JOURNAL OF COMPUTER AND SYSTEM SCIENCES **54**, 393–399 (1997)
ARTICLE NO. SS971484

An Excursion to the Kolmogorov Random Strings

Harry Buhrman*

CWI, PO Box 94079, 1090 GB Amsterdam, The Netherlands

and

Elvira Mayordomo†

Dept. Ingeniería Informática, Univ. de Zaragoza, María de Luna 3, 50015 Zaragoza, Spain

Received September 20, 1995; revised September 24, 1996

We study the sets of resource-bounded Kolmogorov random strings: $R_t = \{x \mid C^{t(n)}(x) \geq |x|\}$ for $t(n) = 2^{n^k}$. We show that the class of sets that Turing reduce to R_t has measure 0 in *EXP* with respect to the resource-bounded measure introduced by Lutz. From this we conclude that R_t is not Turing-complete for *EXP*. This contrasts with the resource-*un*bounded setting. There R is Turing-complete for *co-RE*. We show that the class of sets to which R_t bounded truth-table reduces, has p_2-measure 0 (therefore, measure 0 in *EXP*). This answers an open question of Lutz, giving a natural example of a language that is not weakly complete for *EXP* and that reduces to a measure 0 class in *EXP*. It follows that the sets that are $\leq^p_{btt}$-hard for *EXP* have p_2-measure 0. © 1997 Academic Press

1. INTRODUCTION

One of the main questions in complexity theory is the relation between complexity classes, such as P, NP, and, EXP. It is well known that $P \subseteq NP \subseteq EXP$. The only strict inclusion that is known is the one between P and EXP. It is conjectured however that all of the inclusions are strict.

In the late sixties and early seventies Cook [Coo71] and Levin [Lev73] discovered a number of NP-complete problems. Since then many people studied the complete problems of this and other complexity classes (see for example [GJ79, BH77, Mah82, Ber77]). From the point of view of complexity theory, the usefulness of these complete problems is that in order to separate P from NP one only has to focus on one particular complete problem and prove for this problem that it is not in P. Similar considerations are valid for EXP since this class also exhibits complete problems.

However, Kolmogorov [Lev94] suggested, even before the notions of P, NP, and NP-completeness existed, that lower bound efforts might best be focused on sets that are relatively devoid of simple structure. That is, the NP-complete problems are probably too structured to be good candidates for separating P from NP. One should rather focus on the intermediate less structured sets that somehow are complex enough to prove separations. As a candidate of such a set he proposed to look at the set of what we call nowadays the resource-bounded Kolmogorov random strings.

In this paper we try to follow this type of approach. We study the sets R_t of strings that are Kolmogorov random with respect to time bounds t of the form $t(n) = 2^{n^k}$: $R_t = \{x \mid C^{t(n)}(x) \geq |x|\}$. A variant of this set was studied before by [BO94] with respect to instance complexity. A more restricted version of this set, namely R_p for p a polynomial, was studied by Ko [Ko91].

It is well known that the time unbounded version of this set, i.e., the *co-RE* set of truly Kolmogorov random strings, is Turing-complete for *co-RE* [Mar66]. In this paper however we will show that the resource bounded version is *not* Turing-complete for EXP, supporting Kolmogorov's intuition at least for EXP. We actually show something stronger. We prove that the sets that Turing reduce to R_t have measure 0 in EXP with respect to the resource-bounded measure introduced by Lutz [Lut92]. Hence R_t is not even weakly Turing-complete.

Applying the results of Kautz and Miltersen [KM94] we get that R_t is not Turing-hard for NP relative to a random oracle.

These results show that R_t mirrors almost none of the structure of EXP and NP. Furthermore, by the results of Ambos-Spies *et al.* [ASTZ94] it follows that sets that have the same property, i.e., sets that are not weakly complete, have measure 0 in EXP and hence are rare and atypical.

On the other hand, it is not hard to see that R_t is P-immune, i.e., it has no infinite subset in P, and thus is complex enough to figure as the set Kolmogorov had in mind.

* Part of this research was done while visiting the Univ. Politècnica de Catalunya in Barcelona. E-mail: buhrman@cwi.nl. Partially supported by the Dutch Foundation for Scientific Research (NWO) through NFI Project ALADDIN, under Contract NF 62-376.

† E-mail: elvira@prometeo.cps.unizar.es. Partially supported by the EC through the Esprit BRA Program (Project 7141, ALCOM II) and through the HCM Program (Project CHRX-CT93-0415, COLORET Network).

0022-0000/97 $25.00

571/54/3-2

We also examine the sets that R_t reduces to, i.e., $\{A \mid R_t \leqslant_r^p A\}$, for some reducibility r. We prove that for $\leqslant_{btt}^p$-reductions this class of sets has p_2-measure 0, therefore *also* has measure 0 in *EXP* (in fact, this result is established for any set having infinitely many hard instances, in the sense of instance complexity). As a consequence of these reflections we establish that the class of sets that are $\leqslant_{btt}^p$-hard for *EXP* have p_2-measure 0. (This last result was improved for complete sets by Ambos-Spies *et al.* in [ASNT94].)

We have thus obtained a natural example of a non-weakly complete set for *EXP* that is not in *P*, answering an open question of Lutz (verbal communication). Juedes and Lutz [JL93] note the existence of sets in *E* whose upper and lower $\leqslant_m^p$-spans are both small. We extend this result by showing that R_t is also a set for which both the lower and upper $\leqslant_{btt}^p$-spans have measure 0 in *EXP*, which in the lattice induced by $\leqslant_{btt}^p$-reductions means that R_t lives in a nowhere land, with almost nothing below or above it.

2. PRELIMINARIES

See [BDG88, BDG90] for standard notation and basic definitions on complexity classes and reductions.

Let $s_0, s_1, s_2, \ldots$ be the standard enumeration of the strings in $\{0,1\}^*$ in lexicographical order. Let λ denote the empty string. Given a string $w \in \{0,1\}^*$, let $\mathbf{C}_w$ be the set

$$\mathbf{C}_w = \{x \in \{0,1\}^\infty \mid w \text{ is a prefix of } x\}.$$

Given a sequence x and $n \in \mathbb{N}$, $x[0 \ldots n-1]$ denotes the finite prefix of x that has length n. Given a set X, $\mathscr{P}(X)$ denotes the power set of X. $\mathbf{Q}$ denotes the set of rational numbers.

We will use the *characteristic sequence* χ_L of a language L, defined as follows:

$$\chi_L \in \{0,1\}^\infty \quad \text{and} \quad \chi_L[i] = 1 \quad \text{iff} \quad s_i \quad \text{belongs to } L.$$

By identifying a language with its characteristic sequence we identify the class of languages over $\{0,1\}$ with the set $\{0,1\}^\infty$ of all sequences.

Consider the random experiment in which a language $A \subseteq \{0,1\}^*$ is chosen probabilistically, using an independent toss of a fair coin to decide membership of each string in A. Given a property of languages Π, let $\Pr_A[\Pi(A)]$ denote the probability that property Π holds for A when A is chosen in this fashion.

We will use the following notation for exponential time complexity classes: $E = \mathrm{DTIME}(2^{O(n)})$ and $EXP = \mathrm{DTIME}(2^{n^{O(1)}})$.

We use the function classes $\mathrm{p} = \bigcup_{k \in \mathbb{N}} \mathrm{DTIMEF}(n^k)$ and $\mathrm{p}_2 = \bigcup_{k \in \mathbb{N}} \mathrm{DTIMEF}(2^{\log(n)^k})$.

Next we include the main definitions of measure in *EXP* and *E*. For a complete introduction to resource-bounded measure see [Lut92] and [May94].

Intuitively, the measure in *EXP* is a function $\mu: \mathscr{P}(EXP) \to [0,1]$ with some additivity properties, whose main purpose is to classify by size criteria the subclasses of *EXP*. In this sense, the smallest classes are those X for which $\mu(X) = 0$ and the largest are those having $\mu(X) = 1$.

We only define measure 0 and measure 1 in *EXP* because we are always interested in classes that are closed under finite variations, and from a resource-bounded generalization of the Kolmogorov 0-1 law [May94] these classes can only have measure 0 or measure 1 in *EXP*, if they are measurable at all.

DEFINITION 1. A martingale is a function $d: \{0,1\}^* \to \mathbf{Q}$ satisfying

$$d(w) = \frac{d(w0) + d(w1)}{2}$$

for all $w \in \{0,1\}^*$.

DEFINITION 2. A martingale d is successful for a language $x \in \{0,1\}^\infty$ iff

$$\limsup_{n \to \infty} d(x[0 \ldots n]) = \infty.$$

For each martingale d, we denote the class of all languages for which d is successful as $S[d]$, that is

$$S[d] = \{x \mid \limsup_{n \to \infty} d(x[0 \ldots n]) = \infty\}.$$

DEFINITION 3. A class $X \subseteq \{0,1\}^\infty$ has p_2-measure 0 (denoted by $\mu_{p_2}(X) = 0$) iff there exists a martingale $d \in p_2$ such that, $X \subseteq S[d]$.

A class $X \subseteq \{0,1\}^\infty$ has p_2-measure 1 (denoted by $\mu_{p_2}(X) = 1$) iff X^c has p_2-measure 0.

A class $X \subseteq \{0,1\}^\infty$ has measure 0 in *EXP* iff $X \cap EXP$ has p_2-measure 0. This is denoted by $\mu(X \mid EXP) = 0$.

A class $X \subseteq \{0,1\}^\infty$ has measure 1 in *EXP* iff X^c has measure 0 in *EXP*. This is denoted by $\mu(X \mid EXP) = 1$.

The measure in *EXP* just defined is known to be non-trivial because of the Measure Conservation Theorem [Lut92], stating that *EXP* does not have p_2-measure 0.

Similarly, p-measure and measure in *E* are defined as follows

DEFINITION 4. A class $X \subseteq \{0,1\}^\infty$ has p-measure 0 (denoted by $\mu_p(X) = 0$) iff there exists a martingale $d \in p$ such that, $X \subseteq S[d]$.

A class $X \subseteq \{0,1\}^\infty$ has p-measure 1 (denoted by $\mu_p(X) = 1$) iff X^c has p-measure 0.

A class $X \subseteq \{0, 1\}^\infty$ has measure 0 in E iff $X \cap E$ has p-measure 0. This is denoted by $\mu(X \mid E) = 0$.

A class $X \subseteq \{0, 1\}^\infty$ has measure 1 in E iff X^c has measure 0 in E. This is denoted by $\mu(X \mid E) = 1$.

The following is an immediate consequence of the definitions

PROPOSITION 5. *If X has p-measure 0 then X has p_2-measure 0. If X has p-measure 0 then X has measure 0 in E. If X has p_2-measure 0 then X has measure 0 in EXP.*

Next we state an important property of measure in EXP and E, the σ-additivity property, that will be an important tool in the proof that certain classes have measure 0.

DEFINITION 6. A class X is a p_2-union (p-union) of the p_2-measure 0 (p-measure 0) classes $X_0, X_1, X_2, \ldots$ iff

$$X = \bigcup_{i=0}^{\infty} X_i$$

and there exists a single constant $k \in \mathbb{N}$ such that for every i, there is a martingale d_i with $X_i \subseteq S[d_i]$, such that d_i is computable in time $2^{(\log n)^k}$ (in time n^k).

LEMMA 7 [Lut92]. *If X is a p_2-union (p-union) of p_2-measure 0 (p-measure 0) classes, then X has p_2-measure 0 (p-measure 0).*

Let $\leqslant_r^p$ be a reducibility and A be a set. $P_r(A) = \{B \mid B \leqslant_r^p A\}$. We will call $P_r(A)$ the lower span of A. $P_r^{-1}(A) = \{B \mid A \leqslant_r^p B\}$ is called the upper span of A.

DEFINITION 8. Given a reducibility $\leqslant_r^p$, we say that a language $A \in EXP$ is $\leqslant_r^p$-weakly complete for EXP if $P_r(A)$ does not have measure 0 in EXP.

Weak completeness, studied in [Lut94, ASTZ94, JL94], is a resource-bounded measure generalization of the classical notion of complete language. In [ASTZ94], Ambos-Spies *et al.* prove that the class of many-one weakly complete sets for EXP has measure 1 in EXP, which contrasts with the fact that the class of complete languages for the same class has measure 0. That is, complete languages are rare in EXP while weakly complete languages are typical.

Very recently, an elegant proof of Regan, Sivakumar and Cai [RSC95] showed that if $P_r(A)$ has measure 1 in EXP, then A is $\leqslant_r^p$-complete. Therefore, for A weakly complete but not complete it must be the case that $P_r(A)$ is not measurable in EXP.

We will use resource bounded Kolmogorov complexity. We will only give an intuitive definition here; see [LV93] for precise definitions. For t a time bound:

$$C^{t(n)}(x) = \min\{|M| \mid M(\lambda) = x \text{ in time } t(|x|)\}.$$

We also will use the notion of instance complexity but also only give an intuitive definition; see [LV93, OKSW94] for exact definitions. A Turing machine M is consistent with a set A if for all x, $M(x)$ outputs YES, NO or ? and furthermore, if $M(x)$ outputs YES (NO) then $x \in A (x \notin A)$. The t-bounded instance complexity with respect to a set A and a string x is:

$$IC^{t(n)}(x: A) = \min\{|M| \mid M \text{ is a } t(n)\text{-bounded Turing-machine consistent with } A \text{ and deciding } x\}.$$

We study the sets $R_t = \{x \mid C^{t(n)}(x) \geqslant |x|\}$, for $t(n) = 2^{n^k}$, for some $k \geqslant 2$. Observe that R_t is decidable in time $2^n t(n)$, therefore $R_t \in EXP$. A variant of this this set was studied before in [BO94]. we will use the following version of Theorem 3.2 in [BO94], concerning the instance complexity of the strings in R_t:

THEOREM 9. *There exists $n_1 \in \mathbb{N}$, $c_1 > 0$, such that for every $x \in R_t$, $|x| \geqslant n_1$,*

$$IC^{2^n}(x: R_T) \geqslant |x| - c_1.$$

We also study the set $R_l = \{x \mid C^{l(n)}(x) \geqslant |x|\}$, for $l(n) = 2^{kn}$, $k \geqslant 3$. For this set we also have

THEOREM 10. *There exists $n_2 \in \mathbb{N}$, $c_2 > 0$, such that for every $x \in R_l$, $|x| \geqslant n_2$,*

$$IC^{2^n}(x: R_l) \geqslant |x| - c_2.$$

3. MAIN RESULTS

In this section we prove our main results. Let in the following t be a function of the form $t(n) = 2^{n^k}$ for some $k \geqslant 2$, and let l be $l(n) = 2^{kn}$ for $k \geqslant 3$. The next theorem shows that R_t is not weakly Turing-complete for EXP.

THEOREM 11. *$P_T(R_t)$ has measure 0 in EXP.*

Proof. We start by showing that every $\leqslant_T^p$-reduction to R_t can be done such that, on every input of the form 0^n, every query length is less than n.

Let N be a Turing machine that decides R_t. Let A be such that $A \leqslant_T^p R_t$ via machine M. Fix $n \in \mathbb{N}$ and denote as $\{q_1, q_2, \ldots, q_m\}$ the queries in the computation of $M(R_t, 0^n)$ (in order of appearance). Assume that there is a $q \in \{q_1, q_2, \ldots, q_m\}$ such that $|q| \geqslant n$ and $q \in R_t$. Let q_j be the first such q to appear. We can generate q_j from 0^n, $R_t^{<n}$ (that is, an algorithm for R_t) and j, because we can simulate the computation of $M(R_t, 0^n)$ up to obtaining the jth query by answering to queries of length smaller than n according to R_t and answering NO to queries of length at least n. The time used in this generation of q_j is at most $p(n) \cdot 2^{n-1} \cdot t(n-1)$, for p a polynomial depending on M. Let n_0 be such

that for each $n \geq n_0$, $p(n) \cdot 2^{n-1} \cdot t(n-1) < t(n)$ and $|M| + |N| + \log n + \log(p(n)) < n$. Then for $n \geq n_0$ if there is a query q in the computation of $M(R_t, 0^n)$ with $q \in R_t$ and $|q| \geq n$ then there exists q_j in R_t such that $|q_j| \geq n$ and $C^t(q_j) < n$. This would contradict the definition of R_t, so no such q can exist.

Thus for each $n \geq n_0$, if there is a query q for $M(R_t, 0^n)$ such that $|q| \geq n$, we can assume that $q \notin R_t$. Thus there is a polynomial time machine M' such that $A = L(M', R_t)$ and for every $n \in \mathbb{N}$, all queries in the computation of $M'(R_t, 0^n)$ have length less than n.

Next we define the classes

$$X_i = \{ A \mid A \leq_T^p R_t \text{ via } M_i \text{ and for all } n \text{, all queries on } 0^n \text{ have length less than } n \},$$

where $\{M_i \mid i \in \mathbb{N}\}$ is a presentation of all polynomial time oracle Turing machines, and $\{q_i \mid i \in \mathbb{N}\}$ are the corresponding polynomial time bounds. By the property of $\leq_T^p$-reductions to R_t that we just proved, we know that $P_T(R_t) \subseteq \bigcup_i X_i$. This allows us to show that $P_T(R_t)$ has measure 0 in EXP by using the p_2-union lemma.

For each $i \in \mathbb{N}$ we define d_i a martingale witnessing that X_i has p_2-measure 0. For each $i \in \mathbb{N}$, let n_i be such that $q_i(n) < 2^n$ for each $n \geq n_i$. Let $i \in \mathbb{N}$, $w \in \Sigma^*$, $b \in \{0, 1\}$.

$$\begin{array}{lll} d_i(w) = 1 & \text{if} & |s_{|w|}| < n_i \\ d_i(wb) = d_i(w) & \text{if} & s_{|w|} \notin \{0\}^*. \\ d_i(wb) = 2 \cdot d_i(w) & \text{if} & s_{|w|} \in \{0\}^*, |s_{|w|}| \geq n_i, \\ & \text{and} & M_i(R^{<|s_{|w|}|}, s_{|w|}) = b. \\ d_i(wb) = 0 & \text{if} & s_{|w|} \in \{0\}^*, |s_{|w|}| \geq n_i, \\ & \text{and} & M_i(R^{<|s_{|w|}|}, s_{|w|}) \neq b. \end{array}$$

By definition d_i is a martingale. To compute $d_i(w)$ we need to compute $R_t^{<\log(|w|)}$ and simulate M_i on inputs of the form 0^n, for $n \leq \log(|w|)$. Thus d_i can be computed in time $t(\log(|w|)) \cdot |w|^2$, and this bound does not depend on i.

Next we show that for each $i \in \mathbb{N}$, $X_i \subseteq S[d_i]$. Fix $i \in \mathbb{N}$ and $A \in X_i$. By the definition of X_i it is clear that for each $n \in \mathbb{N}$, $M_i(R_t^{<n}, 0^n) = A(0^n)$, i.e., $A[2^n - 1] = A(s_{2^n - 1}) = M_i(R_t^{<|s_{2^n-1}|}, s_{2^n - 1})$. Thus by the definition of d_i, for each $n > n_i d_i(A[0...2^n - 1]) = 2 \cdot d_i(A[0...2^n - 2])$ and if m is not of the form $2^n - 1$ then $d_i(A[0...m]) = d_i(A[0...m-1])$. Thus $\lim_m d_i(A[0...m] = \infty$ and $A \in S[d_i]$.

The proof is finished by applying the p_2-union lemma (Lemma 7). ∎

With the same proof technique we can show the next theorem for R_t. This time the Kolmogorov complexity argument implying that reductions to R_t are length increasing can be done without computing membership in R_t at all, because queries are nonadaptive and there are only a polynomial number of them.

THEOREM 12. *$P_{tt}(R_t)$ has pleasure 0, hence measure 0 in E.*

As a corollary of the proof of Theorem 11 we have that the theorem holds for any infinite subset of R_t.

COROLLARY 13. *Let $A \in EXP$ be an infinite subset of R_t. Then*

$$\mu(P_T(A) \mid EXP) = 0.$$

Let $A \in E$ be an infinite subset of R_t. Then

$$\mu_p(P_{tt}(A)) = \mu(P_{tt}(A) \mid EXP) = 0.$$

As an immediate consequence of Theorems 11 and 12 we have the following:

COROLLARY 14. *R_t is not Turing-complete for EXP and R_t is not truth-table-complete for EXP.*

Also Theorem 11 shows that R_t is not weakly Turing-complete for *EXP*, and Theorem 12 shows that R_t is not weakly truth-table-complete for *EXP* or *E*. Note that weak completeness for *EXP* does not necessarily imply weak completeness for *E* [JL94].

Corollary 14 contrasts with the situation in the recursion-theoretic setting. Let $R = \{x \mid C(x) \geq |x|\}$. It is not hard to see that $\bar{R}$ is effectively simple (see [Odi89] for a definition). Moreover in [Mar66] it is shown that every effectively simple set is Turing-complete for *RE* from which it follows that R is Turing-complete for *co-RE*. Kummer [Ku96] has recently shown that R is truth-table-complete for *co-RE*.

Moreover R_t is a *natural* example of a Turing-incomplete set in $EXP - P$. R_t is not in P since it is P-immune, this can be proven with basically the same argument that shows that $\bar{R}$ is effectively simple.

Lutz has proposed to study the reasonableness and consequences of the hypothesis '*NP* does not have measure 0 in *EXP*' (see [LuMa94]). We have the following corollary

COROLLARY 15. *If NP does not have measure 0 in EXP, then R_t is not Turing-hard for NP.*

Applying the results of Kautz and Miltersen [KM94] we get the following:

COROLLARY 16. *Relative to a random oracle, R_t is not Turing-hard for NP.*

Note that R_t relative to an oracle can be defined using a relativization of resource bounded Kolmogorov complexity.

It would be interesting to connect our results with those obtained in [Ko91] for the set R_p, with p a polynomial. In this case R_p is in *co-NP*. Ko [Ko91] shows that there exists an oracle relative to which R_p is incomplete for *co-NP* and not in P.

Another application comes from the results in [ASTZ94]. They show that the majority of *EXP*, i.e. a subclass of sets with measure 1, is weakly complete. It follows thus that R_t is atypical in *EXP*.

Next we will turn our attention to the upper span of R_t—the class of sets that R_t reduces to. We start by proving a general result about the $\leqslant^p_{k-tt}$-upper span of any set having infinitely many hard instances, in the following sense.

DEFINITION 17. Let $f: \mathbb{N} \to \mathbb{N}$. A set C has infinitely many $f(n)$-hard instances if there exist infinitely many $x \in \{0, 1\}^*$ such that,

$$IC^{f(n)}(x: C) \geqslant |x|.$$

THEOREM 18. *Let $k \in \mathbb{N}$, let C be a set in E that has infinitely many $n^{\log n}$-hard instances. Then $P^{-1}_{k-\mathrm{tt}}(C)$ has p-measure* 0.

Proof. We start by showing that every $\leqslant^p_{k-tt}$-reduction from C, there are infinitely many $x \in \{0, 1\}^*$ on which there are useful queries of length greater than $|x|/(5k)$. We say that a query is useful if the answer to that query is necessary to compute the answer to the oracle computation, even if the answers to smaller queries are known.

Let A be such that $C \leqslant^p_{k-tt} A$ via machine M. Fix $x \in \{0, 1\}^*$ and denote as $\{q_1, q_2, ..., q_k\}$ the set of queries in the computation of $M(A, x)$, in lexicographical order. Let $Q_M(A, x) = \{q_1, q_2, ..., q_j\}$, for $j \leqslant k$, be such that the answers to the queries $\{q_1, q_2, ..., q_j\}$ determine $M(A, x)$, but the answers to the queries $\{q_1, q_2, ..., q_{j-1}\}$ don't.

Assume that $Q_M(A, x) \subseteq \{0, 1\}^{\leqslant |x|/5k}$. We are going to construct a short program that is consistent with C and decides membership of x.

The program consists basically of a codification of both $Q_M(A, x)$ and $Q_M(A, x) \cap A$, therefore the program size is at most $4k^{|x|/5k}$. On an input y, the program simulates the computation of $M(A, y)$ by answering only to queries that belong to $Q_M(A, x)$ according to $Q_M(A, x) \cap A$. If queries out of $Q_M(A, x)$ are needed, the program halts with undefined output, otherwise it outputs the result of the simulation. The time used by this program on input x is at most $p(|x|)$, for p a polynomial depending on M. Let n_0 be such that for each $n \geqslant n_0$, $p(n) < n^{\log n}$. Then for each $x \in L$, with $|x| \geqslant n_0$, if $Q_M(A, x) \subseteq \{0, 1\}^{\leqslant |x|/5k}$ then $IC^{n \log n}(x: C) \leqslant 4k\, |x|/5k < |x|$.

Since C has infinitely many $n^{\log n}$-hard instances, this implies that there exist infinitely many $x \in \{0, 1\}^*$ such that $Q_M(A, x) \not\subseteq \{0, 1\}^{\leqslant |x|/5k}$.

Next we define the classes

$$X_i = \{A \mid C \leqslant^p_{k-tt} A \text{ via } M_i\},$$

where $\{M_i \mid i \in \mathbb{N}\}$ is a presentation of all k-tt-polynomial-time oracle Turing machines, and $\{q_i \mid i \in \mathbb{N}\}$ are the corresponding polynomial time bounds. It is clear that $P^{-1}_{k-\mathrm{tt}}(C) \subseteq \bigcup_i X_i$. This allows us to show that $P^{-1}_{k-\mathrm{tt}}(C)$ has p-measure 0 by using the p-union lemma.

For each $i \in \mathbb{N}$, let n_i be such that $q_i(n) < 2^n$ for each $n \geqslant n_i$. For each $w \in \{0, 1\}^*$ and $i \in \mathbb{N}$, let $x(w, i)$ be the minimum $x \in \{0, 1\}^*$ such that $|x| \geqslant n_i$ and for every $B \in \mathbf{C}_w$, $Q_{M_i}(B, x) \not\subseteq \{s_0, ..., s_{|x|-1}\}$. That is, $x(w, i)$ is the minimum input for which queries out of the prefix w of the oracle are needed.

For each $i \in \mathbb{N}$ we define d_i a martingale witnessing that X_i has p-measure 0. Let $i \in \mathbb{N}$, let $w \in \{0, 1\}^*$, $b \in \{0, 1\}$.

$d_i(\lambda) = 1$.

If $|x(w, i)| \geqslant 5k \lfloor \log(|w|) \rfloor$ then $d_i(wb) = d_i(w)$.

If $|x(w, i)| < 5k \lfloor \log(|w|) \rfloor$ then $d_i(wb) = d_i(w)$.

$$\cdot 2 \cdot \frac{\Pr_B[(M_i(B, x(w, i)) = C(x(w, i))) \wedge (\mathbf{C}_{wb} \sqsubseteq B)]}{\Pr_B[(M_i(B, x(w, i)) = C(x(w, i))) \wedge (\mathbf{C}_w \sqsubseteq B)]}.$$

By definition d_i is a martingale. To compute $d_i(w)$ we need to find $x(w, i)$, simulating M_i on at most all strings in $C^{<5k \lfloor \log(|w|) \rfloor}$, thus d_i can be computed in time $2^{c5k \lfloor \log(|w|) \rfloor} \cdot |w|^2$, for $c > 0$ a constant such that $C \in \mathrm{DTIME}(2^{cn})$, and this bound does not depend on i.

Let us show that for each $i \in \mathbb{N}$, $X_i \subseteq \mathrm{S}[d_i]$. Fix $i \in \mathbb{N}$ and $A \in X_i$. By definition of X_i, there exist infinitely many $m \in \mathbb{N}$ such that $|x(A[0...m], i)| < 5k \lfloor \log(|A[0...m]|) \rfloor$.

We define $\{a_n \mid n \in \mathbb{N}\}$, an increasing sequence of natural numbers, as follows:

$$a_1 = \min\{m \mid |x(A[0...m], i)| < 5k \lfloor \log(|A[0...m]|) \rfloor\}$$

$$a_{n+1} = \min\{m \mid m > a_n,\ x(A[0...m], i) \neq x(A[0...a_n], i) \text{ and } |x(A[0...m], i)| < 5k \lfloor \log(|A[0...m]|) \rfloor\},$$

for each $n \in \mathbb{N}$.

We show that for each $n \in \mathbb{N}$,

$$d_i(A[0...a_{n+1} - 1]) \geqslant \frac{2^k}{2^k - 1} d_i(A[0...a_n - 1]).$$

Let $n \in \mathbb{N}$. We define the string

$$x = x(A[0...a_n], i) = x(A[0...a_{n+1} - 1], i).$$

Notice that for each $n \in \mathbb{N}$,

$$Q_{M_i}(x, A) \subseteq \{s_0, ..., s_{a_{n+1}-1}\}.$$

Notice also that, by definition of x, $Q_{M_i}(x, A) \not\subseteq \{s_0, ..., s_{a_n} - 1\}$, and therefore

$$\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...a_n - 1]} \sqsubseteq B)] < 1.$$

By definition of d_i,

$$d_i(A[0...a_{n+1} - 1]) = d_i(A[0...a_n - 1]) \cdot 2^{a_{n+1} - a_n}.$$

$$\prod_{j=a_n}^{j=a_{n+1}-1} \frac{\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...j]} \sqsubseteq B)]}{\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...j-1]} \sqsubseteq B)]}$$

$$= d_i(A[0...a_n - 1]) \cdot 2^{a_{n+1} - a_n}.$$

$$\cdot \frac{\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...a_{n+1} - 1]} \sqsubseteq B)]}{\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...a_n - 1]} \sqsubseteq B)]}$$

Since $A \in X_i$ and $Q_{M_i}(x, A) \subseteq \{s_0, ..., s_{a_{n+1} - 1}\}$,

$$\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...a_{n+1} - 1]} \sqsubseteq B)] = 2^{-a_{n+1}}.$$

Thus

$$d_i(A[0...a_{n+1} - 1]) = d_i(A[0...a_n - 1]) \cdot \frac{2^{-a_n}}{\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...a_n - 1]} \sqsubseteq B)]}$$

Also since

$$\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...a_n - 1]} \sqsubseteq B)]$$

is smaller than one, and $M_i(B, x)$ depends only on a maximum of k bits of B, the values of

$$\Pr_B[(M_i(B, x) = C(x)) \wedge (\mathbf{C}_{A[0...a_n - 1]} \sqsubseteq B)]$$

can only be of the form $m \cdot 2^{-k} \cdot 2^{-a_n}$, for $m \in \{0, ..., 2^k - 1\}$. Thus

$$d_i(A[0...a_{n+1} - 1]) \geqslant \frac{2^k}{2^k - 1} \cdot d_i(A[0...a_n - 1])$$

and $\lim_m d_i(A[0...m]) = \infty$.

The proof is finished by applying the p-union lemma (Lemma 7). ∎

The following theorem is basically an application of the p_2-union lemma to the previous result.

THEOREM 19. *Let C be a set in EXP that has infinitely many $n^{\log n}$-hard instances. Then $P_{\text{btt}}^{-1}(C)$ has p_2-measure 0, therefore measure 0 in EXP.*

For R_t and R_l we have the next corollary

COROLLARY 20. *$P_{\text{btt}}^{-1}(R_t)$ has p_2-measure 0. For each $k \in \mathbb{N}$, $P_{k-\text{tt}}^{-1}(R_l)$ has p-measure 0.*

Proof. Use Theorems 9, 10, 18, and 19. ∎

This leaves us with a somewhat strange situation. The sets below R_t with respect to Turing reductions and the sets above R_t with respect to $\leqslant_{btt}^p$-reductions are few and far between.

The small span theorem of Juedes and Lutz [JL93] says that at least one of the lower and upper spans must have measure 0; formally, for every $A \in EXP$, either $P_{\text{m}}(A)$ has measure 0 in EXP, or $P_{\text{m}}^{-1}(A)$ has p_2-measure 0. In fact what they prove is that for every $A \in EXP$, if $P_{\text{m}}(A)$ does not have measure 0 in EXP, then $P_{\text{m}}^{-1}(A)$ has p_2-measure 0. These results were later proved for $\leqslant_{btt}^p$-reductions in [ASNT94], that is,

THEOREM 21 [ASNT94]. *Let $A \in EXP$. If $P_{\text{btt}}(A)$ does not have measure 0 in EXP, then $P_{\text{btt}}^{-1}(A)$ has p_2-measure 0.*

Our results show that the converse of Theorem 21 is false, since $P_{\text{btt}}^{-1}(R_t)$ has p_2-measure 0 and $P_{\text{btt}}(R_t)$ has measure 0 in EXP. (Juedes and Lutz proved in [JL93] that the converse of the many-one version of Theorem 21 is also false.) In fact we have seen that even a much weaker converse of Theorem 21 is false, since the following holds

COROLLARY 22. *There exists $A \in EXP$ such that both $\mu_{p_2}(P_{\text{btt}}^{-1}(A)) = 0$ and $\mu_{p_2}(P_{\text{T}}(A)) = 0$.*

For the case of measure in E, we have a similar consequence. From [ASNT94] we know that:

THEOREM 23 [ASNT94]. *Let $A \in E, k \in \mathbb{N}$. If $P_{k-\text{tt}}(A)$ does not have measure 0 in E, then $P_{k-\text{tt}}^{-1}(A)$ has p-measure 0.*

We have shown that the converse of Theorem 23 is false,

COROLLARY 24. *There exists $A \in E$ such that both $\mu_p(P_{k-\text{tt}}^{-1}(A)) = 0$ and $\mu(P_{\text{tt}}(A) \mid E) = 0$.*

Another corollary is:

COROLLARY 25. *The class of sets that are $\leqslant_{btt}^p$-hard for EXP has p_2-measure 0.*

This corollary has been improved recently by Ambos-Spies *et al.* for the class of complete sets in [ASNT94], where they show that the class of sets that are $\leqslant_{btt}^p$-complete for E has measure 0 in E.

Results similar to those in this section can be proven for the case of space bounds instead of time bounds, by defining the set $RS_s = \{x \mid CS^{s(n)}(x) \geqslant |x|\}$.

THEOREM 26. *There exists $A \in ESPACE$ such that both $\mu_{pspace}(P_{k-\text{tt}}^{-1}(A)) = 0$ and $\mu_{pspace}(P_{\text{T}}(A)) = 0$. There exists*

$A \in EXPSPACE$ *such that both* $\mu_{p_2space}(P^{-1}_{btt}(A)) = 0$ *and* $\mu_{p_2space}(P_T(A)) = 0$.

Here pspace and $p_2$space-measure are defined similarly to p and p_2-measure (see [Lut92]). Notice that there is a slight improvement with respect to the time bound case, here the Turing-lower span has pspace-measure 0.

As a last remark, the whole paper could have been written considering $R^{\varepsilon}_{t} = \{x \mid C^{t(n)}(x) \geqslant |x|^{\varepsilon}\}$, for $\varepsilon < 1$ a fixed positive constant.

4. CONCLUSIONS AND QUESTIONS

We studied the lower span of R_t with respect to Turing reductions. We showed that this lower span has measure 0 in *EXP*. As a consequence we obtained that relative to a random oracle R_t is not Turing-hard for *NP*. It would be interesting to connect these results to the set studied in [Ko91] and show that similar results are true with respect to the set studied there. We also studied the upper span of R_t and showed that with respect to $\leqslant^{p}_{btt}$-reductions this upper span also has measure 0 in *EXP*. In fact, our proof shows that this upper span has p_2-measure 0. If we could push these results up to polynomial-time truth-table reductions it would result in proving that $BPP \neq EXP$, since it is known ([TB91], [AS]) that for every $A \in BPP$, $P^{-1}_{tt}(A)$ has Lebesgue measure 1, and therefore this upper span can't have p_2-measure 0.

ACKNOWLEDGMENTS

Both authors thank Jack Lutz for helpful remarks on the first version of this paper and Eric Allender and an anonymous referee for pointing out a mistake in the proof of the main theorems.

REFERENCES

[AS] K. Ambos-Spies, unpublished.

[ASNT94] K. Ambos-Spies, H-C. Neis, and S. A. Terwijn, Genericity and measure for exponential time, *in* "Proc. 19th International Symposium on Mathematical Foundations of Computer Science, 1994," Lecture Notes in Computer Science, Vol. 841, pp. 221–232, Springer-Verlag, New York/Berlin, 1994; also *Theoret. Comput. Sci.*, to appear.

[ASTZ94] K. Ambos-Spies, S. A. Terwijn, and X. Zheng, Resource bounded randomness and weakly complete problems, *in* "Proc. 5th International Symposium on Algorithms and Computation, 1994," Lecture Notes in Computer Science, Vol. 834, pp. 369–377, Springer-Verlag, New York/Berlin, 1994; also *Theoret. Comput. Sci.*, to appear.

[BDG88] J. Balcázar, J. Díaz, and J. Gabarró, "Structural Complexity, I," Springer-Verlag, New York/Berlin, 1988.

[BDG90] J. Balcázar, J. Díaz, and J. Gabarró, "Structural Complexity, II," Springer-Verlag, New York/Berlin, 1990.

[Ber77] L. Berman, "Polynomial Reducibilities and Complete Sets," Ph.D. thesis. Cornell University, 1977.

[BH77] L. Berman and H. Hartmanis, On isomorphisms and density of NP and other complete sets, *SIAM J. Computing* **6** (1977), 305–322.

[BO94] H. Buhrman and P. Orponen, Random strings make hard instances, *in* "Proc. Structure in Complexity Theory, 9th Annual Conference, 1994," pp. 217–222, IEEE Computer Society Press, New York; also *J. Comput. and System Sci.*, to appear.

[Coo71] S. Cook, The complexity of theorem-proving procedures, *in* "Proc. 3rd ACM Symposium Theory of Computing, 1971," pp. 151–158.

[GJ79] M. Garey and D. Johnson, "Computers and Intractability: A Guide to the Theory of NP-Completeness," Freeman, San Francisco, 1979.

[JL93] D. W. Juedes and J. H. Lutz, The complexity and distribution of hard problems, *SIAM J. Computing* **24** (1995), 279–295.

[JL94] D. W. Juedes and J. H. Lutz, Weak completeness in E and E_2, *Theoret. Comput. Sci.* **143** (1995), 149–158.

[KM94] S. M. Kautz and P. B. Miltersen, Relative to a random oracle NP is not small, *in* "Proc. Structure in Complexity Theory 9th Annual Conference, 1994," pp. 162–174, IEEE Computer Society Press, New York, 1994.

[Ko91] K. Ko, On the complexity of learning minimum time-bounded Turing machines, *SIAM J. Computing* **20** (1991), 962–986.

[Ku96] M. Kummer, On the complexity of random strings, *in* "Proc. 13th Symposium on Theoretical Aspects of Computer Science, 1996," Lecture Notes in Computing Science, Vol. 1046, pp. 25–36, Springer-Verlag, New York/Berlin, 1996.

[Lev73] L. Levin, Universal sorting problems, *Probl. Peredaci Inform.* **9** (1973), 115–116 [in Russian].

[Lev94] L. Levin, personal communication, 1994.

[LV93] M. Li and P. M. B. Vitányi, "An Introduction to Kolmogorov Complexity and Its Applications," Springer-Verlag, New York/Berlin, 1993.

[Lut92] J. H. Lutz, Almost everywhere high nonuniform complexity *J. Comput. System Sci.* **44** (1992), 220–258.

[Lut94] J. H. Lutz, Weakly hard problems, *SIAM J. Comput.* **24** (1995), 1170–1189.

[LuMa94] J. H. Lutz and E. Mayordomo, Cook versus Karp–Levin: Separating reducibilities if NP is not small, *Theoret. Comput. Sci.* **164** (1996), 141–163.

[Mah82] S. Mahaney, Sparse complete sets for NP: solution of a conjecture of Berman and Hartmanis, *J. Comput. System Sci.* **25** (1982), 130–143.

[Mar66] D. A. Martin, Completeness, the recursion theorem and effectively simple sets, *Proc. Am. Math. Soc.* **17** (1966), 838–842.

[May94] E. Mayordomo, "Contributions to the Study of Resource-Bounded Measure," Ph.D. thesis. Universitat Politècnica de Catalunya, 1994.

[Odi89] P. Odifreddi, "Classical Recursion Theory," Studies in Logic and the Foundations of Mathematics, Vol. 125, North-Holland, Amsterdam, 1989.

[OKSW94] P. Orponen, K.-I Ko, U. Schöning, and O. Watanabe, Instance complexity, *J. Assoc. Comput. Mach.* **41**, No. 1 (1994), 96–121.

[RSC95] K. Regan, D. Sivakumar, and J.-Y. Cai, Pseudorandom generators, measure theory, and natural proofs, *in* "Proc. 36th Symposium on Foundations of Computer Science, 1995," pp. 26–35.

[TB91] S. Tang and R. V. Book, Polynomial-time reducibilities and "Almost-all" oracle sets, *Theoret. Comput. Sci.* **81** (1991), 36–47.