An Excursion To The Kolmogorov Random Strings

Harry Buhrman *   Elvira Mayordomo †

September 6, 1995

Abstract

We study the set of resource bounded Kolmogorov random strings: $R_t = \{x \mid K^t(x) \geq |x|\}$ for t a time constructible function such that $t(n) \geq 2^{n^2}$ and $t(n) \in 2^{n^{O(1)}}$. 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 [Lut92]. From this we conclude that R_t is not Turing -complete for EXP. This contrasts 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.

1 Introduction

One of the main questions in complexity theory is the relation between complexity classes, such as for example 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, early seventies Cook [Coo71] and Levin [Lev73] discovered a number of NP -complete problems. 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. Since then many people studied the complete problems of these and other complexity classes (among many others see for example [GJ79, BH77, Mah82, Ber77]).

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

*CWI. PO Box 94079, 1090 GB Amsterdam, The Netherlands. Part of this research was done while visiting the Univ. Politècnica de Catalunya in Barcelona. E-mail: buhrman@cwi.nl. Partially suported by the Dutch foundation for scientific research (NWO) through NFI Project ALADDIN, under contract number NF 62-376

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

on the intermediate less structured sets, that somehow were complex enough to prove separations. As a candidate of such a set he proposed to look at the set of, what we call nowadays, resource bounded Kolmogorov Random strings.

In this paper we try to follow this type of approach. We study the set of strings R_t that are Kolmogorov random with respect to time bounds t such that $t(n) \geq 2^{n^2}$ and $t(n) \in 2^{n^{O(1)}}$: $R_t = \{x \mid K^t(x) \geq |x|\}$. 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, ie 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, ie sets that are not weakly-complete, have measure 0 in EXP and hence are rare and a-typical.

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

We also examine the sets that R_t reduces to, i.e. $\{A \mid R_t \leq^p A\}$. We prove that for $\leq^p_{btt}$ -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 Instant Complexity sense). As a consequence of these reflections we establish that the class of sets that are $\leq^p_{btt}$ -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 $\leq^p_m$-spans are both small. We extend this result by showing that R_t is also a set for which both the lower and upper $\leq^p_{btt}$-spans have measure 0 in EXP, which in the lattice induced by $\leq^p_{btt}$-reductions means that R_t lives in a nowhere land, with almost nothing below and above it.

2 Preliminaries

We will use what is now standard notation, see [BDG88, BDG90]. Let $s_0, s_1, s_2, \ldots$ be the standard enumeration of the strings in $\{0,1\}^*$ in lexicographical order.

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

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

We identify through characteristic sequences the class of all languages over $\{0,1\}$ with the set $\{0,1\}^\infty$ of all sequences.

E is the class defined by linear exponential time.

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

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 $\mu: \mathcal{P}(EXP) \rightarrow [0,1]$ 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 [Lut92] 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 $d: \{0,1\}^* \rightarrow \mathbf{Q}$ 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 set of all languages for which d is successful as $\mathrm{S}[d]$, that is

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

Definition 3 *A class $X \subseteq \{0,1\}^\infty$ has p_2-measure 0 (and we denote it $\mu_{\mathrm{p}_2}(X) = 0$) iff there exists a martingale $d \in \mathrm{p}_2$ such that, $X \subseteq S[d]$.*

Definition 4 *A set $X \subseteq \{0,1\}^\infty$ has p_2-measure 1 (and we denote it $\mu_{\mathrm{p}_2}(X) = 1$) iff X^c has p_2-measure 0.*

Definition 5 *A set $X \subseteq \{0,1\}^\infty$ has measure 0 in EXP iff $X \cap EXP$ has p_2-measure 0. This is denoted as $\mu(X \mid EXP) = 0$.*

Definition 6 *A set $X \subseteq \{0,1\}^\infty$ has measure 1 in EXP iff X^c has measure 0 in EXP. This is denoted as $\mu(X \mid EXP) = 1$.*

The measure in *EXP* just defined is known to be nontrivial 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 7 *A class $X \subseteq \{0,1\}^\infty$ has p-measure 0 (and we denote it $\mu_{\mathrm{p}}(X) = 0$) iff there exists a martingale $d \in p$ such that, $X \subseteq S[d]$.*
A set $X \subseteq \{0,1\}^\infty$ has p-measure 1 (and we denote it $\mu_{\mathrm{p}}(X) = 1$) iff X^c has p-measure 0.

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

The following is an immediate consequence of the definitions

Proposition 8 *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 9 *A set X is a p_2-union (p-union) of the p_2-measure 0 (p-measure 0) sets $X_0, X_1, X_2, \ldots$ iff*

$$X = \bigcup_{j=0}^{\infty} X_j$$

and there exists a function $d \in p_2$ ($d \in p$), $d\colon \mathbb{N} \times \{0,1\}^* \to \mathbf{Q}$ such that for every j, d_j is a martingale and $X_j \subseteq S[d_j]$.

Lemma 10 *[Lut92] If X is a p_2-union (p-union) of p_2-measure 0 (p-measure 0) sets, then X has p_2-measure 0 (p-measure 0).*

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

Definition 11 *Given a reducibility $\leq_r^p$, we say that a language $A \in EXP$ is $\leq_r^p$ -weakly complete for EXP if and only if $P_{\mathrm{r}}(A)$ does not have measure 0 in EXP.*

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

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

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

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:

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

We study the set $R_t = \{x \mid K^t(x) \geq |x|\}$, for $t(n) \geq 2^{n^2}$ and $t(n) \in 2^{n^{O(1)}}$. 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 12 *There exists $n_1 \in \mathbb{N}$ such that for every $x \in R_t$, $|x| \geq n_1$,*

$$IC^{2^n}(x : R_t) \geq |x|.$$

We also study the set $R_l = \{x \mid K^l(x) \geq |x|\}$, for $l(n) \geq 2^{3n}$ and $l(n) \in 2^{O(1)n}$. For this set we also have

Theorem 13 *There exists $n_2 \in \mathbb{N}$ such that for every $x \in R_l$, $|x| \geq n_2$,*

$$IC^{2^n}(x : R_l) \geq |x|.$$

3 Main results

In this section we prove our main results. Let in the following t be a time constructible function such that for almost every $n \in \mathbb{N}, t(n) \geq 2^{n^2}$ and $t(n) \in 2^{n^{O(1)}}$, and let l be a time constructible function such that for almost every $n \in \mathbb{N}, l(n) \geq 2^{3n}$ and $l(n) \in 2^{O(1)n}$. The next theorem shows that R_t is not weakly Turing-complete for EXP.

Theorem 14 *$P_{\mathrm{T}}(R_t)$ has measure 0 in EXP.*

Proof: We start by seeing that every $\leq_T^p$-reduction to R_t can be done with only not length increasing queries on inputs of the form 0^n.

Let N be a Turing Machine that recognizes R_t. Let A be such that $A \leq_T^p R_t$ 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 $|q| \geq n$ and $q \in R_t$. Fix q_j the first-to-appear such q. 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 al least n. The time used in this generation of q_j is at most $p(n) \cdot t(n-1)$, for p a polynomial depending on M. Let n_0 be such that for each $n \geq n_0$, $p(n) \cdot t(n-1) < t(n)$, $|n| + |M| + |N| + |p(n)| < n$. 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 $K^t(q_j) < n$. This would contradict the definition of R_t, thus 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 $q \notin R_t$, and 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 smaller than n.

Next we define the classes

$X_i = \{A \mid A \leq_T^p R_t$ via M_i and $\forall n$, all queries
to 0^n have length smaller than $n\}$,

where $\{M_i \mid i \in I\!N\}$ is a presentation of all polynomial time Oracle Turing machines. By the property of $\leq_T^p$-reductions to R_t we just proved, we know that $P_{\mathrm{T}}(R_t) \subseteq \cup_i X_i$. This allows us to show that $P_{\mathrm{T}}(R_t)$ has measure 0 in *EXP* by using the p_2-union property.

Let us define $d \in \mathrm{p}_2$ such that for each $i \in I\!N$, d_i is a martingale witnessing that X_i has p_2-measure 0.

Let $i \in I\!N$, $w \in \Sigma^*$, $b \in \Sigma$.

$$\begin{array}{lcll} d_i(\lambda) & = & 1 & \\ d_i(wb) & = & d_i(w) & \text{if } s_{|w|} \notin \{0\}^*. \\[1em] d_i(wb) & = & 2 \cdot d_i(w) & \text{if } s_{|w|} \in \{0\}^* \\ & & & \text{and } M_i(R_t^{<|s_{|w|}|}, s_{|w|}) = b. \\[1em] d_i(wb) & = & 0 & \text{if } s_{|w|} \in \{0\}^* \\ & & & \text{and } M_i(R_t^{<|s_{|w|}|}, s_{|w|}) \neq b. \end{array}$$

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 $t(\log(|w|)) \cdot |w|^3$, and $d \in \mathrm{p}_2$.

Next we show that for each $i \in I\!N$, $X_i \subseteq \mathrm{S}[d_i]$. Fix $i \in I\!N$ and $A \in X_i$. By the definition of X_i it is clear that for each $n \in I\!N$, $M_i(R_t^{<n}, 0^n) = A(0^n)$, equivalently, $A[2^n - 1] = A(s_{2^n-1}) = M_i(R_t^{<|s_{2^n-1}|}, s_{2^n-1})$. Thus by the definition of d_i, for each $n \in I\!N$ $d_i(A[0..2^n - 1]) = 2 \cdot d_i(A[0..2^n - 2])$ 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 $A \in \mathrm{S}[d_i]$.

The proof is finished by applying the p_2-union lemma (Lemma 10). □

With the same proof technique we can show the next theorem for R_l.

Theorem 15 *$P_{\mathrm{tt}}(R_l)$ has p-measure 0, therefore, it has measure 0 in E.*

As a corollary of the proof of Theorem 14 we have that the theorem holds for any infinite subset of R_t.

Corollary 16 *Let $A \in EXP$ be an infinite subset of R_t. Then*

$$\mu(P_{\mathrm{T}}(A) \mid EXP) = 0.$$

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

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

As an immediate consequence ot Theorems 14 and 15 we have the following:

Corollary 17 *R_t is not Turing -complete for EXP.*
R_l is not truth-table -complete for EXP.

Also Theorem 14 shows that R_t is not weakly Turing complete for EXP, and Theorem 15 that R_l is not weakly truth-table complete for EXP and E. Note that weak completeness for EXP not always implies weak-completeness for E [JL94].

Corollary 17 contrasts with the situation in the recursion theoretical setting. Let $R = \{x \mid K(x) > |x|\}$. It is not hard to see that $\overline{R}$ 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*.

Moreover R_t is a *natural* example of a Turing incomplete set in $EXP - P$.

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 18 *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 19 *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 in-complete for *co-NP* and not in P.

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

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

Definition 20 *Let $f : \mathbb{N} \to \mathbb{N}$. A set C has infinitely many f-hard instances if there exist infinitely many $x \in \{0,1\}^*$ such that,*

$$IC^f(x : C) \geq |x|.$$

Theorem 21 *Let $k \in \mathbb{N}$, let C be a set in E that has infinitely many $n^{\log n}$-hard instances. Then ${P_{k-\mathrm{tt}}}^{-1}(C)$ has p-measure 0.*

Proof:

We start by seeing that every $\leq^p_{k\text{-}tt}$-reduction from C can be done such that on infinitely many $x \in \{0,1\}^*$ there are useful queries of length bigger than $|x|/(5k)$. We say that a query is usefull 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 $C \leq^p_{k\text{-}tt} A$ via machine M. Fix $x \in \{0,1\}^*$ and denote as $\{q_1, q_2, \ldots, q_k\}$ the set of queries in the computation of $M(A,x)$, in lexicographical order. Let $Q_M(A,x) = \{q_1, q_2, \ldots, q_j\}$, for $j \leq k$, be such that $M(A,x)$ is fixed by the answers to queries in $Q_M(A,x)$, and $M(A,x)$ is not fixed by the answers to queries in $Q_M(A,x) - \{q_j\}$.

Assume that $Q_M(A,x) \subseteq \{0,1\}^{\leq \frac{|x|}{5k}}$. From $Q_M(A,x)$ and $Q_M(A,x) \cap A$ we have an instance complexity program for C that gives an answer on input x. The program on input y simulates the computation of $M(A,y)$ by answering only to queries in $Q_M(A,x)$ 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 $n \geq n_0$, $p(n) < n^{\log n}$. Then for each $x \in L$, with $|x| \geq n_0$, if $Q_M(A,x) \subseteq \{0,1\}^{\leq \frac{|x|}{5k}}$ then $IC^{n^{\log n}}(x : C) \leq 4k\frac{|x|}{5k} < |x|$.

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

Next we define the classes

$$X_i = \{A \mid A \leq^p_{k\text{-}tt} C \text{ via } M_i \text{ and } \exists^\infty x \in \{0,1\}^*, \\ \text{such that } Q_{M_i}(A,x) \not\subseteq \{0,1\}^{\leq \frac{|x|}{5k}}\},$$

where $\{M_i \mid i \in \mathbb{N}\}$ is a presentation of all $k$tt-polynomial-time Oracle Turing machines. By the property of $\leq^p_{k\text{-}tt}$-reductions from C we just proved, we know that $P_{k-\mathrm{tt}}{}^{-1}(C) \subseteq \cup_i X_i$. This allows us to show that $P_{k-\mathrm{tt}}{}^{-1}(C)$ has p-measure 0 by using the p -union property.

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

Let us define $d \in \mathrm{p}$ such that for each $i \in \mathbb{N}$, d_i is 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 $|x(w,i)| \geq 5k\lfloor\log(|w|)\rfloor$ then $d_i(wb) = d_i(w)$.
If $|x(w,i)| < 5k\lfloor\log(|w|)\rfloor$ then $d_i(wb) = d_i(w)\cdot$

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

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 $d \in \mathrm{p}$.

Let us show that for each $i \in \mathbb{N}$, $\subseteq \mathrm{S}[d_i]$. Fix $i \in \mathbb{N}$ and $A \in X_i$. By definition of X_i, there exists 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 $n \in \mathbb{N}$,

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

Let $n \in I\!N$. We denote as x the string

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

Notice that for each $n \in I\!N$,

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

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

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

By definition of d_i,

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

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

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

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

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

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

$$2^{-a_{n+1}}.$$

Thus

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

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

Also since

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

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

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

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

Thus

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

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

The proof is finished by applying the p -union lemma (Lemma 10). □

With a similar proof we can show the following

Theorem 22 *Let C be a set in EXP that has infinitely many $n^{\log n}$-hard instances. Then ${P_{\mathrm{btt}}}^{-1}(C)$ has p_2-measure 0, therefore measure 0 in EXP.*

For R_t and R_l we have the next corollary

Corollary 23 *${P_{\mathrm{btt}}}^{-1}(R_t)$ has p_2-measure 0. For each $k \in I\!N$, ${P_{k-\mathrm{tt}}}^{-1}(R_l)$ has p-measure 0.*

Proof: Use Theorems 12, 13, 21 and 22. □

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 $\leq^p_{btt}$ -reductions are few and far apart.

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 $P_{\mathrm{m}}(A)$ has measure 0 in EXP, or ${P_{\mathrm{m}}}^{-1}(A)$ has p_2-measure 0. In fact what they prove is that for every $A \in EXP$, if $P_{\mathrm{m}}(A)$ does not have measure 0 in EXP, then ${P_{\mathrm{m}}}^{-1}(A)$ has p_2-measure 0. These results were later proved for $\leq^p_{btt}$ reductions in [ASNT94], that is,

Theorem 24 *[ASNT94] Let $A \in EXP$. If $P_{\mathrm{btt}}(A)$ does not have measure 0 in EXP, then ${P_{\mathrm{btt}}}^{-1}(A)$ has p_2-measure 0.*

Our results show that the converse of Theorem 24 is false, since both ${P_{\mathrm{btt}}}^{-1}(R_t)$ has p_2-measure 0 and $P_{\mathrm{btt}}(R_t)$ has measure 0 in EXP. (Juedes and Lutz proved in [JL93] that the converse of the many-one version of Theorem 24 is also false.) In fact we have seen that even a much weaker converse of Theorem 24 is false, since the following holds

Corollary 25 *There exists $A \in EXP$ such that both $\mu_{p_2}({P_{\mathrm{btt}}}^{-1}(A)) = 0$ and $\mu_{p_2}(P_{\mathrm{T}}(A)) = 0$.*

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

Theorem 26 *[ASNT94] Let $A \in E$, $k \in I\!N$. If $P_{k-\mathrm{tt}}(A)$ does not have measure 0 in E, then ${P_{k-\mathrm{tt}}}^{-1}(A)$ p-measure 0.*

And we have shown that the converse of Theorem 26 is false,

Corollary 27 *There exists $A \in E$ such that both $\mu p({P_{k-\mathrm{tt}}}^{-1}(A)) = 0$ and $\mu(P_{\mathrm{tt}}(A) \mid E) = 0$.*

Another corollary is:

Corollary 28 *The class of sets that are $\leq^p_{btt}$ -hard for EXP have 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 $\leq^p_{btt}$ -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 $RS_s = \{x \mid KS^s(x) \geq |x|\}$.

Theorem 29 *There exists $A \in ESPACE$ such that both $\mu_{pspace}({P_{k-\mathrm{tt}}}^{-1}(A)) = 0$ and $\mu_{pspace}(P_{\mathrm{T}}(A)) = 0$. There exists $A \in EXPSPACE$ such that both $\mu_{p_2space}({P_{\mathrm{btt}}}^{-1}(A)) = 0$ and $\mu_{p_2space}(P_{\mathrm{T}}(A)) = 0$.*

Where pspace and $\mathrm{p}_2$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 developed by considering $R_t^p = \{x \mid K^t(x) \geq p(|x|)\}$, for p any fixed sublinear polynomial.

4 Conclusions and questions

We studied the lower span of R_t with respect to Turing -reductions. We showed that that 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 $\leq_{btt}^p$ -reductions this upper span also has measure 0 in EXP. In fact, our proof shows that this upper span has p_2-measure 0, thus if we could push these results up to polynomial-time truth-table reductions it would result in proving that $BPP \neq EXP$.

Acknowledgements

Both authors would like to thank Jack Lutz for helpful remarks on the first version of this paper.

References

[ASNT94] K. Ambos-Spies, H-C. Neis, and S.A. Terwijn. Genericity and measure for exponential time. *Proc. 19th International Symposium on Mathematical Foundations of Computer Science,* pages 221–232, 1994. Springer-Verlag LNCS 841. To appear in *Theoretical Computer Science.*

[ASTZ94] K. Ambos-Spies, S.A. Terwijn, and X. Zheng. Resource bounded randomness and weakly complete problems. *Proc. 5th International Symposium on Algorithms and Computation,* pages 369–377, 1994. Springer-Verlag LNCS 834. To appear in *Theoretical Computer Science.*

[BDG88] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I.* Springer-Verlag, 1988.

[BDG90] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity II.* Springer-Verlag, 1990.

[Ber77] L. Berman. *Polynomial Reducibilities and Complete Sets.* PhD thesis, Cornell University, 1977.

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

[BO94] H. Buhrman and P. Orponen. Random strings make hard instances. *Proc. Structure in Complexity Theory 9th annual conference*, pages 217–222, 1994. IEEE computer society press.

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

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

[JL93] D.W. Juedes and J.H. Lutz. The Complexity and Distribution of Hard Problems. *Proc. 34th Symposium on Foundations of Computer Science,* pages 177–185, 1993. *SIAM J. Comput.*, 24:279–295, 1995.

[JL94] D.W. Juedes and J.H. Lutz. Weak Completeness in E and E_2. *Theoretical Computer Science*, 143:149–158, 1995.

[KM94] S.M. Kautz and P.B. Miltersen. Relative to a random oracle NP is not small. *Proc. Structure in Complexity Theory 9th annual conference*, pages 162–174, 1994. IEEE computer society press.

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

[Lev73] L. Levin. Universal sorting problems. *Problemy Peredaci Informacii*, 9:115–116, 1973. 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, 1993.

[Lut92] J.H. Lutz. Almost everywhere high nonuniform complexity. *J. Computer and System Sciences*, 44:220–258, 1992.

[Lut94] J.H. Lutz. Weakly Hard Problems. *Proc. Structure in Complexity Theory 9th annual conference*, pages 146–161, 1994. IEEE computer society press. To appear in *SIAM J. on Computing.*

[LuMa94] J.H. Lutz and E. Mayordomo. Cook Versus Karp-Levin: Separating Reducibilities if NP is not Small. *Proc. 11th Annual Symposium on Theoretical Aspects of Computer Science*, pages 415–426, 1994. Springer-Verlag LNCS 775. To appear in *Theoretical Computer Science.*

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

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

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

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

[OKSW94] P. Orponen, K-I Ko, U. Schöning, and O. Watanabe. Instance complexity. *J. Assoc. Comput. Mach.*, 41(1):96–121, 1994.

[RSC95] K. Regan, D. Sivakumar, and J.-Y. Cai. Pseudorandom generators, measure theory, and natural proofs. Technical Report UB-CS-TR 95-02, Computer Science Dept., SUNY University at Buffalo, 1995. To appear in *Proc. 36th Symposium on Foundations of Computer Science,* 1995.