Hard Sets Are Hard to Find

H. Buhrman*

CWI
PO Box 94079
1090 GB Amsterdam
The Netherlands

D. van Melkebeek†

Fields Institute &
Department of Computer Science
The University of Chicago
Chicago, IL 60637, USA

Abstract

We investigate the frequency of complete sets for various complexity classes within EXP under several polynomial-time reductions in the sense of resource bounded measure. We show that these sets are scarce:

- *The sets that are complete under $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-reductions for NP, the levels of the polynomial-time hierarchy, and PSPACE have p_2-measure zero for any constant $\alpha < 1$.*
- *The $\leq^{\mathrm{p}}_{n^c-\mathrm{T}}$-complete sets for EXP have p_2-measure zero for any constant c.*
- *Assuming* MA $\neq$ EXP, *the $\leq^{\mathrm{p}}_{\mathrm{tt}}$-complete sets for EXP have p-measure zero.*

A key ingredient is the Small Span Theorem, which states that for any set A in EXP at least one of its lower span (i.e., the sets that reduce to A) or its upper span (i.e., the sets that A reduces to) has p_2-measure zero. Previous to our work, the theorem was only known to hold for $\leq^{\mathrm{p}}_{\mathrm{btt}}$-reductions. We establish it for $\leq^{\mathrm{p}}_{n^{o(1)}-\mathrm{tt}}$-reductions.

1 Introduction

Lutz introduced resource bounded measure [15] to formalize the notions of scarceness and abundance in complexity theory. His approach makes it possible to express statements like "only a few" or "most" sets in a complexity class $\mathcal{C}$ have property P. Many papers investigate resource bounded measure in relation with complexity theory [13, 19, 21, 1, 20, 24, 18, 2].

We can also use resource bounded measure as a tool for separating complexity classes. For example, if we could show that the complete sets in complexity class $\mathcal{C}$ have measure zero and the complete sets in $\mathcal{D}$ do not, we would have separated $\mathcal{C}$ from $\mathcal{D}$.

In this paper we follow that line of research. We investigate complete and hard sets for NP, the levels of the polynomial-time hierarchy, PSPACE and EXP, and give some evidence that they have p_2-measure zero. On the other hand, the results of Bennett and Gill [8] imply that the $\leq^{\mathrm{p}}_{\mathrm{tt}}$-hard sets for BPP do not have p_2-measure zero; Allender and Strauss [1] even showed they have p_2-measure 1 in EXP.

We use three different approaches to obtain our results. Two of them yield unhypothesized statements on the border of what is provable by relativizable techniques. First, we significantly improve the Small Span Theorem of Juedes and Lutz [13]. The Small Span Theorem for a reducibility $\leq^{\mathrm{p}}_r$ states that for any set A in EXP, either the class of sets that $\leq^{\mathrm{p}}_r$-reduce to A (called the lower span of A) or the class of sets that A $\leq^{\mathrm{p}}_r$-reduces to (the upper span of A) or both have p_2-measure 0. Since the degree of a set is the intersection of its lower and upper span, it implies that every $\leq^{\mathrm{p}}_r$-degree has p_2-measure zero, and in particular the $\leq^{\mathrm{p}}_r$-complete degree of any complexity class within EXP. The strongest Small Span Theorem previous to our work was due to Ambos-Spies, Neis, and Terwijn [4], who proved it for $\leq^{\mathrm{p}}_{\mathrm{btt}}$-reductions. The extension to reductions with a non-constant number of queries was a notorious open problem in the area. We establish the Small Span Theorem for $\leq^{\mathrm{p}}_{n^{o(1)}-\mathrm{tt}}$-reductions, i.e., for non-adaptive reductions that make a subpolynomial number of queries. Longpré [14] informed us that he obtained independently a Small Span The-

*Partially supported by the Dutch foundation for scientific research (NWO) through SION project 612-34-002, and by the European Union through NeuroCOLT ESPRIT Working Group Nr. 8556, and HC&M grant ERB-4050-PL-93-0516. E-mail: buhrman@cwi.nl. URL: http://www.cwi.nl/cwi/people/Harry.Buhrman.html.

†Partially supported by the European Union through Marie Curie Research Training Grant ERB-4001-GT-96-0783, by the U.S. National Science Foundation through grant CCR 92-53582, and by the Fields Institute. Most of the research done while visiting CWI and the University of Amsterdam. Email: dieter@cs.uchicago.edu. URL: http://www.cs.uchicago.edu/~dieter.

1093-0159/98 $10.00 © 1998 IEEE

orem for $\leq^p_{\log^{o(1)} n-\mathrm{tt}}$-reductions using the compressibility method [9].

Lutz [17] obtained a Small Span Theorem for non-uniform reductions w.r.t. *pspace*-measure. Similar to his proof, our Small Span Theorem follows from the fact that most sets in EXP have a $\leq^{\mathrm{P}}_{n^{o(1)}-\mathrm{tt}}$-upper span with p_2-measure zero. We actually establish this fact for $\leq^{\mathrm{P}}_{n^{\alpha}-\mathrm{tt}}$-reductions for any constant $\alpha < 1$. This way, we get stronger results on the scarceness of complete sets than the ones that follow from the Small Span Theorem: Any $\leq^{\mathrm{P}}_{n^{\alpha}-\mathrm{tt}}$-degree within EXP has p_2-measure zero. Previously, it was only known for $\leq^{\mathrm{P}}_{\mathrm{btt}}$-reductions that the p_2-measure of the complete sets for EXP have p_2-measure zero [4, 10]. We also obtain that the p_2-measure of the $\leq^{\mathrm{P}}_{n^{\alpha}-\mathrm{tt}}$-hard sets for E and EXP is zero.

Then we take a look at EXP in particular, and use an ad hoc technique to improve the results of the first approach for this particular case. We show that the $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-complete sets for EXP have p_2-measure zero for any constant c. Our proofs relativize and are on the edge of the scope of relativizable techniques: Showing the last theorem for unbounded growing exponent c would separate BPP from EXP.

Therefore, we next look at what we can show under a non-relativizing reasonable but yet unproven complexity theoretic hypothesis, namely the assumption that MA $\neq$ EXP. Babai, Fortnow, Nisan and Wigderson [5] established the existence of a pseudo-random generator that can be used to simulate BPP in subexponential time for infinitely many input lengths unless MA = EXP. Using this pseudo-random generator, Buhrman *et al.* [11] showed that the class of $\leq^{\mathrm{P}}_{\mathrm{tt}}$-complete sets for each of the Δ-levels of the polynomial-time hierarchy has p-measure zero unless EXP = MA. Combining our second approach with theirs and some new ingredients, we are able to prove that the complete sets for EXP under $\leq^{\mathrm{P}}_{\mathrm{T}}$-reductions that make their queries in lexicographic order, have p-measure zero unless EXP = MA. In particular, the $\leq^{\mathrm{P}}_{\mathrm{tt}}$-complete sets for EXP have p-measure zero unless EXP = MA.

Summarizing our results:

- We prove a Small Span Theorem for $\leq^{\mathrm{P}}_{n^{o(1)}-\mathrm{tt}}$-reductions.
- We show that the complete sets for NP, the levels of the polynomial-time hierarchy, and PSPACE under $\leq^{\mathrm{P}}_{n^{\alpha}-\mathrm{tt}}$-reductions have p_2-measure zero for any $\alpha < 1$.
- We show that the hard sets for E and EXP under $\leq^{\mathrm{P}}_{n^{\alpha}-\mathrm{tt}}$-reductions have p_2-measure zero for any $\alpha < 1$.
- We show that the $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-complete sets for EXP have p_2-measure zero for any constant c.
- We show that the $\leq^{\mathrm{P}}_{\mathrm{tt}}$-complete sets for EXP have p-measure zero unless MA = EXP (and the polynomial-time hierarchy collapses).

The organization of this paper is as follows. We first give the necessary background on resource bounded measure and on pseudo-random generators. Section 3 describes our results for arbitrary subclasses of EXP. Then we discuss our results particular to EXP. Section 4 contains those without any complexity theoretic assumption; Section 5 those using the hypothesis MA $\neq$ EXP. Finally, we give some comments and mention remaining open problems.

2 Notation and Preliminaries

Most of our complexity theoretic notation is standard. We refer the reader to the textbooks by Balcázar, Díaz and Gabarró [7, 6], and by Papadimitriou [23].

A *reduction* of a set A to a set B is a polynomial-time oracle Turing machine M such that $M^B = A$. We say that A reduces to B and write $A \leq^{\mathrm{P}}_{\mathrm{T}} B$ ('T' for Turing). The reduction M is *non-adaptive* if the oracle queries M makes on any input are independent of the oracle. In that case we write $A \leq^{\mathrm{P}}_{\mathrm{tt}} B$ ('tt' for truth-table). If in addition, the number of queries on an input of length n is bounded by $q(n)$, we write $A \leq^{\mathrm{P}}_{q(n)-\mathrm{tt}} B$. For a reducibility $\leq^{\mathrm{P}}_{r}$, we define the *lower span* of a set A as $\mathrm{P}_r(A) = \{B \mid B \leq^{\mathrm{P}}_r A\}$, and the *upper span* of A as $\mathrm{P}_r^{-1}(A) = \{B \mid A \leq^{\mathrm{P}}_r B\}$. The $\leq^{\mathrm{P}}_r$*-degree* of A equals $\mathrm{P}_r(A) \cap \mathrm{P}_r^{-1}(A)$.

An *autoreduction* M is a reduction that never queries its own input, i.e., for any input x and any oracle B, M^B with input x does not query x. A set A is *autoreducible* if there is an autoreduction of A to itself.

2.1 Background on Resource Bounded Measure

For our purposes, we only have to define what it means to have resource bounded measure zero.

Definition 2.1 *A* supermartingale *is a function* $d : \Sigma^* \to [0, \infty)$ *satisfying*

$$d(w) \geq \frac{d(w0) + d(w1)}{2} \tag{1}$$

for every $w \in \Sigma^*$. *If equality holds in (1) for all* w, d *is called a* martingale.
A supermartingale succeeds *on a sequence* $\omega \in \Sigma^\infty$ *if*

$d(\omega) = \limsup_{w \sqsubseteq \omega, w \to \omega} d(w) = \infty$. *It* covers *a class $\mathcal{C}$ of sequences if it succeeds on every sequence in $\mathcal{C}$.*

A martingale d describes a strategy for an infinite one-person betting game. At the beginning of the game, an infinite bit sequence ω is fixed but not revealed. The player starts with initial capital $d(\lambda)$, and in each round guesses the next bit of ω and bets some of his capital on that outcome. Then the actual value of the bit is revealed. On a correct guess, the player earns the amount of money he bet; otherwise he loses it. The value of $d(w)$ equals the capital of the player after being revealed the bit sequence w. The player wins on ω if he manages to make his capital arbitrarily high during the game. A supermartingale describes a similar game, but now the player is allowed to throw away some of his capital in every round.

Martingales yield the following characterization.

Theorem 2.1 *A class $\mathcal{C} \subseteq \Sigma^\infty$ has Lebesgue measure zero iff it can be covered by a martingale iff it can be covered by a supermartingale.*

We obtain a resource bounded variant by putting resource bounds on the martingales.

Definition 2.2 ([16]) *A (super)martingale d is a p-(super)martingale (resp. p_2-(super)martingale) if we can compute $d(w)$ in time polynomial in $|w|$ (resp. in time $2^{\log^{O(1)}|w|}$).*
A system d_i of (super)martingales is p-uniform (resp. p_2-uniform) if we can compute $d_i(w)$ in time polynomial in $|w|+i$ (resp. in time $2^{\log^{O(1)}(|w|+i)}$).
A class $\mathcal{C} \subseteq \Sigma^\infty$ has p-measure (resp. p_2-measure) zero if it can be covered by a p-supermartingale (resp. p_2-supermartingale). We denote this by $\mu_p(\mathcal{C}) = 0$ (resp. $\mu_{p_2}(\mathcal{C}) = 0$).

As in the unbounded case, the resource bounded measure-zero relations are monotone and closed under union. The following resource bounded version of closure under countable unions holds.

Theorem 2.2 ([16]) *Let d_i be a p-uniform (resp. p_2-uniform) system of supermartingales such that d_i covers the class $\mathcal{C}_i$. Then $\cup_i \mathcal{C}_i$ has p-measure (resp. p_2-measure) zero.*

Characteristic sequences provide the link between resource bounded measure and complexity theory: We associate with a set $A \subseteq \Sigma^*$ its characteristic sequence $\chi_A = A(s_0)A(s_1)A(s_2)\ldots$, where $s_0, s_1, s_2, \ldots$ is the enumeration of Σ^* in lexicographical order.

The crucial property of the resource bounded measure-zero concepts not shared with the Lebesgue measure-zero concept, is that $\mu_p(\mathrm{E}) \neq 0$ and $\mu_{p_2}(\mathrm{EXP}) \neq 0$ [16].

2.2 Background on Pseudo-Random Generators

Definition 2.3 ([22]) *The* hardness *$H_A(n)$ of a set A at length n is the largest integer s such that for any circuit C of size at most s with n inputs*

$$|\Pr_x[C(x) = A(x)] - \frac{1}{2}| \leq \frac{1}{s},$$

where x is uniformly distributed over Σ^n.
A pseudo-random generator *is a function G that, for each n, maps Σ^n into $\Sigma^{r(n)}$ where $r(n) > n$. The* security *$S_G(n)$ of G at length n is the largest integer s such that for any circuit C of size at most s with $r(n)$ inputs*

$$|\Pr_x[C(x) = 1] - \Pr_y[C(G(y)) = 1]| \leq \frac{1}{s},$$

where x is uniformly distributed over $\Sigma^{r(n)}$ and y over Σ^n.

For our purposes, we will need a pseudo-random generator computable in E that stretches seeds superpolynomially and has superpolynomial security at infinitely many lengths. We will use the one provided by the following theorem:

Theorem 2.3 *If* MA $\neq$ EXP, *there is a pseudo-random generator G computable in E with $r(n) \in n^{\theta(\log n)}$ such that for any integer k, $S_G(n) \geq n^k$ for infinitely many n.*

The proof follows directly from the next results of Babai, Fortnow, Nisan and Wigderson [5], and Nisan and Wigderson [22], combined with some padding.

Theorem 2.4 ([5]) *If* MA $\neq$ EXP, *there is a set $A \in$* EXP *such that for any integer k, $H_A(n) \geq n^k$ for infinitely many n.*

Theorem 2.5 ([22]) *Given any set $A \in$* EXP*, there is a pseudo-random generator G computable in EXP with $r(n) \in n^{\theta(\log n)}$ such that $S_G(n) \geq \sqrt{H_A(\sqrt{n})}$.*

3 Complete Sets under Non-Adaptive Reductions with n^α Queries and a Small Span Theorem

In this section, we establish our results on the measure of complete and hard sets for complexity classes within EXP. The following theorem forms the main ingredient. It states that most sets in EXP have a small upper span under $\leq^{p}_{n^\alpha-tt}$-reductions for constant $\alpha < 1$, and has a strong connection with the Small Span Theorem we will prove further.

Theorem 3.1 *For any $\alpha < 1$,*

$$\mu_p(\{A \in \mathrm{EXP} \mid \mu_{p_2}(\mathrm{P}^{-1}_{n^\alpha-\mathrm{tt}}(A)) \neq 0\}) = 0.$$

We first give an outline of the proof.

Fix a $\leq^{\mathrm{P}}_{n^\alpha-\mathrm{tt}}$-reduction M running in time n^c for some constant $c > 0$, and a set $A \in \mathrm{EXP}$. We would like to construct a p_2-martingale that succeeds on any set B for which $M^B = A$. Suppose we are given the initial segment w_i of χ_B corresponding to all strings of length less than m_i. See Figure 1. We can select an input x of length $n_i = m_i^{1/\epsilon}$ for some constant $\epsilon > 0$, and divide the available capital uniformly among the extensions w'_{i+1} of w_i corresponding to all strings of length less than m_{i+1} ($m_{i+1} \geq n_i^c$) for which $M^{w'_{i+1}}(x) = A(x)$. This way, our capital at the end of stage i is definitely not smaller than at the beginning, and in case only half or fewer of the extensions pass the consistency test on x, we actually double it or even better. In order to be able to bet on the sets $A \in \mathrm{EXP}$ for which this strategy fails on some set B such that $M^B = A$, we will perform the consistency check not for a single input x of length n_i, but for a certain collection $I_{M,i}$ of $n_i^\alpha + 1$ inputs x of length n_i: We distribute the available capital uniformly over all extensions w'_{i+1} for which $M^{w'_{i+1}}(x) = A(x)$ for every $x \in I_{M,i}$. If there is an input $x \in I_{M,i}$ for which only half or fewer of the extensions w'_{i+1} satisfy $M^{w'_{i+1}}(x) = A(x)$, we gain a factor of 2 or more in stage i while betting on B. We will try this strategy at every stage i, and we succeed on B if the latter situation occurs for infinitely many of them.

Now, suppose that for some B to which M reduces A, this situation only occurs for finitely many stages. So for almost all stages i, on any input $x \in I_{M,i}$ more than half of the extensions w'_{i+1} of w_i satisfy $M^{w'_{i+1}}(x) = A(x)$. We would like to construct a p-martingale that succeeds on any such $A \in \mathrm{EXP}$ by betting on these x's according to the majority vote of the extensions. We do not know the prefix w_i of χ_B we need for that, but we can guess the values of the bits in this prefix which M queries on inputs $x \in I_{M,i}$, i.e., divide our capital uniformly over all possible corresponding strategies. In order for this to work, we will make sure that the set $I_{M,i}$ consists of $n_i^\alpha + 1$ strings of length n_i on which M makes the *same* queries of length less than m_i. This implies we have to distribute our capital among no more than $2^{n_i^\alpha}$ strategies, and at least one of them will realize a relative gain of $2^{|I_{M,i}|} = 2^{n_i^\alpha+1} = 2 \cdot 2^{n_i^\alpha}$. So, if we do this at every stage with $\frac{2}{3}$ of the capital available at the beginning of that stage, and leave the other $\frac{1}{3}$ intact, we succeed on A: At almost all stages, we increase our capital with a factor of $\frac{2}{3} \cdot 2 = \frac{4}{3}$, and at the finitely many other stages, we do not loose all of it.

We define the stages as follows:

$$\begin{cases} m_0 &= 1 \\ m_{i+1} &= 2^{m_i} \\ n_i &= m_i^{1/\epsilon}. \end{cases} \tag{2}$$

Note that, no matter for what constant c the reduction M runs in time n^c, the stages do not interfere at sufficiently high levels, i.e., $m_{i+1} \leq n_i^c$ for i sufficiently large.

Next, we show that for sufficiently large i, the sets $I_{M,i}$ exist for any $\leq^{\mathrm{P}}_{n^\alpha-\mathrm{tt}}$-reduction M, and that we can construct them efficiently. Here we need the fact that $\alpha < 1$.

Lemma 3.2 *Let $\alpha < 1$, $\epsilon \in (0, 1-\alpha)$, and m_i and n_i defined by (2). There is an integer i_0 such that for any $i \geq i_0$ and for any $\leq^{\mathrm{P}}_{n^\alpha-\mathrm{tt}}$-reduction M, there is a set of strings $Q_{M,i}$ such that*

$$|\{x \in \Sigma^{n_i} \mid Q_M(x) \cap \Sigma^{<m_i} = Q_{M,i}\}| \geq n_i^\alpha + 1,$$

where $Q_M(x)$ denotes the set of queries M makes on input x. Moreover, we can find the lexicographically first set $Q_{M,i}$ and the lexicographically first subset $I_{M,i}$ of

$$\{x \in \Sigma^{n_i} \mid Q_M(x) \cap \Sigma^{<m_i} = Q_{M,i}\}$$

with $|I_{M,i}| = n_i^\alpha + 1$ in time 2^{2n_i}.

Proof (of Lemma 3.2)
For sufficiently large i, the number of possible values of $Q_M(x) \cap \Sigma^{<m_i}$ for $x \in \Sigma^{n_i}$ is bounded by

$$\sum_{i=0}^{n_i^\alpha} \binom{2^{m_i} - 1}{i} \leq (2^{m_i})^{n_i^\alpha} = 2^{n_i^{\alpha+\epsilon}} \leq \frac{2^{n_i}}{n_i^\alpha + 1}, \tag{3}$$

from which the existence of $Q_{M,i}$ follows. A brute force search does the job. □

We now formalize the above outline.

Proof (of Theorem 3.1)
We use the notation from Lemma 3.2. Fix $A \in \mathrm{DTIME}[2^{n^k}]$. Let

$$\pi_{A,M}(w) = \begin{cases} 1 & \text{if } |w| < 2^{m_{i_0}} \\ \Pr_{\omega \sqsupseteq w}[\forall x \in I_{M,i} : M^\omega(x) = A(x)] & \\ & \text{if } 2^{m_{i_0}} \leq 2^{m_i} \leq |w| < 2^{m_{i+1}}. \end{cases}$$

We define the martingale $d_{A,M}$ as follows:

$$\begin{aligned} d_{A,M}(\lambda) &= 1 \\ d_{A,M}(wb) &= \begin{cases} \frac{2 \cdot \pi_{A,M}(wb)}{\pi_{A,M}(wb) + \pi_{A,M}(w\bar{b})} \cdot d_{A,M}(w) \\ \quad \text{if } \pi_{A,M}(wb) + \pi_{A,M}(w\bar{b}) \neq 0 \\ d_{A,M}(w) \qquad \text{otherwise.} \end{cases} \end{aligned}$$

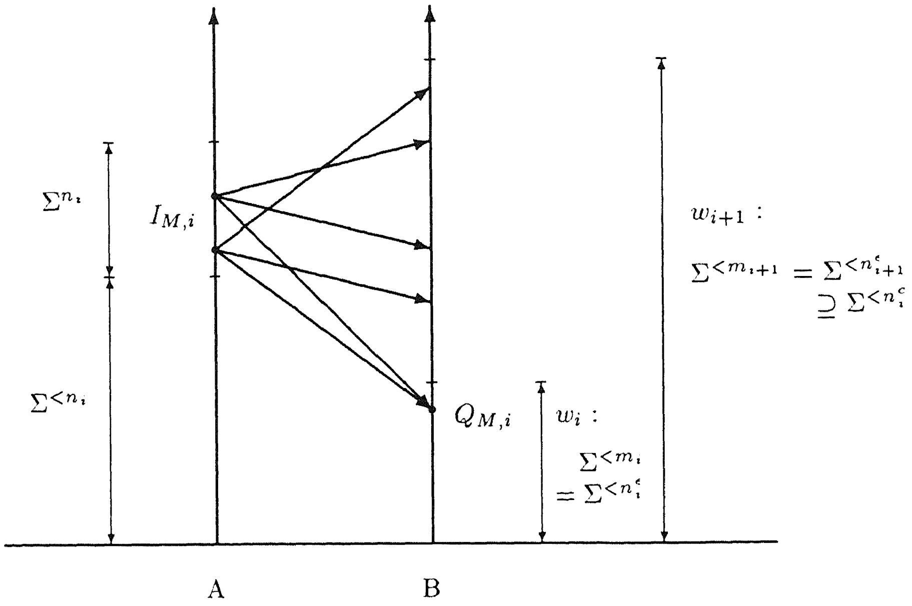

Figure 1: Betting strategies at stage i

This means that for any sufficiently large i (such that $i \geq i_0$ and stage $i+1$ does not interfere with stage i) and for any prefix w_i of length $2^{m_i}-1$, the martingale $d_{A,M}$ distributes $2^{2^{m_{i+1}}-2^{m_i}} \cdot d_{A,M}(w_i)$ uniformly over all extensions w'_{i+1} of w_i with $|w'_{i+1}| = 2^{m_{i+1}}-1$ for which $M^{w'_{i+1}}$ and A agree on the membership of every string in $I_{M,i}$.

The defining predicate of $\pi_{A,M}$ depends on at most $|I_{M,i}| \cdot n_i^\alpha \in O((\log|w|)^{\frac{2\alpha}{\epsilon}})$ positions of ω not fixed by w. It follows that $\pi_{A,M}$ and $d_{A,M}$ can be computed in time $2^{(\log|w|)^{O(\frac{\alpha+k}{\epsilon})}}$.

We distinguish between two cases for the behavior of M and A: Either there are infinitely many stages i such that no matter what the prefix w_i is, there is always an input in $I_{M,i}$ on which only half or fewer of the extensions pass the consistency check between M and A; or else for almost all stages i, there is a prefix w_i such that for any input from $I_{M,i}$, a strict majority of the extensions of w_i make M and A agree on that input.

Case 1 $\exists^\infty i, \forall w \in \Sigma^{2^{m_i}-1}, \exists x \in I_{M,i}$: $\Pr_{\omega \sqsupseteq w}[M^\omega(x) = A(x)] \leq \frac{1}{2}$.

Then for any $\omega = \chi_B$ such that M reduces A to B, and for any sufficiently large stage i for which the Case 1 condition holds,

$$d_{A,M}(w_{i+1}) \geq 2d_{A,M}(w_i),$$

where w_j represents the prefix of ω of length $2^{m_j}-1$. This is because at least half of the extensions w'_{i+1} of w_i with $|w'_{i+1}| = 2^{m_{i+1}}-1$ fail some consistency test. It follows that $d_{A,M}(\omega) = \infty$, and that

$$\mu_{p_2}(\{B \mid M \text{ reduces } A \text{ to } B\}) = 0. \qquad (4)$$

Case 2 $\forall^\infty i, \exists w \in \Sigma^{2^{m_i}-1}, \forall x \in I_{M,i}$: $\Pr_{\omega \sqsupseteq w}[M^\omega(x) = A(x)] > \frac{1}{2}$.

For any stage i and any $b \in \Sigma^{|Q_{M,i}|}$, let $\delta_{M,i,b}$ be the martingale with initial capital 1 that only bets on strings of $I_{M,i}$, and for such a string $x \in I_{M,i}$ bets all of its money according to the majority of $M^\omega(x)$ over all sequences $\omega \sqsupseteq v_i$, where v_i is the characteristic string of length $2^{m_i}-1$ in which the bit corresponding to the j-th element of $Q_{M,i}$ equals the j-th bit of b, and all other bits are say 0. Ties are broken arbitrarily. The martingale

$$\delta_{M,i} = \frac{1}{2^{|Q_{M,i}|}} \Sigma_b \delta_{M,i,b}$$

has initial capital 1 and is computable in time $O(n^2)$. It has the property that

$$\delta_{M,i}(\chi_A|_{\Sigma^{<n_{i+1}}}) \geq \frac{2^{|I_{M,i}|}}{2^{|Q_{M,i}|}} \geq 2 = 2\delta_{M,i}(\chi_A|_{\Sigma^{<n_i}}),$$

provided i satisfies the Case 2 condition. Since almost all i's do, the following p-martingale δ_M succeeds on A: During stage i, it uses $\delta_{M,i}$ as a strategy on $\frac{2}{3}$ of the capital it has at the beginning of stage i, and does nothing with the other $\frac{1}{3}$.

Fix an enumeration M_j of all $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-reductions such that we can compute $M_j(x)$ in time polynomial in $2^{|x|}+j$. Then the martingale system δ_{M_j} is p-uniform, so there is a p-martingale δ that succeeds on all sets A for which Case 2 applies for some $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-reduction M. Consider any set $A \in \mathrm{EXP}$ not covered by δ. Since the martingale system d_{A,M_j} is p_2-uniform, equation (4) implies that the p_2-measure of $\mathrm{P}^{-1}_{n^\alpha-\mathrm{tt}}(A)$ is zero. □

Luc Longpré noticed that Theorem 3.1 also holds for $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{T}}$-reductions that make their queries in lexicographical order. It actually suffices that the queries are made in length non-decreasing order.

Theorem 3.3 *Let $\leq^{\mathrm{p}}_r$ denote the reducibility by polynomial-time Turing machines that query no more than n^α strings on inputs of length n for some constant $\alpha < 1$, and make these queries in lexicographical order. Then*

$$\mu_p(\{A \in \mathrm{EXP} \mid \mu_{p_2}(\mathrm{P}_r^{-1}(A)) \neq 0\}) = 0.$$

Proof sketch

The betting strategy for $\mathrm{P}_r^{-1}(A)$ is the same as in Theorem 3.1, except that we choose the set $I_{M,i}$ from Lemma 3.2 now of size n_i. The construction in the proof of Lemma 3.2 still works, because for any $x \in \Sigma^{n_i}$, the set of small queries $Q_{M^\omega}(x) \cap \Sigma^{<m_i}$ only depends on the prefix of ω of length $2^{m_i}-1$, since M^ω makes its queries in length non-decreasing order.

The martingale $\delta_{M,i}$ is the average over several strategies. Now there is one strategy corresponding to every candidate set $Q \subseteq \Sigma^{<m_i}$ of small queries, and every possible answer string b to these queries. The strategy only bets on the lexicographically first n_i strings of length n_i for which M queries exactly Q in the range $\Sigma^{<m_i}$, assuming the answers b to these queries. On such an input, it bets all of its money according to the majority of $M^\omega(x)$ over all sequences ω that are consistent with b on Q. Note that we can determine this majority in time $2^{O(n_i^\alpha)} \subseteq O(2^{n_i})$ by computing the fraction of strings $\beta \in \Sigma^{n_i^\alpha}$ such that M^ω queries exactly Q in the range $\Sigma^{<m_i}$ on input x and accepts/rejects, when the oracle queries of length less than m_i are answered according to b, and the i-th different query of length at least m_i is answered as β_i.

By a similar argument as in (3), we can upper bound the total number of strategies by $2^{n_i^{\alpha+\epsilon}} \cdot 2^{n_i^\alpha} \ll 2^{n_i}$. Their average yields the p-martingale $\delta_{M,i}$. Since at least one strategy always bets correctly, $\delta_{M,i}$ realizes a gain factor of at least

$$\frac{2^{n_i}}{2^{n_i^{\alpha+\epsilon}} \cdot 2^{n_i^\alpha}} \gg 1$$

during stage i.

The rest of the construction and the analysis is the same as in the proof of Theorem 3.1. □

Our results on the measure of complete sets follow directly from Theorem 3.1. By Theorem 3.3, they also hold for the more general reducibility introduced in Theorem 3.3.

Corollary 3.4 *For any $\alpha < 1$ and $C \in \mathrm{EXP}$, the $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-degree of C has p_2-measure zero. In particular, the classes of $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-complete sets for NP, the levels of the polynomial-time hierarchy, PSPACE, and EXP all have p_2-measure zero.*

Proof

Suppose not, then for any set A in the $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-degree of C, the p_2-measure of $\mathrm{P}^{-1}_{n^\alpha-\mathrm{tt}}(A)$ is not zero, since it contains the $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-degree of C. But, by Theorem 3.1 this would imply that the p-measure of the $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-degree of C is zero. □

For the class of $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-hard sets, we get:

Corollary 3.5 *For any $\alpha < 1$ and any complexity class $\mathcal{C}$ such that $\mu_p(\mathcal{C} \cap \mathrm{EXP}) \neq 0$, the class of $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-hard sets for $\mathcal{C}$ has p_2-measure zero. In particular, the $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-hard sets for E and EXP have p_2-measure zero.*

Proof

By definition, for any set $A \in \mathcal{C}$, the $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-hard sets for $\mathcal{C}$ are contained in $\mathrm{P}^{-1}_{n^\alpha-\mathrm{tt}}(A)$. If the class of $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-hard sets for $\mathcal{C}$ does not have p_2-measure zero, Theorem 3.1 yields that $\mu_p(\mathcal{C} \cap \mathrm{EXP}) = 0$. □

The $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$-hard sets for NP, the levels of the polynomial-time hierarchy, and PSPACE also have p_2-measure zero, provided these classes themselves do not have p-measure zero.

From Theorem 3.1, we can also deduce a Small Span Theorem. However, we have to settle for a more restrictive reducibility than $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$, because we need transitivity in the proof, and $\leq^{\mathrm{p}}_{n^\alpha-\mathrm{tt}}$ is in general not transitive for any constant $\alpha > 0$. It suffices to keep the number of queries subpolynomial, i.e., asymptotically smaller than n^ϵ for any $\epsilon > 0$.

Theorem 3.6 (Small Span Theorem) *For any set A, at least one of the following holds: $\mu_p(\mathrm{P}_{n^{o(1)}-\mathrm{tt}}(A) \cap \mathrm{EXP}) = 0$ or $\mu_{p_2}(\mathrm{P}^{-1}_{n^{o(1)}-\mathrm{tt}}(A)) = 0$.*

Proof

We distinguish between two cases:

- Either $\mathrm{P}_{n^{o(1)}-\mathrm{tt}}(A)$ contains a set B such that $\mu_{p_2}(\mathrm{P}^{-1}_{n^{o(1)}-\mathrm{tt}}(B)) = 0$. Then the transitivity of $\leq^{\mathrm{P}}_{n^{o(1)}-\mathrm{tt}}$ and the monotonicity of p_2-measure imply that $\mu_{p_2}(\mathrm{P}^{-1}_{n^{o(1)}-\mathrm{tt}}(A)) = 0$.
- Or else $\mathrm{P}_{n^{o(1)}-\mathrm{tt}}(A) \cap \mathrm{EXP}$ is included in $\{B \in \mathrm{EXP} \mid \mu_{p_2}(\mathrm{P}^{-1}_{n^{\alpha}-\mathrm{tt}}(B)) \neq 0\}$ for any $\alpha > 0$. Then Theorem 3.1 says that $\mu_p(\mathrm{P}_{n^{o(1)}-\mathrm{tt}}(A) \cap \mathrm{EXP}) = 0$.

□

For any set $A \in \mathrm{EXP}$, Theorem 3.6 states that at least one of its lower span or upper span under $\leq^{\mathrm{P}}_{n^{o(1)}-\mathrm{tt}}$-reductions is small.

4 Complete Sets for EXP under Adaptive Reductions with n^c Queries

We now show how, in the case of EXP, we can extend the results of the previous section on the measure of complete sets from $\leq^{\mathrm{P}}_{n^{\alpha}-\mathrm{tt}}$-reductions for any $\alpha < 1$ to $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-reductions for any constant c:

Theorem 4.1 *For any constant c, the class of $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-complete sets for EXP has p_2-measure zero.*

The proof technique differs significantly. We exploit the diagonalization power of EXP against $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-reductions to show that all $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-complete sets for EXP share a structural property that allows the construction of a p_2-martingale succeeding on all of them. We first establish the structural property.

Let $M_1, M_2, \ldots$ be an enumeration of $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-reductions, where M_i runs in time n^i.

Lemma 4.2 *For any constant c, and for any $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-complete set C for EXP, there is an index j such that*

$$\forall n, \forall x \in \Sigma^n : M_j^C(\langle 0^j, x\rangle) = \mathrm{minority}_{\omega \sqsupseteq \chi_C|_{\Sigma^{<n}}}[M_j^{\omega}(\langle 0^j, x\rangle)]. \tag{5}$$

The right-hand side of (5) denotes the least probable value of $M_j^{\omega}(\langle 0^j, x\rangle)$ when ω is uniformly distributed over all extensions of the initial segment of χ_C corresponding to all strings of length up to n. Ties are broken in some fixed way, say always 0.

Proof (of Lemma 4.2)
Let

$$D = \{\langle 0^i, x\rangle \mid \Pr_{\omega \sqsupseteq \chi_C|_{\Sigma^{<|x|}}}[M_i^{\omega}(\langle 0^i, x\rangle) = 1] < \frac{1}{2}\}.$$

The above probability is a weighted sum of the accepting leaves of the reduction tree of M_i on input $\langle 0^i, x\rangle$. The weight of a leaf is only nonzero if on its path P all queries of length less than $|x|$ are answered consistent with C, and in that case its weight equals $2^{-q(P)}$, where $q(P)$ denotes the number of other queries made along P. Wlog. we are assuming here that on no path the reduction asks the same query more than once. So, we can decide D on instances $\langle 0^i, x\rangle$ of length n in time $2^{n^c}(n^c \cdot \mathrm{time}_C(n) + n^i)$. Since $C \in \mathrm{EXP}$, this implies $D \in \mathrm{EXP}$, and since C is $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-hard for EXP, that there is a $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-reduction M_j reducing D to C. The index j satisfies (5), because for any $x \in \Sigma^n$,

$$\begin{aligned} M_j^C(\langle 0^j, x\rangle) = 1 \\ &\Leftrightarrow \langle 0^j, x\rangle \in D \\ &\Leftrightarrow \Pr_{\omega \sqsupseteq \chi_C|_{\Sigma^{<n}}}[M_j^{\omega}(\langle 0^j, x\rangle) = 1] < \frac{1}{2} \\ &\Leftrightarrow \mathrm{minority}_{\omega \sqsupseteq \chi_C|_{\Sigma^{<n}}}[M_j^{\omega}(\langle 0^j, x\rangle)] = 1. \end{aligned}$$

□

Lemma 4.2 provides a consistency test that eliminates at least half of the remaining possibilities. We now use it in a straightforward way to construct a p_2-martingale covering all $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-complete sets for EXP.

Proof (of Theorem 4.1)
For any index j, we construct a (uniform) p_2-martingale d_j that succeeds on any set C for which (5) holds. The martingale d_j has initial capital 1, and works in stages defined by

$$\begin{cases} n_1 &= 1 \\ n_{i+1} &= (n_i + j)^j. \end{cases}$$

The i-th stage starts when the martingale has to bet on the string 0^{n_i}. Let w_i denote the prefix seen up to that moment. During stage i, d_j distributes $2^{2^{n_{i+1}}-2^{n_i}} \cdot d_j(w_i)$ uniformly over all extensions w'_{i+1} of w_i with $|w'_{i+1}| = 2^{n_{i+1}} - 1$ for which $M_j^{w'_{i+1}}(\langle 0^j, 0^{n_i}\rangle) = \mathrm{minority}_{\omega \sqsupseteq w_i}[M_j^{\omega}(\langle 0^j, 0^{n_i}\rangle)]$.

Note that for any set C satisfying (5), d_j at least doubles its capital along C at every stage, so it succeeds on any such C. Therefore, by Lemma 4.2, the martingale system $(d_j)_{j=1}^{\infty}$ covers the class of $\leq^{\mathrm{P}}_{n^{c}-\mathrm{T}}$-complete sets for EXP.

Using the approach of Lemma 4.2, we can compute the minority and the probabilities underlying $d_j(w)$ in time $O(2^{(\log|w|+j)^c}(\log|w| + j)^j)$. So, the martingale system $(d_j)_{j=1}^{\infty}$ is p_2-uniform. □

In an analogous way, we get the following theorem for E:

Theorem 4.3 *For any constant c, the class of $\leq^{\mathrm{P}}_{cn-\mathrm{T}}$-complete sets for E has p-measure zero.*

Ambos-Spies informed us very recently that he and Lempp have a new proof of Theorems 4.1 and 4.3 [3].

5 Complete Sets for EXP under Adaptive Reductions

Theorem 4.1 cannot be improved using relativizable techniques, since it fails for unbounded growing exponent c in a world where BPP = EXP, and such a world exists [12]. This follows from the relativizable result of Allender and Strauss [1] that the class of sets that are not $\leq^{\mathrm{P}}_{\mathrm{T}}$-hard for BPP has p-measure zero. In this section, we will see what results we can get on the measure of the EXP-complete sets for polynomial-time reductions without an explicit bound an the number of queries, under the likely but unrelativizing hypothesis MA $\neq$ EXP. We obtain:

Theorem 5.1 *The class of sets complete for EXP (or E) under $\leq^{\mathrm{P}}_{\mathrm{T}}$-reductions that make their queries in lexicographical order, has p-measure zero unless* EXP = MA. *In particular, the class of $\leq^{\mathrm{P}}_{\mathrm{tt}}$-complete sets for EXP (or E) has p-measure zero unless* EXP = MA.

Buhrman *et al.* [11] used the hypothesis MA $\neq$ EXP to show that the class of autoreducible sets under the same type of reductions has p-measure zero. We will use the same idea, namely applying pseudo-random generators to efficiently approximate the probabilities underlying the martingales constructed in the previous section, and that way mimic their behavior by an easier-to-compute martingale. The pseudo-random generators whose existence is known to follow from the assumption MA $\neq$ EXP by Theorem 2.3, have super-polynomial security at infinitely many lengths. They will allow us to approximate the underlying probabilities well enough, but only at infinitely many lengths. Therefore, in order for the mimicing martingale to succeed, we will make sure we make a lot of money on these lengths. We will use the following lemma instead of Lemma 4.2 to do so:

Lemma 5.2 *Fix a pseudo-random generator computable in time 2^{an} for some constant $a > 1$, and with stretching $r(n)$. There is an oracle Turing machine T running in time 2^{2an} with the following property: For any set C complete for EXP under $\leq^{\mathrm{P}}_{\mathrm{T}}$-reductions that make their queries in lexicographic order, there is an index j of such a reduction M_j such that for any string x,*

$$\begin{cases} \Pr_{\omega \sqsupseteq \chi_C|_{\Sigma^{<n}}}[\forall\, i \in I_n : M_j^{\omega}(\langle 0^j, x, 0^i\rangle) = \\ \qquad T^{C\cap\Sigma^{<n}}(\langle 0^j, x, 0^i\rangle)] \leq \frac{2}{n^3} \\ \forall\, i \in I_n : M_j^{C}(\langle 0^j, x, 0^i\rangle) = \\ \qquad T^{C\cap\Sigma^{<n}}(\langle 0^j, x, 0^i\rangle), \end{cases} \tag{6}$$

where $n = |x|$ and $I_n = \{1, 2, \ldots, 3\log n\}$, provided $r(n), S_G(n) \geq n^{j+1}$ and n is sufficiently large.

Lemma 5.2 also holds if we substitute 'length non-decreasing' for 'lexicographic'.

Proof (of Lemma 5.2)
Consider an input $x \in \Sigma^n$, a prefix $w \in \Sigma^{2^n-1}$, a string $b \in \Sigma^{3\log n}$, and an index j such that M_j makes its queries in length non-decreasing order. We can compute the probability

$$\pi_j(x, w, b) = \Pr_{\omega \sqsupseteq w}[\forall\, i \in I_n : M_j^{\omega}(\langle 0^j, x, 0^i\rangle) = b_i]$$

as the fraction of strings $\beta \in \Sigma^{n^{j+1}}$ such that the predicate underlying π_j holds when the oracle queries of length less than n are answered according to w, and the k-th different query of length at least n is answered as β_k. The predicate depends on $o(n^{j+1})$ bits of the prefix w in total, because the queries of length less than n made by M are the same for any β. It follows that the test has circuit complexity, say n^{j+1} for sufficiently large n. Therefore, we can approximate $\pi_j(x, w, b)$ to within an additive term of $\frac{1}{n^4}$ using the pseudo-random generator G at length n, provided $r(n) \geq n^{j+1}$ and $S_G(n) \geq n^{j+1}$.

On input $\langle 0^j, x, 0^i\rangle$, the machine T^w will compute these approximations $\tilde{\pi}_j(x, w, b)$ to $\pi_j(x, w, b)$ for every $b \in \Sigma^{3\log n}$, select the lexicographically first value $\tilde{b}$ for b that minimizes $\tilde{\pi}_j(x, w, b)$, and output the i-th bit of $\tilde{b}$. T can do this in time 2^{2an}.

Note that there is a setting $b^* \in \Sigma^{3\log n}$ such that $\pi_j(x, w, b^*) \leq \frac{1}{n^3}$: Inductively set b_i^* such that at least half of the extensions $\omega \sqsupseteq w$ satisfying $M_j^{\omega}(\langle 0^j, x, 0^k\rangle) = b_k^*$ for $1 \leq k < i$, fail the test $M_j^{\omega}(\langle 0^j, x, 0^i\rangle) = b_i^*$. Therefore,

$$\begin{aligned} \pi_j(x, w, \tilde{b}) &\leq \tilde{\pi}_j(x, w, \tilde{b}) + \frac{1}{n^4} \\ &\leq \tilde{\pi}_j(x, w, b^*) + \frac{1}{n^4} \\ &\leq \tilde{\pi}_j(x, w, b^*) + \frac{2}{n^4} \leq \frac{1}{n^3} + \frac{2}{n^4} \leq \frac{2}{n^3}, \end{aligned}$$

which establishes the first part of (6) for any set C.

Now fix a set C complete for EXP under $\leq_T^p$-reductions that make their queries in lexicographic order, and consider the set

$$D = \{\langle 0^j, x, 0^i\rangle \mid 1 \leq i \leq 3\log|x| \text{ and } T^{C\cap\Sigma^{<|x|}}(\langle 0^j, x, 0^i\rangle) \text{ accepts}\}.$$

Since $C \in$ EXP, we can also decide D in EXP, and since C is hard for EXP under $\leq_T^p$-reductions that make their queries in lexicographic order, there is such a reduction M_j reducing D to C. This establishes the second part of (6). □

Lemma 5.2 gives a consistency test that eliminates a fraction at least $1 - \frac{2}{n^3}$ of the possibilities, and therefore multiplies the capital by a factor of $\frac{n^3}{2}$. For Lemma 4.2 these figures are $\frac{1}{2}$ and 2 respectively. We will now see how we can exploit the larger increase in capital to construct a p-martingale that succeeds on the complete sets for EXP under $\leq_T^p$-reductions that make their queries in lexicographical order, using the above pseudo-random generator once more.

Proof (of Theorem 5.1 for EXP)
Fix a $\leq_T^p$-autoreduction M_j running in time n^j that makes its queries in lexicographical order. Let T be the oracle Turing machine given by Lemma 5.2 based on the pseudo-random generator G that follows from the hypothesis MA $\neq$ EXP by Theorem 2.3.

Let

$$\pi_{j,m}(w) = \Pr_{\omega \sqsupseteq w}[\forall\, i \in I_m : M_j^{\omega}(\langle 0^j, 0^m, 0^i\rangle) = T^{w\cap\Sigma^{<m}}(\langle 0^j, 0^m, 0^i\rangle)],$$

and consider

$$d_{j,m}(w) = \begin{cases} m^3 \cdot \pi_{j,m}(w) & \text{if } |w| \geq 2^m \\ 2 & \text{otherwise.} \end{cases}$$

The function $d_{j,m}$ is computable in time $2^{O(\log^{j+1} n)}$, as well as the function $d_j = \sum_{m=1}^{\infty} \frac{1}{m^2} d_{j,m}$. They are non-negative and satisfy the supermartingale inequality (1) for all strings w, except possibly for those of length $2^m - 1$. In case of a set C satisfying (6) for $x = 0^m$, the inequality also holds for $w \sqsubseteq \chi_C$ of length $2^m - 1$. Moreover, $d_{j,m}(\chi_C) = m^3$, and $d_j(\chi_C) = \infty$.

We now want to construct (super)martingales $\tilde{d}_{j,m}$ and $\tilde{d}_j$ that behave like $d_{j,m}$ and d_j along χ_C, and are computable uniformly in time $|w|^a$ for some constant a, i.e., independent of the running time of M_j. The key idea is to efficiently approximate the probability $\pi_{j,m}$ using the pseudo-random generator G as we did in the proof of Lemma 5.2. Following that approach, for some constant a_1, we can compute in time $|w|^{a_1}$ an approximation $\tilde{\pi}_{j,m}(w)$ of $\pi_{j,m}(w)$ to within $\epsilon_{j,m} = m^{-(j+4)}$, provided $r(m) \geq m^{j+1}$ and $S_G(m) \geq m^{j+4}$. By Theorem 2.3 (assuming MA $\neq$ EXP), infinitely many m satisfy the latter conditions; we call such m's good.

There are still two technical problems we have to solve in order to make sure that $\tilde{d}_{j,m}$ is a supermartingale: First, what to do along sets C for which (6) does not hold for $x = 0^m$, and what if m is not good? We will deal with that in a moment. Second, even for a good m along a set C satisfying (6) for $x = 0^m$, just replacing $\pi_{j,m}$ with $\tilde{\pi}_{j,m}$ in the definition of $d_{j,m}$ might not work. For example, if $\tilde{\pi}_{j,m}$ underestimates $\pi_{j,m}$ on input w, and overestimates it on input $w0$ and $w1$, condition (1) is violated. Note that such a situation can only occur in case the string corresponding to the position right after w is either an element of the form $\langle 0^j, 0^m, 0^i\rangle$ for some $i \in I_m$, or a query M_j makes on such an input. As the queries are made in lexicographical order, there can be no more than $3m^j \log m$ such strings along any sequence ω. Since the limit $\epsilon_{j,m}$ on the estimation error is such that $(3m^j \log m) \cdot \epsilon_{j,m}$ remains bounded, we can remedy this problem by accumulatively subtracting a term $2\epsilon_{j,m}$ from the approximation for $\pi_{j,m}$, and adding a constant to the resulting approximation for $d_{j,m}$. The former modification guarantees that condition (1) is met; the latter is needed after the former in order to keep the values non-negative. More precisely, we define

$$d^*_{j,m}(w) = \begin{cases} m^3(\tilde{\pi}_{j,m}(w) - 2q_{j,m}(w)\epsilon_{j,m}) + 1 \\ \qquad \text{if } |w| \geq 2^m \\ 4 \qquad \text{otherwise,} \end{cases} \tag{7}$$

where $q_{j,m}(w)$ denotes the number of positions in w that correspond to elements of the form $\langle 0^j, 0^m, 0^i\rangle$ for some $i \in I_m$, or a query M_j makes on such an input. Note that $0 \leq q_{j,m}(w) \leq q_{j,m}(\omega) \leq 3m^j \log m$.

We solve the first problem by explicitly checking for each prefix w that the values $d^*_{j,m}$ proposes for the one bit extensions $w0$ and $w1$, satisfy the defining conditions of a supermartingale. If they do, we accept them; otherwise we enforce the conditions by not betting. So, we define the function $\tilde{d}_{j,m}$ as follows: $\tilde{d}_{j,m}(\lambda) = 4$ and

$$\tilde{d}_{j,m}(wb) = \begin{cases} d^*_{j,m}(wb) \\ \quad \text{if } d^*_{j,m}(w0) \geq 0 \text{ and } d^*_{j,m}(w1) \geq 0 \text{ and} \\ \qquad d^*_{j,m}(w0) + d^*_{j,m}(w1) \leq 2\tilde{d}_{j,m}(w) \\ \tilde{d}_{j,m}(w) \qquad \text{otherwise.} \end{cases} \tag{8}$$

It follows that $\tilde{d}_{j,m}$ is a supermartingale computable in time $|w|^{a_2}$ for some constant a_2 independent of M_j and m.

Claim 5.1 *If m is good and sufficiently large, $\tilde{d}_{j,m}(w) = d^*_{j,m}(w)$ for any $w \sqsubseteq \chi_C$, where C is a set satisfying (6).*

Proof (of Claim 5.1)
We show that $\tilde{d}_{j,m}(w) = d^*_{j,m}(w)$ for any $w \sqsubseteq \chi_C$ by induction on $|w|$. Clearly, the statement holds for $w = \lambda$. So, it suffices to argue for any string w that the conditions on the right-hand side of (8) are met, assuming that $\tilde{d}_{j,m}(w) = d^*_{j,m}(w)$.

If $|w| < 2^m - 1$, this is true because $d^*_{j,m}(v) = 4$ for $|v| < 2^m$. If $|w| \geq 2^m - 1$, the first two conditions on the right-hand side of (8) are satisfied, since for any string v of length $|v| \geq 2^m$,

$$\begin{aligned} d^*_{j,m}(v) &\geq 1 - 2q_{j,m}(v)m^3\epsilon_{j,m} \\ &\geq 1 - 6\epsilon_{j,m}m^{j+3}\log m = 1 - \frac{6\log m}{m}, \end{aligned}$$

which is positive for sufficiently large m. In case $|w| = 2^m - 1$, the remaining condition is met, because

$$\begin{aligned} & d^*_{j,m}(w0) + d^*_{j,m}(w1) \\ \leq\ & m^3(\tilde{\pi}_{j,m}(w0) + \tilde{\pi}_{j,m}(w1)) + 2 \\ \leq\ & m^3(\pi_{j,m}(w0) + \pi_{j,m}(w1) + 2\epsilon_{j,m}) + 2 \\ =\ & 2m^3(\pi_{j,m}(w) + \epsilon_{j,m}) + 2 \\ \leq\ & 2(2+1+1) = 2\tilde{d}_{j,m}(w). \end{aligned}$$

In case $|w| \geq 2^m$, the remaining condition certainly holds if $d^*_{j,m}(w0) = d^*_{j,m}(w1) = d^*_{j,m}(w)$. Otherwise, $q_{j,m}(w0) = q_{j,m}(w1) = q_{j,m}(w) + 1$, and we have that

$$\begin{aligned} & d^*_{j,m}(w0) + d^*_{j,m}(w1) \\ =\ & m^3(\tilde{\pi}_{j,m}(w0) + \tilde{\pi}_{j,m}(w1)) + 2 \\ & -2(q_{j,m}(w0) + q_{j,m}(w1))m^3\epsilon_{j,m} \\ \leq\ & m^3(\pi_{j,m}(w0) + \pi_{j,m}(w1) + 2\epsilon_{j,m}) \\ & +2 - 4(q_{j,m}(w) + 1)m^3\epsilon_{j,m} \\ =\ & 2m^3(\pi_{j,m}(w) - \epsilon_{j,m}) + 2 - 4q_{j,m}(w)m^3\epsilon_{j,m} \\ \leq\ & 2m^3\tilde{\pi}_{j,m}(w) + 2 - 4q_{j,m}(w)m^3\epsilon_{j,m} \\ =\ & 2d^*_{j,m}(w) = 2\tilde{d}_{j,m}(w). \end{aligned}$$

□

So, for a good and sufficiently large m we get that

$$\begin{aligned} & \tilde{d}_{j,m}(\chi_C) \\ =\ & d^*_{j,m}(\chi_C) \\ \geq\ & d_{j,m}(\chi_C) + 1 - (2q_{j,m}(\omega) + 1)m^3\epsilon_{j,m} \\ \geq\ & d_{j,m}(\chi_C) \end{aligned}$$

for any set C satisfying (6). Since there are infinitely many good m's and $d_{j,m}(\chi_C) = m^3$, this implies that $\tilde{d}_j = \sum_{m=1}^{\infty} \frac{1}{m^2}\tilde{d}_{j,m}$ is a supermartingale that succeeds on any such set C. It is computable in time $|w|^a$ for some constant a independent of j.

Since for a standard enumeration M_i including all $\leq^{\mathrm{P}}_{\mathrm{T}}$-reductions that make their queries in lexicographical order and such that $M_i(x)$ is computable in time $(2^{|x|} + i)^{O(1)}$, the supermartingale system $\tilde{d}_i$ is p-uniform, Lemma 5.2 finishes the proof of the theorem.
□

6 Discussion and Open Problems

The question of whether Theorem 3.1 holds for some constant $\alpha \geq 1$, remains open. A positive answer would be the best result provable by relativizable techniques, because of a similar reason why our results in Section 4 are optimal. By the same token, relativizable techniques cannot establish the Small Span Theorem for $\leq^{\mathrm{P}}_{\mathrm{tt}}$-reductions.

It seems unlikely that our approach allows to establish Theorem 3.1 for $\alpha \geq 1$, because of Lemma 3.2. For some constant $\epsilon > 0$ and a given $\leq^{\mathrm{P}}_{n^\alpha-\mathrm{tt}}$-reduction M, this would require the construction of sets $I_{M,i}$ containing $n_i^{O(1)}$ strings of length n_i and slightly smaller sets $Q_{M,i}$, such that all queries of length less than n_i^ϵ that M makes on inputs from $I_{M,i}$ are in $Q_{M,i}$. However, the following argument shows that for $\alpha \geq 1$, it is not even possible for $|I_{M,i}|$ to equal $|Q_{M,i}|$ when for every input $x \in \Sigma^{n_i}$ the queries are chosen from $\Sigma^{<n_i^\epsilon}$ in a Kolmogorov random way. The concatenation σ of all these queries is a Kolmogorov random string of length $2^{n_i}n_i^{\alpha+\epsilon}$. Given a listing of the elements of $Q_{M,i}$, we can describe the queries for elements of $I_{M,i}$ by pointers to that list. Assuming $|I_{M,i}| = |Q_{M,i}| = q$, this leads to a description of σ of length at most $qn_i^\epsilon + q(n_i + n_i^\alpha \log q) + (2^{n_i} - q)n_i^{\alpha+\epsilon} + O(\log q)$, which is asymptotically less than $|\sigma|$ as long as $\log q \leq cn_i^\epsilon$ for some constant $c < 1$. Since we have $\log q \in O(\log n_i)$, we get a contradiction to the Kolmogorov randomness of σ.

Ambos-Spies, Neis, and Terwijn [4] focused on p-measure, and they established the equivalent of Theorem 3.1 and the Small Span Theorem within E for $\leq^{\mathrm{P}}_{k-\mathrm{tt}}$-reductions for any constant k. A similar Kolmogorov argument as above indicates that our techniques are not powerful enough to extend these results to stronger reductions. Even the $\leq^{\mathrm{P}}_{\mathrm{btt}}$-case remains open.

Acknowledgments

We are grateful to Jack Lutz and Lance Fortnow for very helpful discussions regarding the Small Span Theorem. We would like to thank Luc Longpré for the extension of Theorem 3.1 he suggested, Klaus Ambos-Spies for explaining his work in the area, Leen Torenvliet for suggesting the title of the paper, and the anonymous referees for their comments.

References

[1] E. Allender and M. Strauss. Measure on small complexity classes, with applications for BPP. In *Proceedings of the 35th IEEE Symposium on Foundations of Computer Science*, pages 807–818, New York, 1994. IEEE.

[2] K. Ambos-Spies and L. Bentzien. Separating NP-completeness notions under strong hypothesis. In *Proceedings of the 12th IEEE Conference on Computational Complexity*, pages 121–127, New York, 1997. IEEE.

[3] K. Ambos-Spies, S. Lempp, and G. Mainhardt. Randomness vs. completeness: On the diagonalization strength of resource-bounded random sets. Manuscript, March 1998.

[4] K. Ambos-Spies, H.-C. Neis, and S. Terwijn. Genericity and measure for exponential time. *Theoretical Computer Science*, 168(1):3–19, 1996.

[5] L. Babai, L. Fortnow, N. Nisan, and A. Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3:307–318, 1993.

[6] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity II*, volume 22 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1990.

[7] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I*, volume 11 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1995.

[8] C. Bennett and J. Gill. Relative to a random oracle, $P^A \neq NP^A \neq co-NP^A$ with probability one. *SIAM Journal on Computing*, 10:96–113, 1981.

[9] H. Buhrman and L. Longpré. Compressibility and resource bounded measure. In *Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science*, volume 1046 of *Lecture Notes in Computer Science*, pages 13–24, Berlin, 1996. Springer-Verlag.

[10] H. Buhrman and E. Mayordomo. An excursion to the Kolmogorov random strings. In *Proceedings of the 10th IEEE Structure in Complexity Theory Conference*, pages 197–205, New York, 1995. IEEE.

[11] H. Buhrman, D. van Melkebeek, K. Regan, D. Sivakumar, and M. Straus. A generalization of resource-bounded measure, with an application. In *Proceedings of the 15th Symposium on Theoretical Aspects of Computer Science*, volume 1373 of *Lecture Notes in Computer Science*, pages 161–171, Berlin, 1998. Springer-Verlag.

[12] H. Heller. On relativized exponential and probabilistic complexity classes. *Information and Compuation*, 71:231–243, 1986.

[13] D. Juedes and J. Lutz. The complexity and distribution of hard problems. *SIAM Journal on Computing*, 24(2):279–295, 1995.

[14] L. Longpré. Personal communication, 1997.

[15] J. Lutz. Category and measure in complexity classes. *SIAM Journal on Computing*, 19(6):1100–1131, 1990.

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

[17] J. Lutz. A small span theorem for P/poly-Turing reductions. In *Proceedings of the 10th IEEE Structure in Complexity Theory Conference*, pages 324–330, New York, 1995. IEEE.

[18] J. Lutz. Observations on measure and lowness for Δ_2^P. In *Proceedings of the 13th Symposium on Theoretical Aspects of Computer Science*, volume 1046 of *Lecture Notes in Computer Science*, pages 87–97, Berlin, 1996. Springer-Verlag.

[19] J. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, 23:762–779, 1994.

[20] J. Lutz and E. Mayordomo. Cook versus Karp–Levin: Separating completeness notions if NP is not small. *Theoretical Computer Science*, 164:141–163, 1996.

[21] E. Mayordomo. Almost every set in exponential time is P-bi-immune. *Theoretical Computer Science*, 136:487–506, 1994.

[22] N. Nisan and A. Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49:149–167, 1994.

[23] Ch. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[24] K. Regan, D. Sivakumar, and J. Cai. Pseudorandom generators, measure theory, and natural proofs. In *Proceedings of the 36th IEEE Symposium on Foundations of Computer Science*, pages 26–35, New York, 1995. IEEE.