A Small Span Theorem for P/Poly-Turing Reductions *

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, Iowa 50011
lutz@iastate.edu

Abstract

This paper investigates the structure of ESPACE under nonuniform Turing reductions that are computed by polynomial-size circuits (P/Poly-Turing reductions). A Small Span Theorem is proven for such reductions. This result says that every language A in ESPACE satisfies at least one of the following two conditions.

(i) The lower P/Poly-Turing span of A (consisting of all languages that are P/Poly-Turing reducible to A) has measure 0 in ESPACE.

(ii) The upper P/Poly-Turing span of A (consisting of all languages to which A is P/Poly-Turing reducible) has pspace-measure 0, hence measure 0 in ESPACE.

The Small Span Theorem implies that every P/Poly-Turing degree has measure 0 in ESPACE, and that there exist languages that are weakly P-many-one complete, but not P/Poly-Turing complete for ESPACE.

The method of proof is a significant departure from earlier proofs of Small Span Theorems for weaker types of reductions.

*This work was supported in part by National Science Foundation Grant CCR-9157382, with matching funds from Rockwell International , Microware Systems Corporation, and Amoco Foundation.

1 Introduction

The measure-theoretic investigation of efficient reductions has recently yielded new insights concerning completeness phenomena. Such insights include the existence and distribution of weakly complete problems [12, 7, 3, 10], lower bounds on the density and complexity of weakly complete problems [15, 9, 8], upper bounds on the complexity and abundance of complete problems [9, 11, 2, 8, 17], and various consequences of the hypothesis that SAT is weakly complete for exponential time [16, 9, 15, 14].

A recurring tool and unifying theme of much of this work is the development of *Small Span Theorems* for various reducibilities and complexity classes. Briefly, given a reducibility $\leq_{\mathcal{R}}$ and a language $A \subseteq \{0,1\}^*$, the *lower* $\leq_{\mathcal{R}}$*-span* of A is the set of $\mathcal{R}(A)$, consisting of all languages that are $\leq_{\mathcal{R}}$-reducible to A; and the *upper* $\leq_{\mathcal{R}}$*-span* of A is the set $\mathcal{R}^{-1}(A)$, consisting of all languages to which A is $\leq_{\mathcal{R}}$-reducible. If $\mathcal{C}$ is a complexity class that has measure structure (in the sense of resource-bounded measure [13]), then the *Small Span Theorem for* $\leq_{\mathcal{R}}$*-reductions in* $\mathcal{C}$ is the assertion that, for all $A \in \mathcal{C}$, at least one of the spans $\mathcal{R}(A)$, $\mathcal{R}^{-1}(A)$ is negligibly small in $\mathcal{C}$. (Specifically, $\mathcal{R}(A)$ has measure 0 in $\mathcal{C}$, or $\mathcal{R}^{-1}(A)$ has Δ-measure 0, hence measure 0 in $\mathcal{C}$, where Δ is the resource bound that induces measure structure in $\mathcal{C}$. See section 2 for more detailed explanations of notation and terminology used in this introduction.)

The first Small Span Theorem, proven by Juedes and Lutz [9], was for $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions in the exponential time complexity class $\mathrm{E} = \mathrm{DTIME}(2^{\mathrm{linear}})$. This result says that, for every $A \in \mathrm{E}$, $\mathrm{P_m}(A)$ has measure 0 in E, or $\mathrm{P_m^{-1}}(A)$ has p-measure 0, hence measure 0 in E. An immediate consequence of this fact is that every $\leq_{\mathrm{m}}^{\mathrm{P}}$-degree — including the complete $\leq_{\mathrm{m}}^{\mathrm{P}}$-degrees for E, NP, PSPACE, etc. — has measure 0 in E. Juedes and Lutz [9] also proved the Small Span Theorem for $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions in the exponential time complexity class $\mathrm{E_2} = \mathrm{DTIME}(2^{\mathrm{polynomial}})$. Part of the interest in these results lies in the fact that $\mathrm{E_2}$ is the smallest deterministic time complexity class known to contain NP, BPP, PP, PH, PSPACE, and other important complexity classes.

The task now confronting us is to determine the extent to which Small Span Theorems hold for stronger types of efficient reductions. This task is important and nontrivial because it is closely related to some of the most fundamental questions of complexity theory. For example, Juedes and Lutz [9] have pointed out that a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P}}$-reductions in E or $\mathrm{E_2}$ would imply that $\mathrm{BPP} \subsetneq \mathrm{E_2}$. More recent work of Regan and Sivakumar [20] — building on the "natural proof" work of Razborov and Rudich [19] — indicates that a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions (nonuniform Turing reductions computed by polynomial-size circuits) in $\mathrm{E_2}$ would imply the nonexistence of pseudorandom generators and one-way functions with exponential nonuniform security. It is thus to be hoped that a systematic investigation of Small Span Theorems will shed useful light on such fundamental questions.

Some initial steps in this investigation have already been taken. Lindner [11] adapted the method of [9] to prove Small Span Theorems for $\leq_{1-\mathrm{tt}}^{\mathrm{P}}$-reductions in E and $\mathrm{E_2}$. Ambos-Spies, Neis, and Terwijn [2] used resource-bounded genericity to generalize the method of [9], thereby obtaining Small Span Theorems for $\leq_{k-\mathrm{tt}}^{\mathrm{P}}$-reductions in E and $\mathrm{E_2}$ for all positive integers k. More recently, Juedes and Lutz [8] have used a nonuniform extension of the method of [9] to prove the Small Span Theorem for $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions — nonuniform

many-one reductions that are computed by polynomial-size circuits — in the exponential space complexity class ESPACE = DSPACE(2^{linear}).

In the present paper, we prove the Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in ESPACE. As noted earlier, $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions are nonuniform Turing reductions that are computed by polynomial-size circuits. These reductions are "combinatorially efficient," even though they need not be algorithmically computable. As noted by Skyum and Valiant [21], the investigation of nonuniform reductions sheds light on the "purely combinatorial" aspects of the completeness phenomenon. More importantly, $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions are *adaptive*. In fact, the present result is the first instance of a Small Span Theorem for adaptive reductions.

Our result immediately implies that every $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-degree has measure 0 in ESPACE. It also implies (in combination with a result of Juedes [7] and Ambos-Spies, Terwijn, and Zheng [3]) that there are languages that are weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, but not $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-complete for ESPACE.

The proof of our result is a significant departure from the methods used in earlier proofs of Small Span Theorems for weaker, nonadaptive types of reductions. We are hopeful that this proof is a significant step toward a better understanding of the conditions under which Small Span Theorems hold for $\leq_{\mathrm{T}}^{\mathrm{P}}$-reductions and $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in E and E_2.

2 Preliminaries

We write $\{0,1\}^*$ for the set of all (finite, binary) *strings* and $\{0,1\}^\infty$ for the set of all (infinite, binary) *sequences*. Every *language* is a set $A \subseteq \{0,1\}^*$, so $\mathcal{P}(\{0,1\}^*)$ is the set of all languages.

We write $|x|$ for the length of a string x and $|S|$ for the cardinality of a set S. (Notation and context clearly distinguish strings from sets.) The *empty string*, λ, is the unique string of length 0. We write $\{0,1\}^n$ for the set of all strings of length n, $\{0,1\}^{\leq n}$ for the set of all strings of length at most n, and $\{0,1\}^{<n}$ for the set of all strings of length less than n. The *standard enumeration* of $\{0,1\}^*$ is the sequence $s_0 = \lambda$, $s_1 = 0$, $s_2 = 1$, $s_3 = 00$, ..., ordered first by length and then lexicographically.

The *Boolean value* of a condition φ is $[\![\varphi]\!] =$ **if** φ **then** 1 **else** 0. For $z \in \{0,1\}^\infty$ and $n \in \mathbf{N}$, the n^{th} *bit* of z is $z[n]$, and the n*-bit prefix* of z is $z[0..n-1]$. We identify each language $A \subseteq \{0,1\}^*$ with its *characteristic sequence* $\chi_A \in \{0,1\}^\infty$ defined by $\chi_A[n] = [\![s_n \in A]\!]$ for all $n \in \mathbf{N}$.

The *cylinder generated by* a string $w \in \{0,1\}^*$ is the set $\mathbf{C}_w = \{A \subseteq \{0,1\}^* \mid w = \chi_A[0..|w|-1]\}$, i.e., the set of all languages A such that w is a prefix of χ_A. The *complement* of a set X of languages is $X^c = \mathcal{P}(\{0,1\}^*) - X$.

Our proof of the Small Span Theorem uses the following theorem of probability theory.

Lemma 2.1 (Large Deviation Lemma — Ajtai and Fagin [1]). Let $c = \frac{1}{864}$, let $b_0, \ldots, b_{n-1}$ be 0/1 - valued random variables, and let $N(n) = |\{i | 0 \leq i < n \text{ and } b_i = 1\}|$. Assume that, for all $0 \leq i < n$ and all $u \in \{0,1\}^i$, $\Pr[b_i = 1 | b_0, \ldots, b_{i-1} = u] \geq \frac{1}{2}$. (If $i = 0$, this says that $\Pr[b_0 = 1] \geq \frac{1}{2}$.) Then $\Pr[N(n) \leq \frac{11n}{24}] < e^{-cn}$.

Note that Lemma 2.1 does *not* require the random variables $b_0, \ldots, b_{n-1}$ to be independent.

Following standard usage, we let Poly denote the set of all polynomially bounded advice functions $h : \mathbf{N} \to \{0,1\}^*$. If A and B are languages, then A is $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-*reducible* to B, and we write $A \leq_{\mathrm{m}}^{\mathrm{P/Poly}} B$, if there exist $f \in \mathrm{PF}$ and $h \in \mathrm{Poly}$ such that

$$A = \{x \in \{0,1\}^* \mid f(\langle x, h(|x|)\rangle) \in B\},$$

where $\langle , \rangle : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ is a standard pairing function.

Fix a standard enumeration $M_0, M_1, M_2, \ldots$ of polynomial time-bounded oracle Turing machines. For $k \in \mathbf{N}$, $B \subseteq \{0,1\}^*$, and h an advice function, the *language accepted by* M_k *with oracle* B and advice h is the language

$$L(M_k^B/h) = \{x \in \{0,1\}^* \mid M_k^B \text{ accepts } \langle x, h(|x|)\rangle\}.$$

If A and B are languages, then A is $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-*reducible* to B, and we write $A \leq_{\mathrm{T}}^{\mathrm{P/Poly}} B$, if there exist $k \in \mathbf{N}$ and $h \in \mathrm{Poly}$ such that $A = L(M_k^B/h)$. Using standard techniques [18], it is easy to see that the $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions (respectively, the $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions) are precisely those Turing reductions (respectively, many-one reductions) that are computed by polynomial-size circuits.

We very briefly review the fragment of resource-bounded measure that is used in this paper. The reader is referred to [13, 12] for motivation and details.

A *martingale* is a function $d : \{0,1\}^* \to [0,\infty)$ such that, for all $w \in \{0,1\}^*$,

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

A martingale d *succeeds* on a language $A \subseteq \{0,1\}^*$ if

$$\limsup_{n\to\infty} d(\chi_A[0..n-1]) = \infty.$$

The *success set* of a martingale d is

$$S^\infty[d] = \{A \subseteq \{0,1\}^* \mid d \text{ succeeds on } A\}.$$

The *unitary success set* of a martingale d is

$$S^1[d] = \bigcup_{d(w)\geq 1} \mathbf{C}_w.$$

A martingale d is pspace-*computable* if there is a function $\widehat{d} : \mathbf{N} \times \{0,1\}^* \to \mathbf{Q}$ such that $\widehat{d}(r,w)$ is computable in space polynomial in $r + |w|$ and, for all $r \in \mathbf{N}$ and $w \in \{0,1\}^*$, $|\widehat{d}(r,w) - d(w)| \leq 2^{-r}$.

Definition. Let X be a set of languages, and let X^c denote the complement of X.

1. X has pspace-*measure 0*, and we write $\mu_{\mathrm{pspace}}(X) = 0$, if there is a pspace-computable martingale d such that $X \subseteq S^\infty[d]$.

2. X has pspace-*measure 1*, and we write $\mu_{\mathrm{pspace}}(X) = 1$, if $\mu_{\mathrm{pspace}}(X^c) = 0$.

3. X has *measure 0 in* ESPACE, and we write $\mu(X \mid \mathrm{ESPACE}) = 0$, if $\mu_{\mathrm{pspace}}(X \cap \mathrm{ESPACE}) = 0$.

4. X has *measure 1 in* ESPACE, and we write $\mu(X \mid \mathrm{ESPACE}) = 1$, if $\mu(X^c \mid \mathrm{ESPACE}) = 0$. In this case, we say that X contains *almost every* element of ESPACE.

For each $k \in \mathbf{N}$, let $\sum_{j=0}^{\infty} a_{k,j}$ be a series of nonnegative real numbers. Then the series $\sum_{j=0}^{\infty} a_{k,j}$, for $k \in \mathbf{N}$, are *uniformly* p-*convergent* if there is a polynomial q such that, for all $k, r \in \mathbf{N}$, $\sum_{j=q(k,r)}^{\infty} a_{k,j} \leq 2^{-r}$.

Our proof of the Small Span Theorem uses the following uniform, polynomial space version of the classical first Borel-Cantelli lemma.

Theorem 2.2 (Lutz [13]). Assume that $d : \mathbf{N} \times \mathbf{N} \times \{0,1\}^* \to \mathbf{Q} \cap [0, \infty)$ is a function with the following properties.

(i) For each $k, j \in \mathbf{N}$, the function $d_{k,j}$, defined by $d_{k,j}(w) = d(k, j, w)$, is a martingale.

(ii) There is an algorithm that, for all $k, j \in \mathbf{N}$ and $w \in \{0,1\}^*$, computes $d_{k,j}(w)$ in space polynomial in $k + j + |w|$.

(iii) The series $\sum_{j=0}^{\infty} d_{k,j}(\lambda)$, for $k \in \mathbf{N}$, are uniformly p-convergent.

Then

$$\mu_{\mathrm{pspace}}(\bigcup_{k=0}^{\infty} \bigcap_{j=0}^{\infty} \bigcup_{i=j}^{\infty} S^1[d_{k,i}]) = 0.$$

Given a reducibility $\leq_{\mathcal{R}}$ and a language A, the *lower* $\leq_{\mathcal{R}}$-*span* $\mathcal{R}(A)$ and the *upper* $\leq_{\mathcal{R}}$-*span* $\mathcal{R}^{-1}(A)$ are defined as in the introduction. The $\leq_{\mathcal{R}}$-*degree* of A is then $\deg_{\mathcal{R}}(A) = \mathcal{R}(A) \cap \mathcal{R}^{-1}(A)$. A language is *weakly* $\leq_{\mathcal{R}}$-*hard* for ESPACE if $\mu(\mathcal{R}(A)|\mathrm{ESPACE}) \neq 0$. (This is the negation of the condition $\mu(\mathcal{R}(A) \mid \mathrm{ESPACE}) = 0$. It does *not* imply that "$\mu(\mathcal{R}(A) \mid \mathrm{ESPACE})$" has some nonzero value.) A language A is *weakly* $\leq_{\mathcal{R}}$-*complete* for ESPACE if $A \in \mathrm{ESPACE}$ and A is weakly $\leq_{\mathcal{R}}$-hard for ESPACE.

3 Small Span Theorem

This section is devoted to proving and exploiting our main result, the Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in ESPACE. Our proof uses a probability measure on a specialized class ADV of advice functions. We now describe this class and its probability measure.

Let ADV be the class of all advice functions $h : \mathbf{N} \to \{0,1\}^*$ satisfying $|h(n)| = a(n)$ for all $n \in \mathbf{N}$, where the function $a : \mathbf{N} \to \mathbf{N}$ is defined by

$$\begin{aligned} a(n) &= b(n+1) - b(n), \\ b(n) &= n^{1+\log(1+n)}. \end{aligned}$$

(Elements of ADV will be called $a(n)$-advice functions.) Note that, for all $n \in \mathbf{N}$,

$$\sum_{m=0}^{n-1} a(m) = b(n).$$

Also, for every polynomial $q(n)$, $q(n) = o(a(n))$. In fact, it is easy to see that, for all $A, B \subseteq \{0,1\}^*$ satisfying $A \leq_{\mathrm{T}}^{\mathrm{P/Poly}} B$, there exist $k \in \mathbf{N}$ and $h \in \mathrm{ADV}$ such that

$$A = L(M_k^B/h),$$

where M_k is the k^{th} polynomial time-bounded oracle Turing machine.

We now specify a probability measure on the set ADV. Define a *partial $a(n)$-advice function* to be a finite function

$$h' : \{0, 1, \ldots, k-1\} \to \{0,1\}^*$$

such that $k \in \mathbf{N}$ and, for all $0 \leq n < k$, $|h'(n)| = a(n)$. For each partial $a(n)$-advice function h', define the *cylinder generated by h'* to be

$$\mathrm{CYL}(h') = \{h \in \mathrm{ADV} \mid h\restriction\{0, 1, \ldots, k-1\} = h'\},$$

where $h\restriction\{0,1,\ldots k-1\}$ denotes the restriction of h to the set $\{0,1,\ldots k-1\}$. The *probability* of this cylinder in the sample space ADV is defined to be

$$\Pr(\mathrm{CYL}(h')) = \prod_{n=0}^{k-1} 2^{-a(n)}.$$

This probability measure is then extended to a complete probability measure on ADV in the usual way [6, 4].

In the proof of the following theorem, we work in the sample space

$$\Omega = \mathrm{ADV} \times \mathcal{P}(\{0,1\}^*)$$

with the product probability measure, where probability on ADV is defined as above and we use the uniform distribution on $\mathcal{P}(\{0,1\}^*)$. Intuitively, an element $(h, B) \in \Omega$ is chosen probabilistically by performing the following two random experiments independently of one another.

(i) For each $n \in \mathbf{N}$ (independently), choose $h(n) \in \{0,1\}^{a(n)}$ according to the uniform distribution.

(ii) For each $x \in \{0,1\}^*$ (independently), toss a fair coin to decide whether $x \in B$.

The following result contains most of the technical content of the Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in ESPACE. It says that almost every element of ESPACE has a very small upper $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-span. The proof is a nonuniform, space-bounded extension of a technique used by Fenner, Lutz, and Mayordomo [5] in the investigation of computational depth.

Theorem 3.1. For almost every $A \in \mathrm{ESPACE}$,

$$\mu_{\mathrm{pspace}}((\mathrm{P/Poly})_{\mathrm{T}}^{-1}(A)) = 0.$$

Proof. For each $k, j \in \mathbf{N}$ and $A \subseteq \{0,1\}^*$, define the event $\mathcal{E}_{k,j}^A \subseteq \Omega$ by

$$\mathcal{E}_{k,j}^A = \{(h, B) \mid (\forall 0 \leq i < j)[\![s_i \in A]\!] = [\![s_i \in L(M_k^B/h)]\!]\}.$$

For each $A \subseteq \{0,1\}^*$, define a function $d^A : \{0,1\}^* \to [0, \infty)$ by

$$d^A(w) = \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} 2^{-\frac{k+j}{4}} d_{k,j}^A(w),$$

where, for all $k, j \in \mathbf{N}$ and $w \in \{0,1\}^*$,

$$d_{k,j}^A(w) = \begin{cases} 2^{|w|} \Pr(\mathrm{ADV} \times \mathbf{C}_w \mid \mathcal{E}_{k,j}^A) & \text{if } \Pr(\mathcal{E}_{k,j}^A) > 0 \\ 1 & \text{if } \Pr(\mathcal{E}_{k,j}^A) = 0. \end{cases}$$

It is routine to check that each d^A is a martingale that is, by depth-first-search on answers to oracle queries, pspace-computable if $A \in \mathrm{ESPACE}$.

For each $k, j \in \mathbf{N}$ and $A \subseteq \{0,1\}^*$, let

$$N_A(k, j) = |\{i < j \mid \Pr(\mathcal{E}_{k,i+1}^A) \leq \frac{1}{2} \Pr(\mathcal{E}_{k,i}^A)\}|.$$

Let

$$X = \{A \subseteq \{0,1\}^* \mid \text{ for all } k \in \mathbf{N}, \text{for all but finitely many } j \in \mathbf{N}, N_A(k, j) > \frac{j}{3}\}.$$

The following four claims are proven at the end of this proof.

Claim 1. For all $k, j \in \mathbf{N}$ and $A \subseteq \{0,1\}^*$,

$$\Pr(\mathcal{E}_{k,j}^A) \leq 2^{-N_A(k,j)}.$$

Claim 2. For all $k, j \in \mathbf{N}$, all $A, B \subseteq \{0,1\}^*$, and all $h \in \mathrm{ADV}$, if $A = L(M_k^B/h)$, then

$$\liminf_{l \to \infty} d_{k,j}^A(\chi_B[0..l-1]) \geq 2^{N_A(k,j) - b(n(j))},$$

where $n(j) = \lceil \log(j+1) \rceil$.

Claim 3. For all $A \in X$, $(\mathrm{P/Poly})_{\mathrm{T}}^{-1}(A) \subseteq S^{\infty}[d^A]$.

Claim 4. $\mu_{\mathrm{pspace}}(X) = 1$.

Let

$$Y = \{A \subseteq \{0,1\}^* \mid \mu_{\mathrm{pspace}}((\mathrm{P/Poly})_{\mathrm{T}}^{-1}(A)) = 0\}.$$

By Claim 3 and the fact that d^A is pspace-computable when $A \in \mathrm{ESPACE}$, we have $X \cap \mathrm{ESPACE} \subseteq Y$. It follows that $Y^c \cap \mathrm{ESPACE} \subseteq X^c$, whence Claim 4 tells us that

$$0 \leq \mu(Y^c \mid \mathrm{ESPACE}) = \mu_{\mathrm{pspace}}(Y^c \cap \mathrm{ESPACE}) \leq \mu_{\mathrm{pspace}}(X^c) = 0,$$

i.e., that $\mu(Y \mid \mathrm{ESPACE}) = 1$. This proves Theorem 3.1. □

Proof of Claim 1. This follows immediately from the definition of $N_A(k,j)$ and the fact that, for all $k, j \in \mathbf{N}$ and $A \subseteq \{0,1\}^*$, $\mathcal{E}^A_{k,j+1} \subseteq \mathcal{E}^A_{k,j}$. □

Proof of Claim 2. Assume the hypothesis. Since $A = L(M^B_k/h)$, we have $(h,B) \in \mathcal{E}^A_{k,j}$, so $\Pr(\mathcal{E}^A_{k,j}) > 0$. Let $l \in \mathbf{N}$ be large enough that, for all $0 \leq i < j$, all queries of $(M^B_k/h)(s_i)$ are among $s_0, s_1, \cdots, s_{l-1}$. That is, l is large enough that $(M^B_k/h)(s_0), \cdots, (M^B_k/h)(s_{l-1})$ are determined by the l-bit prefix $w_l = \chi_B[0..l-1]$ of B.

Let $h_j = h\restriction\{0,1,\ldots,n(j)-1\}$. Note that $n(j)$ is the least n such that $\{s_0,\ldots,s_{j-1}\} \subseteq \{0,1\}^{<n}$, so h_j is the smallest partial $a(n)$-advice function that is a restriction of h and provides advice for all the inputs $s_0,\ldots,s_{j-1}$. In particular, since $A = L(M^B_k/h)$, it follows that $\mathrm{CYL}(h_j) \times \mathbf{C}_{w_l} \subseteq \mathcal{E}^A_{k,j}$, whence

$$\begin{aligned}
\Pr(\mathcal{E}^A_{k,j} | \mathrm{ADV} \times \mathbf{C}_{w_l}) &\geq \Pr(\mathrm{CYL}(h_j) \times \mathbf{C}_{w_l} | \mathrm{ADV} \times \mathbf{C}_{w_l}) \\
&= \Pr(\mathrm{CYL}(h_j)) \\
&= \prod_{n=0}^{n(j)-1} 2^{-a(n)} \\
&= 2^{-\sum_{n=0}^{n(j)-1} a(n)} \\
&= 2^{-b(n(j))}.
\end{aligned}$$

It follows that

$$\begin{aligned}
d^A_{k,n}(w_l) &= 2^{|w_l|} \Pr(\mathrm{ADV} \times \mathbf{C}_{w_l} | \mathcal{E}^A_{k,j}) \\
&= 2^{|w_l|} \frac{\Pr(\mathrm{ADV} \times \mathbf{C}_{w_l}) \Pr(\mathcal{E}^A_{k,j} | \mathrm{ADV} \times \mathbf{C}_{w_l})}{\Pr(\mathcal{E}^A_{k,j})} \\
&= \frac{\Pr(\mathcal{E}^A_{k,j} | \mathrm{ADV} \times \mathbf{C}_{w_l})}{\Pr(\mathcal{E}^A_{k,j})} \\
&\geq \frac{2^{-b(n(j))}}{\Pr(\mathcal{E}^A_{k,j})} \\
&\geq 2^{N_A(k,j) - b(n(j))}
\end{aligned}$$

by Claim 1. □

Proof of Claim 3. Assume that $A \in X$, and let $B \in (\mathrm{P/Poly})^{-1}_{\mathrm{T}}(A)$. Fix $k \in \mathbf{N}$ and $h \in \mathrm{ADV}$ such that $A = L(M^B_k/h)$. Then, writing $w_l = \chi_B[0..l-1]$, Claim 2 tells us that

$$\limsup_{l\to\infty} d^A(w_l) \geq \limsup_{l\to\infty} \sum_{j=0}^{\infty} 2^{-\frac{k+j}{4}} d^A_{k,j}(w_l)$$

$$\geq \sum_{j=0}^{\infty} 2^{-\frac{k+j}{4}} \liminf_{l\to\infty} d_{k,j}^{A}(w_l)$$
$$\geq \sum_{j=0}^{\infty} 2^{N_A(k,n)-b(n(j))-\frac{k+j}{4}}.$$

Since $A \in X$, we have $N_A(k,n) - b(n(j)) > \frac{j}{4}$ for all but finitely many $j \in \mathbf{N}$. Thus there is a constant $c \in \mathbf{N}$ such that

$$\limsup_{l\to\infty} d^A(w_l) \geq -c + \sum_{j=0}^{\infty} 2^{-\frac{k}{4}} = \infty.$$

Thus $B \in S^{\infty}[d^A]$. □

Proof of Claim 4. For each $k, j \in \mathbf{N}$, let

$$Z_{k,j} = \{A \subseteq \{0,1\}^* | N_A(k,j) \leq \frac{j}{3}\}.$$

Define

$$d : \mathbf{N} \times \mathbf{N} \times \{0,1\}^* \to [0,\infty)$$

by

$$d_{k,j}(w) = \Pr(Z_{k,j} | \mathbf{C}_w)$$

for all $k, j \in \mathbf{N}$ and $w \in \{0,1\}^*$. It is easy to check that d satisfies conditions (i) and (ii) of Theorem 2.2.

By the Large Deviation Lemma (Lemma 2.1) for each $k, j \in \mathbf{N}$,

$$d_{k,j}(\lambda) = \Pr(Z_{k,j}) \leq \Pr[N_A(k,j) \leq \frac{11j}{24}] < e^{-cj},$$

where $c = \frac{1}{864}$. Thus the series $\sum_{j=0}^{\infty} d_{k,j}(\lambda)$, for $k \in \mathbf{N}$, are uniformly p-convergent.

For all $k, j \in \mathbf{N}$ and $A \in Z_{k,j}$, it is clear that, for all sufficiently large l, $d_{k,j}(\chi_A[0..l-1]) = 1$. Thus, for all $k, j \in \mathbf{N}$, $Z_{k,j} \subseteq S^1[d_{k,j}]$

The preceding two paragraphs, together with the uniform, pspace first Borel-Cantelli lemma (Theorem 2.2), tell us that

$$\mu_{\text{pspace}}(X^c) = \mu_{\text{pspace}}(\bigcup_{k=0}^{\infty} \bigcap_{j=0}^{\infty} \bigcup_{i=j}^{\infty} Z_{k,i}) = 0,$$

whence $\mu_{\text{pspace}}(X) = 1$. □

Our main result is now easily proven.

Theorem 3.2 (Small Span Theorem). For every $A \in \text{ESPACE}$,

$$\mu((\text{P/Poly})_{\text{T}}(A) \mid \text{ESPACE}) = 0$$

or

$$\mu_{\text{pspace}}((\text{P/Poly})_{\text{T}}^{-1}(A)) = \mu((\text{P/Poly})_{\text{T}}^{-1}(A) \mid \text{ESPACE}) = 0.$$

Proof. Let $A \in \text{ESPACE}$, and let

$$X = \{B \subseteq \{0,1\}^* \mid \mu_{\text{pspace}}((\text{P/Poly})_{\text{T}}^{-1}(B)) = 0\}.$$

We have two cases.

Case I. If $(\mathrm{P/Poly})_{\mathrm{T}}(A) \cap X \cap \mathrm{ESPACE} = \emptyset$, then Theorem 3.1 tells us that

$$\mu((\mathrm{P/Poly})_{\mathrm{T}}(A) \mid \mathrm{ESPACE}) = 0.$$

Case II. If $(\mathrm{P/Poly})_{\mathrm{T}}(A) \cap X \cap \mathrm{ESPACE} \neq \emptyset$, then fix a language $B \in (\mathrm{P/Poly})_{\mathrm{T}}(A) \cap X$. Then $\mu_{\mathrm{pspace}}((\mathrm{P/Poly})_{\mathrm{T}}^{-1}(B)) = 0$ and $(\mathrm{P/Poly})_{\mathrm{T}}^{-1}(A) \subseteq (\mathrm{P/Poly})_{\mathrm{T}}^{-1}(B)$, so

$$\mu_{\mathrm{pspace}}((\mathrm{P/Poly})_{\mathrm{T}}^{-1}(A)) = \mu((\mathrm{P/Poly})_{\mathrm{T}}^{-1}(A) \mid \mathrm{ESPACE}) = 0.$$

□

We conclude this section with some consequences of the Small Span Theorem. Let $\mathcal{H}_{\mathrm{T}}^{\mathrm{P/Poly}}(\mathrm{ESPACE})$ and $\mathcal{C}_{\mathrm{T}}^{\mathrm{P/Poly}}(\mathrm{ESPACE})$ denote the sets of languages that are $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-hard and $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-complete, respectively, for ESPACE. We first show that the set of $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-hard languages for ESPACE is very small.

Theorem 3.3. $\mu_{\mathrm{pspace}}(\mathcal{H}_{\mathrm{T}}^{\mathrm{P/Poly}}(\mathrm{ESPACE})) = 0$.

Proof. Fix a language C that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE. Then $\mathrm{ESPACE} \subseteq \mathrm{P}_{\mathrm{m}}(C) \subseteq (\mathrm{P/Poly})_{\mathrm{T}}(C)$, so $\mu((\mathrm{P/Poly})_{\mathrm{T}}(C) \mid \mathrm{ESPACE}) \neq 0$. Hence, the Small Span Theorem tells us that $\mu_{\mathrm{pspace}}((\mathrm{P/Poly})_{\mathrm{T}}^{-1}(C)) = 0$. Since $\mathcal{H}_{\mathrm{T}}^{\mathrm{P/Poly}}(\mathrm{ESPACE}) \subseteq (\mathrm{P/Poly})_{\mathrm{T}}^{-1}(C)$, it follows that $\mu_{\mathrm{pspace}}(\mathcal{H}_{\mathrm{T}}^{\mathrm{P/Poly}}(\mathrm{ESPACE})) = 0$. □

Corollary 3.4. $\mu(\mathcal{C}_{\mathrm{T}}^{\mathrm{P/Poly}}(\mathrm{ESPACE}) \mid \mathrm{ESPACE}) = 0$. □

Theorem 3.2, Theorem 3.3, and Corollary 3.4 generalize the corresponding results for $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions, proven by Juedes and Lutz [8]. Corollary 3.4 also generalizes Mayordomo's proof [17] that the set of all $\leq_{\mathrm{tt}}^{\mathrm{P}}$-complete languages for ESPACE has measure 0 in ESPACE.

The method of Ambos-Spies, Terwijn, and Zheng [3] can be modified in a straightforward way to show that, in contrast with Theorem 3.3 and Corollary 3.4, almost every language in ESPACE is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE. We thus have the following.

Corollary 3.5. Almost every language in ESPACE is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, but not $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-complete, for ESPACE. □

We next show that every $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-degree has measure 0 in ESPACE.

Theorem 3.6. For all $A \subseteq \{0,1\}^*$,

$$\mu(\deg_{\mathrm{T}}^{\mathrm{P/Poly}}(A) \mid \mathrm{ESPACE}) = 0.$$

Proof. Let $A \subseteq \{0,1\}^*$. If $\deg_{\mathrm{T}}^{\mathrm{P/Poly}}(A) \cap \mathrm{ESPACE} = \emptyset$, the theorem is clearly affirmed, so assume that $\deg_{\mathrm{T}}^{\mathrm{P/Poly}}(A) \cap \mathrm{ESPACE} \neq \emptyset$, and fix $B \in \deg_{\mathrm{T}}^{\mathrm{P/Poly}}(A) \cap \mathrm{ESPACE}$. Then, by the Small Span Theorem, we have

$$\mu((\mathrm{P/Poly})_{\mathrm{T}}(B) \mid \mathrm{ESPACE}) = 0$$

or

$$\mu((\mathrm{P/Poly})_{\mathrm{T}}^{-1}(B) \mid \mathrm{ESPACE}) = 0.$$

Either of these alternatives implies that $\mu(\deg_{\mathrm{T}}^{\mathrm{P/Poly}}(B) \mid \mathrm{ESPACE}) = 0$. Since $\deg_{\mathrm{T}}^{\mathrm{P/Poly}}(A) = \deg_{\mathrm{T}}^{\mathrm{P/Poly}}(B)$, this completes the proof. □

Theorem 3.6 generalizes the previously known facts that P/Poly has measure 0 in ESPACE [13] and every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-degree has measure 0 in ESPACE [8].

4 Conclusion

The most important problems arising from this work are to determine whether Small Span Theorems hold for $\leq_{\mathrm{T}}^{\mathrm{P}}$-reductions or $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in the exponential-time complexity classes E and E_2. As noted in the introduction, these problems are closely related to fundamental questions of complexity theory, so they may be very difficult. More modest, but nevertheless useful, objectives, would be to (i) investigate whether the work of Ambos-Spies, Neis, and Terwijn [2] can be extended to obtain Small Span Theorems for unbounded query reductions in E and E_2; and (ii) find complexity-theoretic characterizations of the Small Span Theorems for $\leq_{\mathrm{T}}^{\mathrm{P}}$-reductions and $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in E and E_2.

There is also an interesting open problem concerning the complexity of $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-complete problems for ESPACE. Juedes and Lutz [8] showed that every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-complete language for ESPACE obeys upper bounds on nonuniform complexity (space-bounded Kolmogorov complexity and size of nonuniform complexity cores) that are violated by almost every language in ESPACE, i.e., that the $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-complete languages for ESPACE are *unusually simple* elements of ESPACE. Similar results hold for $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages for E and E_2 [9]. However, it remains an open problem whether there is a natural sense in which the $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-complete languages for ESPACE are unusually simple elements of ESPACE.

Acknowledgments. I thank David Juedes and Elvira Mayordomo for useful conversations.

References

[1] M. Ajtai and R. Fagin, Reachability is harder for directed than for undirected graphs, *Journal of Symbolic Logic* **55** (1990), pp. 113–150.

[2] K. Ambos-Spies, C. Neis, and S. A. Terwijn, Genericity and measure for exponential time, *Proceedings of the* 19^{th} *Symposium on Mathematical Foundations of Computer Science*, 1994. Springer–Verlag.

[3] K. Ambos-Spies, S. A. Terwijn, and Zheng Xizhong, Resource bounded randomness and weakly complete problems, *Proceedings of the Fifth Annual International Symposium on Algorithms and Computation*, 1994, pp. 369–377. Springer–Verlag.

[4] P. Billingsley, *Probability and Measure,* second edition, John Wiley and Sons, New York, 1986.

[5] S. A. Fenner, J. H. Lutz, and E. Mayordomo, Weakly useful sequences, submitted, 1994.

[6] P. R. Halmos, *Measure Theory*, Springer-Verlag, New York, 1950.

[7] D. W. Juedes, Weakly complete problems are not rare, submitted, 1994.

[8] D. W. Juedes and J. H. Lutz, Completeness and weak completeness under polynomial-size circuits, *Proceedings of the Twelfth Symposium on Theoretical Aspects of Computer Science*, 1995. Springer–Verlag, to appear.

[9] D. W. Juedes and J. H. Lutz, The complexity and distribution of hard problems, *SIAM Journal on Computing* **24** (1995), to appear. See also *Proceedings of the* 34^{th} *IEEE Symposium on Foundations of Computer Science* , Palo Alto, CA, 1993, pp. 177–185. IEEE Computer Society Press.

[10] D. W. Juedes and J. H. Lutz, Weak completeness in E and E_2, *Theoretical Computer Science* (1995), to appear.

[11] W. Lindner, On the polynomial time bounded measure of one-truth-table degrees and p-selectivity, Diplomarbeit, Technische Universität Berlin, 1993.

[12] J. H. Lutz, Weakly hard problems, *SIAM Journal on Computing*, to appear. See also *Proceedings of the Ninth Structure in Complexity Theory Conference*, 1994, pp. 146–161. IEEE Computer Society Press.

[13] J. H. Lutz, Almost everywhere high nonuniform complexity, *Journal of Computer and System Sciences* **44** (1992), pp. 220–258.

[14] J. H. Lutz and E. Mayordomo, Cook versus Karp-Levin: Separating completeness notions if NP is not small, *Theoretical Computer Science*, to appear. See also *Proceedings of the Eleventh Symposium on Theoretical Aspects of Computer Science*, Springer–Verlag, 1994, pp. 415–426.

[15] J. H. Lutz and E. Mayordomo, Measure, stochasticity, and the density of hard languages, *SIAM Journal on Computing* **23** (1994), pp. 762–779.

[16] E. Mayordomo, Almost every set in exponential time is P-bi-immune, *Theoretical Computer Science*, to appear. Also in *Seventeenth International Symposium on Mathematical Foundations of Computer Science*, 1992, pp. 392–400, Springer-Verlag.

[17] E. Mayordomo, *Contributions to the study of resource-bounded measure*, PhD thesis, Universitat Politècnica de Catalunya, 1994.

[18] N. Pippenger, On simultaneous resource bounds, *Proceedings of the* 20^{th} *IEEE Symposium on Foundations of Computer Science*, 1979, pp. 307–311.

[19] A. Razborov and S. Rudich, Natural proofs, *Proceedings of the* 26^{th} *ACM Symposium on Theory of Computing*, 1994, pp. 204–214.

[20] K. W. Regan and D. Sivakumar, On resource-bounded measure and pseudorandom generators, manuscript, 1994.

[21] S. Skyum and L. G. Valiant, A complexity theory based on boolean algebra, *Journal of the ACM* **32** (1985), pp. 484–502.