Genericity and Measure for Exponential Time[1]

Klaus Ambos-Spies
Universität Heidelberg
Mathematisches Institut
D-69120 Heidelberg

Hans-Christian Neis
Universität Freiburg
Mathematisches Institut
D-79106 Freiburg

Sebastiaan A. Terwijn
Universiteit van Amsterdam
Faculteit Wiskunde en Informatica
NL-1018 TV Amsterdam

Abstract. Recently Lutz [14,15] introduced a polynomial time bounded version of Lebesgue measure. He and others (see e.g. [11,13,14,15,16,17,18,20]) used this concept to investigate the quantitative structure of Exponential Time (**E=DTIME** (2^{lin})). Previously, Ambos-Spies, Fleischhack and Huwig [2,3] introduced polynomial time bounded genericity concepts and used them for the investigation of structural properties of **NP** (under appropriate assumptions) and **E**. Here we relate these concepts to each other. We show that, for any $c \geq 1$, the class of n^c-generic sets has p-measure 1. This allows us to simplify and extend certain p-measure 1-results. To illustrate the power of generic sets we take the Small Span Theorem of Juedes and Lutz [11] as an example and prove a generalization for bounded query reductions.

1. Introduction

The classical Lebesgue measure was effectivized by Martin-Löf [19], Schnorr [21], and others. Recently Lutz [14,15] further persued this approach to define a feasible, i.e., polynomial time computable, measure concept. He and others showed that this p-measure is a natural tool for the quantitative analysis of the class **E=DTIME**(2^{lin}) of exponential time

[1] This work was supported in part by the Human Capital and Mobility program of the European Community under grant CHRX-CT93-0415. The third author was supported by the Dutch VSB foundation during the time of this research.

computable sets (see [16] for a survey). E.g., Mayordomo [20] and Juedes and Lutz [11] showed that concepts like p-bi-immunity and p-incompressibility, respectively, which play a fundamental role in the structural analysis of **E**, have p-measure 1. Another important result with various applications is the Small Span Theorem of Juedes and Lutz [11] which asserts that, for any set $A \in \mathbf{E}$, the class $P_m(A) \cap \mathbf{E}$ of sets in **E** which are p-m-reducible to A or the class $P_m^{-1}(A)$ of the sets to which A is p-m-reducible has p-measure 0.

Preceeding Lutz's work on resource bounded measure, Ambos-Spies, Fleischhack and Huwig [2,3,7,8] introduced resource bounded genericity concepts. These genericity concepts, which were inspired by restricted arithmetical forcing concepts in recursion theory (see e.g. Jockusch [10]), formalize standard diagonalization concepts and classify these concepts by the complexity of the conditions corresponding to the single diagonalization steps. The corresponding *generic* sets share *all* properties which can be enforced by the diagonalization arguments of given complexity. In [2] Ambos-Spies et al. consider only such diagonalizations which have tally witnesses. (This restriction became necessary by the goal to characterize a diagonalization concept which pertains to **P**, in the sense that it allows diagonalization over **P** but not over any larger complexity class. I.e. for this concept generic sets can be found in any "smooth" hyperpolynomial time class.) Then, in [3], general diagonalization concepts were studied. Here we will relate these latter concepts to the p-measure of Lutz.

In Section 2 we introduce the genericity concept adequate for p-measure, namely n^c-genericity ($c \geq 1$), which in [3] was called $\mathbf{DTIME}(n^c)$-2-genericity. By modifying the proof in [3] that **P**-2-generic sets exist in $\mathbf{DTIME}(2^{n^2})$ we obtain a general existence theorem for t(n)-generic sets, for t any time constructible time bound. In particular this result implies that there are n^c-generic sets in $\mathbf{DTIME}(2^{(c+2)n})$ of arbitrary density. To show how to work with generic sets we prove that, for any n^c-generic set A ($c \geq 2$), $A \notin \mathbf{DTIME}(2^{cn})$, A is 2^{cn}-bi-immune and A is $2^{(c-1)n}$-incompressible. Moreover, we show that the n^c-generic sets witness the separation of the common polynomial reducibilities between one-one and (bounded) truth-table. As a corollary we obtain that, for $c \geq 2$, n^c-generic sets are not p-btt-complete for **E**. Finally we complement the latter by constructing n^c-generic sets which are p-tt-complete for **E**.

Then, in Section 3, we relate genericity to measure. Fleischhack [7,8] has shown that, for any recursive t, the class of t(n)-generic sets has measure 1 in the classical sense. Here we prove the analogous result for p-measure, by showing that, for any $c \geq 1$, the class of n^c-generic sets has p-measure 1. So any property implied by n^c-genericity occurs with p-measure 1. This gives a new way to obtain p-measure 1-results which can be technically

and combinatorically considerably simpler than the direct approach.

We illustrate this approach in Section 4, by first reproving the Small Span Theorem of Juedes and Lutz [11] (for p-m-reducibility) using genericity. The technical main result required for this approach is that, for any n^k-generic set $A \in \mathbf{DTIME}(2^{cn})$, no set $B \in P_m^{-1}(A)$ is $n^{d(c)}$-generic (for some constant d(c) depending on c), whence $\mu_p(P_m^{-1}(A))=0$. Then we extend the Small Span Theorem to polynomial-time bounded-query (p-k-tt) reductions. The proof of this theorem, which is considerably more complex, depends -besides the results on the measure of generic sets from Section 3- only on structural properties of the generic sets. We conclude this section by discussing some serious obstacles for extending the Small Span Theorem to still weaker polynomial reducibilities. Moreover, we apply our results to determine the p-measure of the **E**-hard and **E**-complete sets under the strong polynomial reducibilities.

Finally, in Section 5, we point out the limitations of our generic-set approach to p-measure 1-results. We show that in general n^c-generic sets are not n^c-random. This distinction follows from the observations (made first in [3] and [17], respectively) that, in contrast to genericity, randomness determines the density of a set.

We conclude this section by introducing some notation. N denotes the set of natural numbers. The lower case letters c,d,i,j,k,m,n denote numbers. Let $\Sigma=\{0,1\}$ and let Σ^* be the set of (finite) binary strings. A subset of Σ^* is called a *language* or simply a *set*. Strings are denoted by lower case letters from the end of the alphabet (u,v,w,x,y,z), languages are denoted by capital letters A, B, C, ... Boldface capital letters **A**, **B**, **C**, denote classes of languages, i.e., subsets of the power set of Σ^*. In particular, **P** is the class of polynomial time computable languages, $\mathbf{E} = \cup_{c\geq 1} \mathbf{DTIME}(2^{cn})$ is the class of linear exponential time sets, and $\mathbf{E}_2 = \cup_{c\geq 1} \mathbf{DTIME}(2^{n^c})$ is the class of polynomial exponential time sets. For a deterministic time class **C** we let **FC** denote the class of functions $f: \Sigma^* \to \Sigma^*$ which can be computed within **C**'s time bound.

The concatenation of two strings x and y is denoted by xy; 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+k is the kth successor of x under $<$ ($k\geq 1$). We identify a language A and its characteristic function, i.e., $x \in A$ iff $A(x)=1$, and we let $\|A\|$ denote the cardinality of A. For $A \subseteq \Sigma^*$ and $x \in \Sigma^*$ we let $A|x$ denote the finite initial segment of A below x, i.e., $A|x = \{y: y<x \ \& \ y \in A\}$, and we identify this initial segment with its

characteristic string, i.e., $A|z_n = A(z_0)...A(z_{n-1}) \in \Sigma^*$. Accordingly we let $|A|x|$ denote the length of the characteristic string of $A|x$. Note that

(1.0) $\quad 2^{|x|}-1 \le |A|x| < 2^{|x|+1}-1.$

We say A is **C**-m-reducible to B ($A \le_{\mathbf{C}-m} B$) via f if $f \in \mathbf{FC}$ and, for every $x \in \Sigma^*$, $A(x)=B(f(x))$. Instead of **P**-m-reducible and **DTIME**(t(n))-m-reducible we shortly say p-m-reducible and t(n)-m-reducible, respectively, and write $\le_{p\text{-}m}$ and $\le_{t(n)\text{-}m}$. In case of the other resource bounded reducibilities we will consider only the polynomial case. We assume the reader to be familiar with the polynomial time bounded versions of one-one (p-1), truth-table (p-tt), and Turing (p-T) reducibility (see Ladner et al. [12]). As intermediate reducibilities between p-m and p-tt we consider the bounded-query reductions: A p–k–tt–*reduction* $h(g_1,\ldots,g_k)$ consists of polynomial time computable functions $h: \Sigma^*\times\Sigma^k\to\Sigma$ (*evaluator*) and $g_i: \Sigma^*\to\Sigma^*$ ($1\le i\le k$; *selectors*). For an evaluator function h we define $h_x(a_1,\ldots,a_k)=h(x,a_1,\ldots,a_k)$. So h_x is the k–ary Boolean function which evaluates the k oracle queries on input x. A set A is p–k–tt–*reducible to* a set B ($A \le_{p-k-tt} B$) *via* $h(g_1,\ldots,g_k)$ if $\forall x\in\Sigma^*$ $(A(x) = h(x,B(g_1(x)),\ldots,B(g_k(x))))$. A is p–k–tt–*reducible to* B if $A \le_{p-k-tt} B$ via some p–k–tt–reduction $h(g_1,\ldots,g_k)$. Finally, A is p-btt-*reducible* to B ($A \le_{p-btt} B$) if $A \le_{p-k-tt} B$ for some $k\ge 1$.

2. Generic Sets

We now introduce the central concept of this paper.

2.1. Definition (Ambos-Spies et al. [3]). A *condition* is a set $C\subseteq\Sigma^*$. A language A *meets* the condition C if, for some string x, $A|x\in C$. C is *dense along* A if

$$\exists^\infty x\in\Sigma^*\ \exists i\in\Sigma\ ((A|x)i\in C);$$

and C is *dense* if C is dense along all languages. A language A is **C**–*generic* if A meets every condition $C\in\mathbf{C}$ which is dense along A.

This genericity concept was introduced by Ambos–Spies, Fleischhack and Huwig in [3]. Of the three types of genericity concepts introduced there, here we consider only the second type. In [3], **C**–generic sets were called **C**–2–generic sets. For deterministic time classes we abbreviate **DTIME**(t(n))–generic by t(n)–*generic* and we call a condition $C\in\mathbf{DTIME}(t(n))$ a t(n)–*condition*.

A condition C should be viewed as a finitary property P of languages, where C contains all

finite initial parts X|x of languages such that all languages Y extending X|x have the property P. So a language A has the property P if and only if A meets C. C is dense along A if and only if in a construction of A along the ordering $<$, where at stage s of the construction we decide whether or not the string z_s belongs to A, there are infinitely many stages s such that by appropriately defining $A(z_s)$ we can ensure that A has the property P (i.e. $A|(z_s+1) \in C$). Finally, in case of a t(n)-condition, the complexity for the correct choice for $A(z_s)$ is t(n)-time bounded in $|A|z_s|$, i.e., by (1.0), $t(2^n)$-time bounded in the length of z_s. So a t(n)-generic set will have all finitary properties P of time complexity t(n) (relative to the length n of the initial segment) which can be ensured in a construction of the above type infinitely often.

In the following we will mainly consider n^c–generic sets ($c \geq 1$) which are adequate for analyzing the structure of **E**. We start, however, with some more general results.

2.2. Proposition. (i) Let **C** and **D** be classes such that $\mathbf{C} \subseteq \mathbf{D}$. Then any **D**-generic set is **C**-generic. In particular, if t and t' are recursive functions such that $t(n) \leq t'(n)$ almost everywhere then any t'(n)-generic set is t(n)-generic.
(ii) For any recursive function t, the complement $\overline{A}$ of a t(n)–generic set A is t(n)–generic too.

Proof. The first part is immediate by definition. The second part follows from closure of **DTIME**(t(n)) under complements.

In [3] Ambos–Spies, Fleischhack and Huwig have shown that there are sparse **P**–generic sets in $\mathbf{DTIME}(2^{n^2})$. By a simple modification of this proof we obtain a strong general existence theorem for t(n)-generic sets.

2.3. Theorem. Let t(n), t'(n) and f(n) be nondecreasing functions on N such that t(n) and t'(n) are time-constructible, $t(n), t'(n) \geq n$, f(n) is polynomial time computable with respect to the unary representation, and the range of f is unbounded. Moreover, let B be a set in **DTIME**(t'(n)). Then there is a t(n)–generic set A such that

$$A \in \mathbf{DTIME}(2^{n+1} \cdot (t'(n) + n^2 \cdot t(2^{n+1}) \cdot \log(t(2^{n+1}))))$$

and, for any $n \geq 0$,

$$\|(A \Delta B) \cap \{x \in \Sigma^* : |x| = n\}\| \leq f(n).$$

Proof. We construct a t(n)–generic set A with the required properties in stages, where at stage s we decide whether or not $z_s \in A$. By means of a standard universal machine we may

fix a recursive enumeration $\{C_e: e\in N\}$ of **DTIME**(t(n)) such that,

(2.0) $C = \{0^e1x: x\in C_e\} \in$ **DTIME**$(e\cdot t(|x|)\cdot\log(t(|x|))+e)$.

Then to ensure that A is t(n)-generic it suffices to meet the requirements

R_e: C_e dense along A $\Rightarrow$ A meets C_e

for all numbers $e\in N$. Simultaneously with A we enumerate a list Sat of the indices of the requirements which are satisfied by diagonalization and we let Sat_s be the part of Sat enumerated by the end of stage s ($Sat_{-1}=\emptyset$). So, by the end of stage s–1, $A|z_s$ and Sat_{s-1} are given.

Stage s. We say that the requirement R_e *requires attention* (at stage s) if $e<f(|z_s|)$, $e\notin SAT_{s-1}$ and

(∗) $\exists i\leq 1\ ((A|z_s)i\in C_e)$.

Distinguish the following two cases.

Case 1: Some requirement requires attention. Fix the least e such that R_e requires attention and fix $i\leq 1$ minimal with $(A|z_s)i\in C_e$. Let $A(z_s)=i$ and $Sat_s = Sat_{s-1}\cup\{e\}$ and say that R_e *receives attention*.

Case 2: Otherwise. Let $A(z_s)=B(z_s)$ and let $Sat_s = Sat_{s-1}$.

This completes the construction. To show that A is t(n)–generic, first note that every requirement receives attention at most once and that Sat_s contains the indices of the requirements which received attention by the end of stage s. So, by a straightforward induction, every requirement requires attention only finitely often. Hence if C_e is dense along A, (∗) will hold at infinitely many stages s, whence R_e will eventually receive attention, thereby ensuring that A meets C_e. So every requirement R_e is met whence A is t(n)-generic.

Moreover, at a stage s with $|z_s|=n$, only a requirement R_e with $e<f(n)$ may receive attention. So Case 1 can apply to at most f(n) such stages, whence, by definition of A in Case 2, $\|(A\Delta B)\cap\{x\in\Sigma^*: |x|=n\}\| \leq f(n)$ will hold.

It remains to show that $A\in$ **DTIME**$(2^{n+1}\cdot(t'(n)+t''(n)))$, where $t''(n) = n^2\cdot t(2^{n+1})\cdot\log(t(2^{n+1}))$. Fix any string z_s of length n. Then, by (1.0), $s<2^{n+1}$ whence it suffices to show that, given $A|z_s$ and Sat_{s-1}, $A(z_s)$ and Sat_s can be computed in t'(n)+t''(n) steps. To do so, without loss of generality assume that $f(n)\leq n$. Moreover, since f(n) can be computed in poly(n) steps, we may assume that f(n) is given. Then t''(n) steps suffice to decide whether Case 1 applies to stage s and if so to perform the corresponding action: Since, by assumption $A|z_s$ and Sat_{s-1} are given, it suffices to check for each of the n numbers $e<|z_s|$ and for $i\leq 1$ whether $(A|z_s)i\in C_e$ which, by (2.0), can be done in

$O(n\cdot t(2^{n+1})\cdot\log(t(2^{n+1})))$ steps for each such e. Finally, since Case 2 can be performed in t'(n) steps this implies the claim.

2.4. Corollary. There is a sparse n^c–generic set in $\mathbf{DTIME}(2^{(c+2)n})$.

Proof. Apply Theorem 2.3 to $t(n)=n^c$, $t'(n)=f(n)=n$ and $B=\emptyset$. Since

$$2^{n+1}\cdot(n+n^2\cdot(2^{n+1})^c\cdot\log((2^{n+1})^c)) < 2^{(c+2)n}$$

almost everywhere, this yields an n^c–generic set $A\in\mathbf{DTIME}(2^{(c+2)n})$ with

$$\|A\cap\{x\in\Sigma^*: |x|=n\}\| \le n.$$

As the following theorem shows, Theorem 2.3 provides an almost optimal lower bound on the time complexity of t(n)-generic sets.

2.5. Theorem. Let A be t(n)-generic. Then $A\notin\mathbf{DTIME}(t(2^n))$. In particular, there is no n^c–generic set in $\mathbf{DTIME}(2^{cn})$.

Proof. For a contradiction assume that $A\in\mathbf{DTIME}(t(2^n))$. Then, by (1.0),

$$C = \{X|(x+1): A(x)\neq X(x)\}$$

is a t(n)–condition which is obviously dense. So, by t(n)–genericity, A meets C. By definition of C this implies that $A(x)\neq A(x)$ for some x, a contradiction.

The argument in the proof of Theorem 2.5 is typical for showing that a generic set has a certain property. In the following we give two further examples: we prove that generic sets are incompressible under many-one reductions and bi-immune. Here as in the following we will restrict ourselves to n^c-genericity.

A function $f: \Sigma^*\to\Sigma^*$ is *almost 1–1* if the *collision set* of f,

$$COLL_f = \{x\in\Sigma^*: \exists y<x\ (f(x)=f(y))\},$$

is finite. f is *consistent* with a set A if, for all $x,y\in\Sigma^*$, $A(x)\neq A(y)$ implies that $f(x)\neq f(y)$. Then A is **C**–*incompressible* if, for any $f\in\mathbf{FC}$ which is consistent with A, f is almost 1–1. Again we abbreviate $\mathbf{DTIME}(t(n))$-incompressible by t(n)-incompressible and we write p-incompressible for **P**-incompressible. Note that $A\le_{\mathbf{C}-m} B$ via f implies that f is consistent with A. So, for **C**-incompressible A, any **C**-m-reduction from A is almost 1–1.

2.6. Theorem. Let A be n^c–generic ($c\ge 2$). Then A is $2^{(c-1)n}$–incompressible.

Proof. Fix $f\in\mathbf{FDTIME}(2^{(c-1)n})$ such that f is consistent with A. To show that f is almost

1-1, define $C = \{X|(x+1): \exists y<x\ (f(x)=f(y)\ \&\ X(x)\neq X(y))\}$. Then C is an n^c–condition. Moreover, by consistency of f with A, A does not meet C. So, by n^c–genericity of A, C is not dense along A. By definition of C, it follows that the collision set of f is finite.

It is easy to show that any 2^{cn}–incompressible set A is 2^{cn}–*bi-immune*, i.e., $A\cap B\neq\emptyset$ and $\overline{A}\cap B\neq\emptyset$ for any infinite $B\in DTIME(2^{cn})$ (see [5]). So Theorem 2.6 implies that any n^c–generic set is $2^{(c-1)n}$–bi-immune ($c\geq 2$). By a direct argument we can slightly improve this result:

2.7. Theorem. Let A be n^c–generic ($c\geq 2$). Then A is 2^{cn}–bi-immune.

Proof. By Proposition 2.2 it suffices to show that $\overline{A}$ is 2^{cn}–immune, i.e., that $A\cap B\neq\emptyset$ for any infinite $B\in DTIME(2^{cn})$. So fix such a set B. Define

$$C = \{X|(x+1): X(x)=B(x)=1\}.$$

Then, by (1.0), C is an n^c–condition which, by infinity of B, is dense. Hence A meets C which, by definition of C, implies that $A\cap B\neq\emptyset$.

We can also apply n^c–genericity to separate the standard polynomial time reducibilities between p-one-one and p-bounded-truth-table (see [12]). As a corollary we obtain that n^c–generic sets cannot be p-btt-complete for **E**.

2.8. Theorem. Let A be n^c–generic ($c\geq 2$).

(i) $A\oplus A \not\leq_{p\text{-}1} A$

(ii) $\overline{A} \not\leq_{p\text{-}m} A$

(iii) $A_k \not\leq_{p\text{-}k\text{-}tt} A$, where $A_k = \{x: \{x,x+1,...,x+k\}\cap A\neq\emptyset\}$ ($k\geq 1$)

(iv) $A_\omega \not\leq_{p\text{-}btt} A$, where $A_\omega = \{0^k1x: x\in A_k\}$

We omit the proof of Theorem 2.8 since it is very similar to the proof of the corresponding facts for the tally p-generic sets in [2] (see [2], Theorem 5.9). Note that, for any set A, $A\oplus A \leq_{p\text{-}m} A$, $\overline{A} \leq_{p\text{-}1\text{-}tt} A$, $A_k \leq_{p\text{-}(k+1)\text{-}tt} A$, and $A_\omega \leq_{p\text{-}tt} A$. So we can mutually distinguish p-1, p-m, p-1-tt, p-(k+1)-tt ($k\geq 1$), p-btt and p-tt reductions to n^c-generic sets:

2.9. Corollary. Let A be n^c–generic ($c\geq 2$). There are sets B_1, B_2, $B_{3,k}$ ($k\geq 1$) and B_4 such that

(i) $B_1 \leq_{p\text{-}m} A$ but $B_1 \not\leq_{p\text{-}1} A$

(ii) $B_2 \leq_{p\text{-}1\text{-}tt} A$ but $B_2 \not\leq_{p\text{-}m} A$

(iii) $B_{3,k} \leq_{p\text{-}(k+1)\text{-}tt} A$ but $B_{3,k} \not\leq_{p\text{-}k\text{-}tt} A$ $(k \geq 1)$

(iv) $B_4 \leq_{p\text{-}tt} A$ but $B_4 \not\leq_{p\text{-}btt} A$

2.10. Corollary. Let A be n^c–generic ($c \geq 2$). Then A is not p-btt-complete for **E**.

Proof. Assume that $A \in \mathbf{E}$. Then, for A_ω as in Theorem 2.8, $A_\omega \in \mathbf{E}$ but $A_\omega \not\leq_{p\text{-}btt} A$. So A is not p-btt-complete for **E**.

We conclude this section with the observation that Corollary 2.10 is optimal. Given $f: N \to N$ we say that A is p-f(n)-tt-reducible to B if there is a p-tt-reduction from A to B for which the number of oracle queries on inputs of length n is bounded by f(n).

2.11. Theorem. Let $f: N \to N$ be nondecreasing, unbounded and polynomial time computable with respect to the unary representation. There is an n^c–generic set A which is complete for **E** under p-f(n)-tt-reductions ($c \geq 1$). In particular, there is an n^c–generic set A which is p-tt-complete for **E**.

Proof. Fix a p-m-complete set C for **E**. We will use the following transitivity law for p-m- and p-f(n)-tt-reductions: Since a p-m-reduction increases the size of the input only by a polynomial factor and since f is nondecreasing, for any sets X, Y, Z,

$$X \leq_{p\text{-}m} Y \;\&\; Y \leq_{p\text{-}f(\log(n))\text{-}tt} Z \;\Rightarrow\; X \leq_{p\text{-}f(n)\text{-}tt} Z.$$

Hence it suffices to show that there is an n^c-generic set $A \in \mathbf{E}$ with $C \leq_{p\text{-}f(\log(n))\text{-}tt} A$.

Let $B = \{xy: |x|=|y| \;\&\; x \in C\}$. Then, by Theorem 2.3, there is an n^c–generic set $A \in \mathbf{E}$ such that

$$\|(A \Delta B) \cap \{x \in \Sigma^*: |x|=2n\}\| \leq 1/3 \cdot f(\log(n)).$$

Hence $x \in C$ if and only if $\|A \cap F_x\| \geq 2/3 \cdot f(\log(|x|))$, where F_x consists of the lexicographically first $f(\log(|x|))$ strings xy with $|x|=|y|$. So C is p-f(log(n))-tt-reducible to A.

2.12. Remark. As the results of this section show, the n^c-generic sets pertain to diagonalizations over the levels of the linear exponential time hierarchy $\mathbf{E} = \cup_{c \geq 1} \mathbf{DTIME}(2^{cn})$. So, since a set is **P**-generic iff it is n^c-generic for all $c \geq 1$, **P**-generic sets relate to diagonalizations over **E**. In particular, by Theorem 2.5, no set in **E** is **P**-generic. In fact, by Theorems 2.6 and 2.7, **P**-generic sets are **E**-incompressible and **E**-bi-immune. On the other hand, by Theorem 2.3, **P**-generic sets can be found in all sufficiently closed, smooth deterministic time classes properly containing **E**. E.g., as shown already in [3], there are **P**-generic sets in the class $\mathbf{DTIME}(2^{(n^2)})$.

In an analogous way, the $2^{(\log n)^c}$-generic sets pertain to the levels $\mathbf{DTIME}(2^{(n^c)})$ of the polynomial exponential time hierarchy $\mathbf{E}_2$. E.g., by Theorem 2.5, there is no $2^{(\log n)^c}$-generic set in $\mathbf{DTIME}(2^{(n^c)})$, and the proofs of Theorems 2.6 and 2.7 can be easily modified to show that $2^{(\log n)^c}$-generic sets are $\mathbf{DTIME}(2^{(n^{c-1})})$-incompressible and $\mathbf{DTIME}(2^{(n^c)})$-bi-immune ($c\geq 2$). On the other hand, by Theorem 2.3, there are $2^{(\log n)^c}$-generic sets in $\mathbf{DTIME}(2^{(n^{c+2})})$. So, for $\mathbf{P}_2 = \cup_{c\geq 1} \mathbf{DTIME}(2^{(\log n)^c})$, the $\mathbf{P}_2$-generic sets relate to diagonalizations over $\mathbf{E}_2$ just as the $\mathbf{P}$-generic sets relate to diagonalizations over $\mathbf{E}$. In particular, observe that the proof of Theorem 2.11 can be easily modified to show that, for any function f as there and for any $c\geq 1$, there is a $2^{(\log n)^c}$-generic set (hence a $\mathbf{P}$-generic set) which is complete for $\mathbf{E}_2$ under p-f(n)-tt-reductions.

3. Genericity and Measure

We first introduce a fragment of Lutz's measure theory which will be sufficient for our investigations. Our presentation follows [16]. A more complete account of resource bounded measure theory can be found in [15].

A *martingale* is a function $d: \Sigma^* \to [0,\infty)$ such that, for all $x \in \Sigma^*$, $d(x0)+d(x1) \leq 2d(x)$. A martingale d *succeeds on* a language $A \subseteq \Sigma^*$ if $\limsup_n d(A|z_n) = \infty$. Note that the values of martingales are reals. So to define computability of a martingale we consider approximations $d_k: \Sigma^* \to Q_+$, where Q_+ is the set of nonnegative rationals, satisfying $|d_k(x)-d(x)| \leq 2^{-k}$ ($k \in N$). For such approximation functions we can define the time complexity in the standard way and we can say that a martingale d is t(n)–*computable* if it has uniformly t(n)–computable approximation functions d_k, $k\geq 0$. If d is p(n)–computable for some polynomial p then we say that d is p–*computable*.

Now a class $\mathbf{C}$ of languages has t(n)–*measure* 0 ($\mu_{t(n)}(\mathbf{C})=0$) if there is a t(n)–computable martingale which succeeds on every language 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 $\mathbf{C}$. We write $\mu_{t(n)}(\mathbf{C})\neq 0$ to indicate that $\mathbf{C}$ does not have t(n)-measure 0. The p–*measure* of a class $\mathbf{C}$ is defined similarly by p–computable martingales and is denoted by $\mu_p(\mathbf{C})$. The measure of a class $\mathbf{C}$ relative to $\mathbf{E}$ is defined 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 $\mu(\mathbf{C}^c|\mathbf{E})=0$. We write $\mu(\mathbf{C}|\mathbf{E})\neq 0$ to indicate that $\mathbf{C}$ does not have measure 0 in $\mathbf{E}$. Lutz has shown that the measure in $\mathbf{E}$ is

nontrivial: Since $\mu_p(\mathbf{E})\neq 0$, $\mu(\mathbf{C}|\mathbf{E})=1$ implies that $\mu(\mathbf{C}|\mathbf{E})\neq 0$.

We should remark that, for technical convenience, our martingale definition differs slightly from Lutz's definition: while he requires that $d(x0)+d(x1) = 2d(x)$ we only require that $d(x0)+d(x1) \leq 2d(x)$ (In the literature such a function is sometimes called a *super-martingale* and Lutz calls it a *density function*). As a consequence the resulting t(n)-measure notions may differ by a linear factor. In both cases, however, we obtain the same notion of p-measure and measure in **E**. As a technical tool we will need the following (weak) version of σ–additivity of the p–measure:

3.1. Lemma (Lutz [15]). Let $\mathbf{C}_e$ ($e\in N$) be classes of languages and let $\mathbf{C}=\cup_{e\geq 0}\mathbf{C}_e$. Assume that, for some $c\geq 1$, there is an n^c–computable function $d: N\times\Sigma^*\to Q_+$ such that, for any $e\in N$, $d_e=\lambda x.d(e,x)$ is a martingale which succeeds on every language in $\mathbf{C}_e$. Then $\mu_{n^{c+1}}(\mathbf{C})=\mu_p(\mathbf{C})=0$.

3.2. Theorem. For any $c\geq 1$, the class of n^c–generic sets has n^{c+3}-measure 1, hence p–measure 1.

Proof. Fix c and let $\{C_e: e\in N\}$ be a recursive enumeration of $\mathbf{DTIME}(n^c)$ such that

$$(3.0)\qquad C = \{0^e1x: x\in C_e\} \in \mathbf{DTIME}(e\cdot|x|^c\cdot\log(|x|^c)+e)$$

holds. Let $\mathbf{C}_e = \{X: C_e \text{ is dense along } X \text{ \& } X \text{ does not meet } C_e\}$ and let $\mathbf{C}=\cup_{e\geq 0}\mathbf{C}_e$. Then **C** is the class of languages which are not n^c–generic. So, by Lemma 3.1, it suffices to define an n^{c+2}–computable function d such that, for $e\in N$, d_e is a martingale which succeeds on every language in $\mathbf{C}_e$. For x with $|x|\leq 2^e$ let $d(e,x)=1$ and, for x with $|x|\geq 2^e$ and for $i\leq 1$, let

$$d(e,xi) = \begin{cases} 0 & \text{if } xi\in C_e \text{ \& } x(1-i)\notin C_e \\ 2d(e,x) & \text{if } x(1-i)\in C_e \text{ \& } xi\notin C_e \\ d(e,x) & \text{otherwise} \end{cases}$$

Then each d_e is a martingale. Moreover, it easily follows from (3.0) that d is n^{c+2}-computable. So it only remains to prove that each d_e succeeds on the languages in $\mathbf{C}_e$. Fix e and $X\in\mathbf{C}_e$. Then C_e is dense along X but X does not meet C_e. By the latter, $X|x\notin C_e$ for all x, whence $d(e,X|x)\neq 0$ for all x. It follows that $d(e,X|z_n)$ is nondecreasing in n. So it suffices to show that there are infinitely many x such that $d(e,X|(x+1)) = 2d(e,X|x)$, i.e., by definition of d, such that, for some $i\leq 1$, $X|(x+1)=(X|x)i$, $(X|x)(1-i)\in C_e$ and $(X|x)i\notin C_e$. But this is immediate by definition of $\mathbf{C}_e$.

By Theorem 3.2, any property shared by all n^c-generic sets (for some $c \geq 1$) occurs with p-measure 1. E.g. from Theorem 2.4 we may conclude that the class of 2^{cn}-incompressible sets has p-measure 1. This was first shown by Juedes and Lutz [11] using a direct argument. Though, in general, the direct proof that a property P has p-measure 1 uses the same ideas as showing that any n^c-generic set (for some c) has this property, the latter may turn out to be less complex, since it suffices to consider single requirements. In particular in more involved arguments this simplified machinery can help to keep down the combinatorical complexity of proofs. In the next section we will give an example for this.

3.3. Remark. Besides the measure on **E** Lutz also introduced a measure on $\mathbf{E}_2$. Let $\mathbf{P}_2 = \bigcup_{c\geq 1} \mathbf{DTIME}(2^{(\log n)^c})$. Then the p_2-measure of a class **C** is defined by letting $\mu_{p_2}(\mathbf{C})=i$ ($i \in 0,1$) if there is a number c such that, for $t(n)=2^{(\log n)^c}$, $\mu_{t(n)}(\mathbf{C})=i$. Moreover, **C** has measure 0 in $\mathbf{E}_2$ ($\mu(\mathbf{C}|\mathbf{E}_2)=0$) if $\mu_{p_2}(\mathbf{C} \cap \mathbf{E}_2)=0$ and **C** has *measure* 1 *in* $\mathbf{E}_2$ ($\mu(\mathbf{C}|\mathbf{E}_2)=1$) if $\mu(\mathbf{C}^c|\mathbf{E}_2)=0$. By duplicating the above argument we can show that, for any c, the class of the $2^{(\log n)^c}$-generic sets has p_2-measure 1, hence measure 1 in $\mathbf{E}_2$. In particular, the class of **P**-generic sets has p_2-measure 1 and measure 1 in $\mathbf{E}_2$.

4. The Small Span Theorem for Bounded Query Reductions.

For a polynomial time bounded reducibility $\leq_{p\text{-}r}$ the *lower* and *upper span* of a set A are defined by $P_r(A) = \{B: B \leq_{p\text{-}r} A\}$ and $P_r^{-1}(A) = \{B: A \leq_{p\text{-}r} B\}$, respectively. The intersection of the upper and lower span of A is the p-r-*degree* of A: $\deg_{p\text{-}r}(A) = \{B: B =_{p\text{-}r} A\}$. Juedes and Lutz [11] have shown that, for any set $A \in \mathbf{E}$, the upper span of A or the lower span of A under p-m-reducibility has measure 0 in **E**. Hence $\deg_{p\text{-}m}(A)$ has measure 0 in **E** for any set $A \in \mathbf{E}$. So, in particular, the class of p-m-complete problems for **E** has measure 0 in **E**.

Here we first deduce the Small Span Theorem for p-m-reducibility from Theorem 3.2 and a theorem on the distribution of the n^c-generic sets under p-m-reducibility which we will prove next. Then, by extending this theorem to bounded truth-table reductions, we generalize the Small Span Theorem to these reductions.

4.1. Theorem. Let A and B be sets such that $A \leq_{p\text{-}m} B$, A is n^c-generic and $A \in \mathbf{DTIME}(2^{dn})$ where $c,d \geq 2$. Then B is not n^{d+1}-generic.

Proof. Fix $f \in \mathbf{FP}$ such that $A \leq_{p\text{-}m} B$ via f and let $D = \{x: |f(x)| \geq |x|\}$. Note that, by Theorem 2.6, A is p-incompressible whence f is almost 1-1. This easily implies that D is infinite. So the condition

$$C = \{X|(y+1): \exists x(|x| \leq |y| \ \& \ f(x)=y \ \& \ A(x) \neq X(y))\}$$

is dense. Moreover, as one can easily check, $C \in \mathbf{DTIME}(n^{d+1})$ and, since $A \leq_{p\text{-}m} B$ via f, B does not meet C. So B is not n^{d+1}-generic.

Note that the main step in the above proof shows that, for any p-incompressible $A \in \mathbf{DTIME}(2^{dn})$ and for any B with $A \leq_{p\text{-}m} B$, B is not $2^{(d+1)n}$-bi-immune. The first proof of this fact is due to Lindner [13].

4.2. Corollary (Small Span Theorem of Juedes and Lutz [11]). Let $A \in \mathbf{E}$. Then

$$\mu(P_m(A)|\mathbf{E}) = 0 \ \text{ or } \ \mu_p(P_m^{-1}(A)) = \mu(P_m^{-1}(A)|\mathbf{E}) = 0.$$

Proof. If there is no n^2-generic set in $P_m(A) \cap \mathbf{E}$ then $\mu(P_m(A)|\mathbf{E}) = \mu_p(P_m(A) \cap \mathbf{E}) = 0$ by Theorem 3.2. Otherwise, fix A' and $d \geq 2$ such that A' is n^2-generic, $A' \leq_{p\text{-}m} A$, and $A' \in \mathbf{DTIME}(2^{dn})$. Since $P_m^{-1}(A)$ is contained in $P_m^{-1}(A')$ it follows from Theorem 4.1, that $P_m^{-1}(A)$ does not contain any n^{d+1}-generic set. So, again by Theorem 3.2, $\mu_p(P_m^{-1}(A)) = \mu(P_m^{-1}(A)|\mathbf{E}) = 0$.

Lutz [16] raised the question whether the Small Span Theorem generalizes to the weaker polynomial reducibilities. Lindner [13] proved the Small Span Theorem for p-1-tt-reducibility. So the positive character of p-m-reducibility is not necessary for the theorem. This still left the question what happens for reducibilities which may ask more than one query. Here we prove the Small Span Theorem for p-k-tt-reductions for any $k \geq 1$, i.e., for reductions where the number of queries does not depend on the input (for the definition of p-k-tt-reducibility, see the introduction). The main step in the proof is an analogue of Theorem 4.1 for p-k-tt-reducibility.

4.3. Theorem. Let A and B be sets such that $A \leq_{p\text{–}k\text{–}tt} B$ for some $k \geq 1$, A is n^c–generic for some $c \geq 2$, and $A \in \mathbf{DTIME}(2^{dn})$ for some $d \geq 2$. Then B is not $n^{(k+1)(d+1)}$–generic.

For the proof of this theorem we need an incompressibility concept for p-k–tt–reductions and some more technical tools.

4.4. Definition. The *collision set* of a p–k–tt–reduction $h(g_1,\ldots,g_k)$ is defined by

$$\mathrm{COLL}_{h(g_1,\ldots,g_k)} = \{x\in\Sigma^*: \exists y<x\ (g_1(x)=g_1(y)\ \&\ \ldots\ \&\ g_k(x)=g_k(y)\ \&\ h_x=h_y)\}.$$

The reduction $h(g_1,\ldots,g_k)$ is *almost 1–1* if $\mathrm{COLL}_{h(g_1,\ldots,g_k)}$ is finite; and $h(g_1,\ldots,g_k)$ is *consistent with* a language A if

$$\forall x,y\in\Sigma^*\ ([g_1(x)=g_1(y)\ \&\ \ldots\ \&\ g_k(x)=g_k(y)\ \&\ h_x=h_y] \Rightarrow A(x)=A(y)).$$

A language A is p–k–tt–*incompressible* if, for any p–k–tt–reduction $h(g_1,\ldots,g_k)$ which is consistent with A, $h(g_1,\ldots,g_k)$ is almost 1–1.

Note that $A \leq_{p-k-tt} B$ via $h(g_1,\ldots,g_k)$ implies that $h(g_1,\ldots,g_k)$ is consistent with A, whence for p–k–tt–incompressible A, $h(g_1,\ldots,g_k)$ is almost 1–1. As we show next, p-k-tt-incompressibility coincides with p-incompressibility. So, by Theorem 2.6, n^c–generic sets are incompressible under p–k–tt–reductions.

4.5. Lemma. For any k≥1, A is p–k–tt–incompressible iff A is p-incompressible.

Proof. Since any p-m-reduction may be viewed as a p-k-tt-reduction, obviously any p-k-tt-incompressible set is p-incompressible. For a proof of the nontrivial direction, let A be p-incompressible and fix any p-k-tt-reduction $h(g_1,\ldots,g_k)$ which is consistent with A (k≥1). We have to show that $h(g_1,\ldots,g_k)$ is almost 1-1. Let

$$A' = \{\langle h_x,g_1(x),\ldots,g_k(x)\rangle: x\in A\}.$$

Since $h(g_1,\ldots,g_k)$ is consistent with A, $A \leq_{p-m} A'$ via $f(x)=\langle h_x,g_1(x),\ldots,g_k(x)\rangle$. So, by p-incompressibility of A, f is almost 1-1, whence $h(g_1,\ldots,g_k)$ is almost 1-1 too.

For technical convenience, in the following we assume that all p-k-tt-reductions are in a normal form, where the queries are listed in decreasing order and redundant queries are replaced by λ: A p–k–tt–reduction $h(g_1,\ldots,g_k)$ is *normal* if, for any $x\in\Sigma^*$, there is some i≤k such that, for $1\leq j<i$, $g_j(x)>g_{j+1}(x)$ and, for j≥i, $g_j(x)=\lambda$. It is easy to show that, for any p–k–tt–reduction, there is an equivalent normal p–k–tt–reduction. For a normal p-k-tt-reduction $h(g_1,\ldots,g_k)$, the *rank* of $h(g_1,\ldots,g_k)$ is defined to be the greatest number $r\in\{1,\ldots,k\}$ such that

$$\exists^{\infty} x\in\Sigma^*\ (|x| \leq (k+1)|g_r(x)|).$$

(If no such r exists then the rank of $h(g_1,\ldots,g_k)$ is 0.)

4.6. Lemma. Let $h(g_1,\ldots,g_k)$ be a normal p–k–tt–reduction which is almost 1–1. Then the rank of $h(g_1,\ldots,g_k)$ is greater than 0.

Proof. Fix n such that $2^n > 2^{2^k}$ and no x with |x|≥n is in the collision set of $h(g_1,\ldots,g_k)$. It

suffices to show that, for some x with $|x|=(k+1)n$, $|g_1(x)|\geq n$. Let

$BC_n=\{(\alpha,y_1,\ldots,y_k)$: α is a k–ary Boolean function and, for $1\leq i\leq k$, $y_i\in\Sigma^*$ and $|y_i|<n\}$.

Since $h(g_1,\ldots,g_k)$ is normal, for any x with $|g_1(x)|<n$, $(h_x,g_1(x),\ldots g_k(x))\in BC_n$. So, since, by choice of n, $h(g_1,\ldots,g_k)$ is 1–1 on $\{x\in\Sigma^*: |x|=(k+1)n\}$, the existence of an x with the desired properties will follow from

$$\|BC_n\| < \|\{x\in\Sigma^*: |x|=(k+1)n\}\| = 2^{(k+1)n}.$$

This holds since there are 2^n-1 strings of length less than n and 2^{2^k} k–ary Boolean functions, whence by choice of n, $\|BC_n\| < 2^{2^k}\cdot(2^n)^k < 2^n\cdot(2^n)^k = 2^{(k+1)n}$.

We are now ready to prove Theorem 4.3.

Proof of Theorem 4.3. Fix a normal p-k-tt-reduction $h(g_1,\ldots,g_k)$ from A to B of minimal rank, say r. Note that, by Lemma 4.5, $h(g_1,\ldots,g_k)$ is almost 1-1 whence, by Lemma 4.6, $r > 0$. We first show that there are infinitely many strings x satisfying

(4.0) $|x| \leq (k+1)|g_1(x)|$ & $h_x(0,B(g_2(x)),\ldots,B(g_k(x))) \neq h_x(1,B(g_2(x)),\ldots,B(g_k(x)))$.

For a contradiction assume that (4.0) fails for almost all strings x, and fix n such that no string x with $|x|\geq n$ has this property. Define a p-k-tt-reduction $h'(g_1',\ldots,g_k')$ as follows. For x with $n \leq |x| \leq (k+1)|g_1(x)|$ let

$$(g_1'(x),\ldots,g_k'(x)) = (g_2(x),\ldots,g_k(x),\lambda) \quad \& \quad h_x'(j_1,\ldots,j_k) = h_x(0,j_1,\ldots,j_{k-1})$$

(for any $j_1,\ldots,j_k\in\Sigma$), and let $(g_1'(x),\ldots,g_k'(x)) = (g_1(x),\ldots,g_k(x))$ and $h_x' = h_x$ otherwise. Note that in the first case,

$$\begin{aligned} h_x'(B(g_1'(x)),B(g_2'(x)),\ldots,B(g_k'(x))) &= h_x(0,B(g_2(x)),\ldots,B(g_k(x))) \\ &= h_x(B(g_1(x)),B(g_2(x)),\ldots,B(g_k(x))), \end{aligned}$$

where the second equality follows from failure of (4.0). So $A \leq_{p\text{-}k\text{-}tt} B$ via $h'(g_1',\ldots,g_k')$. Moreover, this reduction is normal, and, for almost all x with $|x| \leq (k+1)|g_1(x)|$, $h'(g_1',\ldots,g_k')$ is obtained from $h(g_1,\ldots,g_k)$ by eliminating the greatest query $g_1(x)$. So the rank of $h'(g_1',\ldots,g_k')$ is r-1, contrary to minimality of r. So (4.0) holds infinitely often. Hence the condition

$$C = \{X|y+1: \exists x\ (|x|\leq(k+1)|y| \ \&\ g_1(x)=y \ \&\ h_x(X(g_1(x)),\ldots,X(g_k(x)))\neq A(x))\}$$

is dense. Moreover, $C\in \mathbf{DTIME}(n^{(k+1)(d+1)})$ and, since $A \leq_{p\text{-}k\text{-}tt} B$ via $h(g_1,\ldots,g_k)$, B does not meet C. So B is not $n^{(k+1)(d+1)}$–generic.

4.7. Corollary (Small Span Theorem for $\leq_{p\text{-}k\text{-}tt}$). Let $A\in\mathbf{E}$ and $k\geq 1$. Then

$$\mu(P_{k\text{-}tt}(A)|\mathbf{E}) = 0 \ \text{ or } \ \mu_p(P^{-1}_{k\text{-}tt}(A)) = \mu(P^{-1}_{k\text{-}tt}(A)|\mathbf{E}) = 0.$$

Proof. This is shown as Corollary 4.2 using Theorem 4.3 in place of Theorem 4.1.

We do not know whether Corollary 4.7 can be extended to p-btt-reducibility. Note that in Theorem 4.3 the polynomial bound on the genericity for the successors (under p-k-tt-reducibility) of the n^c-generic set A in **E** grows with k so that we do not get a polynomial bound for the successors under all btt-reductions. We expect that an extension of Theorem 4.3 and Corollary 4.7 to p-btt-reducibility (if possible) will be of technical interest.

An interesting consequence of Corollary 4.7 is that, for any $k \geq 1$, the class of p-k-tt-hard languages for **E** has p-measure 0. A corresponding result for generic sets follows from Theorem 4.3.

4.8. Corollary. Let A be $n^{5(k+1)}$-generic ($k \geq 1$). Then A is not **E**-hard under p-k-tt-reductions. Hence, the class of **E**-hard languages under p-k-tt-reducibility has p-measure 0.

Proof. By Corollary 2.4 there is an n^2-generic set in $\mathbf{DTIME}(2^{4n})$, whence, by Theorem 4.3, no p-k-tt-hard set for **E** can be $n^{5(k+1)}$-generic.

Though Corollary 4.8 does not settle the question whether the class of the p-btt-hard languages for **E** has p-measure 0, we obtain two partial results: First, by Corollary 4.8, no **P**-generic set is p-btt hard for **E**, whence, by Remark 3.3, the class of p-btt-hard problems for **E** has p_2-measure 0. The second partial result concerns the complete sets. Here, a p-measure-0 result follows immediately from Corollary 2.10 and Theorem 3.2:

4.*9. Theorem.* $\mu_p(\{A: A \text{ p-btt-complete for } \mathbf{E}\})=0$.

By using a different method, Buhrman and Mayordomo (private communication) independently but earlier proved a weaker version of the latter two results, namely that the class of the p-btt-complete languages for **E** has p_2-measure 0.

The question, whether there are Small Span Theorems for the *weak* p-reducibilities, namely polynomial truth-table (p-tt) and polynomial Turing (p-T) reducibility, and the more specific question whether the classes of **E**-hard problems under these reducibilities have p-measure 0 seem to be much more fundamental. By Theorem 2.11 our approach by generic sets fails for the weak reducibilities. Moreover, as observed already by Lutz, these questions may depend on the relation between **E** and **BPP**: For the classical measure μ, Bennet and Gill [6] have shown that $\mu(P_T^{-1}(A)) = 1$ iff $A \in \mathbf{BPP}$ while Ambos-Spies [1] has shown that $\mu(P_m^{-1}(A)) = 1$ iff $A \in \mathbf{P}$. Moreover, Ambos-Spies (unpublished) and, independently, Tang and Book [22] extended these results to the intermediate reducibilities

by showing that $\mu(P_{tt}^{-1}(A)) = 1$ iff $A \in \mathbf{BPP}$ while $\mu(P_{btt}^{-1}(A)) = 1$ iff $A \in \mathbf{P}$. Since $\mu(\mathbf{C}) = 1$ implies that **C** does not have p-measure 0, these results imply that, assuming $\mathbf{E} \subseteq \mathbf{BPP}$, the Small Span Theorem fails for p-tt-reducibility and p-Turing-reducibility and the classes of the **E**-hard sets under these reducibilities do not have p-measure 0. Moreover, Heller [9] has constructed an oracle relative to which $\mathbf{E}_2 = \mathbf{BPP}$. So a proof of the Small Span Theorem for the weak p-reducibilities would require nonrelativizable techniques.

5. Conclusion

We have shown that many properties which occur with p-measure 1 are shared by all n^c-generic sets (some $c \geq 2$). This gives a new, modular approach to some p-measure 1-results which can be combinatorically much simpler than the direct approach. This approach, however, does not cover all p-measure 1-results. Generic sets are designed to be universal for standard resource bounded diagonalization arguments. In such a diagonalization argument, a single diagonalization step corresponding to one of the subrequirements has to be performed only once and only under the proviso that there are infinitely many chances to do so. Though, in general, this easily implies that the action for a single requirement will be performed infinitely often (provided there are infinitely many chances to do so), we cannot say anything about the frequency with which the opportunities are taken. The latter contrasts with a typical measure 1 construction where we have to take the majority of the opportunities. To illustrate this difference we consider the density of a set. We have shown already that a generic set can be sparse (Corollary 2.4). As first observed in [17], the class of sparse sets, however, has p-measure 0. To see this consider the n^2-martingale $d: \Sigma^* \to Q_+$ defined by $d(\lambda)=1$, $d(x0)=3/2 \cdot d(x)$, and $d(x1)=1/2 \cdot d(x)$. Then it is easy to see that d succeeds on any sparse set, in fact on any set which is not exponentially dense.

Though this example points out limitations of the generic set approach to p-measure 1-results, we would like to emphasize that the generic sets help us to distinguish between those properties which can be forced by standard diagonalizations and those which require a measure diagonalization argument. Moreover, this example also shows that the assumption that a class **C** contains an n^c-generic set is weaker than the assumption that **C** has nonzero p-measure. This observation might be of particular interest when studying the structure of **NP** assuming that **NP** is sufficiently large. Lutz defines that **NP** is *not small* if $\mu_p(\mathbf{NP}) \neq 0$, and in [18] he and Mayordomo proved that under this non-smallness hypothesis p-T-completeness and p-m-completeness for **NP** do not coincide. We can show that this result already follows from the (apparently weaker) assumption that **NP** contains

an n^2-generic set.

Moreover, the relations between resource bounded genericity and measure which we explored here for the polynomial case hold for arbitrary time (and space) bounds. In particular, as shortly indicated in Remarks 2.12 and 3.3 already, we obtain corresponding results for the p_2-measure analysis of $\mathbf{E}_2$ by Lutz.

Finally we want to remark that there is a *general* modular approach to p-measure 1-results by using random sets in place of generic ones. Following Schnorr [21] and Lutz [16] we say that a language A is t(n)-random if no t(n)-computable martingale succeeds on A, i.e., if A does not belong to any class of t(n)-measure 0. The existence of n^c-random sets in **E** is shown in [4]. In fact, there it is shown that the class of n^c-random sets has p-measure 1, and random sets are used to further analyze the p-measure on **E**. Moreover, as also shown in [4], randomness is a refinement of genericity, namely, any n^{c+1}-random set is n^c-generic whence any **P**-random set is **P**-generic, whereas, by the above observation on sparseness, the converse is not true.

References

1 K. Ambos-Spies, Randomness, relativizations, and polynomial reducibilities, in: Proc. First Structure in Complexity Theory Conference 1986, Lect. Notes Comput. Sci. 223 (1986) 23-34, Springer Verlag.

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

3 K. Ambos-Spies, H. Fleischhack, and H. Huwig, Diagonalizing over deterministic polynomial time, in: Proc. CSL '87, Lect. Notes Comput. Sci. 329 (1988) 1-16, Springer Verlag.

4 K. Ambos-Spies, S. A. Terwijn, X. Zheng, Resource bounded randomness and weakly complete problems, Theor. Comput. Sci (to appear) (Extended abstract in: Proc. ISAAC '94, Lect. Notes Comput. Sci. 834 (1994) 369-377, Springer Verlag.)

5 J. L. Balcazar and U. Schöning. Bi-immune sets for complexity classes, Math. Systems Theory 18 (1985) 1-10.

6 C. H. Bennett and J. Gill, Relative to a random oracle A, $P^A \neq NP^A \neq co\text{-}NP^A$ with probability 1, SIAM J. Comput. 10 (1981) 96-113.

7 H. Fleischhack, On Diagonalizations over Complexity Classes, Dissertation, Universität Dortmund, Dept. Comput. Sci. Tech. Rep. 210, 1985.

8 H. Fleischhack, P-genericity and strong P-genericity, in: Proc. MFCS 1986, Lect.

Notes Comput. Sci. 233 (1986) 341-349, Springer Verlag.

9 H. Heller, On relativized exponential and probabilistic complexity classes, Information and Control 71 (1986) 231-243.

10 C. Jockusch, Degrees of generic sets, in: Recursion Theory: its Generalisations and Applications, London Math. Soc. Lect. Notes Series 45 (1980) 110-139, Cambridge University Press.

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

12 R. E. Ladner, N. A. Lynch and A. L. Selman, A comparison of polynomial time reduciblities, Theor. Comput. Sc. 1 (1975) 103-123.

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

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

15 J. H. Lutz, Almost everywhere high nonuniform complexity, J. Comput. System Sci. 44 (1992) 220-258.

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

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

18 J. H. Lutz and E. Mayordomo, Cook versus Karp-Levin: Separating completeness notions if NP is not small, Theor. Comp. Sci. 164 (1996) 141-163.

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

20 E. Mayordomo, Almost every set in exponential time is P-bi-immune, Theor. Comput. Sci. 136 (1994) 487-506.

21 C. P. Schnorr, Zufälligkeit und Wahrscheinlichkeit, Lect. Notes Mathematics 218, 1971, Springer Verlag.

22 S. Tang and R. Book, Polynomial-time reducibilities and "almost all" oracle sets, Theor. Comput. Sci. 81 (1991) 35-47.