Completeness and Weak Completeness under Polynomial-Size Circuits *

David W. Juedes
School of Electrical Engineering and Computer Science
Ohio University
Athens, Ohio 45701
U.S.A.

Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, Iowa 50011
U.S.A.

Abstract

This paper investigates the distribution and nonuniform complexity of problems that are complete or weakly complete for ESPACE under nonuniform reductions that are computed by polynomial-size circuits (P/Poly-Turing reductions and P/Poly-many-one reductions). A tight, exponential lower bound on the space-bounded Kolmogorov complexities of weakly P/Poly-Turing-complete problems is established. A Small Span Theorem for P/Poly-Turing reductions in ESPACE is proven and used to show that *every* P/Poly-Turing degree — including the complete degree — has measure 0 in ESPACE. (In contrast, it is known that almost every element of ESPACE is weakly P-many-one complete.) Every weakly P/Poly-many-one-complete problem is shown to have a dense, exponential, nonuniform complexity core. More importantly, the P/Poly-many-one-complete problems are shown to be *unusually simple* elements of ESPACE, in the sense that they obey nontrivial *upper* bounds on nonuniform complexity (size of nonuniform complexity cores and space-bounded Kolmogorov complexity) that are violated by almost every element of ESPACE.

1 Introduction

The most prominent structural aspect of a complexity class is the presence or absence of complete problems under efficient reductions. A complete problem, when it is present, contains complete information about all problems in the class, and this information is organized in such a way as to be accessible by efficient reductions.

A measure-theoretic generalization of completeness, called *weak completeness*, was proposed by Lutz [36] and has recently been a subject of several investigations [26, 42, 41, 39, 25, 6, 27, 24, 45]. Briefly, if $\leq_{\mathcal{R}}$ is an efficient reducibility and $\mathcal{C}$ is a complexity class, then a *weakly* $\leq_{\mathcal{R}}$*-complete* problem for $\mathcal{C}$ is a decision problem (i.e., language) $C \subseteq \{0,1\}^*$ such that $C \in \mathcal{C}$ and all the problems in

*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.

a non-measure 0 subset of $\mathcal{C}$ (in the sense of resource-bounded measure [38, 40]) are $\leq_{\mathcal{R}}$-reducible to $\mathcal{C}$. That is, a problem $C \in \mathcal{C}$ is weakly $\leq_{\mathcal{R}}$-complete for $\mathcal{C}$ if C contains complete information about all the problems in a non-negligible subset of $\mathcal{C}$, and this information is organized in such a way as to be accessible by $\leq_{\mathcal{R}}$-reductions. For classes such as $\mathrm{E} = \mathrm{DTIME}(2^{\mathrm{linear}})$, $\mathrm{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$, and $\mathrm{ESPACE} = \mathrm{DSPACE}(2^{\mathrm{linear}})$, that have well-understood measure structure, Lutz [39] has shown that weak $\leq_{\mathrm{m}}^{\mathrm{P}}$-completeness is a proper generalization of $\leq_{\mathrm{m}}^{\mathrm{P}}$-completeness. (See sections 2 and 3 for precise definitions of notation and terminology used in this introduction.)

Juedes and Lutz [26] began the systematic investigation of the complexity and distribution of problems that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete or weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for the exponential time complexity classes E and E_2. Main results of [26] (in the case of E) include

(i) a proof that every weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete problem for E has a dense exponential complexity core;

(ii) a proof that almost every problem in E has $\{0,1\}^*$ as an exponential complexity core;

(iii) a proof that (essentially) every exponential complexity core of every $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete problem for E has a dense complement, whence by (ii) the set $\mathcal{C}_{\mathrm{m}}^{\mathrm{P}}(\mathrm{E})$, consisting of all problems that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for E, has measure 0 in E; and

(iv) a Small Span Theorem, which implies (among other things) that *every* $\leq_{\mathrm{m}}^{\mathrm{P}}$-degree has measure 0 in E.

In the present paper, we conduct a similar investigation, but we now focus on nonuniform reductions that are computed by polynomial-size circuits. Such reductions are "combinatorially efficient," even though they need not be algorithmically computable. As noted by Skyum and Valiant [54], the investigation of such reductions sheds light on the "purely combinatorial" aspects of the completeness phenomenon.

We work in the complexity class ESPACE. There are two related reasons for this choice. First, ESPACE has a rich, well-behaved structure that is well enough understood that we can prove absolute results, unblemished by oracles or unproven hypotheses. In particular, much is known about the Kolmogorov complexities and circuit-size complexities of languages in ESPACE[28, 38], while little is known at lower complexity levels. For example, ESPACE is not contained in P/Poly [28], but the relationships among NP, E, and P/Poly are not known. Our second reason for this choice is that the structure of ESPACE is closely related to the structure of important polynomial complexity classes. For example, Hartmanis and Yesha [21] have shown that

$$\mathrm{E} \subsetneqq \mathrm{ESPACE} \iff \mathrm{P} \subsetneqq \mathrm{P/Poly} \cap \mathrm{PSPACE}. \tag{1.1}$$

This, together with the first reason, suggests that the separation of P from PSPACE might best be achieved by separating E from ESPACE. We thus seek a detailed, quantitative account of the nonuniform structure of ESPACE.

We work with two types of nonuniform reductions. These are the P/Poly-Turing reductions ($\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions) and the P/Poly-many-one reductions ($\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions). These are natural nonuniform extensions of the polynomial-time Turing reductions ($\leq_{\mathrm{T}}^{\mathrm{P}}$-reductions, introduced by Cook [14]) and the polynomial-time many-one reductions ($\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions, introduced by Karp [29] and Levin [32]), respectively. The $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions (respectively, $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions), are precisely those nonuniform Turing (respectively, many-one) reductions that can be computed by polynomial-size circuits. The four reduction types that we have mentioned have distinct strengths, even when attention is restricted to languages in ESPACE. Specifically, the implications

$$\begin{array}{ccc} A \leq_{\mathrm{m}}^{\mathrm{P/Poly}} B & \Longrightarrow & A \leq_{\mathrm{T}}^{\mathrm{P/Poly}} B \\ \Uparrow & & \Uparrow \\ A \leq_{\mathrm{m}}^{\mathrm{P}} B & \Longrightarrow & A \leq_{\mathrm{T}}^{\mathrm{P}} B \end{array}$$

are the only implications that hold among these four conditions for all $A, B \in \mathrm{ESPACE}$.

We are interested in the nonuniform complexities of languages that are complete or weakly complete for ESPACE under $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions or $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions. We use two quantities to measure the nonuniform complexities of such languages. These are the density of nonuniform complexity cores and space-bounded Kolmogorov complexity. For the first measure, we use the density of a language's "largest" nonuniform complexity core. Intuitively, a *complexity core* is a set of *uniformly hard instances*. This concept was introduced by Lynch[43] and has been investigated by many others [15, 17, 47, 48, 11, 23, 52, 12, 16, 56, etc.]. Roughly speaking, a complexity core for a language A is a fixed set K of inputs such that *every* machine whose decisions are consistent with A fails to decide efficiently on almost all elements of K. The meanings of "efficiently" and "almost all" are parameters of this definition that may be varied according to the context.

Space-bounded Kolmogorov complexity is our second measure of nonuniform complexity. Kolmogorov complexity was introduced by Solomonoff[55], Kolmogorov[31], and Chaitin[13]. Resource-bounded Kolmogorov complexity has been investigated extensively [31, 20, 53, 33, 35, 7, 22, 30, 2, 3, 4, 36, 38, etc.]. We work with the *space-bounded Kolmogorov complexity* of languages. Roughly speaking, for $A \subseteq \{0,1\}^*$, $n \in \mathbf{N}$, and a space bound t, the space-bounded Kolmogorov complexity $KS^t(A_{=n})$ is the length of the shortest program that prints the 2^n-bit characteristic string of $A_{=n} = A \cap \{0,1\}^n$, using at most t units of workspace. Similarly, $KS^t(A_{\leq n})$ is the length of the shortest program that prints the $(2^{n+1}-1)$-bit characteristic string of $A_{\leq n} = A \cap \{0,1\}^{\leq n}$, using at most t units of workspace. The quantities $KS^t(A_{=n})$ and $KS^t(A_{\leq n})$ are frequently interpreted as the "amount of information" that is contained in $A_{=n}$ and $A_{\leq n}$, respectively, and that is "accessible" by computation using $\leq t$ space.

Let us now be more precise about our main results. In section 3 we prove two new almost everywhere lower bounds on the nonuniform complexity of languages in ESPACE. First, we show

that, for all $c \in \mathbf{N}$ and $\epsilon > 0$, almost every language A in ESPACE satisfies

$$KS^{2^{cn}}(A_{=n}) > 2^n - n^\epsilon \text{ a.e.} \tag{1.2}$$

This improves the $2^n - 2^{\epsilon n}$ lower bound of [38]. Second, we show that, for all $c \in \mathbf{N}$, almost every language in ESPACE has $\{0,1\}^*$ as a DSPACE(2^{cn})/Poly-complexity core. (A language is P-bi-immune if and only if it has $\{0,1\}^*$ as a P-complexity core [8], so this can be regarded as a very strong bi-immunity property.)

In section 4, we investigate the complexity and distribution of languages that are complete or weakly complete for ESPACE under $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions. We establish a tight, exponential lower bound on the space-bounded Kolmogorov complexities of languages that are weakly $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-complete for ESPACE. Specifically, we prove that for every such language H, there exists $\epsilon > 0$ such that

$$KS^{2^{n^\epsilon}}(H_{\leq n}) > 2^{n^\epsilon} \text{ a.e.} \tag{1.3}$$

This extends Huynh's proof [22] that (1.3) holds for every language H that is $\leq_{\mathrm{T}}^{\mathrm{P}}$-complete for ESPACE.

In section 4, we also prove a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in ESPACE. This result requires some explanation.

A recurring tool and unifying theme of much work on the measure structure of complexity classes is the development of *Small Span Theorems* for various reducibilities and 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 $\mathcal{R}(A)$, 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, 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 $\mathcal{C}$.)

The first Small Span Theorem, proven by Juedes and Lutz [26], 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 [26] 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 [26] have pointed out that a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P}}$-reductions in E or $\mathrm{E_2}$ would imply

that BPP$\subsetneq$E$_2$. More recent work of Regan, Sivakumar, and Cai [51] — building on the "natural proof" work of Razborov and Rudich [50] — indicates that a Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions (nonuniform Turing reductions computed by polynomial-size circuits) in 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 [34] adapted the method of [26] to prove Small Span Theorems for $\leq_{1-\mathrm{tt}}^{\mathrm{P}}$-reductions in E and E$_2$. Ambos-Spies, Neis, and Terwijn [5] used resource-bounded genericity to generalize the method of [26], thereby obtaining Small Span Theorems for $\leq_{k-\mathrm{tt}}^{\mathrm{P}}$-reductions in E and E$_2$ for all positive integers k.

In section 4, 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 reductions that are "combinatorially efficient," even though they need not be algorithmically computable. 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. Its proof 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$_2$.

Our Small Span Theorem 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 [25] and Ambos-Spies, Terwijn, and Zheng [6]) that there are languages that are weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, but not $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-complete, for ESPACE.

In section 5, we investigate the nonuniform complexities of languages that are complete or weakly complete for ESPACE under $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions. Lower bounds on the densities of complexity cores for complete languages have already been proven by Orponen and Schöning [48] and Huynh [23]. In particular, Huynh [23] proved that every language that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE has a dense P/Poly-complexity core. In section 5, we strengthen Huynh's result by proving that, for every weakly $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-complete language H for ESPACE, there exists $\epsilon > 0$ such that H has a dense DSPACE(2^{n^ϵ})/Poly-complexity core. Furthermore, we prove that this lower bound is tight, even when attention is restricted to languages that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE.

More importantly, in section 5, we establish tight *upper* bounds on the nonuniform complexities of complete languages for ESPACE. We prove that for every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-complete language H for ESPACE, there exists $\epsilon > 0$ such that

$$KS^{2^{2n}}(H_{=n}) < 2^n - 2^{n^\epsilon} \text{ i.o.} \tag{1.4}$$

We also prove that every DSPACE(2^{2n})/Poly-complexity core of every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-complete language for ESPACE has a dense complement. Moreover, we show that these upper bounds are tight, even

when attention is restricted to languages that are $\leq_m^P$-complete for ESPACE.

By combining the upper bound results of section 5 with the almost everywhere lower bound results of section 3 (e.g., comparing (1.2) with (1.4) above), we conclude that the $\leq_m^{P/Poly}$-complete languages for ESPACE obey upper bounds on nonuniform complexity that are violated by almost every element of ESPACE. Thus the $\leq_m^{P/Poly}$-complete languages are *unusually simple* for languages in ESPACE.

Although several of our results are similar *in form* to those of [26], the nonuniform nature of the reductions and complexity measures force us to use quite different methods in the present paper.

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 $n \in \mathbf{N}$.

We say that a condition $\Theta(n)$ holds *almost everywhere* (*a.e.*) if it holds for all but finitely many $n \in \mathbf{N}$. We say that $\Theta(n)$ holds *infinitely often* (*i.o.*) if it holds for infinitely many $n \in \mathbf{N}$.

For $A \subseteq \{0,1\}^*$ and $n \in \mathbf{N}$, we use the notations $A_{=n} = A \cap \{0,1\}^n$ and $A_{\leq n} = A \cap \{0,1\}^{\leq n}$. A language A is *dense* if there is a real number $\epsilon > 0$ such that $|A_{\leq n}| > 2^{n^\epsilon}$ a.e. A language A is *sparse* if there exists $k \in \mathbf{N}$ such that $|A_{\leq n}| \leq n^k$ a.e. (Equivalently, there is a polynomial p such that, for all $n \in \mathbf{N}$, $|A_{\leq n}| \leq p(n)$.)

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

$$A = \{x \in \{0,1\}^* \mid f(\langle x, h(|x|)\rangle) \in B\}, \tag{2.1}$$

where $\langle , \rangle : \{0,1\}^* \times \{0,1\}^* \to \{0,1\}^*$ is a standard pairing function. If $s : \mathbf{N} \to \mathbf{N}$, then A is $\leq_{\mathrm{m}}^{\mathrm{DSPACE}(s(n))/\mathrm{Poly}}$-*reducible* to B, and we write $A \leq_{\mathrm{m}}^{\mathrm{DSPACE}(s(n))/\mathrm{Poly}} B$, if there exists $f \in \mathrm{DSPACEF}(s(n))$ and $h \in \mathrm{Poly}$ such that (2.1) holds.

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 [49], 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 [38, 39] 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 [38]). 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

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

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 $\deg_{\mathcal{R}}(A) = \mathcal{R}(A) \cap \mathcal{R}^{-1}(A)$.

Definition. 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.

The existence of languages that are weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete, but not $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for E was first proven by Lutz [39]. It was subsequently proven by Juedes [25] that the set of such languages

does not have measure 0 in E, and by Ambos-Spies, Terwijn, and Zheng [6] that the set of such languages has measure 1 in E. All these proofs are easily modified to apply to such larger classes as E_2 and ESPACE. We thus have the following.

Theorem 2.3 (Ambos-Spies, Terwijn, and Zheng [6]). Almost every language in ESPACE is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE.

3 The Distribution of Nonuniform Complexity in ESPACE

In this section we investigate the distribution of languages that have high nonuniform complexity. We use space-bounded Kolmogorov complexity, nonuniform complexity cores and incompressibility by nonuniform reductions as measures of nonuniform complexity. The main results of this section show that almost every language in ESPACE is very complex with respect to each of these measures.

This section has three parts. In part 3.1 we investigate the distribution of languages with high space-bounded Kolmogorov complexity. Specifically, we prove that almost every language A in ESPACE has space-bounded Kolmogorov complexity $KS^{2^{cn}}(A_{=n}) > 2^n - \sqrt{n}$ for almost every n. In part 3.2 we investigate the distribution of languages with large nonuniform complexity cores. We prove that almost every language in ESPACE has $\{0,1\}^*$ as a DSPACE(2^{cn})/Poly-complexity core. Finally, in part 3.3, we investigate the distribution of languages that are incompressible by nonuniform many-one reductions. There we prove that almost every language in ESPACE is $n^{\log n}$-incompressible by $\leq_m^{\mathrm{DSPACE}(2^{cn})/\mathrm{Poly}}$-reductions.

3.1 Space-Bounded Kolmogorov Complexity

The distribution of languages in ESPACE with high space-bounded Kolmogorov complexity was first investigated in [38]. Here we strengthen the results of [38] in two important directions. First, we show that the almost-everywhere lower bound of $2^{n+1} - 2^{\epsilon n}$ on the space-bounded Kolmogorov complexity $KS^{2^{cn}}(A_{\leq n})$ is tight and cannot be improved (Theorem 3.3). Next, we improve the almost everywhere lower bound on the space-bounded Kolmogorov complexity $KS^{2^{cn}}(A_{=n})$ from $2^n - 2^{\epsilon n}$ to $2^n - n^{\epsilon}$ (Corollary 3.5).

Some terminology and notation will be useful. For a fixed machine M and "program" $\pi \in \{0,1\}^*$ for M, we say that "$M(\pi, n) = w$ in $\leq s$ space" if M, on input (π, n), outputs the string $w \in \{0,1\}^*$ and halts without using more than s cells of workspace. We are especially interested in situations where the output is of the form $\chi_{A_{=n}}$ or of the form $\chi_{A_{\leq n}}$, i.e., the 2^n-bit characteristic string of $A_{=n}$ or the $(2^{n+1}-1)$-bit characteristic string of $A_{\leq n}$, for some language A.

Given a machine M, a space bound $s : \mathbf{N} \to \mathbf{N}$, a language $A \subseteq \{0,1\}^*$, and a natural number n, the *$s(n)$-space-bounded Kolmogorov complexity* of $A_{=n}$ relative to M is

$$KS_M^{s(n)}(A_{=n}) = min\{|\pi| \,\big|\, M(\pi, n) = \chi_{A_{=n}} \text{ in } \leq s(n) \text{ space } \}.$$

Similarly, the $s(n)$-*space-bounded Kolmogorov complexity* of $A_{\leq n}$ relative to M is

$$KS_M^{s(n)}(A_{\leq n}) = min\{|\pi| \,\big|\, M(\pi, n) = \chi_{A_{\leq n}} \text{ in } \leq s(n) \text{ space } \}.$$

Well-known simulation techniques show that there is a machine U that is *optimal* in the sense that for each machine M there is a constant c such that for all s, A and n, we have

$$KS_U^{c \cdot s(n)+c}(A_{=n}) \leq KS_M^{s(n)}(A_{=n}) + c$$

and

$$KS_U^{c \cdot s(n)+c}(A_{\leq n}) \leq KS_M^{s(n)}(A_{\leq n}) + c.$$

As is standard in this subject, we fix an optimal machine U and omit it from the notation.

We now recall the following almost-everywhere lower bound result.

Theorem 3.1 (Lutz [38]). Let $c \in \mathbf{N}$ and $\epsilon > 0$.

(a) If

$$X = \{A \subseteq \{0,1\}^* \mid KS^{2^{cn}}(A_{=n}) > 2^n - 2^{\epsilon n} \text{ a.e.}\},$$

then $\mu_{\text{pspace}}(X) = \mu(X \mid \text{ESPACE}) = 1$.

(b) If

$$Y = \{A \subseteq \{0,1\}^* \mid KS^{2^{cn}}(A_{\leq n}) > 2^{n+1} - 2^{\epsilon n} \text{ a.e.}\},$$

then $\mu_{\text{pspace}}(Y) = \mu(Y \mid \text{ESPACE}) = 1$.

Though the lower bounds of Theorem 3.1 have been useful in a variety of applications (see [37, 38], for example), they are not strong enough for our purposes. For this reason, we ask the natural question: Can the almost-everywhere lower bounds of Theorem 3.1 be improved?

We first consider Theorem 3.1(b). Martin-Löf [44] has shown that, for every $c \in \mathbf{N}$ and every real $a > 1$, almost every language $A \subseteq \{0,1\}^*$ has space-bounded Kolmogorov complexity

$$KS^{2^{cn}}(A_{\leq n}) > 2^{n+1} - an \text{ a.e.} \tag{3.1}$$

(In fact, Martin-Löf showed that this holds even in the absence of a space bound.) The following known bounds show that the lower bound (3.1) is relatively tight.

Theorem 3.2. There exist constants $c_1, c_2 \in \mathbf{N}$ such that every language A satisfies the following two conditions.

(i) $KS^{2^n}(A_{\leq n}) < 2^{n+1} + c_1$ for all n.

(ii) $KS^{2^{c_2 \cdot n}}(A_{\leq n}) < 2^{n+1} - \log n + c_1$ i.o.

(Part (i) of Theorem 3.2 is well known and obvious. Part (ii) extends a result of Martin-Löf [44].)

Since the bound of Theorem 3.1(b) is considerably lower than that of (3.1), one might expect to improve Theorem 3.1(b). However, the following upper bound shows that Theorem 3.1(b) is also tight. (In comparing Theorems 3.1(b) and 3.3 it is critical to note the order in which A and ϵ are quantified.)

Theorem 3.3. For every language $A \in$ ESPACE, there exists a real $\epsilon > 0$ such that

$$KS^{2^{2n}}(A_{\leq n}) < 2^{n+1} - 2^{\epsilon n} \text{ a.e.}$$

Proof. Fix $A \in$ ESPACE and $a \in \mathbf{N}$ such that $A \in$ DSPACE(2^{an}). For each $n \in \mathbf{N}$, let $n' = \lfloor \frac{n}{a+1} \rfloor$, and let y_n be the string of length $2^{n+1} - 2^{n'+1}$ such that $\chi_{A_{\leq n}} = \chi_{A_{\leq n'}} y_n$. Let M be a machine that, on input (y, n), computes $\chi_{A_{\leq n'}}$ using $\leq 2^{an'}$ space and then outputs $\chi_{A_{\leq n'}} y$. Let c be the optimality constant for the machine M (given by the definition of the optimal machine U at the beginning of this section). Then $M(y_n, n)$ outputs $\chi_{A_{\leq n}}$ in $\leq 2^{an'}$ space, so for all sufficiently large n, we have

$$\begin{aligned} KS^{2^{2n}}(A_{\leq n}) &\leq KS_M^{2^{an'}}(A_{\leq n}) + c \\ &\leq |y_n| + c \\ &= 2^{n+1} - 2^{n'+1} + c \\ &< 2^{n+1} - 2^{\epsilon n}, \end{aligned}$$

where $\epsilon = \frac{1}{a+2}$. □

Thus we cannot hope to improve Theorem 3.1(b).

An elementary counting argument shows that, for every $c \in \mathbf{N}$, there *exists* a language $A \in$ ESPACE with $KS^{2^{cn}}(A_{=n}) \geq 2^n$ for all $n \in \mathbf{N}$. This suggests that the prospect for improving Theorem 3.1(a) may be more hopeful. In fact, we have the following almost-everywhere lower bound result.

Theorem 3.4. Let $c \in \mathbf{N}$ and let $f : \mathbf{N} \to \mathbf{N}$ be such that $f \in$ pspace and $\sum_{n=0}^{\infty} 2^{-f(n)}$ is p-convergent. If

$$X = \{A \subseteq \{0,1\}^* \mid KS^{2^{cn}}(A_{=n}) > 2^n - f(n) \text{ a.e.}\},$$

then $\mu_{\text{pspace}}(X) = \mu(X \mid \text{ESPACE}) = 1$.

Proof. Assume the hypothesis. By Theorem 2.2, it suffices to exhibit a pspace-computable function d such that each d_n is a martingale,

$$\sum_{n=0}^{\infty} d_n(\lambda) \text{ is p-convergent,} \tag{3.2}$$

and

$$X^c \subseteq \bigcap_{t=0}^{\infty} \bigcup_{n=t}^{\infty} S^1[d_n]. \tag{3.3}$$

Some notation will be helpful. For $n \in \mathbf{N}$, let

$$B_n = \{\pi \in \{0,1\}^{\leq 2^n - f(n)} \mid U(\pi, n) \in \{0,1\}^{2^n} \text{ in } \leq 2^{cn} \text{ space } \}. \tag{3.4}$$

For $n \in \mathbf{N}$ and $\pi \in B_n$, let

$$Z_{n,\pi} = \bigcup_{|z|=2^n-1} \mathbf{C}_{zU(\pi,n)}.$$

(Thus $Z_{n,\pi}$ is the set of all languages A such that $U(\pi, n)$ is the 2^n-bit characteristic string of $A_{=n}$.) For $n \in \mathbf{N}$ and $w \in \{0,1\}^*$, let

$$\sigma(n, w) = \sum_{\pi \in B_n} \Pr(Z_{n,\pi} \mid \mathbf{C}_w), \tag{3.5}$$

where the conditional probabilities $\Pr(Z_{n,\pi} \mid \mathbf{C}_w) = \Pr_A[A \in Z_{n,\pi} \mid A \in \mathbf{C}_w]$ are computed according to the random experiment in which a language $A \subseteq \{0,1\}^*$ is chosen probabilistically, using an independent toss of a fair coin to decide membership of each string in A. Finally, define the function $d : \mathbf{N} \times \{0,1\}^* \to [0, \infty)$ as follows. (In all three clauses, $n \in \mathbf{N}$, $w \in \{0,1\}^*$, and $b \in \{0,1\}$.)

(i) If $0 \leq |w| \leq 2^n - 1$, then $d_n(w) = 2^{1-f(n)}$.

(ii) If $2^n - 1 \leq |w| < 2^{n+1} - 1$, then $d_n(wb) = d_n(w)\frac{\sigma(n,wb)}{\sigma(n,w)}$.

(iii) If $|w| \geq 2^{n+1} - 1$, then $d_n(wb) = d_n(w)$.

(The condition $\sigma(n, w) = 0$ can only occur if $d_n(w) = 0$, in which case we understand clause (ii) to mean that $d_n(wb) = 0$.)

It is clear from (3.5) that

$$\sigma(n, w) = \frac{\sigma(n, w0) + \sigma(n, w1)}{2}$$

for all $n \in \mathbf{N}$ and $w \in \{0,1\}^*$. It follows by a routine induction on the definition of d that each d_n is a martingale. It is also routine to check that d is pspace-computable. (The crucial point here is that we are only required to perform computations of the type (3.5) when $|w| \geq 2^n - 1$, so the 2^{cn} space bound of (3.4) is polynomial in $|w|$.) Since $\sum_{n=0}^{\infty} 2^{-f(n)}$ is p-convergent, it is immediate from clause (i) that (3.2) holds. All that remains, then, is to verify (3.3).

For each language $A \subseteq \{0,1\}^*$, let

$$I_A = \{n \in \mathbf{N} \mid KS^{2^{cn}}(A_{=n}) \leq 2^n - f(n)\}.$$

Fix a language A for a moment and let $n \in I_A$. Then there exists $\pi_0 \in B_n$ such that $A \in Z_{n,\pi_0}$. Fix such a program π_0 and let $x, y \in \{0,1\}^*$ be the characteristic strings of $A_{<n}$, $A_{\leq n}$, respectively. (Thus $|x| = 2^n - 1$, $|y| = 2^{n+1} - 1$, and $y = xU(\pi_0, n)$.) The definition of d tells us that $d_n(y)$ is $d_n(x)$ times a telescoping product, i.e.,

$$\begin{aligned} d_n(y) &= d_n(x) \prod_{i=0}^{2^n-1} \frac{\sigma(n, y[0..2^n-1+i])}{\sigma(n, y[0..2^n-2+i])} \\ &= d_n(x) \frac{\sigma(n,y)}{\sigma(n,x)} \\ &= 2^{1-f(n)} \frac{\sigma(n,y)}{\sigma(n,x)}. \end{aligned} \tag{3.6}$$

Since $\mathbf{C}_y \subseteq Z_{n,\pi_0}$, we have

$$\sigma(n,y) = \sum_{\pi \in B_n} \Pr(Z_{n,\pi} \mid \mathbf{C}_y) \geq \Pr(Z_{n,\pi_0} \mid \mathbf{C}_y) = 1. \tag{3.7}$$

For each $\pi \in B_n$, the events $\mathbf{C}_x$ and $Z_{n,\pi}$ are independent, so

$$\begin{aligned} \sigma(n,x) &= \sum_{\pi \in B_n} \Pr(Z_{n,\pi} \mid \mathbf{C}_x) \\ &= \sum_{\pi \in B_n} \Pr(Z_{n,\pi}) \\ &= |B_n| 2^{-2^n} \\ &< 2^{1-f(n)}. \end{aligned} \tag{3.8}$$

By (3.6), (3.7), and (3.8), we have $d_n(y) > 1$. It follows that $A \in \mathbf{C}_y \subseteq S^1[d_n]$. Since $n \in I_A$ is arbitrary here, we have shown that $A \in S^1[d_n]$ for all $A \subseteq \{0,1\}^*$ and $n \in I_A$. It follows that, for all $A \subseteq \{0,1\}^*$,

$$\begin{aligned} A \in X^c &\Rightarrow |I_A| = \infty \\ &\Rightarrow A \in S^1[d_n] \text{ i.o.} \\ &\Rightarrow A \in \bigcap_{t=0}^{\infty} \bigcup_{n=t}^{\infty} S^1[d_n], \end{aligned}$$

i.e., (3.3) holds. This completes the proof. □

Corollary 3.5. Let $c \in \mathbf{N}$ and $\epsilon > 0$. If

$$X = \{A \subseteq \{0,1\}^* \mid KS^{2^{cn}}(A_{=n}) > 2^n - n^\epsilon \text{ a.e.}\},$$

then $\mu_{\text{pspace}}(X) = \mu(X \mid \text{ESPACE}) = 1$.

Proof. Routine calculus shows that the series $\sum_{n=0}^{\infty} 2^{-n^\epsilon}$ is p-convergent. □

Corollary 3.5 is a substantial improvement of Theorem 3.1(a). We exploit this improvement throughout the paper.

3.2 Complexity Cores

The distribution of languages with large uniform complexity cores in E was investigated in [26]. In this subsection we investigate the distribution of languages with large nonuniform complexity cores in ESPACE. We first present the necessary notation and definitions.

Given a machine M, an advice function h, and an input $x \in \{0,1\}^*$, we write $M/h(x) = 1$ if M accepts $\langle x, h(|x|)\rangle$, $M/h(x) = 0$ if M rejects $\langle x, h(|x|)\rangle$, and $M(x) = \perp$ in any other case (i.e., if M fails to halt or M halts without deciding $\langle x, h(|x|)\rangle$). If $M(x) \in \{0,1\}$, we write $space_{M/h}(x)$ for the number of steps used in the computation of $M(\langle x, h(|x|)\rangle)$. If $M(x) = \perp$, we define $space_{M/h}(x) = \infty$. We partially order the set $\{0, 1, \perp\}$ by $\perp < 0$ and $\perp < 1$, with 0 and 1 incomparable. A machine/advice pair M/h is *consistent* with a language $A \subseteq \{0,1\}^*$ if $M/h(x) \leq [\![x \in A]\!]$ for all $x \in \{0,1\}^*$.

Nonuniform complexity cores were first defined and investigated by Huynh [23] with respect to the complexity class P/Poly.

Definition (Huynh [23]). Let $s : \mathbf{N} \to \mathbf{N}$ be a space bound and let $A, K \subseteq \{0,1\}^*$. Then K is a DSPACE($s(n)$)/Poly-*complexity core* of A if, for every $c \in \mathbf{N}$ the following holds. For every machine M and polynomially bounded advice function h, if M/h is consistent with A, then the fast set

$$F = \{x \mid space_{M/h}(x) \leq c \cdot s(|x|) + c\}$$

has the property that $|F \cap K|$ is sparse.

(Note: Huynh's original definition is only meaningful for $A \in$ REC/Poly because it only quantifies over those M/h that *decide* A. The above definition coincides with Huynh's for $A \in$ REC/Poly, but is meaningful for all languages A.)

Intuitively, very complex languages must have large nonuniform complexity cores. This intuition is supported by the following technical lemma.

Lemma 3.6. If $s : \mathbf{N} \to \mathbf{N}$ is space constructible and p is a polynomial, then every language A with

$$KS^{n \cdot s}(A_{=n}) > 2^n - p(n) \text{ a.e.}$$

has $\{0,1\}^*$ as a DSPACE(s)/Poly-complexity core.

Proof. We show the contrapositive. Assume that A does not have $\{0,1\}^*$ as a DSPACE(s)/Poly-complexity core. Under this assumption, there exist a machine M, polynomially bounded advice function h, and constant c such that M given h is consistent with A and the set

$$F = \{x \mid space_{M/h}(x) \leq c \cdot s(|x|) + c\}$$

is non-sparse. Using M, c, and a machine for s, we construct a machine M' to output $\chi_{A_{=n}}$ as in Figure 1.

```
M'(⟨h, y⟩, n):
begin
    for i = 2^n to 2^{n+1} − 1 do
    begin
        simulate M(s_i, h);
(1)     if M decides s_i in ≤ c · s(n) + c space then
            output [[M(s_i, h)]];
(2)     Otherwise output head(y); y = tail(y);
    end for
end.
```

Figure 1: An algorithm that computes $\chi_{A_{=n}}$ in the proof of Lemma 3.6.

Now consider the action of M' on input $(\langle h(n), y\rangle, n)$, where y is the string $A_{=n}$ with the bits corresponding to the elements of $F_{=n}$ removed. On this input, the machine M' correctly outputs the bits of $A_{=n}$ either (1) by deciding $[\![s_i \in A]\!]$ directly, or (2) by using the bits of y. Thus we have the following.

$$\begin{aligned} KS_{M'}^{c \cdot s(n)+c}(A_{=n}) &\leq |\langle h(n), y\rangle| \\ &\leq 2|h(n)| + 2 + |A_{=n}| - |F_{=n}| \end{aligned}$$

$$\leq \quad 2|h(n)| + 2 + 2^n - |F_{=n}|$$

By universal simulation, there exists a constant $c_1 \in \mathbf{N}$ such that

$$\begin{aligned} KS^{c_1(c\cdot s(n)+c)+c_1}(A_{=n}) &\leq KS^{c\cdot s(n)+c}_{M'}(A_{=n}) + c_1 \\ &\leq 2^n - |F_{=n}| + 2|h(n)| + 2 + c_1. \end{aligned}$$

The above inequality, combined with the fact that F is not sparse, proves that for every polynomial p,

$$KS^{n\cdot s(n)}(A_{=n}) \leq KS^{c_1(c\cdot s(n)+c)+c_1}(A_{=n}) < 2^n - p(n) \text{ i.o.}$$

□

Since almost every language in ESPACE has high space-bounded Kolmogorov complexity almost everywhere, Lemma 3.6 implies that almost every language in ESPACE has maximal nonuniform complexity cores.

Corollary 3.7. Fix $c \in \mathbf{N}$. Then, almost every language in ESPACE has $\{0,1\}^*$ as a DSPACE(2^{cn})/Poly-complexity core.

Proof. By Corollary 3.5, the set

$$X = \{A \subseteq \{0,1\}^* \mid KS^{2^{(c+1)n}}(A_{=n}) > 2^n - \sqrt{n} \text{ a.e.}\}$$

has pspace-measure 1. By Lemma 3.6, each element of X has $\{0,1\}^*$ as a DSPACE(2^{cn})/Poly-complexity core. It follows that almost every language in ESPACE has $\{0,1\}^*$ as a DSPACE(2^{cn})/Poly-complexity core. □

3.3 Incompressibility

In [26] it is shown that almost every language in E is incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions. Here we show that almost every language in ESPACE is $n^{\log n}$-incompressible by $\leq^{\mathrm{P/Poly}}_{\mathrm{m}}$-reductions. First we explain "incompressibility by many-one reductions," an idea originally exploited by Meyer [46].

Definition. The *collision set* of a function $f : \{0,1\}^* \to \{0,1\}^*$ is

$$C_f = \{x \in \{0,1\}^* \mid (\exists y < x) f(y) = f(x)\}.$$

Here, we are using the standard ordering $s_0 < s_1 < s_2 < \cdots$ of $\{0,1\}^*$.

Definition. A function $f : \{0,1\}^* \to \{0,1\}^*$ is *one-to-one almost everywhere* (or, briefly, *one-to-one a.e.*) if its collision set C_f is finite.

Definition. A language $A \subseteq \{0,1\}^*$ is *incompressible by* $\leq_{\mathrm{m}}^{\mathrm{P}}$*-reductions* if every $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduction of A is one-to-one a.e.

Definition. Let $g : \mathbf{N} \to \mathbf{N}$. A language $A \subseteq \{0,1\}^*$ is $g(n)$*-incompressible by* $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$*-reductions* if every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reduction f of A satisfies satisfies $|(C_f)_{\leq n}| \leq g(n)$ a.e.

Definition. Let $s, g : \mathbf{N} \to \mathbf{N}$. A language $A \subseteq \{0,1\}^*$ is $g(n)$*-incompressible by* $\leq_{\mathrm{m}}^{\mathrm{DSPACE}(s)/\mathrm{Poly}}$*-reductions* if every $\leq_{\mathrm{m}}^{\mathrm{DSPACE}(s)/\mathrm{Poly}}$-reduction f of A satisfies $|(C_f)_{\leq n}| \leq g(n)$ a.e.

Intuitively, if f is a many-one reduction of A to B and C_f is large, then f compresses many questions "$x \in A$?" to fewer questions "$f(x) \in B$?" If A is incompressible by a class of many-one reductions, then very little such compression can occur.

Note that there are certain classes of many-one reductions for which no language is incompressible. Specifically, no language is incompressible by $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$or $\leq_{\mathrm{m}}^{\mathrm{DSPACE}(s)/\mathrm{Poly}}$-reductions, because an infinite set of inputs can be encoded into an advice function. Similarly, if $p(n)$ is a polynomial then no language is $p(n)$-incompressible by $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions. However, we now show that, if g is *superpolynomial* (i.e., for every polynomial p, $g(n) > p(n)$ a.e.), nondecreasing, and computable in exponential space, then almost every language in ESPACE is $g(n)$-incompressible.

Theorem 3.8. Fix $c \in \mathbf{Z}^+$. Let $g : \mathbf{N} \to \mathbf{N}$ be superpolynomial and nondecreasing, and assume that $g(n)$ is computable in 2^{cn} space. If

$$X = \{A \subseteq \{0,1\}^* \mid A \text{ is } g(n)\text{-incompressible by } \leq_m^{\mathrm{DSPACE}(2^{cn})/\mathrm{Poly}}\text{-reductions}\},$$

then $\mu_{\mathrm{pspace}}(X) = \mu(X \mid \mathrm{ESPACE}) = 1$.

Proof. We follow the format of the proof of Theorem 3.4. Assume the hypothesis. By Theorem 2.2, it suffices to exhibit a pspace-computable function d such that each d_n is a martingale,

$$\sum_{n=0}^{\infty} d_n(\lambda) \text{ is p-convergent}, \tag{3.9}$$

and

$$X^c \subseteq \bigcap_{t=0}^{\infty} \bigcup_{n=t}^{\infty} S^1[d_n]. \tag{3.10}$$

Some notation will be helpful for the remainder of the proof. For $n \in \mathbf{N}$ and $g : \mathbf{N} \to \mathbf{N}$, let

$$\mathcal{F}/Adv(g)(n) = \left\{ f : \{0,1\}^* \to \{0,1\}^* \;\middle|\; \begin{array}{l} \text{there exist } n_0 \leq n \text{ and } h_0, \ldots, h_n \in \{0,1\}^{\leq g(n)} \\ \text{such that, for all } x \in \{0,1\}^{\leq n}, \\ M_{n_0}(x, h_{|x|}) = f(x) \text{ in } \leq 2^{cn} \text{ space.} \end{array} \right\}$$

Informally, the class $\mathcal{F}/Adv(g)(n)$ is the set of functions that are computed correctly over $\{0,1\}^{\leq n}$ by one of the first n machines with advice bounded in length by $g(n)$.

For $n \in \mathbf{N}$, let

$$\mathcal{G}_n = \{f \in \mathcal{F}/Adv(\frac{g(n)}{4n^2(2n+2)} - 3)(n) \;\Big|\; |(C_f)_{=n}| \geq \frac{g(n)}{2n^2}\}, \tag{3.11}$$

and let

$$\mathcal{G}'_n = \{f \restriction \{0,1\}^{\leq n} \mid f \in \mathcal{G}_n\}, \tag{3.12}$$

where $f \restriction \{0,1\}^{\leq n}$ denotes the restriction of f to $\{0,1\}^{\leq n}$. For $n \in \mathbf{N}$ and $f \in \mathcal{G}'_n$, let

$$B_{n,f} = \{x \in \{0,1\}^{2^{n+1}-1} \;\Big|\; \forall i, j \leq 2^{n+1} - 1, f(s_i) = f(s_j) \Rightarrow x[i] = x[j]\}$$

and

$$Z_{n,f} = \bigcup_{x \in B_{n,f}} \mathbf{C}_x.$$

(Thus $Z_{n,f}$ is the set of all languages A such that no counterexample to the statement "f is a many-one reduction of A" exists among the strings in $\{0,1\}^{\leq n}$.) For $n \in \mathbf{N}$ and $w \in \{0,1\}^*$, let

$$\sigma(n,w) = \sum_{f \in \mathcal{G}'_n} \Pr(Z_{n,f} \mid \mathbf{C}_w), \tag{3.13}$$

where the conditional probabilities $\Pr(Z_{n,f} \mid \mathbf{C}_w) = \Pr_A[A \in Z_{n,f} \mid A \in \mathbf{C}_w]$ are computed according to the random experiment in which a language $A \subseteq \{0,1\}^*$ is chosen probabilistically, using an independent toss of a fair coin to decide membership of each string in A. Finally, define a function $d : \mathbf{N} \times \{0,1\}^* \to [0,\infty)$ as follows. (In all three clauses, $n \in \mathbf{N}$, $w \in \{0,1\}^*$, and $b \in \{0,1\}$.)

(i) If $0 \leq |w| \leq 2^n - 1$, then $d_n(w) = 2^{-n}$.

(ii) If $2^n - 1 \leq |w| < 2^{n+1} - 1$, then $d_n(wb) = d_n(w)\frac{\sigma(n,wb)}{\sigma(n,w)}$.

(iii) If $|w| \geq 2^{n+1} - 1$, then $d_n(wb) = d_n(w)$.

(Note that the condition $\sigma(n,w)=0$ can only occur if $d_n(w)=0$, in which case we understand clause (ii) to mean that $d_n(wb)=0$.)

It is clear from (3.13) that

$$\sigma(n,w)=\frac{\sigma(n,w0)+\sigma(n,w1)}{2}$$

for all $n\in\mathbf{N}$ and $w\in\{0,1\}^*$. It follows by a routine induction on the definition of d that each d_n is a martingale. It is also routine to check that d is pspace-computable. Furthermore, since the sum $\sum_{n=0}^{\infty}2^{-n}$ is p-convergent, it is immediate from clause (i) that (3.9) holds. All that remains is to verify (3.10).

Let $A\in X^c$ and fix $f\in\mathrm{DSPACEF}(2^{cn})/\mathrm{Poly}$ such that f is a many-one reduction of A with $|(C_f)_{\leq n}|>g(n)$ i.o. Define the set

$$I_{A,f}=\{n\in\mathbf{N}\mid f\in\mathcal{G}_n\}.$$

Since g is superpolynomial and f has $|(C_f)_{\leq n}|>g(n)$ i.o., it follows that $I_{A,f}$ is infinite. Let $n\in I_{A,f}$ and let $x,y\in\{0,1\}^*$ be the characteristic strings of $A_{<n}$, $A_{\leq n}$, respectively. The definition of d tells us that $d_n(y)$ is the product of $d_n(x)$ and a telescoping product, i.e.,

$$\begin{aligned} d_n(y) &= d_n(x)\prod_{i=0}^{2^n-1}\frac{\sigma(n,y[0..2^n-1+i])}{\sigma(n,y[0..2^n-2+i])} \\ &= d_n(x)\frac{\sigma(n,y)}{\sigma(n,x)} \\ &= 2^{-n}\frac{\sigma(n,y)}{\sigma(n,x)}. \end{aligned} \tag{3.14}$$

Since $\mathbf{C}_y\subseteq Z_{n,f}$, we have

$$\sigma(n,y)=\sum_{f\in\mathcal{G}'_n}\Pr(Z_{n,f}\mid\mathbf{C}_y)\geq\Pr(Z_{n,f}\mid\mathbf{C}_y)=1. \tag{3.15}$$

Now a simple counting argument shows that there are at most $2^{\frac{g(n)}{4n^2}-n}$ functions in $\mathcal{G}'_n$ that have distinct behaviors on $\{0,1\}^{\leq n}$. Furthermore, for each $f\in\mathcal{G}_n$, there are at most $2^{2^n-\frac{|(C_f)=n|}{2}}$ possible 2^n bit extensions of x satisfying f. (That is, there are at most $2^{2^n-\frac{|(C_f)=n|}{2}}$ strings z such that $xz\in Y_{n,f}$.) Thus we have $\Pr(Z_{n,f}\mid\mathbf{C}_x)\leq 2^{-\frac{|(C_f)=n|}{2}}=2^{-\frac{g(n)}{4n^2}}$, so

$$\begin{aligned} \sigma(n,x) &= \sum_{f\in\mathcal{G}'_n}\Pr(Z_{n,f}\mid\mathbf{C}_x) \\ &\leq \sum_{f\in\mathcal{G}'_n}2^{-\frac{g(n)}{4n^2}} \\ &= |\mathcal{G}'_n|2^{-\frac{g(n)}{4n^2}} \\ &< 2^{-n}. \end{aligned} \tag{3.16}$$

By (3.14), (3.15), and (3.16), we have $d_n(y) > 1$. It follows that $A \in \mathbf{C}_y \subseteq S^1[d_n]$. Since $n \in I_{A,f}$ is arbitrary here, we have shown that $A \in S^1[d_n]$ for all $A \in X^c$ and $n \in I_{A,f}$. It follows that, for all $A \subseteq \{0,1\}^*$,

$$\begin{aligned} A \in X^c &\Rightarrow \exists f \text{ such that } |I_{A,f}| = \infty \\ &\Rightarrow A \in S^1[d_n] \text{ i.o.} \\ &\Rightarrow A \in \bigcap_{t=0}^{\infty} \bigcup_{n=t}^{\infty} S^1[d_n], \end{aligned}$$

i.e., (3.10) holds. This completes the proof. □

Corollary 3.9. Almost every language in ESPACE is $n^{\log n}$-incompressible by $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions. □

Corollary 3.9 implies the existence of an $n^{\log n}$-incompressible language A in ESPACE, but does not specify a constant c such that $A \in \mathrm{DSPACE}(2^{cn})$. However, a straightforward diagonalization shows that there is such an A in $\mathrm{DSPACE}(2^{cn})$, provided that c is larger than 1. Thus we have the following useful fact.

Lemma 3.10. There is a language $A \in \mathrm{DSPACE}(2^{2n})$ that is $n^{\log n}$-incompressible by $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions.

4 Completeness and Weak Completeness under P/Poly-Turing Reductions

In this section, we investigate the complexity and distribution of languages that are hard or weakly hard for ESPACE under $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions — nonuniform Turing reductions that are computed by polynomial-size circuits. We establish a tight, exponential lower bound on the space-bounded Kolmogorov complexities of languages that are weakly $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-hard for ESPACE. We also prove the Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reducibility in ESPACE. This latter result implies that the set of all $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-hard languages for ESPACE has pspace-measure 0, and that *every* $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-degree has measure 0 in ESPACE.

The following theorem extends a result of Huynh [22].

Theorem 4.1. For every weakly $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-hard language H for ESPACE, there exists $\epsilon > 0$ such that

$$KS^{2^{n^\epsilon}}(H_{\leq n}) > 2^{n^\epsilon} \text{ a.e.}$$

Proof. Let H be weakly $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-hard for ESPACE, and let

$$X = \{A \subseteq \{0,1\}^* \mid KS^{2^{2n}}(A_{=n}) > 2^n - \sqrt{n} \text{ a.e.}\}.$$

Since $(\mathrm{P/Poly})_{\mathrm{T}}(H)$ does not have measure 0 in ESPACE and X has measure 1 in ESPACE (by Corollary 3.5), the set $(\mathrm{P/Poly})_{\mathrm{T}}(H) \cap X \cap \mathrm{ESPACE}$ is not empty. Fix $A \in (\mathrm{P/Poly})_{\mathrm{T}}(H) \cap X$, and let M/h be an oracle machine/polynomial advice pair that decides A in polynomial time using H as an oracle. Moreover, fix $k \in \mathbf{N}$ such that, independently of the oracle, the computation $M(x, h(|x|))$ queries the oracle on strings of length at most $|x|^k$ for all sufficiently large x, and let $\epsilon = \frac{1}{3k}$. We will essentially show that

$$KS^{2^{n^\epsilon}}(H_{\leq n}) \geq KS^{2^{2\lfloor n^{2\epsilon} \rfloor}}(A_{\leq \lfloor n^{2\epsilon} \rfloor}) > 2^{n^\epsilon} \text{ a.e.}$$

Let $\widehat{M}$ be a machine that efficiently implements the algorithm in Figure 2, let $n \in \mathbf{N}$, and let π be a minimal 2^{n^ϵ}-space-bounded program for $\chi_{H_{\leq n}}$. If $m = \lfloor n^{2\epsilon} \rfloor$, then the machine $\widehat{M}$, on input $(\langle h(0), h(1), \ldots, h(m)\rangle \pi, m)$, outputs $\chi_{A_{\leq m}}$ using less than $c_0 \cdot 2^{n^\epsilon}$ space. Thus there is a constant c_1 such that, for all sufficiently large n,

$$\begin{aligned} KS^{2^{2m}}(A_{\leq m}) &\leq KS_{\widehat{M}}^{c_0 \cdot 2^{n^\epsilon}}(A_{\leq m}) + c_1 \\ &\leq |\langle h(0), h(1), \ldots, h(m)\rangle \pi| + c_1 \\ &\leq KS^{2^{n^\epsilon}}(H_{\leq n}) + |\langle h(0), \ldots, h(m)\rangle| + c_1. \end{aligned}$$

Since $KS^{2^{2m}}(A_{\leq m}) > 2^m - \sqrt{m}$ a.e., and the length of $\langle h(0), \ldots, h(m)\rangle$ is bounded by $q(m)$ for some polynomial q, it follows that

$$\begin{aligned} KS^{2^{n^\epsilon}}(H_{\leq n}) &\geq KS^{2^{2m}}(A_{\leq m}) - q(m) - c_1 \\ &\geq 2^{\lfloor n^{2\epsilon} \rfloor} - \sqrt{\lfloor n^{2\epsilon} \rfloor} - q(\lfloor n^{2\epsilon} \rfloor) - c_1 \\ &> 2^{n^\epsilon} \text{ a.e.} \end{aligned}$$

This completes the proof. □

Corollary 4.2 (Huynh[22]). For every $\leq_{\mathrm{T}}^{\mathrm{P}}$-hard language H for ESPACE, there exists $\epsilon > 0$ such that

$$KS^{2^{n^\epsilon}}(H_{\leq n}) > 2^{n^\epsilon} \text{ a.e.}$$

□

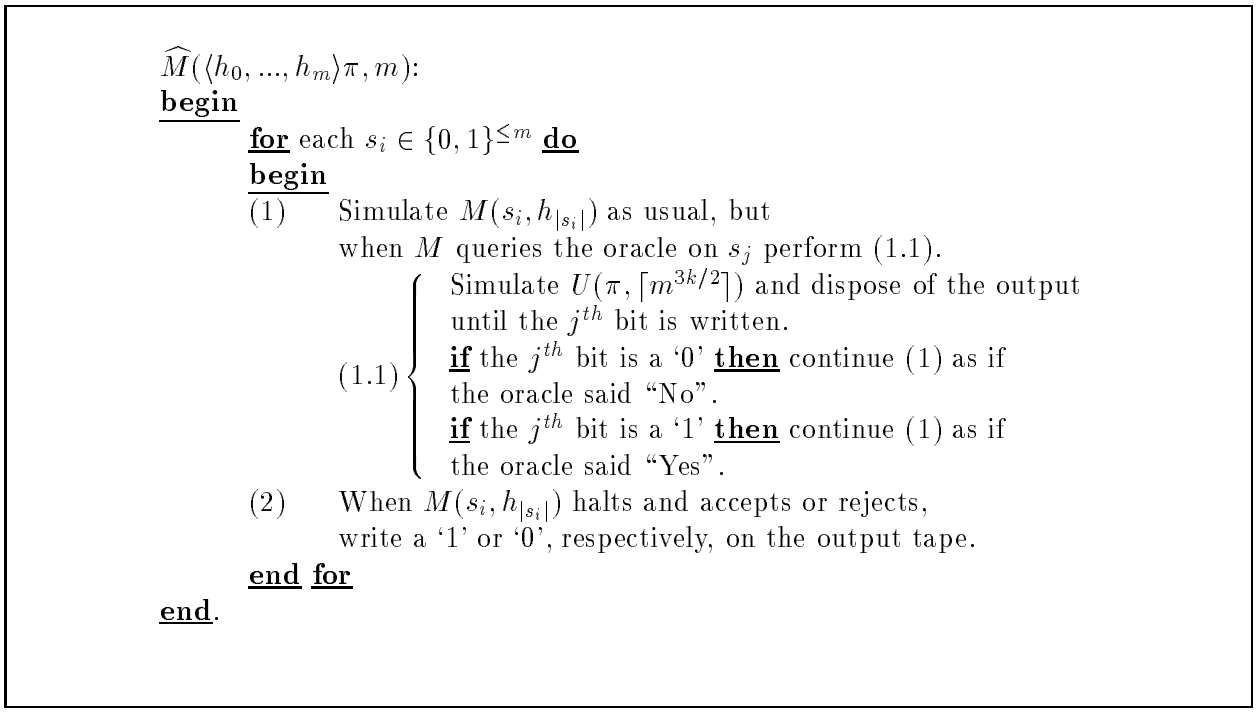

Figure 2: The algorithm for $\widehat{M}$ in the proof of Theorem 4.1.

Note that Theorem 4.1 extends Corollary 4.2 in two directions. First, Theorem 4.1 uses a more general reducibility. Second, and more importantly, Theorem 4.1 uses a more general notion of hardness.

The following result shows that Theorem 4.1 cannot be significantly improved, even if we restrict our attention to languages that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE.

Fact 4.3. For every $\epsilon > 0$, there exist a constant $c \in \mathbf{N}$ and a $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language C for ESPACE such that

$$KS^{2^{n^\epsilon}}(C_{=n}) \leq c \text{ a.e.}$$

and

$$KS^{2^{n^\epsilon}}(C_{\leq n}) \leq c \text{ a.e.}$$

Proof. By a routine padding argument, there is a language $C \in \mathrm{DSPACE}(2^{n^{\frac{\epsilon}{2}}})$ that is $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE. Then there are fixed programs π_0, π_1 such that

(1) $U(\pi_0, n) = \chi_{C_{=n}}$ in less than 2^{n^ϵ} space, and

(2) $U(\pi_1, n) = \chi_{C_{\leq n}}$ in less than 2^{n^ϵ} space.

□

The rest of this section is devoted to proving and exploiting the Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in ESPACE. We first show that the Small Span Theorem has two equivalent formulations.

We call a reducibility $\leq_{\mathcal{R}}$ an *extension of* $\leq_{\mathrm{m}}^{\mathrm{P}}$ if, for all $A, B \subseteq \{0,1\}^*$, $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ implies $A \leq_{\mathcal{R}} B$.

Lemma 4.4. If $\leq_{\mathcal{R}}$ is a transitive extension of $\leq_{\mathrm{m}}^{\mathrm{P}}$, then the following two conditions are equivalent.

(1) For every $A \in \mathrm{ESPACE}$,

$$\mu(\mathcal{R}(A) \mid \mathrm{ESPACE}) = 0$$

or

$$\mu_{\mathrm{pspace}}(\mathcal{R}^{-1}(A)) = \mu(\mathcal{R}^{-1}(A) \mid \mathrm{ESPACE}) = 0.$$

(2) For almost every $A \in \mathrm{ESPACE}$,

$$\mu_{\mathrm{pspace}}(\mathcal{R}^{-1}(A)) = 0.$$

(Note that (1) is the Small Span Theorem for $\leq_{\mathcal{R}}$-reductions in ESPACE.)

Proof. Let

$$X = \{A \subseteq \{0,1\}^* \mid \mu_{\mathrm{pspace}}(\mathcal{R}^{-1}(A)) = 0\}.$$

Assume that (1) holds. Then X contains every weakly $\leq_{\mathcal{R}}$-complete language for ESPACE. Since $\leq_{\mathcal{R}}$ is an extension of $\leq_{\mathrm{m}}^{\mathrm{P}}$, it follows by Theorem 2.3 that X has measure 1 in ESPACE. Thus (2) holds.

Conversely, assume that (2) holds, and let $A \in \mathrm{ESPACE}$. We have two cases.
Case I. If $\mathcal{R}(A) \cap X \cap \mathrm{ESPACE} = \emptyset$, then (2) tells us that $\mu(\mathcal{R}(A)|\mathrm{ESPACE}) = 0$.
Case II. If $\mathcal{R}(A) \cap X \cap \mathrm{ESPACE} \neq \emptyset$, then fix a language $B \in \mathcal{R}(A) \cap X$. Then $\mu_{\mathrm{pspace}}(\mathcal{R}^{-1}(B)) = 0$ and $\mathcal{R}^{-1}(A) \subseteq \mathcal{R}^{-1}(B)$ (because $\leq_{\mathcal{R}}$ is transitive), so

$$\mu_{\mathrm{pspace}}(\mathcal{R}^{-1}(A)) = \mu(\mathcal{R}^{-1}(A) \mid \mathrm{ESPACE}) = 0.$$

In either case, condition (1) is affirmed. □

Our proof of the Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in ESPACE 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 [19, 10].

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 $x \in B$.

We now prove the Small Span Theorem for $\leq_{\mathrm{T}}^{\mathrm{P/Poly}}$-reductions in ESPACE. Our proof is a nonuniform, space-bounded extension of a technique used by Fenner, Lutz, and Mayordomo [18] in the investigation of computational depth.

Theorem 4.5 (Small Span Theorem). For every $A \in \mathrm{ESPACE}$,

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

or

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

Proof. Let

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

By Lemma 4.4, it suffices to prove that

$$\mu(Y \mid \mathrm{ESPACE}) = 1. \tag{4.1}$$

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

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

Note that, for all $k, j \in \mathbf{N}$ and $A \subseteq \{0,1\}^*$,

$$\Pr(\mathcal{E}_{k,j}^A) \leq 2^{-N_A(k,j)}. \tag{4.2}$$

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 $w \in \{0,1\}^*$,

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

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 $A \in \mathrm{ESPACE}$.

We now show that, for all $k, j \in \mathbf{N}$, all $A, B \subseteq \{0,1\}^*$, and all $h \in \mathrm{ADV}$, if $A = L(M^B_k/h)$, then

$$\liminf_{l \to \infty} d^A_{k,j}(\chi_B[0..l-1]) \geq 2^{N_A(k,j) - b(n(j))}, \tag{4.3}$$

where $n(j) = \lceil \log(j+1) \rceil$. To see this, 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 $(M^B_k/h)(s_0), \cdots, (M^B_k/h)(s_{j-1})$ 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 by (4.2) that

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

$$\geq \quad 2^{N_A(k,j)-b(n(j))}.$$

This confirms (4.3).

Now let

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

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 $w_l = \chi_B[0..l-1]$, (4.3) tells us that

$$\begin{aligned}
\limsup_{l\to\infty} d^A(w_l) &\geq \limsup_{l\to\infty} \sum_{j=0}^{\infty} 2^{-\frac{k+j}{4}} d^A_{k,j}(w_l) \\
&\geq \sum_{j=0}^{\infty} 2^{-\frac{k+j}{4}} \liminf_{l\to\infty} d^A_{k,j}(w_l) \\
&\geq \sum_{j=0}^{\infty} 2^{N_A(k,j)-b(n(j))-\frac{k+j}{4}}.
\end{aligned}$$

Since $A \in X$, we have $N_A(k,j) - b(n(j)) > \frac{j}{4}$ 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 $B \in S^\infty[d^A]$. This proves that, for all $A \in X$,

$$(\mathrm{P/Poly})^{-1}_{\mathrm{T}}(A) \subseteq S^\infty[d^A]. \tag{4.4}$$

We next show that

$$\mu_{\mathrm{pspace}}(X) = 1. \tag{4.5}$$

To see this, 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 (4.5) holds.

We now conclude the proof. By (4.4) and the fact that d^A is pspace-computable when $A \in$ ESPACE, we have $X \cap \text{ESPACE} \subseteq Y$. It follows that $Y^c \cap \text{ESPACE} \subseteq X^c$, whence (4.5) tells us that

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

i.e., that (4.1) holds. □

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

Theorem 4.6. $\mu_{\text{pspace}}(\mathcal{H}_{\text{T}}^{\text{P/Poly}}(\text{ESPACE})) = 0$.

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

Corollary 4.7. $\mu_{\text{pspace}}(\mathcal{C}_{\text{T}}^{\text{P/Poly}}(\text{ESPACE})) = 0$. □

Let $\mathcal{WH}_{\mathcal{R}}(\text{ESPACE})$ and $\mathcal{WC}_{\mathcal{R}}(\text{ESPACE})$ denote the sets of languages that are weakly $\leq_{\mathcal{R}}$-hard and weakly $\leq_{\mathcal{R}}$-complete, respectively, for ESPACE. Theorem 2.3 tells us that, in contrast with Theorem 4.6 and Corollary 4.7,

$$\mu_{\text{pspace}}(\mathcal{WH}_{\text{m}}^{\text{P}}(\text{ESPACE})) = \mu(\mathcal{WC}_{\text{m}}^{\text{P}}(\text{ESPACE}) \mid \text{ESPACE}) = 1.$$

Thus, *almost every* language in ESPACE is weakly $\leq_m^P$-complete, hence certainly weakly $\leq_T^{P/Poly}$-complete, for ESPACE.

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

Theorem 4.8. For all $A \subseteq \{0,1\}^*$,

$$\mu(\deg_T^{P/Poly}(A) \mid \text{ESPACE}) = 0.$$

Proof. Let $A \subseteq \{0,1\}^*$. If $\deg_T^{P/Poly}(A) \cap \text{ESPACE} = \emptyset$, the theorem is clearly affirmed, so assume not, and fix $B \in \deg_T^{P/Poly}(A) \cap \text{ESPACE}$. Then, by the Small Span Theorem, we have

$$\mu((P/Poly)_T(B) \mid \text{ESPACE}) = 0$$

or

$$\mu((P/Poly)_T^{-1}(B) \mid \text{ESPACE}) = 0.$$

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

Finally, we note that Theorem 4.8 generalizes the following known result.

Corollary 4.9 (Lutz [38]). $\mu(P/Poly \mid \text{ESPACE}) = 0$.

5 Completeness and Weak Completeness Under P/Poly-Many-One Reductions

We now investigate the nonuniform complexities of languages that are hard or weakly hard for ESPACE under $\leq_m^{P/Poly}$-reductions — nonuniform many-one reductions that are computed by polynomial-size circuits. We establish an exponential lower bound on the sizes of complexity cores of weakly $\leq_m^{P/Poly}$-hard languages for ESPACE. More importantly, we establish nontrivial *upper* bounds on the sizes of nonuniform complexity cores, and on the space-bounded Kolmogorov complexities, of $\leq_m^{P/Poly}$-hard languages for ESPACE. Our upper bounds are violated by almost every element of ESPACE, so the fact that they hold for the $\leq_m^{P/Poly}$-hard languages provides a concrete sense in which the $\leq_m^{P/Poly}$-complete languages for ESPACE are *unusually simple* elements of ESPACE. All the above bounds are shown to be tight.

The following theorem extends work of Huynh [23], who showed that every $\leq_m^P$-hard language for ESPACE has a dense P/Poly-complexity core. Our proof uses the following special notation.

The *nonreduced image* of a language $S \subseteq \{0,1\}^*$ under a function $f : \{0,1\}^* \to \{0,1\}^*$ is

$$f^{\geq}(S) = \{f(x) \mid x \in S \text{ and } |f(x)| \geq |x|\}.$$

Note that

$$f^{\geq}(f^{-1}(S)) = S \cap f^{\geq}(\{0,1\}^*)$$

for all f and S.

Theorem 5.1. For every weakly $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-hard language H for ESPACE, there is a real $\epsilon > 0$ such that H has a dense DSPACE(2^{n^ϵ})/Poly-complexity core.

Proof. Let H be weakly $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-hard for ESPACE, let

$$X = \{A \subseteq \{0,1\}^* \mid A \text{ is } n^{\log n}\text{-incompressible by } \leq_m^{\mathrm{DSPACE}(2^n)/\mathrm{Poly}}\text{-reductions}\},$$

and let

$$Y = \{A \subseteq \{0,1\}^* \mid A \text{ has } \{0,1\}^* \text{ as a DSPACE}(2^n)/\text{Poly-complexity core}\}.$$

By Corollary 3.7 and Theorem 3.8 the set $X \cap Y$ has measure 1 in ESPACE. Moreover, since $(\mathrm{P/Poly})_{\mathrm{m}}(H)$ does not have measure 0 in ESPACE, $X \cap Y \cap (\mathrm{P/Poly})_{\mathrm{m}}(H)$ is not empty. Fix $A \in X \cap Y \cap (\mathrm{P/Poly})_{\mathrm{m}}(H)$, let f be a $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reduction of A to H, let q be a strictly increasing polynomial bound on the length of strings produced by f (i.e., $q(n) \geq \max\{|f(x)| \mid x \in \{0,1\}^{\leq n}\}$), and let $\epsilon = \frac{1}{3 \cdot deg(q)}$. We show that

$$K = f^{\geq}(\{0,1\}^*)$$

is a dense DSPACE(2^{n^ϵ})/Poly-complexity core of H.

By our choice of ϵ, $q(\lfloor n^{2\epsilon} \rfloor) < n$ for all sufficiently large n. Let $W = \{x \mid |f(x)| < |x|\}$. Then, for all sufficiently large $n \in \mathbf{N}$, writing $m = \lfloor n^{2\epsilon} \rfloor$, we have

$$\begin{aligned} f(\{0,1\}^{\leq m}) - \{0,1\}^{<m} &\subseteq f(\{0,1\}^{\leq m}) - f(W_{\leq m}) \\ &\subseteq f^{\geq}(\{0,1\}^{\leq m}) \\ &\subseteq K_{\leq q(m)} \\ &\subseteq K_{\leq n}, \end{aligned}$$

whence

$$\begin{aligned} |K_{\leq n}| &\geq |f(\{0,1\}^{\leq m})| - |\{0,1\}^{<m}| \\ &\geq |\{0,1\}^{\leq m}| - |(C_f)_{\leq m}| - |\{0,1\}^{<m}| \\ &= 2^m - |(C_f)_{\leq m}| \\ &\geq 2^{\lfloor n^{2\epsilon} \rfloor} - |(C_f)_{\leq n}|. \end{aligned}$$

Since $|(C_f)_{\leq n}| < n^{\log n}$ a.e., it follows that $|K_{\leq n}| > 2^{n^\epsilon}$ for all sufficiently large n. Thus K is dense.

To see that K is a DSPACE(2^{n^ϵ})/Poly-complexity core of H, let $c \in \mathbf{N}$, let M be a machine and h be a polynomial advice function such that M/h is consistent with H, and define the fast set

$$F = \{x \mid space_{M/h}(x) \leq c \cdot 2^{|x|^\epsilon} + c\}.$$

Let $\widehat{M}/\widehat{h}$ be a machine/polynomial advice pair (constructed in the obvious way) such that

$$\widehat{M}/\widehat{h}(x) = M/h(f(x))$$

for all $x \in \{0,1\}^*$. Since f reduces A to H and M/h is consistent with H, $\widehat{M}/\widehat{h}$ is consistent with A. Since A has $\{0,1\}^*$ as a DSPACE(2^n)/Poly-complexity core, the fast set

$$\widehat{F} = \{x \mid space_{\widehat{M}/\widehat{h}}(x) \leq c \cdot 2^n + c\}$$

is sparse. By our choice of ϵ, $y \in F \cap f(\{0,1\}^*)$ implies $y \in f(\widehat{F})$ for all but finitely many y. Since $\widehat{F}$ is sparse, there is a polynomial p such that, for all $n \in \mathbf{N}$,

$$\begin{aligned} |(F \cap K)_{\leq n}| &= |(F \cap f^{\geq}(\{0,1\}^{\leq n})_{\leq n}| \\ &\leq |(f^{\geq}(\widehat{F} \cap \{0,1\}^{\leq n}))_{\leq n}| + c \\ &\leq |\widehat{F} \cap \{0,1\}^{\leq n}| + c \\ &\leq p(n) + c. \end{aligned}$$

Hence $F \cap K$ is sparse. Thus K is a DSPACE(2^{n^ϵ})/Poly-complexity core of H. □

Corollary 5.2 (Huynh [23]). Every $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard language for ESPACE has a dense P/Poly-complexity core. □

The following result shows that Theorem 5.1 cannot be significantly improved, even if we restrict attention to languages that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for ESPACE.

Fact 5.3. For every $\epsilon > 0$, there is a $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete language C for ESPACE such that each DSPACE(2^{n^ϵ})/Poly-complexity core of C is sparse.

Proof. Let $C \in$ DSPACE(2^{n^ϵ}) be $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for ESPACE. Since C can be decided in 2^{n^ϵ} space, every DSPACE(2^{n^ϵ})/Poly-complexity core of C must be sparse. □

The rest of this section is devoted to upper bounds on the nonuniform complexities of $\leq^{\mathrm{P/Poly}}_{\mathrm{m}}$-hard languages for ESPACE.

Lemma 5.4. Let $A, H \subseteq \{0,1\}^*$. If $A \in \mathrm{DSPACE}(2^{cn})$, A is $n^{\log n}$-incompressible by $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reductions, and $A \leq_{\mathrm{m}}^{\mathrm{P/Poly}} H$, then there exist $B, D \in \mathrm{DSPACE}(2^{cn})/\mathrm{Poly}$ such that D is dense and $B = H \cap D$.

Proof. Assume the hypothesis and let f be a $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-reduction of A to H. Let $B = f^{\geq}(A)$ and $D = f^{\geq}(\{0,1\}^*)$. (Recall that $f^{\geq}(S) = \{f(x) \mid x \in S \text{ and } |f(x)| \geq |x|\}$.) Since $A \in \mathrm{DSPACE}(2^{cn})$ and $f \in \mathrm{PF/Poly}$, it is clear that $B, D \in \mathrm{DSPACE}(2^{cn})/\mathrm{Poly}$. Furthermore, it is clear that D is dense (using the argument given for K in the proof of Theorem 5.1), and $B = f^{\geq}(A) = f^{\geq}(f^{-1}(H)) = H \cap f^{\geq}(\{0,1\}^*) = H \cap D$. □

By Lemma 5.4 and Lemma 3.10, we now have the following result, which says that every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-hard language for ESPACE is $\mathrm{DSPACE}(2^{2n})/\mathrm{Poly}$-decidable on a dense, $\mathrm{DSPACE}(2^{2n})/\mathrm{Poly}$-decidable set of inputs.

Theorem 5.5. For every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-hard language H for ESPACE, there exist B, D in $\mathrm{DSPACE}(2^{2n})/\mathrm{Poly}$ such that D is dense and $B = H \cap D$. □

We now derive our upper bound on the sizes of complexity cores of $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-hard languages for ESPACE.

Theorem 5.6. Every $\mathrm{DSPACE}(2^{2n})/\mathrm{Poly}$-complexity core of every $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-hard language for ESPACE has a dense complement.

Proof. Let H be $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-hard for ESPACE, and let K be a $\mathrm{DSPACE}(2^{2n})/\mathrm{Poly}$-complexity core of H. Choose B, D for H as in Theorem 5.5, and fix machine/advice pairs M_B/h_B, M_D/h_D that decide B, D and testify that $B, D \in \mathrm{DSPACE}(2^{2n})/\mathrm{Poly}$. (To be more precise, let M_B, M_D be machines and h_B, h_D be polynomially bounded advice functions such that $[\![M_B(\langle x, h_B(|x|)\rangle)]\!] = [\![x \in B]\!]$, $[\![M_D(\langle x, h_D(|x|)\rangle)]\!] = [\![x \in D]\!]$, $\mathrm{space}_{M_B}(\langle x, h_B(|x|)\rangle) = O(2^{2|x|})$, and $\mathrm{space}_{M_D}(\langle x, h_D(|x|)\rangle) = O(2^{2|x|})$.) Let M be a machine that implements the following algorithm.

$M(\langle x, \langle y, z\rangle\rangle)$
begin
  if $M_D(\langle x, z\rangle)$ accepts
    then simulate $M_B(\langle x, y\rangle)$
  else run forever.
end M.

Then $x \in D \Rightarrow M(\langle x, \langle h_B(|x|), h_D(|x|)\rangle\rangle) = [\![x \in B]\!] = [\![x \in H \cap D]\!] = [\![x \in H]\!]$ and $x \notin D \Rightarrow M(\langle x, \langle h_B(|x|), h_D(|x|)\rangle\rangle) = \bot \leq [\![x \in H]\!]$, so $M/\langle h_B, h_D\rangle$ is consistent with H. Furthermore,

there is a constant $c \in N$ such that for all $x \in D$,

$$\text{space}_M(\langle x, \langle h_B(|x|), h_D(|x|)\rangle\rangle) \leq c \cdot 2^{2|x|} + c.$$

Since K is a DSPACE(2^{2n})/Poly-complexity core of H, it follows that $K \cap D$ is sparse. Since D is dense, it follows that $D - K \subseteq K^c$ is dense. □

We now use Theorem 5.5 to show that every $\leq_{\text{m}}^{\text{P/Poly}}$-hard language for ESPACE has unusually low space-bounded Kolmogorov complexity infinitely often.

Theorem 5.7. For every $\leq_{\text{m}}^{\text{P/Poly}}$-hard language H for ESPACE, there exists $\epsilon > 0$ such that

$$KS^{2^{3n}}(H_{=n}) < 2^n - 2^{n^\epsilon} \text{ i.o.}$$

Proof. Let H be $\leq_{\text{m}}^{\text{P/Poly}}$-hard for ESPACE and fix B, D as in Theorem 5.5. Let the machines M_B, M_D and the advice functions h_B, h_D testify that $B, D \in$ DSPACE(2^{2n})/Poly, and fix $\epsilon > 0$ such that $|D_{=n}| > 2^{n^{2\epsilon}}$ i.o.

```
M(⟨u, v⟩y, n);
begin
        z = ⊥^(2^n);
        for i = 0 to 2^n − 1 do
        begin
                if M_D(w_i, u) accepts then
                   simulate M_B(w_i, v);
                   if this simulation accepts or rejects
                   then set z[i] = 1 or z[i] = 0, respectively
                else
                        (z[i], y) = (head(y), tail(y));
        end;
        output z;
end.
```

Figure 3: The machine M in the proof of Theorem 5.7.

Let M be a machine that efficiently implements the algorithm in Figure 3, and let y_n be the string $\chi_{H_{=n}}$, with the bits corresponding to $D_{=n}$ removed. Then the machine M, on input

$(\langle h_D(n), h_B(n)\rangle y_n, n)$, outputs the string $\chi_{H_{=n}}$ and uses $O(2^{2n})$ space. It follows that, for all sufficiently large n,

$$\begin{aligned} KS^{2^{3n}}(H_{=n}) &\leq KS_M^{c2^{2n}+c}(H_{=n}) + c \\ &\leq |\langle h_D(n), h_B(n)\rangle y_n| + c \\ &\leq 2^n - |D_{=n}| + |\langle h_D(n), h_B(n)\rangle| + c. \end{aligned}$$

Because both h_B and h_D are bounded in length by a polynomial, there is a polynomial p such that $|\langle h_D(n), h_B(n)\rangle| \leq p(n)$. Thus, for infinitely many n,

$$KS^{2^{3n}}(H_{=n}) < 2^n - |D_{=n}| + p(n) + c \leq 2^n - 2^{n^\epsilon}.$$

□

By Corollaries 3.5 and 3.7, almost every element of ESPACE fails to obey the upper bounds on nonuniform complexity given by Theorems 5.6 and 5.7. Thus, with respect to size of nonuniform complexity cores and space-bounded Kolmogorov complexity, the $\leq_{\mathrm{m}}^{\mathrm{P/Poly}}$-complete languages are *unusually simple* elements of ESPACE.

By Theorem 2.3, almost every element of ESPACE is weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete. It follows by Corollaries 3.5 and 3.7 that the upper bounds on nonuniform complexity given by Theorems 5.6 and 5.7 do *not* hold for all weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages.

Our next theorem shows that Theorem 5.6 cannot be significantly improved.

Theorem 5.8. For every $\epsilon > 0$, there exists a $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language C for ESPACE with a DSPACE(2^{2n})/Poly-complexity core K with density

$$|K_{\leq n}| \geq 2^{n+1} - 2^{n^\epsilon} \text{ a.e.}$$

Proof. Fix $\epsilon > 0$ and $k \in \mathbf{N}$ such that $\epsilon > \frac{1}{k} > 0$, let A be $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE, and fix $D \in$ ESPACE such that D has $\{0,1\}^*$ as a DSPACE(2^{2n})/Poly-complexity core. Let $B = \{0^{|x|^k}1x \mid x \in A\}$, let $K = \{0,1\}^* - \{0^{|x|^k}1x \mid x \in \{0,1\}^*\}$, and define $C = (D \cap K) \cup B$. Since B is $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE, K is decidable in polynomial time, and $K \cap B$ is empty, it is clear that C is $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for ESPACE. Moreover, notice that

$$\begin{aligned} |K_{\leq n}| &= |\{0,1\}^{\leq n} - \{0^{|x|^k}1x | x \in \{0,1\}^*\}_{\leq n}| \\ &= 2^{n+1} - 1 - |\{0^{|x|^k}1x \;\Big|\; |x|^k + 1 + |x| \leq n\}| \\ &\geq 2^{n+1} - 2^{n^{\frac{1}{k}}+1} \\ &\geq 2^{n+1} - 2^{n^\epsilon} \text{ a.e.} \end{aligned}$$

Thus it suffices to show that K is a DSPACE(2^{2^n})/Poly-complexity core of C.

Let M/h be a machine/polynomial advice pair that is consistent with C, let c be a constant, and define the fast set

$$F = \{x \in \{0,1\}^* \mid space_{M/h}(x) \leq c \cdot 2^{2|x|} + c\}.$$

Let $\widehat{M}$ be a machine (designed in the obvious way) such that

$$\widehat{M}/h(x) = \begin{cases} \perp & \text{if } x \in K^c \\ M/h(x) & \text{otherwise,} \end{cases}$$

and define the fast set

$$\widehat{F} = \{x \in \{0,1\}^* \mid space_{\widehat{M}/h}(x) \leq (c+1) \cdot 2^{2|x|} + c\}.$$

Since membership in K^c is decidable in polynomial time, it is clear that the symmetric difference $F \triangle \widehat{F}$ has finite intersection with K. Furthermore, since $\widehat{M}$ is consistent with D, $\widehat{F}$ is sparse. Since

$$\begin{aligned} F \cap K &= (F \cap \widehat{F}^c \cap K) \cup (F \cap \widehat{F} \cap K) \\ &\subseteq ((F \triangle \widehat{F}) \cap K) \cup (F \cap \widehat{F} \cap K) \\ &\subseteq ((F \triangle \widehat{F}) \cap K) \cup \widehat{F}, \end{aligned}$$

it follows that $F \cap K$ is sparse. Thus K is a DSPACE(2^{2^n})/Poly-complexity core of C.

□

As the following theorem shows, the upper bound given by Theorem 5.7 is also tight.

Theorem 5.9. For every $\epsilon > 0$, there exists a $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete language C for ESPACE such that

$$KS^{2^{2^n}}(C_{=n}) > 2^n - 2^{n^\epsilon} \text{ a.e.}$$

Proof. Fix $\epsilon > 0$ and $k \in \mathbf{N}$ such that $\epsilon > \frac{1}{k} > 0$. Let A be $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for ESPACE, let $B = \{0^{|x|^k}1x \mid x \in A\}$, and let $K = \{0^{|x|^k}1x \mid x \in \{0,1\}^*\}$. Note that B is $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for ESPACE and K is decidable in polynomial time. Now construct C in stages as in Figure 4. Since $C \cap K = B$, it is clear that C is $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for ESPACE. It thus suffices to show that

$$KS^{2^{2^n}}(C_{=n}) > 2^n - 2^{n^\epsilon} \text{ a.e.}$$

Stage 0:
$C = B_{=0}$;

Stage n:
for each subset C^n of $\{0,1\}^n$ **do**
  done = true;
  if $(C^n \cap K_{=n}) = B_{=n}$ **then**
  begin
    for each program $\pi \in \{0,1\}^{<2^n - 2^{n^{\frac{1}{k}}}}$ **do**
      done=false if $U(\pi, n) = \chi_{C^n}$ in $\leq 2^{2n}$ space
    if done **then**
      $C = C \cup C^n$;
      exit stage n;
end
$C = C \cup B_{=n}$;
END OF CONSTRUCTION

Figure 4: The construction of a $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language with high KS a.e.

There are $|\mathcal{P}(K^c_{=n})|$ subsets C^n of $\{0,1\}^n$ that satisfy $(C^n \cap K_{=n}) = B_{=n}$. For almost every n, since $|\mathcal{P}(K^c_{=n})| > 2^{2^n - 2^{n^{\frac{1}{k}}}}$, there is some set C^n such that $(C^n \cap K_{=n}) = B_{=n}$ and no string π in $\{0,1\}^{<2^n - 2^{n^{\frac{1}{k}}}}$ produces χ_{C^n} in $\leq 2^{2n}$ space. Hence, we have

$$\begin{aligned} KS^{2^{2n}}(C_{=n}) = KS^{2^{2n}}(C^n) &\geq 2^n - 2^{n^{\frac{1}{k}}} \\ &> 2^n - 2^{n^\epsilon} \text{ a.e.} \end{aligned}$$

□

6 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 [5] 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 $\leq_T^P$-reductions and $\leq_T^{P/Poly}$-reductions in E and E_2.

There is also an interesting question concerning the complexities of $\leq_T^{P/Poly}$-complete problems for ESPACE. It was shown in section 5 that every $\leq_m^{P/Poly}$-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 $\leq_m^{P/Poly}$-complete languages for ESPACE are *unusually simple* elements of ESPACE. Similar results hold for $\leq_m^P$-complete languages for E and E_2 [26]. However, it remains an open problem whether there is a natural sense in which the $\leq_T^{P/Poly}$-complete languages for ESPACE are unusually simple elements of ESPACE.

Acknowledgments. The second author thanks Elvira Mayordomo and Martin Strauss for useful discussions. Both authors thank two anonymous referees for their careful reading, for pointing out an error in the first version of Theorem 3.8, and for several useful suggestions.

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] E. Allender and R. Rubinstein, P-printable sets, *SIAM Journal on Computing* **17** (1988), pp. 1193–1202.

[3] E. W. Allender, Some consequences of the existence of pseudorandom generators, *Journal of Computer and System Sciences* **39** (1989), pp. 101–124.

[4] E. W. Allender and O. Watanabe, Kolmogorov complexity and degrees of tally sets, *Information and Computation* **86** (1990), pp. 160–178.

[5] K. Ambos-Spies, H.-C. Neis, and S. A. Terwijn, Genericity and measure for exponential time, *Theoretical Computer Science*, to appear. See also *Proceedings of the* 19^{th} *Symposium on Mathematical Foundations of Computer Science*, 1994, pp. 221–232. Springer–Verlag.

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

[7] J. L. Balcázar and R. V. Book, Sets with small generalized Kolmogorov complexity, *Acta Informatica* **23** (1986), pp. 679–688.

[8] J. L. Balcázar and U. Schöning, Bi-immune sets for complexity classes, *Mathematical Systems Theory* **18** (1985), pp. 1–10.

[9] L. Berman and J. Hartmanis, On isomorphism and density of NP and other complete sets, *SIAM Journal on Computing* **6** (1977), pp. 305–322.

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

[11] R. Book and D.-Z. Du, The existence and density of generalized complexity cores, *Journal of the ACM* **34** (1987), pp. 718–730.

[12] R. Book, D.-Z Du, and D. Russo, On polynomial and generalized complexity cores, *Proceedings of the Third Structure in Complexity Theory Conference*, 1988, pp. 236–250. IEEE Computer Society Press.

[13] G. J. Chaitin, On the length of programs for computing finite binary sequences, *Journal of the Association for Computing Machinery* **13** (1966), pp. 547–569.

[14] S. A. Cook, The complexity of theorem proving procedures, *Proceedings of the Third ACM Symposium on the Theory of Computing*, 1971, pp. 151–158. Association for Computing Machinery.

[15] D.-Z. Du, *Generalized complexity cores and levelability of intractable sets*, PhD thesis, University of California, Santa Barbara, 1985.

[16] D.-Z. Du and R. Book, On inefficient special cases of *NP*-complete problems, *Theoretical Computer Science* **63** (1989), pp. 239–252.

[17] S. Even, A. Selman, and Y. Yacobi, Hard core theorems for complexity classes, *Journal of the ACM* **35** (1985), pp. 205–217.

[18] S. A. Fenner, J. H. Lutz, and E. Mayordomo, Weakly useful sequences, *Proceedings of the* 22^{nd} *International Colloquium on Automata, Languages, and Programming*, 1995, pp. 393–404. Springer–Verlag.

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

[20] J. Hartmanis, Generalized Kolmogorov complexity and the structure of feasible computations, *Proceedings of the 24th IEEE Symposium on the Foundations of Computer Science*, 1983, pp. 439–445. Institute of Electrical and Electronics Engineers.

[21] J. Hartmanis and Y. Yesha, Computation times of NP sets of different densities, *Theoretical Computer Science* **34** (1984), pp. 17–32.

[22] D. T. Huynh, Resource-bounded Kolmogorov complexity of hard languages, *Structure in Complexity Theory*, 1986, pp. 184–195, Berlin. Springer-Verlag.

[23] D. T. Huynh, On solving hard problems by polynomial-size circuits, *Information Processing Letters* **24** (1987), pp. 171–176.

[24] D. W. Juedes, *The Complexity and Distribution of Computationally Useful Problems*, PhD thesis, Iowa State University, 1994.

[25] D. W. Juedes, Weakly complete problems are not rare, *Computational Complexity*, to appear.

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

[27] D. W. Juedes and J. H. Lutz, Weak completeness in E and E_2, *Theoretical Computer Science* **143** (1995), pp. 149–158.

[28] R. Kannan, Circuit-size lower bounds and non-reducibility to sparse sets, *Information and Control* **55** (1982), pp. 40–56.

[29] R. M. Karp, Reducibility among combinatorial problems, In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pp. 85–104. Plenum Press, New York, 1972.

[30] K. Ko, On the notion of infinite pseudorandom sequences, *Theoretical Computer Science* **48** (1986), pp. 9–33.

[31] A. N. Kolmogorov, Three approaches to the quantitative definition of 'information', *Problems of Information Transmission* **1** (1965), pp. 1–7.

[32] L. A. Levin, Universal sequential search problems, *Problems of Information Transmission* **9** (1973), pp. 265–266.

[33] L. A. Levin, Randomness conservation inequalities; information and independence in mathematical theories, *Information and Control* **61** (1984), pp. 15–37.

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

[35] L. Longpré, *Resource Bounded Kolmogorov Complexity, a Link Between Computational Complexity and Information Theory*, PhD thesis, Cornell University, 1986, Technical Report TR-86-776.

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

[37] J. H. Lutz, An upward measure separation theorem, *Theoretical Computer Science* **81** (1991), pp. 127–135.

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

[39] 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.

[40] J. H. Lutz, Resource-bounded measure, in preparation.

[41] 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*, 1994, pp. 415–426. Springer–Verlag.

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

[43] N. Lynch, On reducibility to complex or sparse sets, *Journal of the ACM* **22** (1975), pp. 341–345.

[44] P. Martin-Löf, Complexity oscillations in infinite binary sequences, *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete* **19** (1971), pp. 225–230.

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

[46] A. R. Meyer, 1977, reported in [9].

[47] P. Orponen, A classification of complexity core lattices, *Theoretical Computer Science* **70** (1986), pp. 121–130.

[48] P. Orponen and U. Schöning, The density and complexity of polynomial cores for intractable sets, *Information and Control* **70** (1986), pp. 54–68.

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

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

[51] K. W. Regan, D. Sivakumar, and J .Cai, On resource-bounded measure and pseudorandom generators, *Proceedings of the* 36^{th} *Symposium on the Foundations of Computer Science*, 1995, to appear.

[52] D. A. Russo and P. Orponen, On P-subset structures, *Mathematical Systems Theory* **20** (1987), pp. 129–136.

[53] M. Sipser, A complexity-theoretic approach to randomness, *Proceedings of the 15th ACM Symposium on Theory of Computing*, 1983, pp. 330–335. Association for Computing Machinery.

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

[55] R. J. Solomonoff, A formal theory of inductive inference, *Information and Control* **7** (1964), pp. 1–22, 224–254.

[56] H. Ye, Complexity cores for P/poly, 1990, manuscript.