The Complexity and Distribution of Hard Problems *

David W. Juedes and Jack H. Lutz
Department of Computer Science
Iowa State University
Ames, IA 50011

Abstract

Measure-theoretic aspects of the $\leq_{\mathrm{m}}^{\mathrm{P}}$-reducibility structure of the exponential time complexity classes E=DTIME(2^{linear}) and E_2 = DTIME($2^{\mathrm{polynomial}}$) are investigated. Particular attention is given to the *complexity* (measured by the size of complexity cores) and *distribution* (abundance in the sense of measure) of languages that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E and other complexity classes.

Tight upper and lower bounds on the size of complexity cores of hard languages are derived. The upper bound says that the $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard languages for E are *unusually simple*, in the sense that they have smaller complexity cores than most languages in E. It follows that the $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages for E form a measure 0 subset of E (and similarly in E_2).

This latter fact is seen to be a special case of a more general theorem, namely, that *every* $\leq_{\mathrm{m}}^{\mathrm{P}}$-degree (e.g., the degree of all $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete languages for NP) has measure 0 in E and in E_2.

1 Introduction

A decision problem (i.e., language) $A \subseteq \{0,1\}^*$ is said to be *hard* for a complexity class $\mathcal{C}$ if every language in $\mathcal{C}$ is efficiently reducible to A. If A is also an element of $\mathcal{C}$, then A is *complete* for $\mathcal{C}$. The most common interpretation of "efficiently reducible" here is "polynomial time many-one reducible," abbreviated "$\leq_{\mathrm{m}}^{\mathrm{P}}$-reducible." (See section 2 for notation and terminology used in this introduction.) For example, in most usages, "NP-complete" means "$\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for NP," the completeness notion introduced by Karp [15] and Levin [16].

*This research was supported in part by National Science Foundation Grants CCR-8809238 and CCR-9157382, with matching funds from Rockwell International and Microware Systems Corporation, and in part by the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS), where the second author was a visitor while part of this work was carried out.

In this paper, we investigate the *complexity* (measured by size of complexity cores) and *distribution* (i.e., abundance in the sense of measure) of languages that are $\leq_m^P$-hard for E (equivalently, E_2) and other complexity classes, including NP. (By "measure" here, we mean *resource-bounded measure* as developed by Lutz [17] and described in section 3 of the present paper.) We give a tight lower bound and, perhaps surprisingly, a tight *upper* bound on the sizes of complexity cores of hard languages. More generally, we analyze measure-theoretic aspects of the $\leq_m^P$-reducibility structure of exponential time complexity classes. We prove that $\leq_m^P$-hard problems are rare, in the sense that they form a p-measure 0 set. We also prove that every $\leq_m^P$-degree has measure 0 in exponential time.

Complexity cores, first introduced by Lynch [24] have been studied extensively [8, 9, 10, 11, 12, 14, 27, 28, 29, etc.]. Intuitively, a complexity core of 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 all but finitely many elements of K. The meaning of "efficiently" is a parameter of the definition that varies according to the context. (See section 4 for a precise definition.)

Orponen and Schöning [28] have established two lower bounds on the sizes of complexity cores of hard languages. First, every $\leq_m^P$-hard language for E has a dense P-complexity core. Second, if P $\neq$ NP, then every $\leq_m^P$-hard language for NP has a non-sparse polynomial complexity core.

In section 4 below, we extend the first of these results to languages that are weakly $\leq_m^P$-hard for E. (A language A is $\leq_m^P$-hard for E if every element of E is $\leq_m^P$-reducible to A. A language A is *weakly* $\leq_m^P$*-hard* for E if every element of some nonnegligible, i.e., non-measure 0, set of languages in E is reducible to A. Very recently, Lutz [21] has proven that "weakly $\leq_m^P$-hard" is more general than "$\leq_m^P$-hard.") Specifically, we prove that every language that is weakly $\leq_m^P$-hard for E or E_2 has a dense exponential complexity core. It follows that, if NP does not have measure 0 in E or E_2, then every $\leq_m^P$-hard language for NP has a dense exponential complexity core. This conclusion is much stronger than Orponen and Schöning's conclusion that every such language has a non-sparse polynomial complexity core, though it is achieved at the cost of a stronger hypothesis. This hypothesis, originally proposed by Lutz, is discussed at some length in [20, 22, 23].

In section 5 we investigate the resource-bounded measure of the lower $\leq_m^P$-spans, the upper $\leq_m^P$-spans, and the $\leq_m^P$-degrees of languages in E and E_2. (The *lower* $\leq_m^P$*-span* of A is the set of all languages that are $\leq_m^P$-reducible to A. The *upper* $\leq_m^P$*-span* of A is the set of all languages to which A is $\leq_m^P$-reducible. The $\leq_m^P$*-degree* of A is the intersection of these two spans.) We prove the Small Span Theorem, which says that, if A is in E or E_2, then at least one of the upper and lower spans must have resource-bounded measure 0. This implies that *every* $\leq_m^P$-degree (e.g., the degree of all $\leq_m^P$-complete languages for NP) has measure 0 in E and in E_2. It also implies that the $\leq_m^P$-hard languages for E form a set of p-measure 0.

As noted in section 7, a proof that is latter fact holds with $\leq^{\mathrm{P}}_{\mathrm{m}}$ replaced by $\leq^{\mathrm{P}}_{\mathrm{T}}$ would imply that E $\not\subseteq$ BPP.

Languages that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E are typically considered to be "at least as complex as" any element of E. Very early, Berman [6] established limits to this interpretation by proving that no $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete language is P-immune, even though E contains P-immune languages. (In fact, Mayordomo [25] has recently shown that almost every language in E is P-bi-immune.) In section 6 below we prove a very strong limitation on the complexity of $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard languages for E. We prove that every $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard language for E is decidable in $\leq 2^{4n}$ steps on a dense set of inputs which is also decidable in $\leq 2^{4n}$ steps. This implies that *every* DTIME(2^{4n})-complexity core of *every* $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard language for E has a *dense complement*. Since almost every language in E has $\{0,1\}^*$ as a DTIME(2^{4n})-complexity core (as proven in section 4), this says that $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard languages for E are *unusually simple*, in that they have *unusually small* complexity cores. Intuitively, we interpret this to mean that the condition of being $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E forces a language to have a high level of organization, thereby forcing it to be unusually simple in some respects.

2 Preliminaries

Here we present the notation and terminology that we use throughout the paper. To begin with, we write $\mathbf{N}$ for the set of natural numbers, $\mathbf{Z}$ for the set of integers, and $\mathbf{Z}^+$ for set of positive integers.

We deal primarily with *strings*, *languages*, *functions*, and *classes*. Strings are finite sequences of characters over the alphabet $\{0,1\}$; we write $\{0,1\}^*$ for the set of all strings. Languages are sets of strings. Functions usually map $\{0,1\}^*$ into $\{0,1\}^*$. A class is either a set of languages or a set of functions.

If $x \in \{0,1\}^*$ is a string, we write $|x|$ for the *length* of x. If $A \subseteq \{0,1\}^*$ is a language, then we write A^c, $A_{\leq n}$, and $A_{=n}$ for $\{0,1\}^* - A$, $A \cap \{0,1\}^{\leq n}$, and $A \cap \{0,1\}^n$, respectively. The sequence of strings over $\{0,1\}$, $s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, ...$, is referred to as the *standard enumeration* of $\{0,1\}^*$.

We use the string-pairing function $\langle x, y\rangle = bd(x)01y$, where $bd(x)$ is x with each bit doubled (e.g., $bd(1101) = 11110011$). For each $g : \{0,1\}^* \to \{0,1\}^*$ and $k \in \mathbf{N}$, we also define the function $g_k : \{0,1\}^* \to \{0,1\}^*$ by $g_k(x) = g(\langle 0^k, x\rangle)$ for all $x \in \{0,1\}^*$.

We say that a property $\phi(n)$ of natural numbers holds *almost everywhere (a.e.)* if $\phi(n)$ is true for all but finitely many $n \in \mathbf{N}$. Similarly, $\phi(n)$ holds *infinitely often (i.o.)* if $\phi(n)$ is true for infinitely many $n \in \mathbf{N}$. We write $[\![\phi]\!]$ for the Boolean value of a condition ϕ. That is, $[\![\phi]\!] = 1$ if ϕ is true, $[\![\phi]\!] = 0$ if ϕ is false.

If A is a finite set, we denote its cardinality by $|A|$. A language D is *dense* if there exists some constant $\epsilon > 0$ such that $|D_{\leq n}| > 2^{n^\epsilon}$ a.e. A language S is *sparse* if there exists a polynomial p such that $|S_{\leq n}| \leq p(n)$ a.e.. A language S is *co-sparse* if S^c is sparse.

All *machines* here are deterministic Turing machines. The language accepted by a machine M is denoted by $L(M)$. The partial function computed by a machine M is denoted by $f_M : \{0,1\}^* \to \{0,1\}^*$. For a fixed machine M, the function $time_M(x)$ represents the number of steps that M uses on input x.

If $t(n)$ is a time bound, then we write

$$\mathrm{DTIME}(t(n)) = \{L(M) \mid (\exists c)(\forall x) time_M(x) \leq c \cdot t(|x|) + c\}$$

for the set of languages decidable in $O(t(n))$ time. Similarly, we write

$$\mathrm{DTIMEF}(t(n)) = \{f_M \mid (\exists c)(\forall x) time_M(x) \leq c \cdot t(|x|) + c\}$$

for the set of functions computable in $O(t(n)$-time. The classes of polynomial time decidable languages and polynomial time computable functions are then $\mathrm{P} = \bigcup_{k=0}^{\infty} \mathrm{DTIME}(n^k)$ and $\mathrm{PF} = \bigcup_{k=0}^{\infty} \mathrm{DTIMEF}(n^k)$, respectively. We are especially interested in classes of languages decidable in exponential time. We write

$$\mathrm{E} = \bigcup_{c=1}^{\infty} \mathrm{DTIME}(2^{cn})$$

and

$$\mathrm{E}_2 = \bigcup_{c=1}^{\infty} \mathrm{DTIME}(2^{n^c})$$

for the classes of languages decidable in 2^{linear} time and $2^{\text{polynomial}}$ time, respectively. Other complexity classes that we use here, such as NP, PH, PSPACE, etc., have completely standard definitions [2, 3].

If A and B are languages, then a *polynomial time, many-one reduction* (briefly $\leq_{\mathrm{m}}^{\mathrm{P}}$-*reduction*) *of* A *to* B is a function $f \in \mathrm{PF}$ such that $A = f^{-1}(B) = \{x \mid f(x) \in B\}$. A $\leq_{\mathrm{m}}^{\mathrm{P}}$-*reduction of* A is a function $f \in \mathrm{PF}$ that is a $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduction of A to some language B. Note that f is a $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduction of A if and only if f is a $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduction of A to $f(A) = \{f(x) \mid x \in A\}$. We say that A is *polynomial time, many-one reducible* (briefly, $\leq_{\mathrm{m}}^{\mathrm{P}}$-*reducible*) to B, and we write $A \leq_{\mathrm{m}}^{\mathrm{P}} B$, if there exists a $\leq_{\mathrm{m}}^{\mathrm{P}}$-reduction f of A to B. In this case, we also say that $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ *via* f.

A language H is $\leq_{\rm m}^{\rm P}$-*hard* for a class $\mathcal{C}$ of languages if $A \leq_{\rm m}^{\rm P} H$ for all $A \in \mathcal{C}$. A language C is $\leq_{\rm m}^{\rm P}$-*complete* for $\mathcal{C}$ if $C \in \mathcal{C}$ and C is $\leq_{\rm m}^{\rm P}$-hard for $\mathcal{C}$. If $\mathcal{C} = {\rm NP}$, this is the usual notion of NP-completeness[13]. In this paper we are especially concerned with languages that are $\leq_{\rm m}^{\rm P}$-hard or $\leq_{\rm m}^{\rm P}$-complete for E or $\rm E_2$.

3 Resource-Bounded Measure

Resource-bounded measure [17, 19] is a very general theory whose special cases include classical Lebesgue measure, the measure structure of the class REC of all recursive languages, and measure in various complexity classes. In this paper we are interested only in measure in E and $\rm E_2$, so our discussion of measure is specific to these classes. The interested reader may consult section 3 of [17] for more discussion and examples.

Throughout this section, we identify every language $A \subseteq \{0,1\}^*$ with its characteristic sequence $\chi_A \in \{0,1\}^\infty$, defined by $\chi_A[i] = [\![s_i \in A]\!]$ for all $i \in \mathbf{N}$. (Recall from section 2 that $s_0, s_1, s_2, \ldots$ is the standard enumeration of $\{0,1\}^*$.) We say that $x \in \{0,1\}^*$ is a *prefix*, or *partial specification*, of $A \subseteq \{0,1\}^*$ if x is a prefix of χ_A, i.e., if there exists $y \in \{0,1\}^\infty$ such that $\chi_A = xy$. In this case, we write $x \sqsubseteq A$. The set of all languages A for which x is a partial specification,

$$\mathbf{C}_x = \{A \subseteq \{0,1\}^* \mid x \sqsubseteq A\},$$

is the *cylinder specified by* the string $x \in \{0,1\}^*$. We say that the *measure* of the set $\mathbf{C}_x$ is $2^{-|x|}$. (Note that this is the probability that $A \in \mathbf{C}_x$ if $A \subseteq \{0,1\}^*$ is chosen probabilistically according to the random experiment in which an independent toss of a fair coin is used to decide membership of each string $x \in \{0,1\}^*$ in A.)

Notation The classes $\rm p_1 = p$ and $\rm p_2$, both consisting of functions $f : \{0,1\}^* \to \{0,1\}^*$, are defined as follows.

$$\begin{aligned} {\rm p_1} &= {\rm p} = \{f | f \text{ is computable in polynomial time}\} \\ {\rm p_2} &= \{f | f \text{ is computable in } n^{(\log n)^{O(1)}} \text{ time}\} \end{aligned}$$

The measure structures of E and $\rm E_2$ are developed in terms of the classes $\rm p_i$, for $i = 1, 2$.

Definition. A *density function* is a function $d : \{0,1\}^* \to [0, \infty)$ satisfying

$$d(w) \geq \frac{d(w0) + d(w1)}{2} \tag{3.1}$$

for all $w \in \{0,1\}^*$. The *global value* of a density function d is $d(\lambda)$. The *set covered by* a density function d is

$$S[d] = \bigcup_{\substack{w \in \{0,1\}^* \\ d(w) \geq 1}} \mathbf{C}_w. \tag{3.2}$$

A density function d *covers* a set $X \subseteq \{0,1\}^\infty$ if $X \subseteq S[d]$.

For all density functions in this paper, equality actually holds in (3.1) above, but this is not required. Consider the random experiment in which a language $A \subseteq \{0,1\}^*$ is chosen by using an independent toss of a fair coin to decide whether each string $x \in \{0,1\}^*$ is in A. Taken together, parts (3.1) and (3.2) of the above definition imply that $\Pr[A \in S[d]] \leq d(\lambda)$ in this experiment. Intuitively, we regard a density function d as a "detailed verification" that $\Pr[A \in X] \leq d(\lambda)$ for all sets $X \subseteq S[d]$.

More generally, we are interested in "uniform systems" of density functions that are computable within some resource bound.

Since density functions are real-valued, their computations must employ finite approximations of real numbers. For this purpose, let

$$\mathbf{D} = \{m2^{-n} \mid m \in \mathbf{Z}, n \in \mathbf{N}\}$$

be the set of *dyadic rationals*. (These are rational numbers with finite binary expansions.) In order to have uniform criteria for computational complexity, we consider all functions of the form $f : X \to Y$, where each of the sets X, Y is $\mathbf{N}$, $\{0,1\}^*$, $\mathbf{D}$, or some Cartesian product of these sets, to really map $\{0,1\}^*$ into $\{0,1\}^*$. For example, a function $f : \mathbf{N}^2 \times \{0,1\}^* \to \mathbf{N} \times \mathbf{D}$ is formally interpreted as a function $\tilde{f} : \{0,1\}^* \to \{0,1\}^*$. Under this interpretation, $f(i,j,w) = (k,q)$ means that $\tilde{f}(\langle 0^i, \langle 0^j, w\rangle\rangle) = \langle 0^k, \langle u, v\rangle\rangle$, where u and v are the binary representations of the integer and fractional parts of q, respectively. Moreover, we only care about the values of $\tilde{f}$ for arguments of the form $\langle 0^i, \langle 0^j, w\rangle\rangle$, and we insist that these values have the form $\langle 0^k, \langle u, v\rangle\rangle$ for such arguments.

Definition. An n-dimensional *density system* (n-*DS*) is a function

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

such that $d_{\vec{k}}$ is a density function for every $\vec{k} \in \mathbf{N}^n$. It is sometimes convenient to regard a density function as a 0-DS.

Definition. A *computation* of an n-DS d is a function $\hat{d} : \mathbf{N}^{n+1} \times \{0,1\}^* \to \mathbf{D}$ such that

$$|\hat{d}_{\vec{k},r}(w) - d_{\vec{k}}(w)| \leq 2^{-r}$$

for all $\vec{k} \in \mathbf{N}^n$, $r \in \mathbf{N}$, and $w \in \{0,1\}^*$. For $i = 1, 2$, a p_i-*computation* of an n-DS d is a computation $\hat{d}$ of d such that $\hat{d} \in \mathrm{p}_i$. An n-DS d is p_i-*computable* if there exists a p_i-computation $\hat{d}$ of d.

If d is an n-DS such that $d : \mathbf{N}^n \times \{0,1\}^* \to \mathbf{D}$ and $d \in \mathrm{p}_i$, then d is trivially p_i-computable. This fortunate circumstance, in which there is no need to compute approximations, occurs frequently in practice. (Such applications typically do involve approximations, but these are "hidden" by invoking fundamental theorems whose proofs involve approximations).

We now come to the key idea of resource-bounded measure theory.

Definition. A *null cover* of a set $X \subseteq \{0,1\}^\infty$ is a 1-DS d such that, for all $k \in \mathbf{N}$, d_k covers X with global value $d_k(\lambda) \leq 2^{-k}$. For $i = 1, 2$, a p_i-*null cover* of X is a null cover of X that is p_i-computable.

In other words, a null cover of X is a uniform system of density functions that cover X with rapidly vanishing global value. It is easy to show that a set $X \subseteq \{0,1\}^\infty$ has classical Lebesgue measure 0 (i.e., probability 0 in the above coin-tossing experiment) if and only if there exists a null cover of X.

Definition. A set X has p_i-*measure 0*, and we write $\mu_{\mathrm{p}_i}(X) = 0$, if there exists a p_i-null cover of X. A set X has p_i-*measure 1*, and we write $\mu_{\mathrm{p}_i}(X) = 1$, if $\mu_{\mathrm{p}_i}(X^c) = 0$.

Thus a set X has p_i-measure 0 if p_i provides sufficient computational resources to compute uniformly good approximations to a system of density functions that cover X with rapidly vanishing global value.

We now turn to the internal measure structures of the classes $\mathrm{E} = \mathrm{E}_1 = \mathrm{DTIME}(2^{\mathrm{linear}})$ and $\mathrm{E}_2 = \mathrm{DTIME}(2^{\mathrm{polynomial}})$.

Definition. A set X has *measure 0 in* E_i, and we write $\mu(X \mid \mathrm{E}_i) = 0$, if $\mu_{\mathrm{p}_i}(X \cap \mathrm{E}_i) = 0$. A set X has *measure 1 in* E_i, and we write $\mu(X \mid \mathrm{E}_i) = 1$, if $\mu(X^c \mid \mathrm{E}_i) = 0$. If $\mu(X \mid \mathrm{E}_i) = 1$, we say that *almost every* language in E_i is in X.

We write $\mu(X|\mathrm{E}_i) \neq 0$ to indicate that X does *not* have measure 0 in E_i. Note that this does *not* assert that "$\mu(X|\mathrm{E}_i)$" has some nonzero value.

The following is obvious but useful.

Fact 3.1. For every set $X \subseteq \{0,1\}^\infty$,

$$\begin{array}{ccccc} \mu_{\mathrm{p}}(X) = 0 & \Longrightarrow & \mu_{\mathrm{p}_2}(X) = 0 & \Longrightarrow & \Pr[A \in X] = 0 \\ \Downarrow & & \Downarrow & & \\ \mu(X|\mathrm{E}) = 0 & & \mu(X|\mathrm{E}_2) = 0, & & \end{array}$$

where the probability $\Pr[A \in X]$ is 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 whether each string $x \in \{0,1\}^*$ is in A.

It is shown in [17] that these definitions endow E and E_2 with internal measure structure. This structure justifies the intuition that, if $\mu(X|\mathrm{E}) = 0$, then $X \cap \mathrm{E}$ is a *negligibly small* subset of E (and similarly for E_2). The next two results state aspects of this structure that are especially relevant to the present work.

Theorem 3.2 ([17]). For all cylinders $\mathbf{C}_w$, $\mu(\mathbf{C}_w|\mathrm{E}) \neq 0$ and $\mu(\mathbf{C}_w|\mathrm{E}_2) \neq 0$. In particular, $\mu(\mathrm{E}|\mathrm{E}) \neq 0$ and $\mu(\mathrm{E}_2|\mathrm{E}_2) \neq 0$.

The next lemma, which is used in proving Theorem 4.3 and Lemma 5.2, involves the following computational restriction of the notion of "countable union."

Definition. Let $i \in \{1,2\}$ and let $Z, Z_0, Z_1, Z_2, \cdots \subseteq \{0,1\}^\infty$. Then Z is a p_i-*union of the* p_i-*measure 0 sets* $Z_0, Z_1, Z_2, \cdots$ if $Z = \bigcup_{j=0}^{\infty} Z_j$ and there exists a p_i-computable 2-DS d such that each d_j is a p_i-null cover of Z_j.

Lemma 3.3 ([17]). Let $i \in \{1,2\}$ and let $Z, Z_0, Z_1, Z_2, \cdots \subseteq \{0,1\}^\infty$. If Z is a p_i-union of the p_i-measure 0 sets $Z_0, Z_1, Z_2, \cdots$, then Z has p_i-measure 0. □

4 Complexity Cores: Lower Bounds

Orponen and Schöning [28] have shown that every $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard language for E has a dense polynomial complexity core. In this section we extend this result by proving that every weakly $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard language for E has a dense exponential complexity core. We begin by explaining our terminology.

Given a machine M and an input $x \in \{0,1\}^*$, we write $M(x) = 1$ if M accepts x, $M(x) = 0$ if M rejects x, and $M(x) = \perp$ in any other case (i.e., if M fails to halt or M halts without deciding x). If $M(x) \in \{0,1\}$, we write $time_M(x)$ for the number of steps used in

the computation of $M(x)$. If $M(x) = \perp$, we define $time_M(x) = \infty$. We partially order the set $\{0, 1, \perp\}$ by $\perp < 0$ and $\perp < 1$, with 0 and 1 incomparable. A machine M is *consistent* with a language $A \subseteq \{0,1\}^*$ if $M(x) \leq [\![x \in A]\!]$ for all $x \in \{0,1\}^*$.

Definition. Let $t : \mathbf{N} \to \mathbf{N}$ be a time bound and let $A, K \subseteq \{0,1\}^*$. Then K is a DTIME($t(n)$)-*complexity core* of A if, for every $c \in \mathbf{N}$ and every machine M that is consistent with A, the "fast set"

$$F = \{x \,|time_M(x) \leq c \cdot t(|x|) + c\}$$

satisfies $|F \cap K| < \infty$. (By our definition of $time_M(x)$, $M(x) \in \{0,1\}$ for all $x \in F$. Thus F is the set of all strings that M "decides efficiently.")

Remark. The above definition quantifies over all machines consistent with A, while the standard definition of complexity cores (cf. [3]) quantifies only over machines that *decide* A. For recursive languages A (and time-constructible bounds t), it is easy to see that the above definition is exactly equivalent to the standard definition. However, the above definition is stronger than the standard definition when A is not recursive. For example, consider *tally* languages (i.e., languages $A \subseteq \{0\}^*$). Under our definition, every DTIME(n)-complexity core K of every tally language must satisfy $|K - \{0\}^*| < \infty$. However, under the standard definition, complexity cores are only defined for recursive sets A (as in [3]), or else *every* set $K \subseteq \{0,1\}^*$ is *vacuously* a complexity core for *every* nonrecursive language (tally or otherwise). Thus by quantifying over all machines consistent with A, our definition makes the notion of complexity core meaningful for nonrecursive languages A. This enables one to eliminate the extraneous hypothesis that A is recursive from several results. In some cases, this improvement is of little interest. However in section 6 below, we show that *every* $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard language H for E has unusually small complexity cores. This upper bound holds regardless of whether H is recursive.

Note that every subset of a DTIME($t(n)$)-complexity core of A is a DTIME($t(n)$)-complexity core of A. Note also that, if $s(n) = O(t(n))$, then every DTIME($t(n)$)-complexity core of A is a DTIME($s(n)$)-complexity core of A.

Definition. Let $A, K \subseteq \{0,1\}^*$.

1. K is a *polynomial complexity core* (or, briefly, a P-*complexity core*) of A if K is a DTIME(n^k)-complexity core of A for all $k \in \mathbf{N}$.

2. K is an *exponential complexity core* of A if there is a real number $\epsilon > 0$ such that K is a DTIME(2^{n^ϵ})-complexity core of A.

Much of our work here uses languages that are "incompressible by many-one reductions," an idea originally exploited by Meyer [26]. The following definitions develop this notion.

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 $\{0,1\}^*$.

Note that f is one-to-one if and only if $C_f = \emptyset$.

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. Let $A, B \subseteq \{0,1\}^*$ and let $t : \mathbf{N} \to \mathbf{N}$. A $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$*-reduction of A to B* is a function $f \in \mathrm{DTIMEF}(t)$ such that $A = f^{-1}(B)$, i.e., such that, for all $x \in \{0,1\}^*$, $x \in A$ iff $f(x) \in B$. A $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$*-reduction of A* is a function f that is a $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$-reduction of A to $f(A)$.

It is easy to see that f is a $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$-reduction of A if and only if there exists a language B such that f is a $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$-reduction of A to B.

Definition. Let $t : \mathbf{N} \to \mathbf{N}$. A language $A \subseteq \{0,1\}^*$ is *incompressible by* $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$*-reductions* if every $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$-reduction of A is one-to-one a.e. A language $A \subseteq \{0,1\}^*$ is *incompressible by* $\leq_{\mathrm{m}}^{\mathrm{P}}$*-reductions* if it is incompressible by $\leq_{\mathrm{m}}^{\mathrm{DTIME}(q)}$-reductions for all polynomials q.

Intuitively, if f is a $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$-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 $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions, then very little such compression can occur.

Our first observation, an obvious generalization of a result of Balcázar and Schöning [4] (see Corollary 4.2 below), relates incompressibility to complexity cores.

Lemma 4.1. If $t : \mathbf{N} \to \mathbf{N}$ is time constructible, then every language that is incompressible by $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$-reductions has $\{0,1\}^*$ as a $\mathrm{DTIME}(t)$-complexity core.

Proof. Let A be a language that does not have $\{0,1\}^*$ as a $\mathrm{DTIME}(t)$-complexity core. It suffices to prove that A is not incompressible by $\leq_{\mathrm{m}}^{\mathrm{DTIME}(t)}$-reductions. This is clear if $A = \emptyset$ or $A = \{0,1\}^*$, so assume that $\emptyset \neq A \neq \{0,1\}^*$. Fix $u \in A$ and $v \in A^c$. Since $\{0,1\}^*$ is

not a DTIME(t)-complexity core of A, there exist $c \in \mathbf{N}$ and a machine M such that M is consistent with A and the fast set

$$F = \{x \mid time_M(x) \leq c \cdot t(|x|) + c\}$$

is infinite. Define a function $f : \{0,1\}^* \to \{0,1\}^*$ by

$$f(x) = \begin{cases} u & \text{if } M(x) = 1 \text{ in} \leq c \cdot t(|x|) + c \text{ steps} \\ v & \text{if } M(x) = 0 \text{ in} \leq c \cdot t(|x|) + c \text{ steps} \\ x & \text{otherwise.} \end{cases}$$

Since t is time-constructible, $f \in \text{DTIMEF}(t)$. Since M is consistent with A, f is a $\leq_{\text{m}}^{\text{DTIME}(t)}$-reduction of A to A. Since F is infinite, at least one of the sets $f^{-1}(\{u\})$, $f^{-1}(\{v\})$ is infinite, so the collision set C_f is infinite. Thus A is not incompressible by $\leq_{\text{m}}^{\text{DTIME}(t)}$-reductions. □

Corollary 4.2. Let $c \in \mathbf{N}$.

1 (Balcazar and Schöning [4]). Every language that is incompressible by $\leq_{\text{m}}^{\text{P}}$-reductions has $\{0,1\}^*$ as a P-complexity core.

2. Every language that is incompressible by $\leq_{\text{m}}^{\text{DTIME}(2^{cn})}$-reductions has $\{0,1\}^*$ as a DTIME(2^{cn})-complexity core.

3. Every language that is incompressible by $\leq_{\text{m}}^{\text{DTIME}(2^{n^c})}$-reductions has $\{0,1\}^*$ as a DTIME(2^{n^c})-complexity core. □

We now prove that, in E and E_2, almost every language is incompressible by $\leq_{\text{m}}^{\text{DTIME}(t)}$-reductions, for exponential time bounds t.

Theorem 4.3. Let $c \in \mathbf{Z}^+$ and define the sets

$$X = \{A \subseteq \{0,1\}^* | A \text{ is incompressible by } \leq_{\text{m}}^{\text{DTIME}(2^{cn})}\text{-reductions}\},$$

$$Y = \{A \subseteq \{0,1\}^* | A \text{ is incompressible by } \leq_{\text{m}}^{\text{DTIME}(2^{n^c})}\text{-reductions}\}.$$

Then $\mu_{\text{p}}(X) = \mu_{\text{p}_2}(Y) = 1$. Thus almost every language in E is incompressible by $\leq_{\text{m}}^{\text{DTIME}(2^{cn})}$-reductions, and almost every language in E_2 is incompressible by $\leq_{\text{m}}^{\text{DTIME}(2^{n^c})}$-reductions.

Proof. Let $c \in \mathbf{Z}^+$. We prove that $\mu_{\text{p}}(X) = 1$. The proof that $\mu_{\text{p}_2}(X) = 1$ is analogous.

Let $f \in \text{DTIMEF}(2^{(c+1)n})$ be a function that is universal for DTIMEF(2^{cn}), in the sense that

$$\text{DTIMEF}(2^{cn}) = \{f_i \mid i \in \mathbf{N}\}.$$

For each $i \in \mathbf{N}$, define a set Z_i of languages as follows: If the collision set C_{f_i} is finite, then $Z_i = \emptyset$. Otherwise, if C_{f_i} is infinite, then Z_i is the set of all languages A such that f_i is a $\leq_{\mathrm{m}}^{\mathrm{DTIME}(2^{cn})}$-reduction of A.

Define a function $d : \mathbf{N} \times \mathbf{N} \times \{0,1\}^* \to [0,\infty)$ as follows: Let $i, k \in \mathbf{N}$ be arbitrary, let $w \in \{0,1\}^*$, and let $b \in \{0,1\}$.

(i) $d_{i,k}(\lambda) = 2^{-k}$.

(ii) If $s_{|w|} \notin C_{f_i}$, then $d_{i,k}(wb) = d_{i,k}(w)$.

(iii) If $s_{|w|} \in C_{f_i}$, then fix the least $j \in \mathbf{N}$ such that $f_i(s_j) = f_i(s_{|w|})$ and set

$$d_{i,k}(wb) = 2 \cdot d_{i,k}(w) \cdot [\![b = w[j]]\!].$$

It is clear that d is a 2-DS. Since $f \in \mathrm{DTIMEF}(2^{(c+1)n})$ and the computation of $d_{i,k}(w)$ only uses values $f_i(u)$ for strings u with $|u| = O(\log |w|)$, it is also clear that $d \in \mathrm{p}$, so d is a p-computable 2-DS.

We now show that $Z_i \subseteq S[d_{i,k}]$ for all $i, k \in \mathbf{N}$. If C_{f_i} is finite, then this is clear (because $Z_i = \emptyset$), so assume that C_{f_i} is infinite and let $A \in Z_i$. Let w be a string consisting of the first l bits of the characteristic sequence of A, where s_{l-1} is the k^{th} element of C_{f_i}. This choice of l ensures that clause (iii) of the definition of d is invoked exactly k times in the recursive computation of $d_{i,k}(w)$. Since f_i is a $\leq_{\mathrm{m}}^{\mathrm{DTIME}(2^{cn})}$-reduction of A (because $A \in Z_i$), we have $b = w[j]$ in each of these k invocations, so

$$d_{i,k}(w) = 2^k \cdot d_{i,k}(\lambda) = 1.$$

Thus $A \in \mathbf{C}_w \subseteq S[d_{i,k}]$. This confirms that $Z_i \subseteq S[d_{i,k}]$ for all $i, k \in \mathbf{N}$. It follows easily that, for each $i \in \mathbf{N}$, d_i is a p-null cover of Z_i. This implies that

$$X^c = \bigcup_{k=0}^{\infty} Z_k$$

is a p-union of p-measure 0 sets, whence $\mu_{\mathrm{p}}(X) = 1$ by Lemma 3.3. □

Corollary 4.4. Almost every language in E and almost every language in E_2 is incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions. □

Corollary 4.5 (Meyer[26]). There is a language $A \in \mathrm{E}$ that is incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions. □

Corollary 4.6. Let $c \in \mathbf{Z}^+$.

1. Almost every language in E has $\{0,1\}^*$ as a DTIME(2^{cn})-complexity core.
2. Almost every language in E_2 has $\{0,1\}^*$ as a DTIME(2^{n^c})-complexity core. □

We now consider complexity cores of $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard languages. Our starting point is the following two known facts.

Fact 4.7 (Orponen and Schöning [28]). Every language that is $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E (equivalently, for E_2) has a dense P-complexity core.

Fact 4.8 (Orponen and Schöning [28]). If $\mathrm{P} \neq \mathrm{NP}$, then every language that is $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for NP has a nonsparse P-complexity core.

We first extend Fact 4.7. For this we need a definition. The *lower* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-span* of a language $A \subseteq \{0,1\}^*$ is

$$\mathrm{P}_{\mathrm{m}}(A) = \{B \subseteq \{0,1\}^* \mid B \leq^{\mathrm{P}}_{\mathrm{m}} A\},$$

i.e., the set of all languages lying "at or below" A in the $\leq^{\mathrm{P}}_{\mathrm{m}}$-reducibility structure of the set of all languages. Recall that a language A is $\leq^{\mathrm{P}}_{\mathrm{m}}$*-hard* for a complexity class $\mathcal{C}$ if $\mathcal{C} \subseteq \mathrm{P}_{\mathrm{m}}(A)$.

Definition. A language $A \subseteq \{0,1\}^*$ is *weakly* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-hard* for E (respectively, for E_2) if $\mu(\mathrm{P}_{\mathrm{m}}(A) \mid \mathrm{E}) \neq 0$ (respectively, $\mu(\mathrm{P}_{\mathrm{m}}(A) \mid \mathrm{E}_2) \neq 0$). A language $A \subseteq \{0,1\}^*$ is *weakly* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-complete* for E (respectively, for E_2) if $A \in \mathrm{E}$ (respectively, $A \in \mathrm{E}_2$) and A is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E (respectively, for E_2).

Thus a language A is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E if a nonnegligible subset of the languages in E are $\leq^{\mathrm{P}}_{\mathrm{m}}$-reducible to A. Very recently, Lutz [21] has established the existence of languages that are weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, but not $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete, for E (and similarly for E_2). Although "$\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E" and "$\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E_2" are equivalent, we do not know the relationship between "weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E" and "weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E_2."

Recall that a language $D \subseteq \{0,1\}^*$ is *dense* if there is a real number $\epsilon > 0$ such that $|D_{\leq n}| > 2^{n^\epsilon}$ a.e.

Theorem 4.9. Every language that is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E or E_2 has a dense exponential complexity core.

Proof. We prove this for E. The proof for E_2 is identical.

Let H be a language that is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E. Then $\mathrm{P}_{\mathrm{m}}(H)$ does not have measure 0 in E, so by Theorem 4.3, there is a language $A \in \mathrm{P}_{\mathrm{m}}(H)$ that is incompressible by $\leq^{\mathrm{DTIME}(2^n)}_{\mathrm{m}}$-reductions. Let f be a $\leq^{\mathrm{P}}_{\mathrm{m}}$-reduction of A to H, let q be a strictly increasing polynomial

bound on the time required to compute f, and let $\epsilon = \frac{1}{3 \cdot deg(q)}$. Then the language $K = f(\{0,1\}^*)$ is a dense DTIME(2^{n^ϵ})-complexity core of H.

□

Lutz has proposed the investigation of the consequences of the strong hypotheses $\mu(\mathrm{NP} \mid \mathrm{E}) \neq 0$ and $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$ [20, 22, 23]. In this regard, we have the following.

Corollary 4.10. If $\mu(\mathrm{NP} \mid \mathrm{E}) \neq 0$ or $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, then every $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard language for NP has a dense exponential complexity core. □

Thus, for example, if NP is not small, then there is a dense set K of Boolean formulas in conjunctive normal form such that every machine that is consistent with SAT performs exponentially badly (either by running for more than $2^{|x|^\epsilon}$ steps or by failing to decide) on all but finitely many inputs $x \in K$.

Note that Theorem 4.9 extends Fact 4.7 and that Corollary 4.10 has a stronger hypothesis and stronger conclusion than Fact 4.8. Note also that Corollary 4.10 holds with NP replaced by PH, PP, PSPACE, or any class whatsoever.

The following result shows that the density bounds of Theorem 4.9 and Corollary 4.10 are tight.

Theorem 4.11. For every $\epsilon > 0$, each of the classes NP, E, and E_2 has a $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete language, every P-complexity core K of which satisfies $|K_{\leq n}| < 2^{n^\epsilon}$ a.e.

Proof. Let $\epsilon > 0$, let $\mathcal{C}$ be any one of the classes NP, E, E_2, and let A be a language that is $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for $\mathcal{C}$. Let $k = \lceil \frac{2}{\epsilon} \rceil$ and define the language

$$B = \{x 10^{|x|^k} \mid x \in A\}.$$

Then B is $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for $\mathcal{C}$ and every P-complexity core K of B satisfies $|K_{\leq n}| < 2^{n^\epsilon}$ a.e.

□

5 Measure of Degrees

In this section we prove that all $\leq^{\mathrm{P}}_{\mathrm{m}}$-degrees have measure 0 in the complexity classes E and E_2. This fact and more follow from the Small Span Theorem, which we prove first.

Recall that the *lower* $\leq^{\mathrm{P}}_{\mathrm{m}}$*-span* of a language $A \subseteq \{0,1\}^*$ is

$$\mathrm{P}_{\mathrm{m}}(A) = \{B \subseteq \{0,1\}^* \mid B \leq^{\mathrm{P}}_{\mathrm{m}} A\}.$$

Similarly, define the *upper* $\leq_{\mathrm{m}}^{\mathrm{P}}$-*span* of A to be

$$\mathrm{P}_{\mathrm{m}}^{-1}(A) = \{B \subseteq \{0,1\}^* \mid A \leq_{\mathrm{m}}^{\mathrm{P}} B\}.$$

The $\leq_{\mathrm{m}}^{\mathrm{P}}$-*degree* of A is then

$$\deg_{\mathrm{m}}^{\mathrm{P}}(A) = \mathrm{P}_{\mathrm{m}}(A) \cap \mathrm{P}_{\mathrm{m}}^{-1}(A),$$

the intersection of the upper and lower spans.

The main result of this section is that, if A is in E or E_2, then at least one of the spans $\mathrm{P}_{\mathrm{m}}(A)$, $\mathrm{P}_{\mathrm{m}}^{-1}(A)$ is small.

Theorem 5.1.(Small Span Theorem)

1. For every $A \in \mathrm{E}$,

$$\mu(\mathrm{P}_{\mathrm{m}}(A) \mid \mathrm{E}) = 0$$

or

$$\mu_{\mathrm{p}}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = \mu(\mathrm{P}_{\mathrm{m}}^{-1}(A) \mid \mathrm{E}) = 0.$$

2. For every $A \in \mathrm{E}_2$,

$$\mu(\mathrm{P}_{\mathrm{m}}(A) \mid \mathrm{E}_2) = 0$$

or

$$\mu_{\mathrm{p}_2}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = \mu(\mathrm{P}_{\mathrm{m}}^{-1}(A) \mid \mathrm{E}_2) = 0.$$

We first use the following lemma to prove Theorem 5.1 We then prove the lemma.

Lemma 5.2. Let A be a language that is incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions.

1. If $A \in \mathrm{E}$, then $\mu_{\mathrm{p}}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = \mu(\mathrm{P}_{\mathrm{m}}^{-1}(A)|\mathrm{E}) = 0$.
2. If $A \in \mathrm{E}_2$, then $\mu_{\mathrm{p}_2}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = \mu(\mathrm{P}_{\mathrm{m}}^{-1}(A)|\mathrm{E}_2) = 0$.

Proof of Theorem 5.1.

To prove 1, let $A \in \mathrm{E}$ and let X be the set of all languages that are incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions. We have two cases.

Case I. If $\mathrm{P}_{\mathrm{m}}(A) \cap \mathrm{E} \cap X = \emptyset$, then Corollary 4.4 tells us that $\mu(\mathrm{P}_{\mathrm{m}}(A) \mid \mathrm{E}) = 0$.

Case II. If $\mathrm{P_m}(A) \cap \mathrm{E} \cap X \neq \emptyset$, then fix a language $B \in \mathrm{P_m}(A) \cap \mathrm{E} \cap X$. Since $B \in \mathrm{E} \cap X$, Lemma 5.2 tells us that

$$\mu_{\mathrm{p}}(\mathrm{P_m^{-1}}(B)) = \mu(\mathrm{P_m^{-1}}(B) \mid \mathrm{E}) = 0.$$

Since $\mathrm{P_m^{-1}}(A) \subseteq \mathrm{P_m^{-1}}(B)$, it follows that

$$\mu_{\mathrm{p}}(\mathrm{P_m^{-1}}(A)) = \mu(\mathrm{P_m^{-1}}(A) \mid \mathrm{E}) = 0.$$

This proves 1. The proof of 2 is identical. □ **Proof of Lemma 5.2.**
To prove 1, let $A \in \mathrm{E}$ be incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions. Let $f \in \mathrm{DTIMEF}(2^n)$ be a function that is universal for PF, in the sense that

$$\mathrm{PF} = \{f_i \;\big|\; i \in \mathbf{N}\}.$$

For each $i \in \mathbf{N}$, define the set Z_i of languages as follows. If the collision set C_{f_i} is infinite, then $Z_i = \emptyset$. Otherwise, if C_{f_i} is finite, then

$$Z_i = \{B \subseteq \{0,1\}^* \;\big|\; A \leq_{\mathrm{m}}^{\mathrm{P}} B \text{ via } f_i\}.$$

Note that

$$\mathrm{P_m^{-1}}(A) = \bigcup_{i=0}^{\infty} Z_i$$

because A is incompressible by $\leq_{\mathrm{m}}^{\mathrm{P}}$-reductions.

Define a function $d : \mathbf{N} \times \mathbf{N} \times \{0,1\}^* \to [0,\infty)$ as follows. Let $i, k \in \mathbf{N}$ be arbitrary, let $w \in \{0,1\}^*$, and let $b \in \{0,1\}$.

(i) $d_{i,k}(\lambda) = 2^{-k}$.

(ii) If there is no $j \leq 2|w|$ such that $f_i(s_j) = s_{|w|}$, then $d_{i,k}(wb) = d_{i,k}(w)$.

(iii) If there exists $j \leq 2|w|$ such that $f_i(s_j) = s_{|w|}$, then fix the least such j and set

$$d_{i,k}(wb) = 2 \cdot d_{i,k}(w) \cdot [\![b = [\![s_j \in A]\!]]\!].$$

It is clear that d is a 2-DS. Also, since $f \in \mathrm{DTIMEF}(2^n)$ and $A \in \mathrm{E}$, it is easy to see that $d \in \mathrm{p}$, whence d is a p-computable 2-DS.

We now show that $Z_i \subseteq S[d_{i,k}]$ for all $i, k \in \mathbf{N}$. If C_{f_i} is infinite, then this is clear (because $Z_i = \emptyset$), so assume that $|C_{f_i}| = c < \infty$ and let $B \in Z_i$, i.e., $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ via f_i. Let v be the

string consisting of the first l bits of the characteristic sequence of B, where l is large enough that

$$f_i(\{s_0, ..., s_{2k+4c-1}\}) \subseteq \{s_0, ..., s_{l-1}\}.$$

Consider the computation of $d_{i,k}(v)$ by clauses (i), (ii), and (iii) above. Since $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ via f_i, clause (iii) does not cause $d_{i,k}(w)$ to be 0 for any prefix w of v. Let

$$S = \{s_n \mid 0 \leq n < 2k + 4c \text{ and } f_i(s_n) \notin \{s_0, ..., s_{\lceil \frac{n}{2} \rceil - 1}\}\}$$

and

$$T = f_i(S).$$

Then clause (iii) doubles the density whenever $s_{|w|} \in T$, so

$$d_{i,k}(v) \geq 2^{|T|} d_{i,k}(\lambda) = 2^{|T|-k} \geq 2^{|S|-k-c}.$$

Also, if

$$S' = \{s_n \mid 0 \leq n < 2k + 4c \text{ and } f_i(s_n) \notin \{s_0, ..., s_{k+2c-1}\}\},$$

then $S' \subseteq S$ and

$$|S'| \geq (2k + 4c) - (k + 2c) - c = k + c.$$

Putting this all together, we have

$$d_{i,k}(v) \geq 2^{|S|-k-c} \geq 2^{|S'|-k-c} \geq 1,$$

whence $B \in \mathbf{C}_v \subseteq S[d_{i,k}]$. This shows that $Z_i \subseteq S[d_{i,k}]$ for all $i, k \in \mathbf{N}$.

Since d is p-computable and $d_{i,k}(\lambda) = 2^{-k}$ for all $i, k \in \mathbf{N}$, it follows that, for all $i \in \mathbf{N}$, d_i is p-null cover of Z_i. This implies that $\mathrm{P}_{\mathrm{m}}^{-1}(A)$ is a p-union of the p-measure 0 sets Z_i. It follows by Lemma 3.3 that $\mu_{\mathrm{p}}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = \mu(\mathrm{P}_{\mathrm{m}}^{-1}(A) \mid \mathrm{E}) = 0$. This completes the proof of 1.

The proof of 2 is identical. One need only note that, if $A \in \mathrm{E}_2$, then $d \in \mathrm{p}_2$. □

Remark. Ambos-Spies [1] has shown that $\mathrm{P}_{\mathrm{m}}(A)$ has Lebesgue measure 0 whenever $A \notin \mathrm{P}$. Lemma 5.2 obtains a stronger conclusion (resource-bounded measure 0) from a stronger hypothesis on A.

It is now straightforward to derive consequences of these results for the structure of E and E_2. We first note that $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard languages for E are extremely rare.

Theorem 5.3. Let $\mathcal{H}_{\mathrm{E}}$ be the set of all languages that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for E. Then $\mu_{\mathrm{p}}(\mathcal{H}_{\mathrm{E}}) = 0$.

Proof. Let A be as in Corollary 4.5. Then $\mathcal{H}_{\mathrm{E}} \subseteq \mathrm{P}_{\mathrm{m}}^{-1}(A)$, so Lemma 5.2 tells us that

$$\mu_{\mathrm{p}}(\mathcal{H}_{\mathrm{E}}) = \mu_{\mathrm{p}}(\mathrm{P}_{\mathrm{m}}^{-1}(A)) = 0.$$

□

Theorem 5.3 immediately yields an alternate proof of the following result.

Corollary 5.4 (Mayordomo[25]). Let $\mathcal{C}_{\mathrm{E}}$, $\mathcal{C}_{\mathrm{E}_2}$ be the sets of languages that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete for E, E_2, respectively. Then $\mu(\mathcal{C}_{\mathrm{E}}|\mathrm{E}) = \mu(\mathcal{C}_{\mathrm{E}_2}|\mathrm{E}_2) = 0$. □

(Mayordomo's proof of Corollary 5.4 used Berman's result [6], that no $\leq_{\mathrm{m}}^{\mathrm{P}}$-complete language for E is P-immune.)

As it turns out, Corollary 5.4 is only a special case of the following general result. *All* $\leq_{\mathrm{m}}^{\mathrm{P}}$-degrees have measure 0 in E and in E_2.

Theorem 5.5. For all $A \subseteq \{0,1\}^*$,

$$\mu(\deg_{\mathrm{m}}^{\mathrm{P}}(A) \mid \mathrm{E}) = \mu(\deg_{\mathrm{m}}^{\mathrm{P}}(A) \mid \mathrm{E}_2) = 0.$$

Proof. Let $A \subseteq \{0,1\}^*$. We prove that $\mu(\deg_{\mathrm{m}}^{\mathrm{P}}(A) \mid \mathrm{E}) = 0$. The proof that $\mu(\deg_{\mathrm{m}}^{\mathrm{P}}(A) \mid \mathrm{E}_2) = 0$ is identical (in fact simpler, because E_2 is closed under $\leq_{\mathrm{m}}^{\mathrm{P}}$).

If $\deg_{\mathrm{m}}^{\mathrm{P}}(A) \cap \mathrm{E} = \emptyset$, then $\mu(\deg_{\mathrm{m}}^{\mathrm{P}}(A) \mid \mathrm{E}) = 0$ holds trivially, so assume that $\deg_{\mathrm{m}}^{\mathrm{P}}(A) \cap \mathrm{E} \neq \emptyset$. Fix $B \in \deg_{\mathrm{m}}^{\mathrm{P}}(A) \cap \mathrm{E}$. Then, by Theorem 5.1,

$$\mu(\deg_{\mathrm{m}}^{\mathrm{P}}(B) \mid \mathrm{E}) = \mu(\mathrm{P}_{\mathrm{m}}(B) \mid \mathrm{E}) = 0$$

or

$$\mu(\deg_{\mathrm{m}}^{\mathrm{P}}(B) \mid \mathrm{E}) = \mu(\mathrm{P}_{\mathrm{m}}^{-1}(B) \mid \mathrm{E}) = 0.$$

Since $\deg_{\mathrm{m}}^{\mathrm{P}}(A) = \deg_{\mathrm{m}}^{\mathrm{P}}(B)$, it follows that $\mu(\deg_{\mathrm{m}}^{\mathrm{P}}(A) \mid \mathrm{E}) = 0$. □

We now have the following two corollaries for NP.

Corollary 5.6. Let $\mathcal{H}_{\mathrm{NP}}$ be the set of languages that are $\leq_{\mathrm{m}}^{\mathrm{P}}$-hard for NP.

1. If $\mu(\mathrm{NP} \mid \mathrm{E}) \neq 0$, then $\mu(\mathcal{H}_{\mathrm{NP}} \mid \mathrm{E}) = 0$.
2. If $\mu(\mathrm{NP} \mid \mathrm{E}_2) \neq 0$, then $\mu(\mathcal{H}_{\mathrm{NP}} \mid \mathrm{E}_2) = 0$.

Proof. This follows immediately from Theorem 5.1, with $A = \mathrm{SAT}$. □

Corollary 5.7. Let $\mathcal{C}_{\mathrm{NP}}$ be the set of languages that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for NP. Then $\mu(\mathcal{C}_{\mathrm{NP}} \mid \mathrm{E}) = \mu(\mathcal{C}_{\mathrm{NP}} \mid \mathrm{E}_2) = 0$.

Proof. Since $\mathcal{C}_{\mathrm{NP}} = \deg^{\mathrm{P}}_{\mathrm{m}}(\mathrm{SAT})$, this follows immediately from Theorem 5.5. □

It is interesting to note that Corollary 5.7, unlike Corollary 5.6, is an absolute result, requiring no unproven hypothesis. The price we pay for this is that we do not know *why* it holds! For example, the Small Span Theorem tells us that $\mathcal{C}_{\mathrm{NP}} = \mathcal{H}_{\mathrm{NP}} \cap \mathrm{NP}$ has measure 0 in E because $\mu(\mathcal{H}_{\mathrm{NP}} \mid \mathrm{E}) = 0$ *or* $\mu(\mathrm{NP} \mid \mathrm{E}) = 0$, but it does *not* tell us which of these two very different situations occurs.

Note that Corollaries 5.6 and 5.7 also hold with NP replaced by *any other class whatsoever*.

We conclude this section by noting two respects in which the Small Span Theorem cannot be improved. First, the hypotheses $A \in \mathrm{E}$ and $A \in \mathrm{E}_2$ are essential for parts 1 and 2, respectively. For example, if A is p-random [18], then $\mu_{\mathrm{p}}(\{A\}) \neq 0$, so none of $\deg^{\mathrm{P}}_{\mathrm{m}}(A)$, $\mathrm{P}_{\mathrm{m}}(A)$, $\mathrm{P}^{-1}_{\mathrm{m}}(A)$ can have p-measure 0.

The second respect in which the Small Span Theorem cannot be improved involves the variety of small-span configurations. In both E and E_2, either one or both of the upper and lower spans of a language can in fact be small. We give examples for E.

(a) It is well known [26] that there is a language $A \in \mathrm{E}$ that is both sparse and incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions. Fix such a language A. By Lemma 5.2, $\mu_{\mathrm{p}}(\mathrm{P}^{-1}_{\mathrm{m}}(A)) = 0$. Also, since A is sparse, the main result of [22] implies that $\mu_{\mathrm{p}}(\mathrm{P}_{\mathrm{m}}(A)) = 0$.

(b) If $A \in \mathrm{P} - \{\emptyset, \{0,1\}^*\}$, then $\mu(\mathrm{P}_{\mathrm{m}}(A) \mid \mathrm{E}) = \mu_{\mathrm{p}}(\mathrm{P}_{\mathrm{m}}(A)) = 0$, but $\mu_{\mathrm{p}}(\mathrm{P}^{-1}_{\mathrm{m}}(A)) \neq 0$ and $\mu(\mathrm{P}^{-1}_{\mathrm{m}}(A) \mid \mathrm{E}) \neq 0$.

(c) If A is $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for E, then $\mu(\mathrm{P}^{-1}_{\mathrm{m}}(A) \mid \mathrm{E}) = \mu_{\mathrm{p}}(\mathrm{P}^{-1}_{\mathrm{m}}(A)) = 0$ by Theorem 5.3, but $\mu(\mathrm{P}_{\mathrm{m}}(A) \mid \mathrm{E}) = \mu(\mathrm{E} \mid \mathrm{E}) \neq 0$.

Similar examples can be given for E_2.

6 Complexity Cores: Upper Bound

In this section we give an explicit *upper* bound on the sizes of complexity cores of languages that are $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E. This bound implies that $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete languages for E have *unusually small* complexity cores, for languages in E.

Theorem 6.1. For every $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard language H for E, there exist $B, D \in \mathrm{DTIME}(2^{4n})$ such that D is dense and $B = H \cap D$.

Proof. By Corollary 4.5, there is a language in E that is incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions. In fact, Meyer's construction [26] shows that there is a language $A \in \mathrm{DTIME}(5^n)$ that is incompressible by $\leq^{\mathrm{P}}_{\mathrm{m}}$-reductions. As in Fact 4.7 and Theorem 4.9, this idea has often been used to establish *lower* bounds on the complexities of $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard languages. Here we use it to establish an *upper* bound.

The following simple notation is useful here. 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.

Let H be $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E. Then there is a $\leq^{\mathrm{P}}_{\mathrm{m}}$-reduction f of A to H. Let $B = f^{\geq}(A), D = f^{\geq}(\{0,1\}^*)$. Since $A \in \mathrm{DTIME}(5^n)$ and $f \in \mathrm{PF}$, it is clear that $B, D \in \mathrm{DTIME}(10^n) \subseteq \mathrm{DTIME}(2^{4n})$.

Fix a polynomial q and a real number $\epsilon > 0$ such that $|f(x)| \leq q(|x|)$ for all $x \in \{0,1\}^*$ and $q(n^{2\epsilon}) < n$ a.e. Let $W = \left\{x \mid |f(x)| < |x|\right\}$. Then, for all sufficiently large $n \in \mathbf{N}$, writing $m = \lfloor n^{2\epsilon} \rfloor$, we have

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

whence

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

Since $|C_f| < \infty$, it follows that $|D_{\leq n}| > 2^{n^\epsilon}$ for all sufficiently large n. Thus D is dense.

Finally, note that $B = f^{\geq}(A) = f^{\geq}(f^{-1}(H)) = H \cap f^{\geq}(\{0,1\}^*) = H \cap D$. This completes the proof of Theorem 6.1.

□

We now use Theorem 6.1 to prove our upper bound on the size of complexity cores for hard languages.

Theorem 6.2. Every DTIME(2^{4n})-complexity core of every $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard language for E has a dense complement.

Proof. Let H be $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E and let K be a DTIME(2^{4n})-complexity core of H. Choose B, D for H as in Theorem 6.1. Fix machines M_B and M_D that decide B and D, respectively, with $time_{M_B}(x) = O(2^{4|x|})$ and $time_{M_D}(x) = O(2^{4|x|})$. Let M be a machine that implements the following algorithm.

begin
    input x;
    if $M_D(x)$ accepts
      then simulate $M_B(x)$
      else run forever
end M.

Then $x \in D \Rightarrow M(x) = [\![x \in B]\!] = [\![x \in H \cap D]\!] = [\![x \in H]\!]$ and $x \notin D \Rightarrow M(x) = \bot \leq [\![x \in H]\!]$, so M is consistent with H. Also, there is a constant $c \in \mathbf{N}$ such that for all $x \in D$,

$$time_M(x) \leq c \cdot 2^{4n} + c.$$

Since K is a DTIME(2^{4n})-complexity core of H, it follows that $K \cap D$ is finite. But D is dense, so this implies that $D - K$ is dense, whence K^c is dense. □

Note that Theorem 5.3 follows from Corollary 4.6 and Theorem 6.2, but that Theorem 6.2 tells us more.

The main construction of [21] shows that, for every $c \in \mathbf{N}$, there is a language H that is weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard for E and has $\{0,1\}^*$ as a DTIME(2^{cn})-complexity core. Thus, in contrast with the lower bound given by Theorem 4.9, the upper bound given by Theorem 6.2 cannot be extended to weakly $\leq^{\mathrm{P}}_{\mathrm{m}}$-hard languages.

Finally, we note that the upper bound given by Theorem 6.2 is tight.

Theorem 6.3. Let $c \in \mathbf{N}$ and $0 < \epsilon \in \mathbf{R}$.

1. E has a $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete language with a DTIME(2^{cn})-complexity core K that satisfies $|K_{\leq n}| > 2^{n+1} - 2^{n^\epsilon}$ a.e.

2. E_2 has a $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete language with a DTIME(2^{n^c})-complexity core K that satisfies $|K_{\leq n}| > 2^{n+1} - 2^{n^\epsilon}$ a.e.

Proof. We prove the result for E. The proof for E_2 is similar.

Let A be a language that is $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for E and let $k = \lceil \frac{2}{\epsilon} \rceil$. By Corollary 4.6, fix a language $B \in \mathrm{E}$ that has $\{0,1\}^*$ as a DTIME(2^{cn})-complexity core. Let

$$D = \{x10^{|x|^k} | x \in \{0,1\}^*\}$$

and define the languages

$$C = (B - D) \cup \{x10^{|x|^k} \mid x \in A\}$$

and

$$K = D^c.$$

It is clear that C is $\leq^{\mathrm{P}}_{\mathrm{m}}$-complete for E. Also, for all sufficiently large n,

$$|D_{\leq n}| = \sum_{m=0}^{n} |D_{=m}| \leq \sum_{m=0}^{n} 2^{m^{\frac{1}{k}}} \leq (n+1)2^{n^{\frac{1}{k}}} \leq (n+1)2^{n^{\frac{\epsilon}{2}}} < 2^{n^\epsilon} - 1,$$

so

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

We complete the proof by showing that K is a DTIME(2^{cn})-complexity core for C. For this, let $s \in \mathbf{N}$, let M be a machine that is consistent with C, and define the fast set

$$F = \{x \mid time_M(x) \leq a \cdot 2^{c|x|} + a\}.$$

It suffices to prove that $|K \cap F| < \infty$.

Let $\hat{M}$ be a machine (designed in the obvious way) such that, for all $y \in \{0,1\}^*$,

$$\hat{M}(y) = \begin{cases} M(y) & \text{if } y \notin D \\ \perp & \text{if } y \in D. \end{cases}$$

Then $\hat{M}$ is consistent with B (because $B - D = C - D$ and M is consistent with C) and $\{0,1\}^*$ is a DTIME(2^{cn})-complexity core for B, so the fast set

$$\hat{F} = \{x \mid time_{\hat{M}}(x) \leq (a+1)2^{c|x|} + a\}$$

is finite. Since $K \cap F = F - D$ and $(F - D) - \hat{F}$ is finite, it follows that $|K \cap F| < \infty$, completing the proof. □

7 Conclusion

In this paper we have investigated measure-theoretic aspects of the $\leq_m^P$-reducibility structure of the exponential time complexity classes E and E_2. Among other things, we have proven the following. (For simplicity we only consider the class E.)

(i) Every weakly $\leq_m^P$-hard language for E has a dense exponential complexity core (Theorem 4.9).

(ii) For every language $A \in E$, at least one of the spans $P_m(A)$, $P_m^{-1}(A)$ has resource-bounded measure 0 (Theorem 5.1, the Small Span Theorem). Thus the $\leq_m^P$-hard languages for E form a p-measure 0 set (Theorem 5.3), *every* $\leq_m^P$-degree has measure 0 in E (Theorem 5.5), and the $\leq_m^P$-complete languages for NP form a set of measure 0 in E (Corollary 5.7).

(iii) Every DTIME(2^{4n})-complexity core of every $\leq_m^P$-hard language for E has a dense complement (Theorem 6.2). Since almost every language in E has $\{0,1\}^*$ as a DTIME(2^{4n})-complexity core (Corollary 4.6), this says that, in E, the $\leq_m^P$-complete languages are *unusually simple*, in the sense that they have *unusually small* complexity cores.

It is reasonable to conjecture that most of our results hold with $\leq_m^P$ replaced by $\leq_T^P$, but investigating this may be difficult. For example, consider Theorem 5.3. Bennett and Gill [5] have shown that $P_T^{-1}(A)$ has (classical) measure 1 for all $A \in$ BPP. Thus we cannot prove that the $\leq_T^P$-hard languages for E form a measure 0 set without also proving that E $\not\subseteq$ BPP.

References

[1] K. Ambos-Spies. Randomness, relativizations, and polynomial reducibilities. In *Proceedings of the First Structure in Complexity Theory Conference*, pages 23–34, 1986.

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

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

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

[5] C. H. Bennett and J. Gill. Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \text{co-NP}^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, 1981.

[6] L. Berman. On the structure of complete sets: Almost everywhere complexity and infinitely often speedup. In *Proceedings of the Seventeenth Annual Conference on Foundations of Computer Science*, pages 76–80, 1976.

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

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

[9] R. Book, D.-Z Du, and D. Russo. On polynomial and generalized complexity cores. In *Proceedings of the Third Structure in Complexity Theory Conference*, pages 236–250, 1988.

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

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

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

[13] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-completeness.* W.H. Freeman and Company, 1979.

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

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

[16] L. A. Levin. Universal sequential search problems. *Problems of Information Transmission*, 9:265–266, 1973.

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

[18] J. H. Lutz. Intrinsically pseudorandom sequences, in preparation.

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

[20] J. H. Lutz. The quantitative structure of exponential time. In *Proceedings of the Eighth Structure in Complexity Theory Conference*, pages 158–175. IEEE Computer Society Press, 1993.

[21] J. H. Lutz. Weakly hard problems. Technical Report 93-13, Iowa State University, 1993. Submitted.

[22] J. H. Lutz and E. Mayordomo. Measure, stochasticity, and the density of hard languages. *SIAM Journal on Computing*, to appear. See also *Proceedings of the Tenth Symposium on Theoretical Aspects of Computer Science*, Springer-Verlag, 1993, pp. 38–47.

[23] J. H. Lutz and E. Mayordomo. Cook versus Karp-Levin: Separating completeness notions if NP is not small. Technical Report 92-24, Iowa State University, 1992. Submitted.

[24] N. Lynch. On reducibility to complex or sparse sets. *Journal of the ACM*, 22:341–345, 1975.

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

[26] A. R. Meyer, 1977. reported in [7].

[27] P. Orponen. A classification of complexity core lattices. *Theoretical Computer Science*, 70:121–130, 1986.

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

[29] D. A. Russo and P. Orponen. On P-subset structures. *Mathematical Systems Theory*, 20:129–136, 1987.