Randomness vs. Completeness: On the Diagonalization Strength of Resource-Bounded Random Sets *

Klaus Ambos-Spies† Steffen Lempp‡ Gunther Mainhardt†

Abstract

We show that the question of whether the p-tt-complete or p-T-complete sets for the deterministic time classes **E** and **EXP** have measure 0 in these classes in the sense of Lutz's resource-bounded measure cannot be decided by relativizable techniques. On the other hand, we obtain the following absolute results if we bound the norm, i.e., the number of oracle queries of the reductions: For $r = tt, T$,

$$\mu_p(\{C : C \text{ } p\text{-}r(kn)\text{-complete for } \mathbf{E}\}) = 0 \text{ and}$$
$$\mu_{p_2}(\{C : C \text{ } p\text{-}r(n^k)\text{-complete for } \mathbf{EXP}\}) = 0.$$

In the second part of the paper we investigate the diagonalization strength of random sets in an abstract way by relating randomness to a new genericity concept. This provides an alternative, quite elegant and powerful approach for obtaining results on resource-bounded measures like the ones in the first part of the paper.

1 Introduction

Lutz's resource-bounded measure provides a framework for the quantitative analysis of complexity classes (see Lutz [13]). The most interesting results of

*Research supported in part by the Human Capital and Mobility Program of the European Community under grant CHRX-CT93-0415 (COLORET). The second author would like to acknowledge partial support by National Science Foundation grant DMS-9504474 and a grant of the British Engineering and Physical Sciences Research Council. The main results of Section 3 were obtained by the first and second author when they visited the University of Leeds in the spring of 1996. In Section 4 some recent work by the first and third author is reported.

†Mathematisches Institut, Universität Heidelberg, e-mail: ambos@math.uni-heidelberg.de and mainhard@math.uni-heidelberg.de

‡Department of Mathematics, University of Wisconsin, Madison, e-mail: lempp@math.wisc.edu

this theory have been obtained for the deterministic exponential time classes $\mathbf{E} = \mathbf{DTIME}(2^{lin})$ and $\mathbf{EXP} = \mathbf{DTIME}(2^{poly})$, which are captured by the p- and p_2-measure, respectively. Here, the question of determining the measure of the complete sets for these classes under the various types of polynomial-time reducibilities became a challenging problem which in part is still unsolved.

Mayordomo [14] has shown that the class of p-m-complete sets for $\mathbf{E}$ (or $\mathbf{EXP}$) has p-measure 0. Ambos-Spies, Neis and Terwijn [5] extended Mayordomo's theorem to bounded truth-table completeness, by showing certain relations between genericity and randomness. The somewhat weaker form of this result for p_2-measure was independently obtained by Buhrman and Mayordomo [8] by looking at resource-bounded Kolmogorov complexity.

For reducibilities with nonconstant norm, however, this question remained open. In fact, Allender and Strauss [1] have shown that, assuming $\mathbf{BPP} = \mathbf{EXP}$, the class of the p-T-hard sets has p-measure 1, whence the class of p-T-complete sets does not have p-measure 0, and their result can be easily extended to p-tt-completeness. Since Heller [12] has constructed an oracle A relative to which $\mathbf{BPP}^A = \mathbf{EXP}^A$, this shows that it is impossible to use relativizable techniques to extend the result of Ambos-Spies et al. from bounded truth-table to truth-table or even Turing reducibility.

The first goal of our paper is to show that the p-measure (and p_2-measure) of the classes of the p-tt-complete and p-T-complete sets for $\mathbf{E}$ and $\mathbf{EXP}$ is in fact oracle dependent. This is shown by complementing the result of Allender and Strauss as follows: Assuming $\mathbf{P} = \mathbf{PSPACE}$ (or at least $\mathbf{PSPACE} \subseteq \mathbf{DTIME}(2^{kn})$ for some k), we show that the p-measure of the class of p-T-complete sets for $\mathbf{EXP}$ is 0. (Recently, this result was independently proved by Buhrman et al. [10] by using a new nonmonotone martingale concept suggested by Regan.)

By analyzing the proof of our theorem, we can extend the absolute smallness results for the classes of complete sets as follows: For arbitrary but fixed k, the class $\{C : C \text{ } p\text{-}T(kn)\text{-complete for } \mathbf{EXP}\}$ has p-measure 0 and $\{C : C \text{ } p\text{-}T(n^k)\text{-complete for } \mathbf{EXP}\}$ has p_2-measure 0, where p-$T(l(n))$ refers to p-T-reductions of norm $l(n)$, i.e., to reductions having the number of oracle queries on an input of length n bounded by $l(n)$ for arbitrary but fixed oracle. (These results were obtained independently by Buhrman and Van Melkebeek [9].) Note that by the theorem of Allender and Strauss, the latter is the best possible result provable by relativizable techniques.

By expressing resource-bounded measure in terms of resource-bounded randomness, the above results can be viewed as consequences of the diagonalizations "built" into random sets. In the second part of the paper we address the question of which types of diagonalizations are subsumed by randomness. Since the most common types of diagonalizations in complexity theory have been formalized by corresponding genericity notions (see [2] for details), this question can be answered by isolating the genericity notions which are implied by randomness.

First results in this direction were obtained by Ambos-Spies et al. in [5], where the compatibility of the genericity concept of [3] with randomness was shown. This genericity concept, however, is too weak for dealing with reducibilities of nonconstant norm. Here, we introduce a new genericity concept compatible with randomness, which captures the diagonalizations of the type required for establishing our smallness results in the first part of the paper. Though this genericity approach is somewhat technical, once the required relations to randomness are established it becomes a quite powerful tool for obtaining results on resource-bounded measure.

Our notation is mainly standard and follows [4]. We let $\Sigma = \{0,1\}$ be the binary alphabet, Σ^* be the set of finite binary strings, and Σ^∞ be the set of infinite binary strings. Sometimes, we identify strings with numbers, and subsets A of Σ^* with their characteristic sequences $A(0)A(1)A(2)\ldots$. The initial segment of A of length n is denoted by $A\restriction n = A(0)\ldots A(n-1)$. We assume the reader to be familiar with the polynomial-time reducibilities m (many-one), btt (bounded truth-table), tt (truth-table) and T (Turing). For $r = tt, T$, $r(l(n))$ will denote that the norm of the reduction is bounded by $l(n)$.

2 Resource-Bounded Measure and Randomness

In this section, we introduce the fragment of Lutz's resource-bounded measure theory required for the following. For more details, we refer to Lutz [13].

Lutz's theory is defined in terms of martingales. A characterization of classical measure by martingales was given by Ville in 1939, while Schnorr [15] was the first to look at computable martingales. He also defined resource-bounded randomness in these terms.

A *martingale* is a function $d : \Sigma^* \to Q_+$, (where Q_+ is the set of nonnegative rationals) which satisfies the so-called *martingale condition* $d(x0) + d(x1) = 2d(x)$ for all strings x. A martingale d *succeeds on a set* X if $\limsup_{n\to\infty} d(X\restriction n) = \infty$, and d *succeeds on a class* $\mathbf{C}$ if d succeeds on all sets $X \in \mathbf{C}$. By Ville, a class $\mathbf{C}$ has (classical) measure 0 iff some martingale succeeds on $\mathbf{C}$.

A $t(n)$-*martingale* is a martingale $d \in \mathbf{DTIME}(t(n))$, and d is called a p-*martingale* [p_2-*martingale*] if d is an n^k-martingale [$2^{(\log n)^k}$-*martingale*] for some $k \geq 1$. A class $\mathbf{C}$ has p-*measure* 0, $\mu_p(\mathbf{C}) = 0$, if some p-martingale succeeds on $\mathbf{C}$. The p_2-*measure* is defined correspondingly. Note that martingales operate on initial segments $X\restriction x$. Since $|X\restriction x|^k \approx 2^{k|x|}$ and $2^{(\log(|X\restriction x|))^k} \approx 2^{|x|^k}$, this implies that p-measure corresponds to $\mathbf{E} = \mathbf{DTIME}(2^{lin})$ while p_2-measure corresponds to $\mathbf{EXP} = \mathbf{DTIME}(2^{poly})$. Lutz has shown that $\mu_p(\mathbf{DTIME}(2^{kn})) = 0$ for all k but $\mu_p(\mathbf{E}) \neq 0$, whence a measure on $\mathbf{E}$ can be defined as follows: A class $\mathbf{C}$ has *measure* 0 *in* $\mathbf{E}$ if $\mu_p(\mathbf{C} \cap \mathbf{E}) = 0$, and $\mathbf{C}$ has *measure* 1 in $\mathbf{E}$ if the complement $\overline{\mathbf{C}}$ of $\mathbf{C}$ has measure 0 in $\mathbf{E}$. Similarly, we obtain a measure on $\mathbf{EXP}$ based on the p_2-measure.

The resource-bounded measure can also be defined in terms of resource-bounded randomness (see, e.g., [4]): A set R is $t(n)$-*random* [p-*random*, p_2-*random*] if no $t(n)$-martingale [p-martingale, p_2-martingale] succeeds on R. For any k, there is an n^k-random set R in $\mathbf{E}$ but there are no such sets in $\mathbf{DTIME}(2^{kn})$. Hence there is no p-random set in $\mathbf{E}$ but such sets exist in $\mathbf{EXP}$. Moreover, a class $\mathbf{C}$ has p-measure 0 iff $\mathbf{C}$ does not contain any n^k-random set for some $k \geq 1$. In a similar way, $2^{(\log n)^k}$-random sets characterize the p_2-measure and the measure on $\mathbf{EXP}$.

3 Randomness vs. Completeness

In this section we show that the measure of the p-Turing and p-truth-table complete sets in $\mathbf{E}$ and $\mathbf{EXP}$ cannot be determined by relativizable techniques. Allender and Strauss [1] have shown that, assuming $\mathbf{BPP} = \mathbf{EXP}$, the p-T-complete sets have measure 1 in $\mathbf{E}$ and $\mathbf{EXP}$, and their result easily extends to the p-tt-complete sets. We complement this result by showing that the p-T-complete sets, and hence the p-tt-complete sets, have measure 0 in $\mathbf{E}$ and $\mathbf{EXP}$ if we assume that $\mathbf{PSPACE} \subseteq \mathbf{P}$. Oracles A and B relative to which $\mathbf{BPP}^A = \mathbf{EXP}^A$ and $\mathbf{PSPACE}^B = \mathbf{P}^B$ have been constructed by Heller [12] and Baker, Gill and Solovay [6], respectively. Our proof also yields the following absolute result: The class of the p-$T(kn)$-complete sets for $\mathbf{E}$ (or $\mathbf{EXP}$) has p-measure 0 and the class of the p-$T(n^k)$-complete sets for $\mathbf{EXP}$ has p_2-measure 0 (for arbitrary but fixed k).

Theorem 3.1 *(Allender and Strauss [1]) Let A be n^2-random. Then A is p-tt-hard for* $\mathbf{BPP}$.

Corollary 3.2 *Assume* $\mathbf{BPP} = \mathbf{EXP}$. *Every n^2-random set is p-tt-hard for* $\mathbf{EXP}$. *Hence, in particular, for $r \in \{tt, T\}$, the class $\{C : C$ p-r-complete for $\mathbf{E}\}$ has measure 1 in $\mathbf{E}$, and the class $\{C : C$ p-r-complete for $\mathbf{EXP}\}$ has measure 1 in $\mathbf{EXP}$.*

Theorem 3.1 extends the result of Bennett and Gill in [7] that the p-T-hard sets for $\mathbf{BPP}$ have classical measure 1. The proof of Allender and Strauss uses results on pseudo-random number generators, and in [1], the result is only claimed for p-T-reducibility. In 1996, the third author obtained an alternative, elementary proof based on the original proof of Bennett and Gill, which also yields the result for p-tt-reducibility. This proof will appear in Mainhardt's Ph.D. thesis.

Corollary 3.2 shows that if $\mathbf{BPP} = \mathbf{EXP}$, i.e., if $\mathbf{BPP}$ is "large", then the p-tt- and p-T-complete sets for $\mathbf{E}$ and $\mathbf{EXP}$ are abundant in the sense of Lutz's measure. We now complement this observation by showing that if $\mathbf{PSPACE}$ (hence $\mathbf{BPP}$) is "small", in particular if $\mathbf{PSPACE} = \mathbf{P}$, then the p-tt- and p-T-complete sets for $\mathbf{E}$ and $\mathbf{EXP}$ are scarce.

Theorem 3.3 *Assume that* **PSPACE** $\subseteq$ **DTIME**(2^{kn}). *There is no* n^{k+2}*-random set which is p-T-complete for* **E** *or* **EXP**. *Hence*

$$\mu_p(\{C : C \text{ p-T-complete for } \mathbf{E} \ (\mathbf{EXP})\}) = 0,$$

whence $\{C : C$ *p-T-complete for* $\mathbf{E}\}$ *and* $\{C : C$ *p-T-complete for* $\mathbf{EXP}\}$ *have measure* 0 *in* **E** *and* **EXP**, *respectively.*

Proof (sketch). Let R be n^{k+2}-random and, for any set X, let

$$L(X) = \{x : \| \{xy : |x| = |y| \ \& \ xy \in X\} \| \text{ even}\}.$$

Then, for $X \in \mathbf{E}$ (**EXP**), we also have $L(X) \in \mathbf{E}$ (**EXP**), whence it suffices to show that $L(R) \not\leq_T^P R$. So, given a p-T-reduction M, we will define an n^{k+2}-martingale d which succeeds on $\mathbf{C} = \{B : L(B) = M^B\}$.

Fix a polynomial time bound p for M where w.l.o.g. $p(n) > 2n$, and let $q(n)$ be a polynomial which bounds the norm of M, i.e., the number of oracle queries in the computation of $M^X(x)$ for any string x of length n and any oracle X. Note that $q(n) \leq p(n)$. Finally, fix an easily recognizable infinite sequence $x_0 < x_1 < x_2 < \ldots$ of strings such that $p(|x_m|) < 2^{|x_m|} < |x_{m+1}|$ for $m \geq 0$. On the interval $[x_m, x_{m+1})$ the martingale d will be defined in such a way that, for any set B,

$$L(B)(x_m) = M^B(x_m) \ \Rightarrow \ d(B\restriction x_{m+1}) \geq \tfrac{3}{2} d(B\restriction x_m) \tag{3.1}$$

will hold. Obviously this will make d succeed on $\mathbf{C}$.

For the definition of d, fix $x = x_m$, $x' = x_{m+1}$ and some initial segment $\sigma = X\restriction x$. Assume that $d(\sigma)$ is given, and let $n = |x|$ and $n' = |x'|$. We will define $d(X\restriction y)$ for all proper extensions $X\restriction y$ of σ with $y < x'$.

Note that, for any set X, $L(X)(x)$ is determined by $X \cap I_x$, where $I_x = \{xy : |y| = |x|\}$. Similarly, $M^X(x)$ only depends on $X\restriction x'$. So, for $\tau = X\restriction x'$, τ determines $L(X)(x)$ and $M^X(x)$ whence we may denote these values by $L(\tau)(x)$ and $M^\tau(x)$, respectively.

We call a proper extension $\tau = X\restriction y$ of σ a *complete* extension if $y = x'$ and a *partial* extension if $y < x'$. A complete extension τ is called *positive* if $L(\tau)(x) = M^\tau(x)$ and *negative* otherwise. For a partial extension σ', let $pos(\sigma')$ be the number of positive extensions of σ'. Note that, for B as in the premise of (3.1), $B\restriction x'$ are positive, and that one half of the complete extensions of σ are positive. So, in order to guarantee (3.1) it suffices to define d on the interval $[x, x')$ in such a way that the capital $d(\sigma)$ is uniformly distributed among the positive extensions (while for the negative extensions $X\restriction x'$, $d(X\restriction x') = 0$). This is achieved by letting

$$\frac{d((X\restriction y)0)}{d((X\restriction y)1)} = \frac{pos((X\restriction y)0)}{pos((X\restriction y)1)}$$

for any partial extension $X\restriction y$.

It remains to show that the martingale d is n^{k+2}-time bounded. For this, it suffices to show that $pos(X\restriction y)$ can be computed in $2^{(k+1)m}$ steps for any partial extension $X\restriction y$ of σ, $m = |y|$. To do so, we distinguish three cases.

Let v be the unique element of I_x such that there are exactly $q(n)$ elements in I_x greater than v, and let w be the greatest element of I_x. Then, for $y < v$, one half of the total extensions are positive. For $y > w$, $L(X\restriction y)$ is already determined by $X\restriction y$. So here we can compute $pos(X\restriction y)$ by looking at the query tree of the computation $M(x)$ and counting the (appropriately weighted) paths giving output $L(X\restriction y)$ which are consistent with $X\restriction y$. Note that this query tree has depth at most $q(n)$ where q is the polynomial norm of the reduction M. So this procedure can be carried out in $poly<(2^{q(n)})$ steps. For $q(n) > kn$, however, this exceeds the time $|X\restriction y|^{kn}$ available to d. This problem is overcome by our assumption that $\mathbf{PSPACE} \subseteq \mathbf{DTIME}(2^{kn})$, since the above search of a tree of polynomial depth requires only polynomial space.

The case of $v \leq y \leq w$ is similar. Here, in addition, we have to cycle through the (at most $2^{q(n)+1}$ many) extensions $X\restriction w$ of $X\restriction y$ in order to determine $L(X\restriction x)$. Then, for each $X\restriction w$, the positive extensions are counted as in the second case. □

By relativizing the proofs of Corollary 3.2 and Theorem 3.3, we obtain

Corollary 3.4 *For $r = tt, T$, the measure of $\{C : C$ p-r-complete for $\mathbf{E}$ $(\mathbf{EXP})\}$ in $\mathbf{E}$ $(\mathbf{EXP})$ is oracle dependent.* □

Corollary 3.4 has been obtained independently by Buhrman et al. [10] by investigating a nonmonotone variant of resource-bounded martingales introduced by Regan.

By analyzing how the complexity of the martingale d defined in the proof of Theorem 3.3 depends on the norm q of the reductions M we consider (without the assumption that $\mathbf{PSPACE} \subseteq \mathbf{DTIME}(2^{kn})$), we obtain the following absolute results, which have been independently obtained by Buhrman and Van Melkebeek [9].

Theorem 3.5 (a) *For any k, there is a number k' such that no $n^{k'}$-random set is p-$T(kn)$-complete for $\mathbf{E}$ or $\mathbf{EXP}$. Hence, for fixed but arbitrary k,*

$$\mu_p(\{C : C \text{ p-}T(kn)\text{-complete for } \mathbf{E}\ (\mathbf{EXP})\}) = 0.$$

(b) *For any k there is a number k' such that no $2^{(\log n)^{k'}}$-random set is p-$T(n^k)$-complete for $\mathbf{EXP}$. Hence, for fixed but arbitrary k,*

$$\mu_{p_2}(\{C : C \text{ p-}T(n^k)\text{-complete for } \mathbf{EXP}\}) = 0. \qquad \square$$

Note that, by Corollary 3.2, the second part of the theorem cannot be improved by relativizable techniques. Also note that, by the first part of Theorem

3.5, no p-random set is p-$T(lin)$-complete for **EXP**. The proof of the second part of the theorem can be easily modified to yield the following resource-bounded random separation for the classes **P** and **PSPACE**, in fact for **P** and $\oplus$**P**.

Theorem 3.6 *For any p_2-random set R, $\mathbf{P}^R \neq \oplus\mathbf{P}^R$, so $\mathbf{P}^R \neq \mathbf{PSPACE}^R$.*

Again by Corollary 3.2, the resource-bound in Theorem 3.6 cannot be improved by relativizable techniques.

4 Genericity Compatible With Randomness

Guided by the results of the preceding section, we now introduce a new resource-bounded genericity concept compatible with measure. This concept will yield simpler proofs of the results above and of related results.

The theorems in Section 3 have been obtained by exploiting the "built-in diagonalizations" in a random set. The construction of an incomplete set is a quite simple exercise in diagonalization. So, once we have isolated the diagonalization arguments subsumed by a randomness concept, properties of the random set which can be forced by this type of diagonalization can be established quite easily. Formalizations of different types of diagonalization techniques have been given in terms of genericity, where a generic set is a set having all properties which can be forced by diagonalizations of this type (see [2] for a survey of genericity concepts introduced in complexity theory). Unfortunately, however, most of the genericity concepts in the literature are too strong for being compatible with randomness.

The first successful attempt to isolate some diagonalizations built into random sets was made by Ambos-Spies, Neis and Terwijn [5] by showing that the genericity concept of Ambos-Spies, Fleischhack and Huwig [3] is compatible with randomness. In particular they showed that every n^{k+1}-random set is AFH-n^k-generic (in the sense of [3]), whence any property shared by all AFH-n^k-generic sets (for any fixed k) has p-measure 1 and measure 1 in **E**. Since no AFH-n^2-generic set is p-btt-complete for **E**, in [5] Ambos-Spies et al. concluded that the class of the p-btt-complete sets for **E** has p-measure 0, hence measure 0 in **E**.

The genericity concept of [3], however, is tailored for diagonalizations over bounded query reductions: As shown in [5], for any unbounded nondecreasing polynomial-time computable function f there are AFH-n^k-generic sets (for $k \geq 1$) which are p-$tt(f(n))$-complete for **E**. So the diagonalization strength of this genericity concept does not suffice to obtain results on reducibilities of unbounded norm as in Theorem 3.5.

Our new genericity concept, which will be sufficiently strong to cope with this situation and which still is subsumed by randomness, refines the concept of [3] by adding a device allowing look-aheads. This additional feature was inspired by

Regan's new concept of a nonmonotone martingale introduced in [10]. The look-aheads give us extra strength similar to nonmonotonicity but – in the context of genericity – our approach is technically simpler. (The difference between the common genericity concepts and our new look-ahead genericity notion parallels the difference between self-reducibility and auto-reducibility. This will be made more explicit in the full version of this paper.)

Definition 4.1 *A* prediction machine M *is an oracle Turing machine where, whenever* $M^X(x)$ *is defined, then* $M^X(x) = (y, i)$ *for some string* $y \geq x$ *and some* $i \in \Sigma$. *Moreover, the computation of* $M^X(x)$ *is subject to the following two constraints:*

(4.1) *If* $M^X(x) = (y, i)$ *then* $M^{X \cup \{y\}}(x) = M^{X - \{y\}}(x)$.

(4.2) *If in the computation of* $M^X(x)$ *the oracle is queried for some string* $z \geq x$ *then* $M^X(x)$ *is defined.*

A prediction function f *is the functional computed by a prediction machine.* f predicts A at x *if* $f^A(x) = (y, A(y))$, *and* f predicts A *if* f *predicts* A *at some* x. f *is* dense along A *if* $f^A(x)$ *is defined for infinitely many* x.

Note that (4.1) is a necessary fairness condition while (4.2) is an optional condition expressing that additional information on X for strings $\geq x$ can be only required if actually a prediction is made at x. In order to get corresponding resource-bounded genericity concepts, we will introduce time bounds (which, in order to make the bounds compatible with those for martingales, will be exponentially blown up) and bounds on the size of the look-ahead.

Definition 4.2 *A* $t(n)$-prediction function f *is a functional computed by a* $t(2^{n+1})$*-time bounded prediction machine* M. *If, moreover,* $M^X(x)$ *queries at most* $l(|x|)$ *strings* $\geq x$ *then the function* f *is an* $l(n)$-l.a. $t(n)$-prediction function. *A set* G *is* l.a. $t(n)$-generic [$l(n)$-l.a. $t(n)$*-generic*] *if every* $t(n)$*-prediction* [$l(n)$*-l.a.* $t(n)$*-prediction*] *function* f *which is dense along* G *predicts* G.

Note that AFH-genericity coincides with 0-l.a. genericity in the above sense. On the other hand, one can easily show that look-ahead genericity is weaker than general genericity in the sense of [2], whence it induces resource-bounded category concepts on $\mathbf{E}$ and $\mathbf{EXP}$. In particular, there are l.a. n^k-generic sets in $\mathbf{E}$ but, for any length bound l, there is no $l(n)$-l.a. n^k-generic set in $\mathbf{DTIME}(2^{kn})$. The following theorem shows the compatibility of the new concept with resource-bounded measure if we appropriately bound the norm of the look-ahead. We omit the proof, which resembles the proof of Theorem 3.5.

Theorem 4.3 *Every* n^{2k+3}*-random set is* (kn)*-l.a.* n^k*-generic. Furthermore, every* $2^{(\log n)^{k+1}}$*-random set is* n^k*-l.a.* $2^{(\log n)^k}$*-generic.*

Now, in order to obtain alternative proofs of the results in Section 3 based on our new genericity concept, it suffices to prove the corresponding results for generic sets. For instance, in order to obtain Theorem 3.5(a) from Theorem 4.3, it suffices to show that no $(2kn)$-l.a. n^2-generic set is complete for $\mathbf{E}$ under p-T-reductions of norm kn. This can be shown by expressing a straightforward diagonalization in terms of prediction functions, which guarantees that, for a $(2kn)$-l.a. n^2-generic set G, $L(G) \not\leq^P_{T(kn)} G$, where $L(G)$ is defined as in the proof of Theorem 3.3.

References

1. E. Allender, M. Strauss. Measure on small complexity classes with applications for BPP. In *Proceedings of the 35th Symposium on Foundations of Computer Science*, 867-818, IEEE Computer Society Press, 1994.
2. K. Ambos-Spies. Resource-bounded genericity. In *Computability, Enumerability, Unsolvability* (S. B. Cooper et al., Eds.), London Mathematical Society Lecture Notes Series 224, 1-59, Cambridge University Press, 1996.
3. K. Ambos-Spies, H. Fleischhack, 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, 1-16, Springer Verlag, 1988.
4. K. Ambos-Spies, E. Mayordomo. Resource-bounded measure and randomness. In *Complexity, Logic and Recursion Theory*, Lecture Notes in Pure and Applied Mathematics 187, 1-47, Dekker, 1997.
5. K. Ambos-Spies, H.-C. Neis, S. A. Terwijn. Genericity and measure for exponential time. Theoretical Computer Science 168 (1996) 3-19.
6. T. Baker, J. Gill, R. Solovay. Relativizations of the $P =? NP$ question. SIAM Journal on Computing 5 (1975) 431-442.
7. C. Bennett, J. Gill. Relative to a random oracle $P^A \neq NP^A \neq co\text{-}NP^A$ with probability 1. SIAM Journal on Computing 10 (1981) 96-113.
8. H. Buhrman, E. Mayordomo. An excursion to the Kolmogorov random strings. In *Proceedings of the 10th IEEE Structure in Complexity Theory Conference*, 197-205, IEEE Computer Society Press, 1995.
9. H. Buhrman, D. v. Melkebeek. Hard Sets are Hard to Find. In *Proceedings of the 13th IEEE Conference on Comput. Complexity*, IEEE Computer Society Press, 1998.
10. H. Buhrman, D. v. Melkebeek, K. W. Regan, D. Sivakumar, M. Strauss. A generalization of resource-bounded measure with an application. In *Proceedings of the Symposium on Theoretical Aspects of Computer Science*, Lecture Notes in Computer Science, Springer Verlag, 1998.
11. S. A. Fenner. Notions of resource-bounded category and genericity. In *Proceedings of the 6th IEEE Structure in Complexity Theory Conference*, 196-212, IEEE Computer Society Press, 1991.
12. H. Heller. On relativized exponential and probabilistic complexity classes. Information and Control 71 (1986) 231-243.

13. J. H. Lutz. The quantitative structure of exponential time. In *Complexity Theory Retrospective II* (L.A. Hemaspaandra, A.L. Selman, eds.), Springer-Verlag, 1997.
14. E. Mayordomo. Almost every set in exponential time is P-bi-immune. Theoretical Computer Science 136 (1994) 487-506.
15. C. P. Schnorr. Zufälligkeit und Wahrscheinlichkeit. Lecture Notes in Mathematics 218, Springer-Verlag, 1971.