An Excursion to the Kolmogorov Random Strings

Harry Buhrman*

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

and

Elvira Mayordomo†

Dept. Ingenieria Informatica, Univ. de Zaragoza, Maria de Luna 3, 50015 Zaragoza, Spain

Received September 20, 1995; revised September 24, 1996

We study the sets of resource-bounded Kolmogorov random strings: $R_t = \{x \mid C^{\leq t}(x) \geq |x|\}$ for $t(n) = 2^n$. We show that the class of sets that Turing reduce to $R_t$ has measure 0 in $\text{EXP}$ with respect to the resource-bounded measure introduced by Lutz. From this we conclude that $R_t$ is not Turing-complete for $\text{EXP}$. This contrasts with the resource-unbounded setting. There $R$ is Turing-complete for co-$\text{RE}$. We show that the class of sets to which $R_t$ bounded truth-table reduces, has $p_2$-measure 0 (therefore, measure 0 in $\text{EXP}$). This answers an open question of Lutz, giving a natural example of a language that is not weakly complete for $\text{EXP}$ and that reduces to a measure 0 class in $\text{EXP}$. It follows that the sets that are $\leq_{\text{P}_2}$-hard for $\text{EXP}$ 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 $\text{EXP}$. It is well known that $P \subseteq NP \subseteq \text{EXP}$. The only strict inclusion that is known is the one between $P$ and $\text{EXP}$. 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 $\text{EXP}$ 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 $t(n) = 2^n$: $R_t = \{x \mid C^{\leq t}(x) \geq |x|\}$. 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, i.e., the co-$\text{RE}$ set of truly Kolmogorov random strings, is Turing-complete for co-$\text{RE}$ [Mar66]. In this paper however we will show that the resource bounded version is not Turing-complete for $\text{EXP}$, supporting Kolmogorov's intuition at least for $\text{EXP}$. We actually show something stronger. We prove that the sets that Turing reduce to $R_t$ have measure 0 in $\text{EXP}$ 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 $R_t$ reflects almost none of the structure of $\text{EXP}$ 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 $\text{EXP}$ 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. Politecnica de Catalunya in Barcelona. E-mail: buhrman@ewi.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.epsi.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).
We also examine the sets that $R_1$ reduces to, i.e., \{ $A : R_1 \leq_r A$ \}, for some reducibility $r$. We prove that for $\leq_{\text{exp}}$-reductions this class of sets has $p_2$-measure 0, therefore also has measure 0 in $\text{EXP}$ (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 $\leq_{\text{exp}}$-hard for $\text{EXP}$ 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 $\text{EXP}$ that is not in $\text{P}$, answering an open question of Lutz (verbal communication). Juedes and Lutz [JL93] note the existence of sets in $\text{EXP}$ having $\text{P}$-measure 0. Intuitively, the measure in $\text{EXP}$ is a function $\mu : \mathcal{P}(\text{EXP}) \to [0, 1]$ with some additivity properties, whose main purpose is to classify by size criteria the subclasses of $\text{EXP}$. 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 $\text{EXP}$ 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 $\text{EXP}$, if they are measurable at all.

**Definition 1.** A martingale is a function $d : \{0, 1\}^* \to \mathbb{Q}$ 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 $x \in \{0, 1\}^*$ if

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

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

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

**Definition 3.** A class $X \subseteq \{0, 1\}^*$ 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 $X \subseteq \{0, 1\}^*$ has $p_2$-measure 1 (denoted by $\mu_{p_2}(X) = 1$) iff $X^c$ has $p_2$-measure 0.

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

**Definition 4.** A class $X \subseteq \{0, 1\}^*$ 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 $X \subseteq \{0, 1\}^*$ has $p$-measure 1 (denoted by $\mu_{p}(X) = 1$) iff $X^c$ has $p$-measure 0.
A class \( X \subseteq \{0, 1\}^* \) has measure 0 in \( E \) iff \( X \cap E \) has \( p \)-measure 0. This is denoted by \( \mu(X \mid E) = 0 \).

A class \( X \subseteq \{0, 1\}^* \) 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 \( \sigma \)-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 \( X_0, X_1, X_2, \ldots \) if

\[
X = \bigcup_{i=0}^{\infty} X_i
\]

and there exists a single constant \( k \in \mathbb{N} \) such that for every \( i \), there is a martingale \( d_i \) with \( X_i \subseteq \mathcal{S}(d_i) \), 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 \( \leq_{p_2} \) be a reducibility and \( A \) be a set. \( P_r(A) = \{ B \mid B \leq_{p_2} A \} \). We will call \( P_r(A) \) the lower span of \( A \). \( P_r^{-1}(A) = \{ B \mid A \leq_{p_2} B \} \) is called the upper span of \( A \).

**Definition 8.** Given a reducibility \( \leq_{p_2} \), we say that a language \( A \in EXP \) is \( \leq_{p_2} \)-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 \( \leq_{p_2} \)-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:

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

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:

\[
IC^{(n)}(x; A) = \min \{|M| \mid M \text{ is a } (t(n)) \text{-bounded Turing-}
\]

\[
\text{machine consistent with } A \text{ and deciding } x\}.
\]

We study the sets \( R_k = \{ x \mid C^{(n)}(x) \geq |x| \} \), for \( t(n) = 2^n \), for some \( k \geq 2 \). Observe that \( R_k \) is decidable in time \( 2^{2^n} \), therefore \( R_k \in EXP \). A variant of 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 \( R_k \):

**Theorem 9.** There exists \( n_1 \in \mathbb{N} \), \( c_1 > 0 \), such that for every \( x \in R_k \), \( |x| \geq n_1 \),

\[
IC^{(n)}(x; R_k) \geq |x| - c_1.
\]

We also study the set \( R_k = \{ x \mid C^{(n)}(x) \geq |x| \} \), for \( t(n) = 2^{2^n} \), \( k \geq 3 \). For this set we also have

**Theorem 10.** There exists \( n_2 \in \mathbb{N} \), \( c_2 > 0 \), such that for every \( x \in R_k \), \( |x| \geq n_2 \),

\[
IC^{(n)}(x; R_k) \geq |x| - c_2.
\]

### 3. MAIN RESULTS

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

**Theorem 11.** \( P_r(R_k) \) has measure 0 in \( EXP \).

**Proof.** We start by showing that every \( \leq_{p_2} \)-reduction to \( R_k \) 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 \( R_k \). Let \( A \) be such that \( A \leq_{p_2} R_k \) via machine \( M \). Fix \( n \in \mathbb{N} \) and denote as \( \{q_1, q_2, \ldots, q_m\} \) the queries in the computation of \( M(R_k, 0^n) \) (in order of appearance). Assume that there is a \( q \in \{q_1, q_2, \ldots, q_m\} \) such that \( |q| \geq n \) and \( q \in R_k \). Let \( q_j \) be the first such query to appear. We can generate \( q_j \) from \( 0^n \), \( R_k \) (that is, an algorithm for \( R_k \)) and \( j \), because we can simulate the computation of \( M(R_k, 0^n) \) up to obtaining the \( j \)th query by answering to queries of length smaller than \( n \) according to \( R_k \) 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 \( M(R_i, 0^n) \) with \( q \in R_i \) and \( |q| \geq n \) then there exists \( q_i \) in \( R_i \) such that \( |q_i| \geq n \) and \( C(q_i) < n \). This would contradict the definition of \( R_i \), so no such \( q \) can exist.

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

Next we define the classes

\[
X_i = \{ A | A \leq \mathcal{R}_i \text{ via } M_i \text{ and for all } n, \text{ all queries on } 0^n \text{ have length less than } n \},
\]

where \( \{ M_i | i \in \mathbb{N} \} \) is a presentation of all polynomial time oracle Turing machines, and \( \{ q_i | i \in \mathbb{N} \} \) are the corresponding polynomial time bounds. By the property of \( \leq \mathcal{R}_i \)-reductions to \( R_i \), that we just proved, we know that \( P_1(R_i) \subseteq \cup_i X_i \). This allows us to show that \( P_1(R_i) \) 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 \( i \in \mathbb{N} \), \( w \in \Sigma^* \), \( b \in \{0, 1\} \).

\[
\begin{align*}
   d_i(w) &= 1 & \text{if } |s_{|w|}| < n_i, \\
   d_i(wb) &= d_i(w) & \text{if } s_{|w|} \neq \{0\}^*. \\
   d_i(wb) &= 2 \cdot d_i(w) & \text{if } s_{|w|} \in \{0\}^*, |s_{|w|}| \geq n_i, \\
   & \quad \text{and } M_i(R_i < |s_{|w|}|, s_{|w|}) = b. \\
   d_i(wb) &= 0 & \text{if } s_{|w|} \in \{0\}^*, |s_{|w|}| \geq n_i, \\
   & \quad \text{and } M_i(R_i < |s_{|w|}|, s_{|w|}) \neq b.
\end{align*}
\]

By definition \( d_i \) is a martingale. To compute \( d_i(w) \) we need to compute \( R_i < \log(|w|) \) 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 \( n \in \mathbb{N} \), \( M_i(R_i < n, 0^n) = A(0^n) \), i.e., \( A[2^n-1] = A(s_{2^n-1}) = M_i(R_i < n, s_{2^n-1}) \). 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 \( \lim_{n \to \infty} d_i(A[0..m]) = \infty \) and \( A \in S[d_i] \).

The proof is finished by applying the \( p_2 \)-union lemma.

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

**Theorem 12.** \( P_1(R_i) \) has measure 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 \( R_i \).

**Corollary 13.** Let \( A \in \text{EXP} \) be an infinite subset of \( R_i \). Then

\[
\mu(P_1(A) | \text{EXP}) = 0.
\]

Let \( A \in \text{E} \) be an infinite subset of \( R_i \). Then

\[
\mu(P_1(A) | \text{EXP}) = 0.
\]

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

**Corollary 14.** \( R_i \) is not Turing-complete for \( \text{EXP} \) and \( R_i \) is not truth-table-complete for \( \text{EXP} \).

Also Theorem 11 shows that \( R_i \) is not weakly Turing-complete for \( \text{EXP} \), and Theorem 12 shows that \( R_i \) is not weakly truth-table-complete for \( \text{EXP} \) or \( E \). Note that weak completeness for \( \text{EXP} \) does not necessarily imply weak completeness for \( E \) [JL94].

Corollary 14 contrasts with the situation in the recursion-theoretic setting. Let \( R = \{ x | C(x) \geq |x| \} \). It is not hard to see that \( R \) is effectively simple (see [Odi89] for a definition). Moreover in [Mat66] it is shown that every effectively simple set is Turing-complete for \( \text{RE} \) from which it follows that \( R \) is Turing-complete for \( \text{co-RE} \). Kummer [Ku96] has recently shown that \( R \) is truth-table-complete for \( \text{co-RE} \).

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

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

**Corollary 15.** If \( \text{NP} \) does not have measure 0 in \( \text{EXP} \), then \( R \) is not Turing-hard for \( \text{NP} \).

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

**Corollary 16.** Relative to a random oracle, \( R \), is not Turing-hard for \( \text{NP} \).

Note that \( R \), 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 $R_p$ is atypical in $\exp$.

Next we will turn our attention to the upper span of $R_p$, the class of sets that $R_p$ reduces to. We start by proving a general result about the $\leq^p_n$ upper span of any set having infinitely many hard instances, in the following sense.

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

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

**Theorem 18.** Let $k \in \mathbb{N}$, let $C$ be a set in $E$ that has infinitely many $n^{k^2}\log n$-hard instances. Then $P_{k-1}(C)$ has $p$-measure 0.

**Proof.** We start by showing that every $\leq^p_n$-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 $C \leq^p_n A$ via machine $M$. Fix $x \in \{0, 1\}^*$ and denote as $\{q_1, q_2, ..., q_j\}$ 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 $j \leq k$, 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 $Q_M(A,x) \subseteq \{0, 1\}^{\leq |x|/5k}$. 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 $4k^{\log |x|/5k}$.

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 $n \geq n_0$, $p(n) < n^{k^2}\log n$. Then for each $x \in L$, with $|x| \geq n_0$, if $Q_M(A,x) \subseteq \{0, 1\}^{\leq |x|/5k}$ then $IC^{n\log}(x : C) \leq 4k^{\log |x|/5k} < |x|$.

Since $C$ has infinitely many $n^{k^2}\log n$-hard instances, this implies that there exist infinitely many $x \in \{0, 1\}^*$ such that $Q_M(A,x) \subseteq \{0, 1\}^{\leq |x|/5k}$.

Next we define the classes

$$X_i = \{ A \mid C \leq^p_n A \text{ via } M_i \},$$

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 $P_{k-1}(C) \subseteq \bigcup_i X_i$. This allows us to show that $P_{k-1}(C)$ has $p$-measure 0 by using the $p$-union lemma.

For each $i \in \mathbb{N}$, let $n_i$ be such that $g(n_i) < 2^n$ for each $n_i \geq n_i$. For each $n \in \{0, 1\}^*$ and $i \in \mathbb{N}$, let $x(w, i)$ be the minimum $x \in \{0, 1\}^*$ such that $|x| \geq n_i$ and for every $B \in C_n$, $Q_M(B,x) \subseteq \{s_0, ..., s_{n-1}\}$. 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 $w \in \{0, 1\}^*$, $b \in \{0, 1\}$.

$$d_i(\lambda) = 1,$$
$$d_i(wb) = d_i(w),$$
$$d_i(wb) = d_i(w).$$

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 $C \leq^p_n \log |w| + 1$, thus $d_i$ can be computed in time $2^{\log |w|} \log |w| + 1$, for $c > 0$ a constant such that $C \in \text{DTIME}(2^{|w|})$, and this bound does not depend on $i$.

Let us 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 definition of $X_i$, there exist infinitely many $m \in \mathbb{N}$ such that $|x(A[0...m])| < 5k \log |A[0...m]|$.

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

$$a_1 = \min \{ m \mid |x(A[0...m])| < 5k \log |A[0...m]| \}$$
$$a_{n+1} = \min \{ m > a_n \mid A[0...m], i \neq x(A[0...a_n], i)$$
$$\text{and } |x(A[0...m])| < 5k \log |A[0...m]| \},$$

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

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

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

$$Q_M(x, A) \subseteq \{ s_0, ..., s_{a_{n+1} - 1} \}.$$
Notice also that, by definition of \( x, Q_M(x, A) \not\subseteq \{s_n, \ldots, s_{n+1}\} \), and therefore
\[
\Pr_{\bar{y}}[(M(B, x) = C(x)) \land (C_{[0..a_n-1]} \subseteq B)] < 1.
\]
By definition of \( d_i \),
\[
d_i(A[0..a_n+1-1]) = d_i(A[0..a_n-1]) \cdot 2^{a_n-1-a_i}.
\]
For \( i = a_n+1 \),
\[
\prod_{i=a_n}^{a_n+1-1} \Pr_{\bar{y}}[(M(B, x) = C(x)) \land (C_{[0..a_n-1]} \subseteq B)]
\]
\[
= d_i(A[0..a_n-1]) \cdot 2^{a_n-1-a_i}.
\]
Since \( A \in X \), and \( Q_M(x, A) \not\subseteq \{s_n, \ldots, s_{n+1}\}, \)
\[
\Pr_{\bar{y}}[(M(B, x) = C(x)) \land (C_{[0..a_n-1]} \subseteq B)] = 2^{-a_n+1}.
\]
Thus
\[
d_i(A[0..a_n+1-1]) = d_i(A[0..a_n-1]).
\]
\[
\Pr_{\bar{y}}[(M(B, x) = C(x)) \land (C_{[0..a_n-1]} \subseteq B)] = \frac{2^{-a_n+1}}{2^m-1}.
\]
Also since
\[
\Pr_{\bar{y}}[(M(B, x) = C(x)) \land (C_{[0..a_n-1]} \subseteq B)]
\]
is smaller than one, and \( M(B, x) \) depends only on a maximum of \( k \) bits of \( B \), the values of
\[
\Pr_{\bar{y}}[(M(B, x) = C(x)) \land (C_{[0..a_n-1]} \subseteq B)]
\]
can only be of the form \( m \cdot 2^{-k} \cdot 2^{-a_i}, \) 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 7).

The following theorem is basically an application of the p₂-union lemma to the previous result.

**Theorem 19.** Let \( C \) be a set in EXP that has infinitely many \( n^p \)-hard instances. Then \( P_{\text{rank}}(C) \) has \( p₂ \)-measure 0, therefore measure 0 in EXP.

For \( R \) and \( R \), we have the next corollary

**Corollary 20.** \( P_{\text{rank}}^{-1}(R) \) has \( p₂ \)-measure 0. For each \( k \in \mathbb{N}, P_{\text{rank}}^{-1}(R) \) has \( p \)-measure 0.

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

This leaves us with a somewhat strange situation. The sets below \( R \), with respect to Turing reductions and the sets above \( R \), with respect to \( \leq^{p₂}_{\text{rank}} \)-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 \( A \in \text{EXP} \), either \( P_m(A) \) has measure 0 in \( \text{EXP} \), or \( P_m^{-1}(A) \) has \( p₂ \)-measure 0. In fact what they prove is that for every \( A \in \text{EXP}, P_m(A) \) does not have measure 0 in \( \text{EXP} \), then \( P_m^{-1}(A) \) has \( p₂ \)-measure 0. These results were later proved for \( \leq^{p₂}_{\text{rank}} \)-reductions in [ASNT94], that is,

**Theorem 21** [ASNT94]. Let \( A \in \text{EXP} \). If \( P_{\text{rank}}(A) \) does not have measure 0 in \( \text{EXP} \), then \( P_{\text{rank}}^{-1}(A) \) has \( p₂ \)-measure 0.

Our results show that the converse of Theorem 21 is false, since \( P_m^{-1}(R) \) has \( p₂ \)-measure 0 and \( P_{\text{rank}}(R) \) has measure 0 in \( \text{EXP} \). 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 \( A \in \text{EXP} \) such that both \( \mu_{P_{\text{rank}}}(P_{\text{rank}}(A)) = 0 \) and \( \mu_{P_{\text{rank}}}(P_{\text{rank}}(A)) = 0 \).

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

**Theorem 23** [ASNT94]. Let \( A \in E \). If \( P_{\text{rank}}^{-1}(A) \) does not have measure 0 in \( E \), then \( P_{\text{rank}}^{-1}(A) \) 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 \( \mu_{P_{\text{rank}}}(P_{\text{rank}}^{-1}(A)) = 0 \) and \( \mu_{P_{\text{rank}}}(P_{\text{rank}}^{-1}(A)) = 0 \).

Another corollary is:

**Corollary 25.** The class of sets that are \( \leq^{p₂}_{\text{rank}} \)-hard for \( EXP \) has \( p₂ \)-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 \( \leq^{p₂}_{\text{rank}} \)-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 \( RS_k = \{x | CS^{sk}(x) \geq |x|\} \).

**Theorem 26.** There exists \( A \in \text{ESPACE} \) such that both \( \mu_{P_{\text{rank}}}(P_{\text{rank}}^{-1}(A)) = 0 \) and \( \mu_{P_{\text{rank}}}(P_{\text{rank}}^{-1}(A)) = 0 \). There exists
\( A \in \text{EXPSPACE} \) such that both \( \mu_{\text{pspace}}(P_{\text{pspace}}(A)) = 0 \) and \( \mu_{\text{pspace}}(P_{\text{pspace}}(A)) = 0 \).

Here pspace and \( p_2 \)-space-measure are defined similarly to \( p \) and \( p_2 \)-measure (see \cite{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 \( R_e(x) = \{ x \mid C_{\text{type}}(x) \geq |x| \} \), for \( e < 1 \) a fixed positive constant.

4. CONCLUSIONS AND QUESTIONS

We studied the lower span of \( R_e \) with respect to Turing reductions. We showed that this lower span has measure 0 in \( \text{EXP} \). As a consequence we obtained that relative to a random oracle \( R_e \), \( \text{PSPACE} \) is not Turing-hard for \( \text{NP} \). It would be interesting to connect these results to the set studied in \cite{Ko91} and show that similar results are true with respect to the set studied there. We also studied the upper span of \( R_e \) and showed that with respect to \( \leq_{\text{m}} \)-reductions this upper span also has measure 0 in \( \text{EXP} \). 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 \( \text{BPP} \neq \text{EXP} \), since it is known (\cite{TB91, AS}) that for every \( A \in \text{BPP} \), \( P_{\text{pspace}}^A(\phi) \) 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

\cite{AS} K. Ambos-Spies, unpublished.
\cite{BH77} L. Berman and H. Hartmanis, On isomorphisms and density of \( \text{NP} \) and other complete sets, SIAM J. Computing 6 (1977), 305–322.
\cite{Lev94} L. Levin, personal communication, 1994.
\cite{LuMa94} J. H. Lutz and E. Mayordomo, Cook versus Karp-Levin: Separating reducibilities if \( \text{NP} \) is not small, Theoret. Comput. Sci. 164 (1996), 141–163.
\cite{Mahan82} S. Mahaney, Sparse complete sets for \( \text{NP} \): solution of a conjecture of Berman and Hartmanis, J. Comput. System Sci. 25 (1982), 130–143.