succeeds on every problem in $\mathbf{C}$.*

Proof. Suppose d is a $t(n)$-martingale which succeeds on every problem in $\mathbf{C}$, and let $\hat{d} : \mathcal{N} \times \Sigma^* \to \mathcal{Q}^+$ be a $t(n)$-computation of d:

$$\forall k \in \mathcal{N}\, \forall w \in \Sigma^* (|d(w) - \hat{d}_k(w)| \leq 2^{-k}).$$

Define a martingale $\tilde{d}$ which succeeds on every $A \in \mathbf{C}$ as follows: $\tilde{d}(w) = \hat{d}_{|w|}(w) + 4 \cdot 2^{-|w|}$. Then $\tilde{d}(w) \geq d(w) + 3 \cdot 2^{-|w|}$ and $\tilde{d}(w) \leq d(w) + 5 \cdot 2^{-|w|}$. Furthermore,

$$\begin{aligned}
\tilde{d}(w0) + \tilde{d}(w1) &\leq d(w0) + 5 \cdot 2^{-|w|-1} + d(w1) + 5 \cdot 2^{-|w|-1} \\
&\leq 2(d(w) + 5/2 \cdot 2^{-|w|}) \\
&\leq 2(d(w) + 3 \cdot 2^{-|w|}) \\
&\leq 2\tilde{d}(w),
\end{aligned}$$

so $\tilde{d}$ is a martingale, and $\tilde{d}$ succeeds on every $A \in \mathbf{C}$ because $\tilde{d}(w) \geq d(w)$ and d succeeds on every $A \in \mathbf{C}$. Finally, $\tilde{d}$ is computable in time $O(t(n))$, because $t(n) \geq n$. □

The existence of recursive $t(n)$-random sets can be shown by diagonalization: Let $\{d_e : e \in \mathcal{N}\}$ be a recursive enumeration of the $t(n)$-martingales $d : \Sigma^* \to \mathcal{Q}^+$ with $d(\lambda) = 1$ (for a martingale d which succeeds on a problem we may assume that d is normed: $d(\lambda) = 1$). Define $A(\lambda) = 0$ and, for $w \neq \lambda$, $A(w) = 1 \Leftrightarrow f((A \restriction w)0) \geq f((A \restriction w)1)$, where

$$f(w) = \sum_{i=0}^{|w|} 2^{-2i} d_i(w).$$

Then, as one can easily check, f is bounded on A whence, by definition of f, any d_i is bounded on A, so that by Lemma 2.1 A is $t(n)$-random.

To show that the class of n^c-random sets has p-measure 1 we need a weak version of σ-additivity for the $t(n)$-measure.

Definition.(Lutz) A class $\mathbf{X}$ is a $t(n)$-*union* of the $t(n)$-measure 0 classes $\mathbf{X}_i$, $i \in \mathcal{N}$, if $\mathbf{X} = \bigcup_{i \in \mathcal{N}} \mathbf{X}_i$ and there exists a $t(n)$-computable function $d : \mathcal{N} \times \Sigma^* \to \mathcal{Q}^+$ such that for every i, $d_i(x) = d(i, x)$ is a martingale and d_i succeeds on every problem in $\mathbf{X}_i$.
By Lemma 2.1 this definition is equivalent to Lutz's definition (see e.g. [8, p 231]). The next lemma is a generalization of Lutz's Δ-Ideal Lemma for arbitrary time bounds $\Delta = O(t(n))$ ([8, Lemma 3.10]).

Lemma 2.2 *If* $\mathbf{X}$ *is a* $t(n)$*-union of the* $t(n)$*-measure* 0 *classes* $\mathbf{X}_i$*,* $i \in \mathcal{N}$*, then* $\mathbf{X}$ *has* $n\,t(2n)$*-measure* 0*.*

Proof. By assumption there exists a $t(n)$-computable function $d : \mathcal{N} \times \Sigma^* \to \mathcal{Q}^+$ such that for every i, d_i is a martingale and d_i succeeds on every problem in

$\mathbf{X}_i$. W.l.o.g. we may assume that $d_i(\lambda) = 1$ for every i. Define $d' : \Sigma^* \to [0, \infty)$ by

$$d'(w) = \sum_{i=0}^{\infty} 2^{-i} d_i(w).$$

Note that by the martingale property of the d_i and the assumption that $d_i(\lambda) = 1$, $d_i(w) \leq 2^{|w|}$ for every i, so this sum is convergent. Now d' is a martingale because all the d_i are, and $d'(w) \geq 2^{-i} d_i(w)$, so d' succeeds on $\mathbf{X}_i$ for every i, hence d' succeeds on $\mathbf{X}$. We show that d' is $n\,t(2n)$-computable. Define

$$\hat{d}_k(w) = \sum_{i=0}^{k+|w|} 2^{-i} d_i(w).$$

Then

$$\begin{aligned} d'(w) - \hat{d}_k(w) &= \sum_{i=k+|w|+1}^{\infty} 2^{-i} d_i(w) \\ &\leq \sum_{i=k+|w|+1}^{\infty} 2^{-i+|w|} = 2^{-k} \end{aligned}$$

(The inequality holds since $d_i(w) \leq 2^{|w|} \cdot d_i(\lambda) = 2^{|w|}$). Since clearly $\hat{d}_k(w) \in$ FDTIME$(n\,t(2n))$, it follows that the sequence $\{\hat{d}_k(w) : k \in \mathcal{N}\}$ is an $n\,t(2n)$-computation of d'. □

Theorem 2.3 *The class of $t(n)$-random sets has $n^3\,t(2n) \log t(2n)$-measure* 1.

Proof. Let $f : \mathcal{N} \times \Sigma^* \to \mathcal{Q}^+$ be a universal function of the class of the unary $t(n)$-computable functions $g : \Sigma^* \to \mathcal{Q}^+$. We may assume that $f \in$ FDTIME$(n\,t(n) \log t(n))$. For any e, define a martingale d_e as follows.

$$\begin{aligned} d_e(\lambda) &= f(e, \lambda) \\ d_e(wi) &= \begin{cases} f(e, wi) & \text{if } f(e, w0) + f(e, w1) \leq 2d_e(w) \\ d_e(w) & \text{otherwise} \end{cases} \end{aligned}$$

Obviously, if f_e, where $f_e(x) = f(e, x)$, is a martingale then $d_e = f_e$. So $\{d_e : e \in \mathcal{N}\}$ is an enumeration of all $t(n)$-martingales, i.e. the function d with $d(e, x) = d_e(x)$ is a universal function of the $t(n)$-martingales and, by definition, $d \in$ FDTIME$(n^2 t(n) \log t(n))$. Let $\mathbf{X}_e = \{A \subseteq \Sigma^* : d_e \text{ succeeds on } A\}$ and $\mathbf{X} = \bigcup_{e \in \mathcal{N}} \mathbf{X}_e$. Then $\mathbf{X}$ is an $(n^2 t(n) \log t(n))$-union of the $(n^2 t(n) \log t(n))$-measure 0 classes $\mathbf{X}_e$, whence, by Lemma 2.2, $\mu_{n^3 t(2n) \log t(2n)}(\mathbf{X}) = 0$. Since, by Lemma 2.1, the class of $t(n)$-random sets is the complement of $\mathbf{X}$, it has $(n^3 t(2n) \log t(2n))$-measure 1. □

Corollary 2.4 *The class of n^c-random sets ($c \geq 1$) has n^{c+4}-measure* 1*, hence p-measure* 1.

Lutz and others also studied the class $\mathbf{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$. In [8] it is shown that the natural measure on this class is the p_2-measure, where p_2 is the class consisting of all the functions $2^{p(\log n)}$, p a polynomial. By the same proof as above we see that

Corollary 2.5 *The class of p-random sets has $n^{\log n}$-measure* 1*, hence* p_2*-measure* 1.

Lutz defines a measure on $\mathbf{E}$ by saying that $\mathbf{C}$ has *measure 0 in* $\mathbf{E}$ ($\mu(\mathbf{C}|\mathbf{E}) = 0$) if $\mu_p(\mathbf{C} \cap \mathbf{E}) = 0$ and $\mathbf{C}$ has *measure 1 in* $\mathbf{E}$ ($\mu(\mathbf{C}|\mathbf{E}) = 1$) if $\mu(\mathbf{C}^c|\mathbf{E}) = 0$. Lutz has shown that this definition is sound: $\mu(\mathbf{C}|\mathbf{E}) = 1$ implies that $\mu(\mathbf{C}|\mathbf{E}) \neq 0$, i.e. that $\mathbf{C}$ does not have measure 0 in $\mathbf{E}$. In particular, if $\mu(\mathbf{C}|\mathbf{E}) = 1$ then $\mathbf{C} \cap \mathbf{E} \neq \emptyset$. Similarly for $\mathbf{E}_2$ and p_2 instead of $\mathbf{E}$ and p. So Corollaries 2.4 and 2.5 imply

Corollary 2.6 (i) *For any $c \geq 1$, the class of n^c-random sets has measure 1 in* $\mathbf{E}$*. In particular there is an n^c-random set in* $\mathbf{E}$*.*

(ii) (Lutz [8]) *The class of p-random sets has measure 1 in* $\mathbf{E}_2$*. In particular there is a p-random set in* $\mathbf{E}_2$*.*

Note that, for time bounds t and t' such that $t'(n) \leq t(n)$ almost everywhere, any $t(n)$-random set is $t'(n)$-random. So any p-random set is n^c-random, and any n^c-random set is $n^{c'}$-random, for any $c' \leq c$. Conversely, by diagonalization we can show that there are n^c-random sets which are not n^{c+1}-random (for any $c \geq 1$). So these concepts of randomness give rise to a proper hierarchy.

Also note that the existence results for n^c-random and p-random sets in Corollary 2.6 can be easily extended to the general case: If in the construction of a $t(n)$-random set A described above (after Lemma 2.1) we use an enumeration of the $t(n)$-martingales as in the proof of Theorem 2.3, then $A \in \mathrm{DTIME}(t'(2^{n+1}))$ for $t'(n) = n^4 t(n) \log t(n)$.

Some further basic properties of random sets are stated in the following lemma.

Lemma 2.7 *Let A be a $t(n)$-random set. Then the following hold:*

(i) *The complement $\overline{A}$ of A is $t(n)$-random.*

(ii) *A is* dense*, i.e. there exists an $\epsilon > 0$ such that $|A_{\leq n}| > 2^{n^\epsilon}$ for almost every n.*

Proof. To prove (i), suppose that the $t(n)$-martingale d succeeds on $\overline{A}$. Then d' defined by $d'(w) = d(\overline{w})$ succeeds on A, where $\overline{w}$ is the unique string of length $|w|$ such that $\overline{w}(i) = 1 - w(i)$ for $i < |w|$.
For a proof of (ii), it suffices to show that the class of nondense sets has n-measure 0, since $t(n) \geq n$ a.e. n. Define the n-martingale $d : \Sigma^* \rightarrow \mathcal{Q}^+$ by

$d(\lambda) = 1$, $d(w0) = 3/2 \cdot d(w)$, and $d(w1) = 1/2 \cdot d(w)$. If B is a nondense set then $|B_{\leq n}| \leq 2^{\sqrt{n}}$ for infinitely many n. However, $|\Sigma^*_{\leq n}| = 2^{n+1} - 1$, so

$$\limsup_n d(B \restriction z_n) \geq \lim_n ((3/2)^{2^{n+1}-1-2^{\sqrt{n}}} \cdot (1/2)^{2^{\sqrt{n}}}) = \infty.$$

□

Note that many more much stronger properties than the above can be proven (such as the various stochastic properties from probability theory, or such as the Weak Stochasticity Theorem from [11]), but we will not need these in the sequel.

3 Resource Bounded Genericity and Randomness

Ambos-Spies, Fleischhack, and Huwig [2, 3] introduced different types of resource bounded genericity. Here we shortly review one of their concepts which is closely related to resource bounded measure (see [4]).

Definition. A *condition* is a set $C \subseteq \Sigma^*$. A problem A *meets* the condition C if, for some string x, $A \restriction x \in C$. C is *dense along* A if

$$\exists^\infty x \in \Sigma^* \exists i \in \Sigma((A \restriction x)i \in C).$$

A problem A is $t(n)$*-generic* if A meets every condition $C \in \mathrm{DTIME}(t(n))$ which is dense along A.
The $t(n)$-generic sets are universal for standard diagonalization constructions where the single diagonalization steps correspond to subrequirements of time complexity $t(n)$ (measured in the length n of the previously built part $A \restriction x$ of A) so that these subrequirements may be described by $t(n)$-bounded conditions. For a more detailed discussion of these concepts see [1, 3].

The proof of the next theorem is essentially the same as the proof in [4] showing that the n^c-generic sets have p-measure 1.

Theorem 3.1 *Let A be n^{c+1}-random. Then A is n^c-generic. Hence any p-random set is p-generic.*

Proof. Let $C \in \mathrm{DTIME}(n^c)$ be a condition which is dense along A. To show that A meets C, define $d : \Sigma^* \to \mathcal{Q}^+$ by $d(\lambda) = 1$ and, for w in Σ^* and $i \leq 1$,

$$d(wi) = \begin{cases} 0 & \text{if } wi \in C \wedge w(1-i) \notin C \\ 2d(w) & \text{if } w(1-i) \in C \wedge wi \notin C \\ d(w) & \text{otherwise} \end{cases}$$

Then $d \in \mathrm{FDTIME}(n^{c+1})$ is a martingale whence, by n^{c+1}-randomness of A, $\limsup_n d(A \restriction z_n) < \infty$. By density of C along A and by definition of d this implies that A meets C. □

The converse of Theorem 3.1 fails: by Lemma 2.7, any n^c-random set is dense whereas, as shown in [4], there exist sparse n^c-generic sets. Intuitively, the difference between $t(n)$-genericity and $t(n)$-randomness can be described as follows: Both concepts are universal for $t(n)$-bounded diagonalizations. In case of genericity, however, we only require that, for any single condition, if there are infinitely many chances to meet the condition then the condition has to be met at least once, or (as one can easily check) equivalently, *infinitely* often. In case of randomness this does not suffice; here a *majority* of the chances has to be taken.

In [4] numerous properties of the n^c-generic sets were proven. By Theorem 3.1 these properties are shared by all n^{c+1}-random sets. For instance, in [4] it is shown that n^c-generic sets are not p-btt-complete for $\mathbf{E}$, that p-generic sets are not p-btt-hard for $\mathbf{E}$, and that the genericity of successors of n^c-generic sets in $\mathbf{E}$ is limited ($c \geq 2$). So we obtain the corresponding results for n^c-random sets:

Corollary 3.2 (i) *If A is n^c-random ($c \geq 3$), then A is not p-btt-complete for* $\mathbf{E}$.

(ii) *If A is p-random, then A is not p-btt-hard for* $\mathbf{E}$.

Corollary 3.3 *Let A and B be sets such that $A \leq^p_m B$, A is n^c-random and $A \in \mathrm{DTIME}(2^{dn})$, where $c,d \geq 3$. Then B is not n^{d+1}-random.*

Corollary 3.3 shows that, for any n^c-random set $A \in \mathbf{E}$ there is a bound on the polynomial randomness of the successors of A (under p-m-reducibility). The reason for this is the following: If $A \leq^p_m B$ via f, then, by n^2-randomness, f cannot compress A, so that $f(A)$ contains an infinite $2^{(d+1)n}$-computable subset of B. An n^{d+1}-random set, however, does not have such *easy* infinite parts.

4 Randomness Below a Random Set

Here we will contrast the preceding result on the limitations on randomness of the successors of an exponential time computable n^c-random set by showing that any such set has *predecessors* of arbitrarily high polynomial randomness.

Theorem 4.1 *Let A be an n^2-random set. For any $k \geq 1$ there is an n^k-random set A_k with $A_k \leq^p_m A$. In fact, there is a p-random set A_∞ with $A_\infty \leq^p_m A$. Also, for any $k \geq 1$, there is a $2^{(\log n)^k}$-random set $B_k \leq^p_m A$. If, moreover, $A \in \mathbf{E}$ then A_k and A_∞ can be chosen so that $A_k \in \mathbf{E}$ and $A_\infty \in \mathrm{DTIME}(2^{n^2})$, and if $A \in \mathbf{E}_2$ then B_k can be chosen to be in $\mathbf{E}_2$.*

The idea underlying the proof of Theorem 4.1 is the following. If we restrict the domain D of a random set A then, relative to this domain, $A \cap D$ remains random. So if we take the restriction of A to some polynomially scattered domain D and polynomially compress $A \cap D$ by mapping D onto Σ^* then, for the compressed version A_D of $A \cap D$, time complexity and randomness increase by a polynomial factor but still A_D can be reduced in polynomial time to $A \cap D$

and hence to A. The formal proof of Theorem 4.1 requires the following lemma, which uses the idea above in a slightly more general form.

Lemma 4.2 *Let A be $n\,t(n)$-random for a nondecreasing function t with $t(n) \geq n$ a.e. , and let $f : \mathcal{N} \to \mathcal{N}$ be a nondecreasing time constructible function. Then*

$$A_f = \{x : 0^{f(|x|)}1x \in A\} \text{ is } t(2^{f(\log(n)-1)})\text{-random.}$$

Proof. Define $t'(n) = t(2^{f(\log(n)-1)})$, and let $d : \Sigma^* \to \mathcal{Q}^+$ be a $t'(n)$-computable martingale. We will show that d does not succeed on A_f. To prove this it suffices, by $n\,t(n)$-randomness of A, to define an $n\,t(n)$-martingale $\hat{d}$ such that

$$d \text{ succeeds on } A_f \Rightarrow \hat{d} \text{ succeeds on } A.$$

For the definition of $\hat{d}$ we will use the following notation: For a string $X \upharpoonright (0^{f(|x|)}1x)$, let $\widetilde{X} \upharpoonright x$ be defined by $\widetilde{X}(y) = X(0^{f(|y|)}1y)$ for $y < x$. Now $\hat{d}$ is defined by induction as follows:

1. $\hat{d}(\lambda) = d(\lambda)$,
2. For $y = 0^{f(|x|)}1x$ and $i \leq 1$, $\hat{d}((X \upharpoonright y)i) = d((\widetilde{X} \upharpoonright x)i)$,
3. For y not of the form $0^{f(|x|)}1x$ and $i \leq 1$, $\hat{d}((X \upharpoonright y)i) = \hat{d}(X \upharpoonright y)$.

Since d is a martingale, a straightforward induction on $|x|$ shows that

$$\hat{d}((X \upharpoonright x)0) + \hat{d}((X \upharpoonright x)1) \leq 2\hat{d}(X \upharpoonright x)$$

and, by definition of A_f and $\hat{d}$, for $i \leq 1$

$$\hat{d}(A \upharpoonright (0^{f(|x|)}1x)i) = d((A_f \upharpoonright x)i).$$

So $\hat{d}$ is a martingale which succeeds on A if d succeeds on A_f. It remains to show that $\hat{d}$ is computable in time $n\,t(n)$. By induction, it suffices to show that, given $\hat{d}(\lambda), \ldots, \hat{d}(X \upharpoonright y)$, the value of $\hat{d}(X \upharpoonright (y+1))$ can be computed in $O(t(|X \upharpoonright (y+1)|))$ steps. Now fix any y and let $m = |X \upharpoonright (y+1)|$. Since f is time constructible the time required for the decision whether or not y is of the form $0^{f(|x|)}1x$ is polynomial in the length of y, hence, by equation (1) and $t(n) \geq n$, linear in $t(m)$. So it suffices to analyze the cases 2. and 3. in the definition of $\hat{d}$ individually. The case 3. is trivial by induction hypothesis. For a proof of the case 2. fix $x \in \Sigma^*$ and $i \leq 1$ such that $y = 0^{f(|x|)}1x$ and $(X \upharpoonright (y+1))(y) = i$. Then, by definition of $\hat{d}$, $\hat{d}(X \upharpoonright (y+1)) = d((\widetilde{X} \upharpoonright x)i)$, whence it suffices to show that $d((\widetilde{X} \upharpoonright x)i)$ can be computed in $O(t(m))$ steps. Now it follows from $|y| = f(|x|) + |x| + 1$ and the monotonicity of t that

$$t(m) = t(|X \upharpoonright (y+1)|) \quad \geq \quad t(2^{|y|}) \qquad \text{(by equation (1))}$$

$$\begin{aligned}
&= t(2^{f(|x|)+|x|+1}) \\
&\geq t(2^{f(|x|)}) \\
&= t'(2^{|x|+1}) \\
&\geq t'(|(\widetilde{X} \restriction x)i|) \qquad \text{(by equation (1)).}
\end{aligned}$$

Since d is $t'(n)$-computable this implies that $d((\widetilde{X} \restriction x)i)$ can be computed in $O(t(m))$ steps. This completes the proof of Lemma 4.2. $\square$

Proof of Theorem 4.1. Let $t(n) = n$ and let A be n^2-random. Fix $k \in \mathcal{N}$ and define $f_0(n) = k \cdot n$, $f_1(n) = (n+1)\log(n+1)$, and $f_2(n) = n^{k+1}$. It is easy to see that for $i \leq 2$,

$$A_{f_i} = \{x : 0^{f_i(|x|)}1x \in A\} \leq_m^p A.$$

Now define $A_k = A_{f_0}$, $A_\infty = A_{f_1}$, and $B_k = A_{f_2}$. Then by Lemma 4.2, A_k is $2^{-k} \cdot n^k$-random, hence n^k-random, A_∞ is $n^{\log\log n}$-random, hence p-random, and B_k is $2^{(\log(n)-1)^{k+1}}$-random, hence $2^{(\log n)^k}$-random. For a proof of the second part fix c such that $A \in \mathrm{DTIME}(2^{cn})$. Then, as one can easily check, $A_k \in \mathrm{DTIME}(2^{(k+1)cn}) \subset \mathbf{E}$ and $A_\infty \in \mathrm{DTIME}(2^{c(n+1)(\log(n+1)+1)}) \subset \mathrm{DTIME}(2^{n^2})$. If A is in $\mathrm{DTIME}(2^{n^c})$ then $B_k \in \mathrm{DTIME}(2^{n^{c(k+2)}}) \subset \mathbf{E}_2$. $\square$

It follows from Theorem 4.1 that classes that are closed under $\leq_m^p$-reductions, like NP, UP, PP, or PSPACE, contain an n^2-random set if and only if they contain a p-random set if and only if they contain a $2^{(\log n)^k}$-random set.

5 Random Sets are Weakly Complete

In this final section we apply our results on random sets to study the weakly complete problems in $\mathbf{E}$ and $\mathbf{E}_2$. We first review this concept of Lutz [9, 10]. For any set A, let $P_m(A) = \{B : B \leq_m^p A\}$. Then A is *weakly hard* for $\mathbf{E}$ if $\mu(P_m(A)|\mathbf{E}) \neq 0$; if moreover $A \in \mathbf{E}$ then we say that A is *weakly complete* for $\mathbf{E}$. Weak completeness for $\mathbf{E}_2$ is defined in the same way, using p_2 and $\mathbf{E}_2$ instead of p and $\mathbf{E}$. Lutz [10] showed that there is a weakly complete set in $\mathbf{E}$ which is not p-m-complete for $\mathbf{E}$. To show this Lutz introduced a quite involved new diagonalization technique which he calls *martingale diagonalization*. Our results on random sets provide an elementary proof of this fact and yield stronger results.

Theorem 5.1 (i) *A is weakly hard for $\mathbf{E}$ if and only if $P_m(A) \cap \mathbf{E}$ contains an n^2-random set.*

(ii) *A is weakly hard for $\mathbf{E}_2$ if and only if $P_m(A) \cap \mathbf{E}_2$ contains an n^2-random set.*

Proof. (i) If A is weakly hard for $\mathbf{E}$ then $P_m(A) \cap \mathbf{E}$ contains an n^2-random set by Corollary 2.6 (i). Now suppose that $P_m(A) \cap \mathbf{E}$ contains an n^2-random set. Then, by Theorem 4.1, $P_m(A) \cap \mathbf{E}$ contains an n^k-random set for every $k \in \mathcal{N}$. But this means that there is no n^k-martingale which succeeds on every set in $P_m(A) \cap \mathbf{E}$, whence $\mu_p(\{B : B \leq_m^p A\} \cap \mathbf{E}) \neq 0$. Assertion (ii) follows from Corollary 2.6 (ii) and Theorem 4.1 with a similar argument. □

Corollary 5.2 *Let $A \in \mathbf{E}$ $(\mathbf{E}_2)$ be n^2-random. Then A is weakly complete for $\mathbf{E}$ $(\mathbf{E}_2)$.*

Proof. Immediate from Theorem 5.1. □

In contrast to Corollary 5.2, note that for any $k \geq 1$ there are n^k-generic sets in $\mathbf{E}$ which are not weakly complete for $\mathbf{E}$. This follows from the result in [4] that for every k there are sparse n^k-generic sets in $\mathbf{E}$, and the result of Lutz and Mayordomo [11] that for sparse sets A, $\mu_p(P_m(A)) = 0$.

Juedes and Lutz recently [6] proved the following relation between completeness for $\mathbf{E}$ and $\mathbf{E}_2$. Their proof was based in part on the padding techniques of Section 4, which appeared in an early draft of this paper circulated at a 1994 Dagstuhl meeting. We now show how Corollary 3.3 and Theorem 5.1 (not present in the early draft) can be used to give a very direct proof of their result.

Corollary 5.3 (Juedes and Lutz [6]) (i) *If A is weakly complete for $\mathbf{E}$ then A is also weakly complete for $\mathbf{E}_2$.*

(ii) *There exists a set $A \in \mathbf{E}$ which is weakly complete for $\mathbf{E}_2$ but not for $\mathbf{E}$.*

Proof. (i) Since $\mathbf{E}$ is contained in $\mathbf{E}_2$, this is immediate by Theorem 5.1.

(ii) By Corollary 2.6 (ii), let $B \in \mathbf{E}_2$ be p-random, and by padding B, let $A \in \mathbf{E}$ be a set with $A \equiv_m^p B$. Then A is weakly complete for $\mathbf{E}_2$ by Theorem 5.1. However, by Corollary 3.3, $P_m(A) \cap \mathbf{E}$ does not contain any n^2-random set, so by Theorem 5.1 A is not weakly complete for $\mathbf{E}$. □

By Corollary 5.2, we can extend Lutz's theorem on the existence of proper weakly complete sets from p-m-reducibility to p-btt-reducibility:

Corollary 5.4 *There is a weakly complete set for $\mathbf{E}$ which is not p-btt-complete for $\mathbf{E}$.*

Proof. By Corollary 2.6 there is an n^2-random set A in $\mathbf{E}$ and, by Corollary 5.2 and Corollary 3.2, A is weakly complete but not p-btt-complete for $\mathbf{E}$. □

We do not know whether there are weakly complete sets which are not p-tt-complete or even not p-T-complete. As our final result shows, however, to prove this it suffices to show that the classes of *in*complete sets under these reducibilities in $\mathbf{E}$ do not have p-measure 0.

Corollary 5.5 *$\mu_p(\{A : A$ weakly complete for $\mathbf{E}\}) \neq 0$. In fact, $\mu(\{A : A$ weakly complete for $\mathbf{E}\} | \mathbf{E}) = 1$. Similarly, for the measure in $\mathbf{E}_2$ we have $\mu(\{A : A$ weakly complete for $\mathbf{E}_2\} | \mathbf{E}_2) = 1$.*

Proof. By Corollary 5.2 this follows from Corollary 2.6 and the fact that every p-random set is n^2-random. $\square$

Juedes independently proved the first part of Corollary 5.5 (namely that the weakly complete sets for $\mathbf{E}$ do not have p-measure 0) using Lutz's martingale diagonalization technique (private communication).

References

[1] K. Ambos-Spies, Resource-bounded genericity, to appear in *Computability, Enumerability and Unsolvability: Directions in Recursion Theory*, B. Cooper et al., Eds., (Cambridge University Press).

[2] K. Ambos-Spies, H. Fleischhack, and H. Huwig, Diagonalizations over polynomial time computable sets, *Theoret. Comput. Sci.* **51** (1987) 177-204.

[3] K. Ambos-Spies, H. Fleischhack, and H. Huwig, Diagonalizing over deterministic polynomial time, in: *Proc. CSL '87*, Lecture Notes in Computer Science, Vol. 329 (Springer Verlag, 1988) 1-16.

[4] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn, Genericity and measure for exponential time, *Theoret. Comput. Sci.* (to appear), an extended abstract appeared in *Proc. MFCS '94*, Lecture Notes in Computer Science, Vol. 841, (Springer Verlag, 1994) 221-232.

[5] D. W. Juedes and J. H. Lutz, The complexity and distribution of hard problems, *SIAM J. Comput.* **24** (1995) 279-295.

[6] D. W. Juedes and J. H. Lutz, Weak Completeness in E and E_2, *Theoret. Comput. Sci.* **143** (1995) 149-158.

[7] J. H. Lutz, Category and measure in complexity classes, *SIAM J. Comput.* **19** (1990) 1100-1131.

[8] J. H. Lutz, Almost everywhere high nonuniform complexity, *J. Comp. System Sci.* **44** (1992) 220-258.

[9] J. H. Lutz, The quantitative structure of exponential time, in: *Proc. 8th Structure in Complexity Theory Conference* (IEEE Comput. Soc. Press, 1993) 158-175.

[10] J. H. Lutz, Weakly hard problems, *Proc. 9th Structure in Complexity Theory Conference* (IEEE Comput. Soc. Press, 1994) 146-161.

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

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

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

[14] C. P. Schnorr, *Zufälligkeit und Wahrscheinlichkeit*, Lecture Notes in Mathematics, Vol. 218 (Springer Verlag, 1971).