



1

The Structure of Complete Degrees

Stuart A. Kurtz¹
Stephen R. Mahaney²
James S. Royer³

1.1 Introduction

The notion of NP-completeness has cut across many fields and has provided a means of identifying deep and unexpected commonalities. Problems from areas as diverse as combinatorics, logic, and operations research turn out to be NP-complete and thus computationally equivalent in the sense discussed in the next paragraph. PSPACE-completeness, NEXP-completeness, and completeness for other complexity classes have likewise been used to show commonalities in a variety of other problems. This paper surveys investigations into how strong these commonalities are. More concretely, we are concerned with:

What do NP-complete sets look like?

To what extent are the properties of particular NP-complete sets, e.g., SAT, shared by *all* NP-complete sets?

If there are structural differences between NP-complete sets, what are they and what explains the differences?

We make these questions, and the analogous questions for other complexity classes, more precise below. We need first to formalize NP-completeness.

There are a number of competing definitions of NP-completeness. (See [Har78a, p. 7] for a discussion.) The most common, and the one we use, is based on the notion of *m-reduction*, also known as *polynomial-time many-one reduction* and *Karp reduction*. A set A is *m-reducible* to B if and only if there is a (total) polynomial-time computable function f such that

$$\text{for all } x, \quad x \in A \iff f(x) \in B. \quad (1)$$

¹Department of Computer Science; University of Chicago; 1100 E. 58th St; Chicago, IL 60637.

²Department of Computer Science, University of Arizona, Tucson, AZ 85721.

³School of Computer & Information Science; Syracuse University; Syracuse, NY 13210.

Intuitively, (1) says that A is no harder than B in the sense that, if one has a means of answering “ $x \in B$?” questions, then one can also answer “ $x \in A$?” questions with the computation of $f(x)$ as the the only additional overhead. An NP-*complete set* is an NP set to which all NP sets are m-reducible. Thus, any two NP-complete sets are m-equivalent, that is, interreducible by m-reductions. Since m-reductions relate the hardness of sets, the NP-complete sets are therefore all of the same degree of difficulty.

The formal definition of m-reduction does not seem to capture all the important aspects of the reductions used by Karp and his successors in NP-completeness proofs. In a Karp-style proof that a problem B is NP-complete, one takes a known NP-complete problem A , and shows how to *translate* the structure of an arbitrary instance of A into an instance of B . (See [GJ79, Chapter 3] for examples of such arguments.) Since these “in practice” m-reductions preserve the structure of individual instances, one might expect that these reductions would also preserve the global structure of a problem, and, that the NP-complete sets shown equivalent by Karp-style proofs would share a strong structural similarity.

Berman and Hartmanis [BH77] showed that this is the case in 1977. They considered a number of well known NP-complete sets and showed that these sets are all pairwise *polynomial-time isomorphic*.⁴ Since many complexity theoretic properties of sets are invariant under polynomial-time isomorphisms, Berman and Hartmanis thus established that, in many respects, these NP-complete sets are *identical* in structure. Moreover, Berman and Hartmanis went through the current literature on “conventional” NP-complete sets⁵ and observed that using their methods these sets could also be shown to be polynomial-time isomorphic to their previous examples. Motivated by this evidence, the lack of any counterexamples, and also by analogy with results in recursion theory, Berman and Hartmanis made the following conjecture.

The Isomorphism Conjecture *All NP-complete sets are polynomial-time isomorphic.*

This conjecture predicts that $P \neq NP$, that NP-complete sets are pad-dable (see §1.2) and self-reducible (see, for example, [Mah89]), and that

⁴ A is *polynomial-time isomorphic to* B if and only if there exists f , an m-reduction from A to B as in (1), that is also 1-1, onto, and whose inverse f^{-1} is computable in polynomial-time, in other words, f is a polynomial-time computable and invertible permutation on $\{0, 1\}^*$ such that $f(A) = B$ and $f^{-1}(B) = A$.

⁵By a *conventional* NP-complete set we mean, informally, a set that results from a straightforward coding of an NP-complete problem that stems from work in combinatorics, optimization, etc.

NP-complete sets and their complements have exponential density.⁶ This last prediction was partially confirmed by P. Berman [Ber78] and Fortune [For79] who showed that if $P \neq NP$, then there are no coNP-complete sparse sets⁷ and by Mahaney [Mah82] who showed that if $P \neq NP$, then there are no NP-complete sparse sets.⁸

The isomorphism conjecture is attractive and intriguing, but there are good reasons to doubt the sufficiency of its supporting evidence. Let us call the sets p-isomorphic to SAT *standard* NP-complete sets.⁹ The NP-complete sets that Berman and Hartmanis showed to be standard are all conventional NP-complete sets as discussed above, and, moreover, since Berman and Hartmanis's sets are all p-isomorphic, they each can be rightly viewed as being a natural encoding of a *single* combinatorial problem—Satisfiability. However, there is no *a priori* reason to expect that every NP-complete set is conventional, much less standard. Joseph and Young [JY85] raised this objection and backed it up by constructing nonconventional NP-complete sets that are not obviously standard. Moreover, they conjectured that some of their NP-complete sets do indeed fail to be standard.

One-way functions¹⁰ played a key role in Joseph and Young's examples. Selman has shown that the Joseph-Young sets have the form $f(A)$ for some standard NP-complete set A and some one-way function f . (Watanabe [Wat85] made related observations.) One can think of $f(A)$ as a highly encrypted version of A . Thus, the essential idea behind Joseph and Young's conjecture is

The Encrypted Complete Set Conjecture *There is a one-way function f and a standard complete set A such that A and the NP-complete set $f(A)$ are not polynomial-time isomorphic.*

One problem with this conjecture is that there is no concrete candidate for the one-way function of the conjecture. Furthermore, any one-way function that fits the conjecture's requirements would seemingly need to possess much stronger properties than just the failure to have a polynomial-time inverse. What these properties should be is uncertain.

⁶ A has *exponential density* if and only if the growth of $\text{Cardinality}(\{x \in A : |x| \leq n\})$ is $\Omega(2^{n^{1/k}})$ for some k .

⁷ A set A is *sparse* if and only if the growth of $\text{Cardinality}(\{x \in A : |x| \leq n\})$ is $\mathcal{O}(n^k)$ for some k .

⁸ This paper does not further discuss sparse sets results. Mahaney surveys this work in [Mah89].

⁹ By Theorem 12 below and the fact that paddability (defined in §1.2) is preserved under p-isomorphisms, the standard NP-complete sets are precisely the paddable NP-complete sets.

¹⁰ A polynomial-time computable function f is *one-way* if and only if f is 1-1 and polynomially honest, but f^{-1} is not polynomial-time computable. These functions are widely conjectured to exist and various forms of one-way functions play important roles in cryptography.

The contention between the isomorphism and the encrypted complete set conjectures has provoked much study. Other than the sparse set results mentioned above, the structure of the NP-complete sets remains a (complete) mystery. However, for certain other complexity classes, a reasonable understanding of their m-complete sets¹¹ has emerged. The best understood class of m-complete sets are those of EXP, the sets decidable in deterministic exponential time.¹² For example, it is known that:

- The EXP-complete sets are all 1-li-equivalent, that is, they are pairwise m-equivalent as witnessed by 1-1, length increasing m-reductions. A 1-li-equivalence is intuitively a very strong equivalence relation on sets. One can show that if one-way functions do not exist, then 1-li-equivalence implies polynomial-time isomorphism. Thus, if one-way functions do not exist, all the EXP-complete sets are polynomial-time isomorphic. (See Theorems 8 and 17 below.)
- There is a characterization of the existence of one-way functions involving the 1-li-equivalence of sets: One-way functions exist if and only if there are two sets in EXP that are 1-li-equivalent, but *not* polynomial-time isomorphic. Moreover, one can take these two sets to be “close” to m-complete for EXP. (See Theorem 28 below.)
- The isomorphism conjecture asserts that a particular m-equivalence class of sets (the class of NP-complete sets) “collapses” in the sense that any two members of this m-equivalence class are polynomial-time isomorphic. One can exhibit such a “collapsing” m-equivalence class of sets in EXP. Moreover, the sets in this m-equivalence class are all “close” to m-complete for EXP in the same sense of “close” as the two sets in the previous item. (See Theorem 27 below.)
- There are certain very strong forms of one-way functions the existence of which would imply that there are “encrypted complete sets” for EXP (and also NP, PSPACE, and many other complexity classes). Such one-way functions do exist relative to random oracles. Therefore, the NP, PSPACE, EXP, ... versions of the encrypted complete set conjecture are correct relative to a random oracle. (See Proposition 25 and Theorem 37 below.)

These results illustrate the miles we have come in answering the questions raised by the two conjectures and the parsecs to go until any final resolution is reached. These questions seem far more complex than anyone had

¹¹That is, the sets in a complexity class to which all sets in the class polynomial-time m-reduce.

¹²In this paper, we say that a set is decidable in exponential time if and only if the set has a deterministic decision procedure that, for some k , runs in $2^{\mathcal{O}(n^k)}$ time.

initially believed and they seem to have interesting connections to other fundamental questions in complexity theory, e.g., the nature of one-way functions.

This article discusses research on the isomorphism and the encrypted complete set conjectures. We have *not* attempted to write a comprehensive survey of this work. We have instead tried to present a coherent sketch of the area's key results and ideas. Towards this end we have included proofs that illustrate some of these ideas. Our goal has been to lead the reader from a basic understanding of NP-completeness to the current frontiers of research on the structure of classes of complete sets. Readers will also benefit from Young's survey in this volume, as well as from consulting the original references.

1.2 Basic Definitions

We shall assume that the reader is familiar with the rudiments of recursion theory, e.g., the s-m-n theorem. See [Cut80] and [DW83] for elementary introductions. We also shall assume the reader is familiar with the basics of machine based computational complexity as discussed in [HU79] and with the definitions of LOGSPACE, P, NP, and PSPACE. Σ_k^p denotes the k -th Σ class in the Meyer and Stockmeyer [MS72] polynomial hierarchy. ($\Sigma_1^p = \text{NP}$ and $\Sigma_2^p =$ the sets in NP relative to an oracle for SAT. See [GJ79] for more discussion.) EXP denotes the class of sets decidable within a $2^{\text{poly}(n)}$ time bound on a deterministic Turing machine, and NEXP denotes the corresponding nondeterministic time class. RE denotes the class of recursively enumerable sets. Logspace, Ptime, and Pspace respectively denote the class of total functions computable in deterministic logarithmic-space, polynomial-time, and polynomial-space.

N denotes the set of natural numbers $\{0, 1, 2, \dots\}$. We identify each $x \in N$ with the x -th string over the symbols $\mathbf{0}$ and $\mathbf{1}$ in the lexicographic ordering on $\{\mathbf{0}, \mathbf{1}\}^*$. We tend to use natural numbers and strings over $\{\mathbf{0}, \mathbf{1}\}$ interchangeably. Unless specified otherwise, functions are over N and total and sets are subsets of N . The length of $x \in N$ (i.e., the length of its string representation) is denoted $|x|$. Let $\langle \cdot, \cdot \rangle$ denote a polynomial-time computable pairing function, see [Rog67] for an example.

CONDITIONS ON FUNCTIONS. A function f is:

h-honest if and only if, for all x , $|x| \leq h(|f(x)|)$.

polynomially honest if and only if for some polynomial p , f is p -honest.

exponentially honest if and only if for some constant c , f is $\lambda n. 2^{cn+c}$ -honest.

length increasing if and only if, for all x , we have $|f(x)| > |x|$.

linear length bounded if and only if there is a constant a such that, for all x , $|f(x)| \leq a(|x| + 1)$.

polynomial length bounded if and only if there is a polynomial p , such that, for all x , $|f(x)| \leq p(|x|)$.

p-invertible if and only if there is a Ptime function g such that $g \circ f$ is the identity.

REDUCIBILITIES. Recall from the introduction that a set A is *m-reducible* (i.e., many-one reducible) to a set B if and only if there is a polynomial-time computable function f such that

$$\text{for all } x \in N, x \in A \iff f(x) \in B. \quad (2)$$

A is *recursively m-reducible to B* if and only if there is a recursive function f such that (2) holds. Logspace, Pspace, . . . m-reductions are defined analogously.

A is *1-reducible to B* if and only if there is a 1-1 function which witnesses that A is m-reducible to B . A is *1-honest-reducible to B* if and only if there is a polynomially honest function which witnesses that A is 1-reducible to B . A is *1-li-reducible to B* if and only if there is a length increasing function which witnesses that A is 1-reducible to B or else $A = B$. (The $A = B$ clause is to make 1-li-reducibility a reflexive relation.) Finally, A is *p-isomorphic to B* if and only if there is an f which witnesses that A is m-reducible to B which is also 1-1, onto, and p-invertible. **N.B.** If A and B are p-isomorphic, then they are necessarily 1-honest-equivalent, but they need not be 1-li comparable.¹³

A set A is *complete* for a class of sets \mathcal{C} with respect to a reducibility R if and only if A is in \mathcal{C} and every set in \mathcal{C} R -reduces to A . So, for example, we can speak of m-complete, 1-complete, 1-li-complete, . . . sets for NP. In this paper “ \mathcal{C} -complete” means “m-complete for the class \mathcal{C} .”

Reducibilities relate the hardness of sets. Hence, an equivalence class of sets with respect to a reducibility relation consists of sets of the same “degree” of difficulty. We thus define a *degree* to be an equivalence class under a reducibility.¹⁴ So, we speak of m-degrees, 1-degrees, 1-honest-degrees and 1-li-degrees according to the reducibility intended.

A degree *collapses* if and only if all of its elements are pairwise p-isomorphic. Thus, the Berman-Hartmanis isomorphism conjecture can be stated succinctly: the complete m-degree for NP collapses. We sometimes use the term “collapses” more generally. For example, we say an m-degree collapses to a 1-li-degree when all of the m-degree’s elements are 1-li-equivalent.

¹³Consider the sets $\{\mathbf{0}^{4^i}, \mathbf{0}^{2 \cdot 4^i + 1} : i \in N\}$ and $\{\mathbf{0}^{4^{i+1}}, \mathbf{0}^{2 \cdot 4^i} : i \in N\}$.

¹⁴The term “degree” comes from Post’s [Pos44]—the paper that founded modern recursion theory.

CYLINDERS. A set A is a *cylinder* if and only if for some B , A is p-isomorphic to the set $\{\langle b, z \rangle : b \in B \ \& \ z \in N\}$. A set A is *paddable* if and only if there exists $p(\cdot, \cdot)$, a polynomial-time computable, p-invertible¹⁵ function, such that, for all a and x ,

$$a \in A \iff p(a, x) \in A.$$

It is clear that cylinders are paddable. Mahaney and Young [MY85] show that all paddable sets are cylinders. Below we shall treat being a cylinder and being paddable as synonymous. Since paddability is, on the surface, a looser condition on a set, it turns out to be the easier of the two notions with which to work.

PROGRAMMING SYSTEMS. We say $\nu(\cdot, \cdot)$ is a *universal function* for a class of partial functions \mathcal{F} if and only if $\nu(\cdot, \cdot)$ is partial recursive and $\mathcal{F} = \{\lambda x.\nu(i, x) : i \in N\}$. Such a $\nu(\cdot, \cdot)$ determines a *programming system* $\langle \nu_i \rangle_{i \in N}$ for \mathcal{F} , where for each i , $\nu_i = \lambda x.\nu(i, x)$. A universal function $\nu(\cdot, \cdot)$ and its associated programming system $\langle \nu_i \rangle_{i \in N}$ are really two different views of the same object. We use ν to denote both the universal function $\nu(\cdot, \cdot)$ and programming system $\langle \nu_i \rangle_{i \in N}$.

A programming system, φ , for the class of partial recursive functions is *acceptable* if and only if for each programming system ψ (for some class of functions), there is a recursive function t such that, for all p , $\psi_p = \varphi_{t(p)}$, i.e., there is an effective way of translating ψ -programs into equivalent φ -programs. (For alternative definitions see [MY78] and [Rog67].) Henceforth, φ will be a fixed acceptable programming system.

We say that $\langle S_i \rangle_{i \in N}$ is a *programming system for a class of sets* \mathcal{S} if and only if (i) $[x \in S_i]$ is partial recursive relation in i and x and (ii) $\mathcal{S} = \{S_i \mid i \in N\}$. For example, for all i , define $W_i = \text{domain}(\varphi_i)$; $\langle W_i \rangle_{i \in N}$ is then a programming system for the class of r.e. sets [Rog67].

The *recursion theorem* holds for a programming system ν if and only if for each “ ν -program” i , there is another ν -program e such that

$$\nu_e = \lambda x.\nu_i(\langle e, x \rangle). \tag{3}$$

Intuitively, e is a self-referential program that, on input x , generates a copy of its own program “text” and subsequently uses that copy as an additional datum together with x on which to run program i .¹⁶ If $\langle A_i \rangle_{i \in N}$

¹⁵In this context, p-invertible means that there is a polynomial time computable g such that, for all x and y , $g(p(x, y)) = \langle x, y \rangle$.

¹⁶**N.B.** This is the Kleene form of the recursion theorem [Rog67, p. 214], *not* the commonly taught fixed point form. In acceptable programming systems the two forms are roughly equivalent. However, for subrecursive programming systems for natural subrecursive classes, Kleene’s form of the recursion theorem is often valid, but the fixed point form is essentially *never* valid. (Consider the possible “fixed points” for an f such that, for all i and x , $\nu_{f(i)} = 1 + \nu_i(x)$.)

is a programming system for a class of sets, then the recursion theorem holds for $\langle A_i \rangle_{i \in \mathbb{N}}$ if and only if, for each i , there is an ϵ such that

$$A_\epsilon = \{ x : \langle \epsilon, x \rangle \in A_i \}.$$

The recursion theorem holds for φ [Rog67, p. 214] and also $\langle W_i \rangle_{i \in \mathbb{N}}$. Let ψ be a programming system for the polynomial-time computable functions such that $\lambda i, x. \psi_i(x)$ is computable in time exponential in $|i| + |x|$ and such that the recursion theorem holds for ψ . See [Koz80] and [RC87] for examples of such ψ .

Suppose C is an m-complete set for a complexity class \mathcal{C} . Observe that f m-reduces a set A to C if and only if $A = f^{-1}(C)$. For all i , let $A_i = \psi_i^{-1}(C)$. It follows that $\langle A_i \rangle_{i \in \mathbb{N}}$ is a programming system for \mathcal{C} . Moreover, the recursion theorem holds for $\langle A_i \rangle_{i \in \mathbb{N}}$.¹⁷

For more about programming systems for subrecursive collections of functions and sets, their properties, and their uses, see [RC87].

ONE-WAY FUNCTIONS. A function f is *one-way* if and only if f is 1-1, polynomially honest, and polynomial-time computable, yet not p-invertible. A set A is in the class UP if and only if there exists a polynomial p and a polynomial-time decidable predicate $Q(\cdot, \cdot)$ such that

$$A = \{ x : (\exists y : |y| \leq p(|x|)) Q(x, y) \},$$

and, for each x , there is at most one y such that $Q(x, y)$. UP is clearly a subclass of NP. Independently, Berman [Ber77], Grollmann and Selman [GS84] [GS88] and Ko [Ko85] observed that one-way functions exist if and only if $P \neq UP$.¹⁸ Below this equivalence is taken for granted.

A special sort of one-way function is introduced in [KMR89]. A function f is a *scrambling function* if and only if f is 1-1, polynomially honest, and polynomial-time computable and, for all nonempty A , $f(A)$ is not paddable.

¹⁷Here is a proof sketch of our claim that the recursion theorem holds for $\langle A_i \rangle_{i \in \mathbb{N}}$. For convenience, we identify sets with their characteristic functions. Thus, the equation $A_i = \psi_i^{-1}(C)$ can be rewritten $A_i = C \circ \psi_i$. Fix i . By the recursion theorem for ψ there is an ϵ such that $\psi_\epsilon = \lambda x. \psi_i(\langle \epsilon, x \rangle)$. Hence,

$$A_\epsilon = C \circ \psi_\epsilon = \lambda x. C \circ \psi_i(\langle \epsilon, x \rangle) = \lambda x. A_i(\langle \epsilon, x \rangle).$$

Therefore, the claim follows.

¹⁸Berman did not explicitly consider one-way functions. Rather, he distinguished between the polynomial-time computable and invertible functions (which he called the ‘‘P-E’’ functions), and polynomial-time computable, 1-1, honest functions (which he called ‘‘P-1B’’ functions). From these definitions, he proved that P-E = P-1B if and only if P = UP.

1.3 Recursion Theoretic Results

Before discussing polynomial-time complete m -degrees, we first consider some important related results from recursion theory on the structure of the class of recursively m -complete r.e. sets. The problem of describing this structure was settled by Myhill. He showed

Theorem 1 ([Myh55]) *Two sets are recursively 1-equivalent if and only if they are recursively isomorphic.*

Theorem 2 ([Myh55]) *The recursively m -complete r.e. sets are pairwise recursively 1-equivalent.*

From these two theorems one immediately obtains

Corollary 3 *The recursively m -complete r.e. sets are pairwise recursively isomorphic.*

Corollary 3 completely describes the recursion theoretic structure of the class of recursively m -complete r.e. sets—there is essentially only one set in the class. These theorems were part of the inspiration for the original paper of Berman and Hartmanis and remain an important influence on the work on polynomial-time m -complete degrees.

We mention a slightly different route to Corollary 3 which uses the notion of recursive cylinder.

Theorem 4 *Two recursive cylinders are recursively m -equivalent if and only if they are recursively isomorphic.*

Theorem 5 *Every recursively m -complete r.e. set is a recursive cylinder.*

Corollary 3 follows immediately from these last two theorems. Both of these theorems are implicit in Myhill's paper [Myh59], also see [You66].

The proofs of Theorems 1 and 2 introduce a number of ideas important for the complexity theoretic work of the following sections. Because of this importance, we sketch proofs for both theorems. Our proof of Theorem 1 is largely based on Myhill's original proof which in turn is partly based on the standard construction for the Cantor-Bernstein theorem (sometimes known as the Schröder-Bernstein theorem or the Cantor-Schröder-Bernstein theorem) from set theory.¹⁹ Our argument for Theorem 2 is based on a proof of

¹⁹Cantor, in his theory of cardinality of sets [Can55], makes the following two basic definitions. Two sets A and B are said to *have the same cardinality* if and only if there is a 1-1 correspondence between A and B ; and A *has cardinality less than or equal to that of B* if and only if there is a 1-1 map from A into B , (i.e., A has the same cardinality as a subset of B). In order for these two definitions to make sense, it should be the case that: If A has cardinality less than or equal

a related result about acceptable programming systems [Sch75, Theorem 2], which Schnorr credits to an anonymous referee.

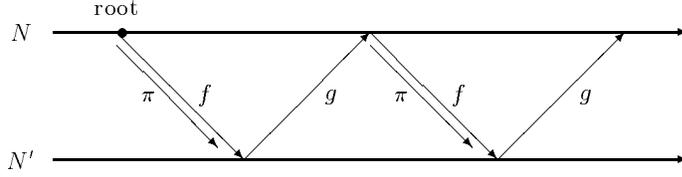
to that of B and B has cardinality less than or equal to that of A , then A and B have the same cardinality. This is the case as shown by

The Cantor-Bernstein Theorem *If there is a 1-1 map from A into B and a 1-1 map from B into A , then there is a 1-1 correspondence between A and B .*

The standard proof of this theorem (see the proof of Theorem 1) is so simple and direct it is difficult to realize that a satisfactory proof of the theorem was hard to obtain. What follows is a partial history of the result taken from Moore's excellent book [Moo82].

- 1882 Cantor claims (without proof) the theorem in a paper.
- 1883 Cantor proves the theorem for subsets of \mathbf{R}^n using the Continuum Hypothesis.
- 1883 Cantor poses the general theorem as an open problem in a letter to Dedekind.
- 1884 Cantor again claims (without proof) the theorem in a paper.
- 1887 Dedekind proves the theorem in his notebook and promptly forgets about solving the problem. This particular solution is first published in 1932 in Dedekind's collected works.
- 1895 Cantor states the theorem as an open problem in a paper.
- 1896 Burali-Forti proves the theorem for countable sets.
- 1897 Bernstein (a Cantor student) proves the general theorem using the Denumerability Assumption, a weak form of the axiom of choice. Cantor shows the proof to Borel.
- 1898 Schröder publishes a "proof" of the theorem. Korselt points out to Schröder that the proof is wrong. Schröder's proof turns out to be unfixable.
- 1898 Borel publishes Bernstein's proof in an appendix of Borel's 1898 book on set theory and complex functions.
- 1899 Dedekind sends Cantor an elementary proof of the theorem, which from Moore's description sounds like the proof used today.
- 1901 Bernstein's thesis appears (with his proof).
- 1902 Korselt sends in a proof of the theorem (along the lines of Dedekind's proof) to *Mathematische Annalen*. Korselt's paper appears in 1911!
- 1907 Jourdain points out that the use of the Denumerability Assumption in Bernstein's proof is removable.

Moore suspects that Cantor had a proof of the theorem that used the well ordering principle (which turns out to be equivalent to the axiom of choice). Cantor was unclear for many years whether the well ordering principle was "a law of thought" or something that needed proof. So, the fact that the theorem came and went several times might have been in part a function of Cantor's uncertainty about well ordering.


 FIGURE 1.1. The N rooted case.

Proof Sketch of Theorem 1 In the following let N' denote a disjoint copy of N . If x is a member of N , then x' denotes the corresponding element of N' . Now, suppose that $A \subseteq N$, $B \subseteq N'$, $f: N \rightarrow N'$ recursively 1-reduces A to B , and $g: N' \rightarrow N$ recursively 1-reduces B to A . We introduce the directed graph $G = (N \cup N', E)$, where

$$E = \{ (x, f(x)) : x \in N \} \cup \{ (x', g(x')) : x' \in N' \}.$$

G is clearly bipartite. Since f and g are functions, every vertex of G has out-degree one. Since f and g are 1-1, every vertex of G has in-degree of at most one.

The maximal connected components of G we call f, g -chains. An f, g -chain C has one of four possible structures.

1. *The cyclic case.* C is a finite cyclic path containing an even number of vertices.

2. *The two-way infinite case.* C is an infinite path in which every vertex has in-degree one.

3. *The N rooted case.* C is an infinite path with a root $r \in N$, i.e., r is a vertex of C with in-degree zero.

4. *The N' rooted case.* C is an infinite path with a root in N' .

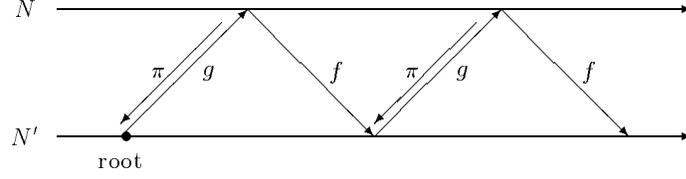
We say a function $h: N \rightarrow N'$ respects f, g -chains if and only if for all x , $h(x)$ is a member of x 's f, g -chain. Since f and g recursively 1-reduce A to B and B to A , respectively, it follows that for any h that respects f, g -chains we have, for each x , that $x \in A \iff h(x) \in B$.

Now, given f and g , the standard construction for Cantor-Bernstein defines

$$\pi = \lambda x \bullet \begin{cases} f(x), & \text{if } x\text{'s } f, g\text{-chain is either cyclic,} \\ & \text{two-way infinite, or } N \text{ rooted;} \\ g^{-1}(x), & \text{if } x\text{'s } f, g\text{-chain is } N' \text{ rooted.} \end{cases} \quad (4)$$

The two rooted cases are illustrated by Figures 1.1 and 1.2. It is straightforward to argue that π is 1-1, onto, and respects f, g -chains. Moreover, since π respects f, g -chains, for each x , we have $x \in A \iff \pi(x) \in B$. The only problem is that π may not be recursive.

The definition of π is based on a global analysis of the structure of f, g -chains. Myhill's construction is much more local. It defines a $\hat{\pi}$ in stages $0, 1, 2, \dots$. Initially, $\hat{\pi} = \emptyset$.


 FIGURE 1.2. The N' rooted case.

Stage $2x$. If $\hat{\pi}(x)$ is defined, go on to stage $2x + 1$. Otherwise, traverse the f, g -chain of x forward until an N' vertex y' is encountered that is not yet in range($\hat{\pi}$). Define $\hat{\pi}(x) = y'$.

Stage $2x + 1$. If $\hat{\pi}^{-1}(x')$ is defined, go on to stage $2x + 2$. Otherwise, traverse the f, g -chain of x' forward until an N vertex y is encountered that is not yet in domain($\hat{\pi}$). Define $\hat{\pi}(y) = x'$.

It is clear from the construction that $\hat{\pi}$ is 1-1 and respects f, g -chains. A simple counting argument shows that, for each stage $2x$, a y' as required exists, and, for each stage $2x+1$, a y as required exists. Thus, the even stages of the construction ensure that $\hat{\pi}$ is total, while the odd stages ensure that it is onto. Since f and g are recursive, it is clear from the construction that $\hat{\pi}$ is too. Finally, since $\hat{\pi}$ respects f, g -chains, it is a recursive m-reduction of A to B . Therefore, $\hat{\pi}$ is a recursive isomorphism between A and B as required. \square

Proof of Theorem 2 Let C be a recursively m-complete r.e. set. Let $K_0 = \{\langle i, x \rangle : x \in W_i\}$. Clearly, K_0 is r.e. and, for each i , the function $\lambda x.\langle i, x \rangle$ 1-reduces W_i to K_0 . As C is a recursively m-complete r.e. set, there is a recursive m-reduction of K_0 to C . Therefore, it follows that there is a recursive function f such that, for each i , $\varphi_{f(i)}$ recursively m-reduces W_i to C , that is,

$$(\forall i, x)[x \in W_i \iff \varphi_{f(i)}(x) \in C]. \quad (5)$$

Fix an arbitrary i . We use the recursion theorem to construct a special W -program e for the set W_i such that $\varphi_{f(e)}$ recursively 1-reduces W_i to C . Intuitively, e takes (unfair) advantage of (5) to force $\varphi_{f(e)}$ to be 1-1.

By the recursion theorem for φ , there exists an φ -program e such that, for all x ,

$$\varphi_e(x) = \begin{cases} \text{undefined,} & \text{if (a) } (\exists w < x)[\varphi_{f(e)}(w) = \varphi_{f(e)}(x)]; \\ 0, & \text{if not (a) and} \\ & \text{[(b) } \varphi_i(x) \text{ is defined or} \\ & \text{(c) } (\exists y > x)[\varphi_{f(e)}(y) = \varphi_{f(e)}(x)]]; \\ \text{undefined,} & \text{otherwise.} \end{cases} \quad (6)$$

Suppose by way of contradiction that $\varphi_{f(e)}$ is not 1-1. Let x_0 be the *least* number such that, for some $y > x_0$, $\varphi_{f(e)}(y) = \varphi_{f(e)}(x_0)$ and let y_0 be the least such y .

When $x = x_0$, clause (a) fails and clause (c) holds in (6). Hence, $x_0 \in W_e$. (Recall that $W_e = \text{domain}(\varphi_e)$.)

When $x = y_0$, clause (a) holds in (6). Hence, $y_0 \notin W_e$.

However, since $\varphi_{f(e)}(x_0) = \varphi_{f(e)}(y_0)$, by (5) we have $x_0 \in W_e \iff y_0 \in W_e$. But this is a contradiction. Therefore, $\varphi_{f(e)}$ is 1-1.

Now, since $\varphi_{f(e)}$ is 1-1, it follows that, for each x , clauses (a) and (c) in (6) fail to hold. Therefore, $W_e = W_i$. Hence, $\varphi_{f(e)}$ recursively 1-reduces W_i to C .

Therefore, since i was chosen arbitrarily, C is recursively 1-complete for the class of r.e. sets. \square

The following corollary formally states what was shown about f in the above proof. The corollary will be useful in the proof of Theorem 16 below.

Corollary 6 *Suppose C is a recursively m -complete r.e. set and that f is a recursive function such that, for all i , $\varphi_{f(i)}$ recursively m -reduces W_i to C . Then, for each r.e. set A , there is a W -program e for A such that $\varphi_{f(e)}$ recursively 1-reduces A to C .*

LESSONS FROM THE RECURSION THEORETIC RESULTS

In the complexity theoretic work that follows we cannot, in general, make direct use of the above recursion theoretic results and proof techniques. (For a nice exception, see the proof of Theorem 16.) However, these recursion theoretic results and proofs embody many nice ideas. We briefly consider what sorts of these ideas might be useful for the complexity theory below.

The most obvious things these results have to offer are the ideas behind their proof techniques. These techniques are elegantly simple, and one would expect variants of them to work in complexity theoretic settings. This is the case; ideas from the proofs of this section will play key roles in what follows. But, it is also the case that the complexity theoretic results obtained through these ideas are generally weaker than the results of this section. This is not unexpected. Complexity theory is a much more constrained subject than recursion theory. It is typical in passing from a theory to a more constrained version of it that new distinctions arise, and, in the context of these new distinctions, the analogs of many key results and techniques of the original theory fail or are much more limited in scope. For example, one-way functions have no recursion theoretic analogs and the possible existence of these functions greatly complicates the complexity theoretic situation. For another example, it turns out that the polynomial-time analog of Theorem 1 is true *if and only if* (as seems unlikely) $P = PSPACE$ —see Theorem 10 below.

Another use of the results of this section is as a basis for questions. As discussed above, one expects the theory of polynomial-time reductions and complete m -degrees to have many more distinctions than the analogous recursion theory. One way to find these distinctions is to consider complexity theoretic variants of these recursion theoretic results. For example, given a complexity class \mathcal{C} , e.g., NP, one might ask the following questions based on Theorem 2.

- Are all the m -complete sets for \mathcal{C} 1-equivalent?
- Are all the 1-complete sets for \mathcal{C} 1-li-equivalent?
- Are all the 1-li-complete sets for \mathcal{C} 1-li, p -invertible equivalent?
- Are all the 1-li, p -invertible-complete sets for \mathcal{C} p -isomorphic?

These sorts of questions have turned out to be productive—at least in our opinion. We have organized this paper around the general principle of considering complexity theoretic versions of the results of this section to see what can be shown true, what can be shown false, and what turns out to be mysterious.

1.4 Sufficient Conditions for P-Isomorphism

1.4.1 COMPLEXITY THEORETIC VERSIONS OF CANTOR-BERNSTEIN

Theorem 1 provides a sufficient (and necessary) condition for the recursive isomorphism of two sets. In this section we consider sufficient conditions for the polynomial-time isomorphism of two sets. Since the results of this section apply to *arbitrary* sets, the sufficient conditions will turn out to be rather strong. When, instead of arbitrary sets, the sets involved are cylinders or are complete for some complexity class, much weaker sufficient conditions can be obtained as discussed later.

Machtey, Winklmann, and Young [MWY78, Proposition 2.3] did a computational complexity analysis of Rogers’s variant of the construction for Theorem 1.²⁰ Not surprisingly, their analysis shows that the complexity properties of the unmodified Myhill and Rogers constructions are dreadful. However, Dowd [Dow82] was able to show the following linear-space analog to Theorem 1 through a construction very much in the same spirit as that in the proof of Theorem 1.

Theorem 7 ([Dow82]) *If A and B are recursively 1-equivalent as witnessed by linear length bounded, linear-space computable reductions, then, A and B are linear-space isomorphic.*

²⁰Rogers’s variant [Rog58] is a relocation of the Theorem 1 construction into the theory of programming systems.

In the theory of polynomial-time reducibilities the closest known analog to Theorem 1 is due to Berman and Hartmanis.

Theorem 8 ([BH77]) *If sets A and B are m -equivalent as witnessed by reductions that are (a) 1-1, (b) length increasing, and (c) p -invertible, then A and B are p -isomorphic.*

Proof Suppose $N, N', A, B, f,$ and g are as in the proof of Theorem 1. Further suppose that f and g satisfy hypotheses (a), (b), and (c). Recall our analysis of the possible structures of f, g -chains from the proof of Theorem 1. Since f and g are length increasing, we have that each f, g -chain is rooted. So, by the Cantor-Bernstein Theorem construction, π , as defined below, is an isomorphism between A and B .

$$\pi = \lambda x. \begin{cases} f(x), & \text{if } x\text{'s } f, g\text{-chain is } N \text{ rooted;} \\ g^{-1}(x), & \text{if } x\text{'s } f, g\text{-chain is } N' \text{ rooted.} \end{cases}$$

Since f and g are length increasing, for each $z \in (N \cup N')$, there are at most $|z|$ many vertices preceding z in its f, g -chain and all of these vertices are of length less than $|z|$. Thus, since f and g are p -invertible, it follows that, given z , one can find the root of z 's f, g -chain in polynomial-time. Hence, π is polynomial-time computable. \square

The length increasing and the p -invertibility hypotheses of Theorem 8 are clearly very strong and it is worth asking whether either of them can be weakened. Watanabe [Wat85] conjectured that, if one-way functions exist, then the p -invertibility hypothesis cannot be weakened. This was confirmed in the following striking result of Ko, Long, and Du.

Theorem 9 ([KLD87]) *$P = UP$ if and only if every 1-li-degree collapses.*

Proof The \implies direction follows from the observation that if one-way functions do not exist, then 1-li-reductions are p -invertible, and, hence, by Theorem 8, 1-li-equivalent sets are p -isomorphic. The \impliedby direction follows from a pretty and insightful construction, see Theorem 28 and its proof below. \square

One of the reasons that Theorem 9 is so striking is that it gives a complexity *characterization* of a degree structure property. Theorem 9 thus essentially settles the question of the general structure of 1-li-degrees. It is a natural question whether there are complexity characterizations of the general collapse of other sorts of degrees, e.g., 1-honest-degrees, 1-degrees, and m -degrees. There has been recent progress on this.

Theorem 10 ([FKR89]) *The following are equivalent:*

- (a) $P = PSPACE$.
- (b) *Every two 1-equivalent sets are p -isomorphic.*

(c) Every two p -invertible equivalent sets²¹ are p -isomorphic.

Proof Sketch By a proof similar to that for Theorem 7, one can show that if two sets are recursively 1-equivalent as witnessed by 1-1, polynomial-size bounded, Pspace-computable reductions, then the two sets are Pspace-isomorphic. It follows from this that if $P = PSPACE$, then every 1-degree collapses. Hence, (a) implies (b). Part (b) trivially implies (c). The proof that (c) implies (a) involves a construction that is partly based on [KLD87], see Theorems 29 and 30 below. \square

The equivalence of parts (b) and (c) is surprising and not yet well understood. Theorem 10 comes close to providing a condition under which the length increasing hypothesis of Berman and Hartmanis's Theorem 8 is necessary.²²

For m -degrees one can show, without any assumptions, the existence of noncollapsing m -degrees. See Theorem 31 below.

Hartmanis established a version of Theorem 8 in the context of Logspace reductions.

Theorem 11 ([Har78b]) *If two sets are m -equivalent as witnessed by Logspace reductions that are (a) 1-1, (b) length squaring, and (c) Logspace-invertible, then the two sets are Logspace-isomorphic.*

Using Corollary 22 below and a modified version of Theorem 9 one can show that Logspace one-way functions exist *if and only if* the Logspace-invertibility hypothesis of Theorem 11 is necessary.

1.4.2 CYLINDERS

The two main technical results of the 1977 Berman and Hartmanis paper are Theorem 8 above and [BH77, Theorem 7], a rough, polynomial-time analog of Theorem 4. In [MY85] Mahaney and Young improve this latter result to obtain the following exact analog of Theorem 4.

Theorem 12 ([BH77] [MY85]) *Two cylinders are m -equivalent if and only if they are p -isomorphic.*

Recall that a *conventional* NP-complete set is, informally, a set that results from a straightforward coding of an NP-complete problem that stems from work in combinatorics, optimization, etc. In their 1977 paper

²¹That is, sets that are 1-equivalent as witnessed by p -invertible reductions.

²²Note that Theorem 10 does not rule out the possibility that “length non-decreasing” can replace “length increasing” in the hypothesis of Theorem 8. We suspect that under a stronger condition than $P \neq PSPACE$, the length increasing hypothesis of Theorem 8 is indeed necessary.

Berman and Hartmanis prove that a number of well known conventional NP-complete sets are paddable, and, moreover, they observed that all of the then known conventional NP-complete sets can also be straightforwardly shown to be paddable. Thus, by Theorem 12 (or [BH77, Theorem 7]) one obtains Berman and Hartmanis's key observation that all of the know (circa 1977) conventional NP-complete sets are p-isomorphic. To date there still is no satisfactory example of a conventional NP-complete set that cannot be shown paddable.

Proof Sketch of Theorem 12 The \Leftarrow direction is obvious. We show the \Rightarrow direction. Suppose that A and B are m-equivalent cylinders that have associated padding functions $p_A(\cdot, \cdot)$ and $p_B(\cdot, \cdot)$, respectively. We argue that A is 1-li, p-invertible reducible to B . By symmetry, then, it is also that case that B is 1-li, p-invertible reducible to A , and, therefore, by Theorem 8, that A and B are p-isomorphic.

Since $p_B(\cdot, \cdot)$ is p-invertible, it follows that $p_B(\cdot, \cdot)$ is polynomial honest in the sense that there is a $k > 0$ such that, for all x and y , $|p_B(x, y)| > (|x| + |y|)^{1/k} - k$. Define

$$p'_B = \lambda x, y \bullet p_B(x, y \mathbf{01}^{(|x|+|y|+k)^k}),$$

where $y \mathbf{01}^{(|x|+|y|+k)^k}$ denotes the string consisting of y (as a string over $\{\mathbf{0}, \mathbf{1}\}$), followed by the symbol $\mathbf{0}$, followed by $(|x| + |y| + k)^k$ many occurrences of the symbol $\mathbf{1}$. It is straightforward to argue that $p'_B(\cdot, \cdot)$ is a padding function for B , and that p'_B is length increasing in the sense that, for all x and y , $|p'_B(x, y)| > |x| + |y|$. Define $f' = \lambda x \bullet p'_B(f(x), x)$. Since f is an m-reduction of A to B and since p'_B is a padding function for B , it follows that f' is an m-reduction of A to B . Since p'_B is 1-1, length increasing, and p-invertible, it follows from our definition of f' that it has these properties too. \square

Cylinders are of independent interest beyond Berman and Hartmanis's observation that the "natural" NP-complete sets are paddable. The following proposition shows that the m-complete sets that have essentially the strongest reducibility properties turn out to be cylinders.

Proposition 13 *Suppose \mathcal{C} is a complexity class that: (i) contains N , (ii) is closed downward under m-reductions, and (iii) has a complete m-degree. Then, (a) and (b) hold.*

- (a) *There is a cylinder that is 1-li, p-invertible complete for \mathcal{C} .*
- (b) *All of the 1-li, p-invertible complete sets for \mathcal{C} are cylinders.*

Before we prove Proposition 13 we note (without proof) an easy corollary of Theorem 12.

Corollary 14 *For each cylinder B , a set A is m-reducible to B if and only if A is 1-li, p-invertible reducible to B .*

Proof Sketch of Proposition 13 Suppose C is an m -complete set for \mathcal{C} . Let $C' = \{ \langle c, z \rangle : c \in C \ \& \ z \in N \}$. It is straightforward to show that C' is a cylinder and an m -complete set for \mathcal{C} . By Corollary 14 we have that C' is a 1-li, p -invertible complete set for \mathcal{C} . Therefore, part (a) follows. Part (b) follows from part (a), Corollary 14, Theorem 8, and the easily verified fact that p -isomorphisms map cylinders to cylinders. \square

Every m -degree contains a cylinder, but there are 1-degrees that do not (see Theorem 31 below.) We say a 1-degree is *cylindrical* if and only if the 1-degree contains a cylinder. By Proposition 13(a) all complete 1-degrees of complexity classes are cylindrical. Now, Theorem 10 gives $P = PSPACE$ as a sufficient condition for every 1-degree to collapse. The next proposition gives an ostensibly weaker sufficient condition for the collapse of every cylindrical 1-degree.

Proposition 15 *If A is a cylinder and B is a set 1-equivalent to A , then A and B are $Ptime^{NP}$ -isomorphic.*

Thus, $P = NP$ implies that cylindrical 1-degrees collapse.

The proof of this proposition is an implicit part of the proof of [MWY78, Theorem 2.6]. We do not know whether the collapse of every cylindrical 1-degree implies $P = NP$. We know of presumably weaker hypotheses than $P = NP$ that imply that cylindrical 1-degrees collapse to 1-li-degrees, but it is open whether there is a complexity characterization of this sort of collapse.

We note in passing that the obvious Logspace analogs of Theorem 12 and Proposition 15 hold.

1.5 Complete Degrees

We now directly address the problem of the structure of complete degrees. Work on this topic has produced some strong positive results. Among these are that

- the complete m -degrees of both RE and NEXP collapse to 1-degrees (Theorems 16 and 18 below);
- the complete m -degree of EXP collapses to a 1-li-degree (Theorem 17 below);
- there is a structural characterization of the collapse/noncollapse of the complete m -degree of EXP (Theorem 26 below); and
- the existence of sufficiently strong one-way functions (i.e., scrambling functions) implies the noncollapse of the complete m -degrees of NP, PSPACE, EXP, NEXP, and RE (Theorem 25 below).

However, there are also results which carry the cautionary message that any resolution of the collapse/noncollapse question of the complete m-degree of NP, or PSPACE, or EXP, or . . . will also resolve some major complexity class problem. For example consider the complete m-degree of RE. The non-collapse of this degree implies $P \neq NP$ (Proposition 15) and the collapse of this degree implies the nonexistence of scrambling functions (Theorem 25). In the face of these “negative” results, it is not a realistic research goal to try to push toward an out right resolution of these complete set problems. A more reasonable goal is to instead try to work toward establishing complexity characterizations of the collapse/noncollapse of particular complete degrees. Such characterizations are potentially very informative. Theorem 26 below (due to Ganesan and Homer) is a first step in this direction.

1.5.1 PROOFS OF PARTIAL COLLAPSE

Below we sketch proofs that the complete m-degrees of RE and NEXP collapse to 1-degrees and that the complete m-degree of EXP collapses to a 1-li-degree. These are pithy proofs which seem to get at the heart of the matters. Following these proofs we also explain why the nice ideas behind these proofs seem to fail in the context of NP and PSPACE.

Our development of Theorems 16, 17, and 18 below parallels Ganesan and Homer’s [GH89] (in which Theorem 18 is introduced) and we refer the reader to that paper for a good alternative treatment of these theorems. Our proofs and Ganesan and Homer’s share many key elements, but differ in points of view.

We begin by considering the complete m-degree of RE.

Theorem 16 ([Dow78]) *The complete m-degree of RE consists of a 1-degree.*

This theorem first appeared in Dowd’s [Dow78]. A cleaner proof of this theorem appears in [GH89]. Our proof is simple, direct application of Corollary 6. The Dowd proof, the Ganesan and Homer proof, and the proof below all use essentially the same diagonalization trick.

Proof Let C be a polynomial-time m-complete r.e. set. By a straightforward argument, there is a recursive function f such that, for each i , $\varphi_{f(i)}$ is polynomial-time computable and $\varphi_{f(i)}$ m-reduces W_i to C . Fix an arbitrary r.e. set A . By Corollary 6 there is a W -program e for A such that $\varphi_{f(e)}$ recursively 1-reduces A to C . But, by assumption, $\varphi_{f(e)}$ is polynomial-time computable. Hence, A is (polynomial-time) 1-reducible to C . Since A was chosen arbitrarily, C is (polynomial-time) 1-complete. \square

We next consider the complete m-degree of EXP.

Theorem 17 ([Ber77]) *The complete m-degree of EXP consists of a 1-li-degree.*

This result first appeared in Berman’s 1977 Ph.D. dissertation. Watanabe published a very clean, clear proof of this result in [Wat85]. (Also see [GH89, Theorem 1].) In [Wat85] Watanabe also shows that the complete m-degree of each of the classes

- $\text{DTIME}(2^{\mathcal{O}(n^{1/k})})$, where $k > 0$, and
- $\text{DSPACE}(s(n))$, where s is space constructible and super-polynomial,

consists of a 1-li-degree.

All of the known proofs of Theorem 17 use essentially the same diagonalization techniques. In our proof below, to diagonalize against m-reductions that are not 1-1, we use a version of the diagonalization trick employed in the proofs of Theorems 2 and 16 above. (See clause (a) in (7) below.) To diagonalize against reductions that are not length increasing we do the following. Suppose that f is a potential m-reduction of E_{e_0} , the set we are constructing, to C , a predetermined complete set. Also suppose that $|f(x_0)| \leq |x_0|$ for some x_0 . Then, to diagonalize against f at x_0 , we put x_0 into E_{e_0} if and only if $f(x_0)$ is *not* in C . (See clause (b) in (7) below.) There are two key points here. First, the diagonalization depends on the fact that one can *decide* the question “ $y \in C?$ ” in time exponential in $|y|$. Thus, this sort of diagonalization does not work for classes like RE and NEXP which are either not closed or not known to be closed under complements. The second key point is that since $|f(x_0)| \leq |x_0|$, one can decide the question “ $f(x_0) \in C?$ ” within a uniform $2^{\text{poly}(|x_0|)}$ time bound *independent of the reduction f* . Since the construction has to be able to diagonalize against all possible m-reductions f that fail to be length increasing, this point is critical to making the construction work in exponential time.

Proof Sketch In the following, for each $A \in \text{EXP}$, $A(\cdot)$ will denote the (exponential time computable) characteristic function of A . Let C be an m-complete set for EXP. For all i , let $E_i = \psi_i^{-1}(C)$. By our discussion in §1.2, $\langle E_i \rangle_{i \in \mathbb{N}}$ is a programming system for EXP for which the recursion theorem holds. Fix an arbitrary set $A \in \text{EXP}$. Define, for all e and x ,

$$D(\langle e, x \rangle) = \begin{cases} 1 - D(\langle e, w_0 \rangle), & \text{if (a) for some } w < x, \psi_e(w) = \\ & \psi_e(x) \text{ and } w_0 \text{ is the least} \\ & \text{such } w; \\ 1 - C(\psi_e(x)), & \text{if (b) } |\psi_e(x)| \leq |x| \text{ and not (a);} \\ A(x), & \text{otherwise.} \end{cases}$$

A straightforward argument shows that D is in EXP. (Recall that the function $\lambda i, x. \psi_i(x)$ is computable in exponential time.) Hence, by the

recursion theorem for $\langle E_i \rangle_{i \in \mathbb{N}}$ there is an E -program e_0 such that $E_{e_0}(\cdot) = \lambda x. D(\langle e_0, x \rangle)$. Thus, for all x ,

$$E_{e_0}(x) = \begin{cases} 1 - E_{e_0}(w_0), & \text{if (a) for some } w < x, \psi_{e_0}(w) = \\ & \psi_{e_0}(x) \text{ and } w_0 \text{ is the least} \\ & \text{such } w; \\ 1 - C(\psi_{e_0}(x)), & \text{if (b) } |\psi_{e_0}(x)| \leq |x| \text{ and not (a);} \\ A(x), & \text{otherwise.} \end{cases} \quad (7)$$

Suppose by way of contradiction that ψ_{e_0} is not 1-1. Let x_0 be the least number such that, for some $w < x_0$, $\psi_{e_0}(w) = \psi_{e_0}(x_0)$. Then, by the case of clause (a) in (7), $w \in E_{e_0} \iff x_0 \notin E_{e_0}$. But, since ψ_{e_0} is an m-reduction of E_{e_0} to C and since $\psi_{e_0}(w) = \psi_{e_0}(x_0)$, we have that $w \in E_{e_0} \iff x_0 \in E_{e_0}$, a contradiction. Therefore, ψ_{e_0} is 1-1.

Suppose by way of contradiction that ψ_{e_0} is not length increasing. Let x_0 be the least number such that $|\psi_{e_0}(x_0)| \leq |x_0|$. Then, by the case of clause (b) in (7), $x_0 \in E_{e_0} \iff \psi_{e_0}(x_0) \notin C$. But, since ψ_{e_0} is an m-reduction of E_{e_0} to C , this is a contradiction. Therefore, ψ_{e_0} is length increasing.

By our definition of the E_i 's, ψ_{e_0} is an m-reduction of E_{e_0} to C . Hence, E_{e_0} is 1-li-reducible to C .

Since ψ_{e_0} is 1-1 and length increasing, for every x , clauses (a) and (b) fail to hold in (7). Hence, $E_{e_0} = A$, and, therefore, A is 1-li-reducible to C .

Since A was an arbitrary member of EXP, we thus have that C is 1-li-complete for EXP. \square

By a clever combination of the ideas behind the proofs of Theorems 16 and 17, Ganesan and Homer established

Theorem 18 ([GH89]) *The complete m-degree of NEXP consists of a 1-degree. In fact, every two m-complete sets for NEXP are 1-equivalent as witnessed by exponentially honest reductions.*

They also show the analogous result for the classes $\text{NTIME}(2^{\mathcal{O}(n^{1/k})})$, where $k > 0$.

Proof Sketch of Theorem 18 To keep to the argument simple, we shall not worry about exponential honesty and show only that the m-complete sets of NEXP are 1-complete.

In the following, for each set A , $A(\cdot)$ will denote the partial function that is 1 on each element of A and undefined otherwise.

Let C be an NEXP-complete set. For all i , let $E_i = \psi_i^{-1}(C)$. By our discussion in §1.2, $\langle E_i \rangle_{i \in \mathbb{N}}$ is a programming system for NEXP for which the recursion theorem holds.

Fix an $A \in \text{NEXP}$. Since NEXP is contained in deterministic double exponential time, it is straightforward to argue that there is a polynomial

p such that, for all x and all w such that $2^{p(|w|)} < |x|$, one can deterministically evaluate $\overline{A}(w)$ within a uniform $\mathcal{O}(2^{|x|})$ time bound.

By the recursion theorem for $\langle E_i \rangle_{i \in \mathbb{N}}$ there is an E -program e_0 such that, for all x ,

$$E_{e_0}(x) = \begin{cases} \overline{A}(w), & \text{if (a) } (\exists w < x)[2^{p(|w|)} < |x| \ \& \\ & \psi_{e_0}(w) = \psi_{e_0}(x)]; \\ \text{undefined,} & \text{if not (a) and} \\ & \text{(b) } (\exists w < x)[|x| \leq 2^{p(|w|)} \ \& \\ & \psi_{e_0}(w) = \psi_{e_0}(x)]; \\ 1, & \text{if not (a) and not (b) and} \\ & [(c) \ x \in A \ \text{or} \\ & (d) \ (\exists y > x)[|y| \leq 2^{p(|x|)} \ \& \\ & \psi_{e_0}(x) = \psi_{e_0}(y)]]; \\ \text{undefined,} & \text{(e) otherwise.} \end{cases} \quad (8)$$

We note that the right hand side of (8), as a function of $\langle e_0, x \rangle$, corresponds to an NEXP set since:

- clause (a) is an EXP test and, by our assumption on p , one can deterministically compute $\overline{A}(w)$ within a uniform $\mathcal{O}(2^{|x|})$ time bound;
- clause (b) is also an EXP test; and
- clauses (c) and (d) are NEXP tests.

So, we can indeed apply the recursion theorem for $\langle E_i \rangle_{i \in \mathbb{N}}$ to the set corresponding to this function of $\langle e_0, x \rangle$.

The case of clause (a) in (8) guarantees that there are no x and x' with $x' < x$ such that $2^{p(|x'|)} < |x|$ and $\psi_{e_0}(x') = \psi_{e_0}(x)$. The cases of clauses (b) and (d) in (8) guarantee that there are no x and x' with $x' < x$ such that $|x| \leq 2^{p(|x'|)}$ and $\psi_{e_0}(x) = \psi_{e_0}(x')$. (We leave these two arguments to the reader.) Therefore, we have that ψ_{e_0} is a 1-reduction of E_{e_0} to C . Now, since ψ_{e_0} is 1-1, clauses (a), (b), and (d) fail to hold for each and every x . Hence, it follows by the cases of clauses (c) and (e) that $E_{e_0} = A$. Therefore, ψ_{e_0} is a 1-reduction of A to C . Since A was chosen arbitrarily, the theorem follows. \square

In contrast to the situation for RE, NEXP, and EXP, there are essentially no details known about the structure of the complete m-degrees of either NP or PSPACE. The proof techniques used for Theorems 16, 17, and 18 do not seem applicable in the context of either NP or PSPACE and there are no presently known alternatives to these techniques. The reason for the apparent failure of these techniques is this. The constructions for Theorems 17 and 18 each makes strong use of the fact that $\lambda i, x. \psi_i(x)$ is

computable in time exponential in $|i| + |x|$. There is no known polynomial-space computable universal function for Ptime and the existence of such a function seems doubtful. (Kozen [Koz80] presents some evidence against the existence of such functions.) However, for the sake of comparison with the previous theorems of this section we note

Proposition 19 *Suppose ψ' is a universal function for Ptime such that the two sets*

$$\{ \langle i, j, x \rangle : \psi'_i(x) = \psi'_j(x) \} \quad \{ \langle i, w, x \rangle : |w| \leq |x| \ \& \ w = \psi'_i(x) \}$$

are both in PSPACE. Then, the complete m -degree of PSPACE consists of a 1-li-degree.

An analogous result holds for NP when one makes the additional assumption that $\text{NP} = \text{coNP}$.

The proof of Proposition 19 is a modification of that for Theorem 17— with a proviso: ψ' may be *so* unnatural that the recursion theorem may fail for it. To obtain the proposition in this case, one is reduced to modifying one of the proofs of Theorem 17 that avoids use of the recursion theorem, see [Wat85] and [GH89] for examples.

Although there may be no polynomial space computable universal functions for Ptime, there is indeed a universal function for Logspace, θ , such that that the two sets

$$\{ \langle i, j, x \rangle : \theta_i(x) = \theta_j(x) \} \quad \{ \langle i, w, x \rangle : |w| \leq |x| \ \& \ w = \theta_i(x) \}$$

are both in PSPACE. The proof Proposition 19 can thus be modified to obtain the following nice analog of Theorem 17 for PSPACE.

Theorem 20 ([Rus86]) *Relative to Logspace reductions, the complete m -degree of PSPACE consists of a 1-li-degree.*

The above theorem can be improved a bit by observing that for θ as above, given any fixed polynomial p , the set

$$\{ \langle i, w, x \rangle : |w| \leq p(|x|) \ \& \ w = \theta_i(x) \}$$

is also in PSPACE. So, by a slight modification of the proof of Proposition 19, one obtains

Theorem 21 *Relative to Logspace reductions, the complete m -degree of PSPACE consists of a 1-length-squaring-degree.*

Theorems 11 and 21 together yield

Corollary 22 *Relative to Logspace reductions, if one-way functions do not exist, then the complete m -degree of PSPACE collapses.*

Allender showed the following related result by techniques similar to the ones discussed above.

Theorem 23 ([All88]) *All the members of the 1-L complete²³ degree for PSPACE are p-isomorphic.*

1.5.2 CONSEQUENCES OF COLLAPSE/NONCOLLAPSE

None of the results of the previous subsection completely settles the question of the structure of any complete m-degree. For instance, in the case of RE, it is known that its complete m-degree collapses to a 1-degree, but the extent to which this degree collapses further (if at all) is open. These questions are likely to be hard—an answer to any of them would have some profound complexity theoretic implications. The next proposition summarizes some of these.

Proposition 24 (a) *The noncollapse of the complete m-degree of EXP implies $P \neq UP$.*

(b) *The noncollapse of the complete m-degree of RE implies $P \neq NP$.*

(c) *The noncollapse of the complete m-degree of NEXP implies $P \neq NP$.*

(d) *The noncollapse of the complete m-degree of PSPACE implies $LOGSPACE \neq NP$.*

(e) *The collapse of the complete m-degree of NP implies $P \neq NP$.*

Proof Sketch Part (a) follows by Theorems 9 and Theorem 17. Using Propositions 15 and 13(a), part (b) follows from Theorem 16 and part (c) by Theorem 18. Part (d) follows by Proposition 15 and Theorem 20. Part (e) follows from the observation that if $P = NP$, then the set $\{1\}$ is NP-complete, but clearly not p-isomorphic to SAT. \square

Until recently, Proposition 24(e) was the only known result that provided a “complexity theoretic” consequence of the *collapse* of a m-complete degree. The next theorem (obtained in 1988) implies that if any of the standard complete m-degrees collapse, then there is a limit on the power of one-way functions. Recall that a scrambling function is a one-way function such that, for all nonempty A , $f(A)$ is nonpaddable.

Theorem 25 ([KMR89]) *If scrambling functions exist, then the complete 1-li-degrees of each of NP, PSPACE, EXP, NEXP, and RE all fail to collapse.*

Thus, if any of the 1-li-complete degrees of NP, PSPACE, EXP, NEXP, and RE collapse, then scrambling functions do not exist.

²³A 1-L reduction [HIM81] is roughly an m-reduction that is computable by a logspace bounded Turing machine that has a one-way input head.

Disproving the existence of scrambling functions is likely to be hard because these functions exist relative to random oracles, see Theorem 37 below. Thus, proving that any of the complete m-degrees of NP, PSPACE, EXP, NEXP, and RE collapse is also probably very hard.

Proof Sketch of Theorem 25 *Terminology.* A complexity class \mathcal{C} is *image complete* if and only if, for each f , a 1-1, length increasing, polynomial-time computable function, and each A , an m-complete set for \mathcal{C} , $f(A)$ is also an m-complete set for \mathcal{C} . It is straightforward to argue that each of NP, PSPACE, EXP, NEXP, and RE is image complete.

Ko, Long, and Du [KLD87] show that if one-way functions exist, then so do length increasing one-way functions. The same argument applies to scrambling functions. So, suppose f is a scrambling function which we assume is length increasing. Suppose also that \mathcal{C} is an image complete complexity class and that C_0 is a paddable, 1-li-complete set for \mathcal{C} . (By Proposition 13(a) such a C_0 must exist.) Consider $f(C_0)$. Since \mathcal{C} is image-complete, $f(C_0)$ is m-complete for \mathcal{C} . Since C_0 is 1-li-complete for \mathcal{C} and since f is 1-1 and length increasing, we have that $f(C_0)$ is 1-li-complete for \mathcal{C} . As f is a scrambling function, $f(C_0)$ is not paddable. Therefore, since p-isomorphisms preserve paddability, it follows that C_0 and $f(C_0)$ are two 1-li-complete sets that are not p-isomorphic. \square

It is natural to ask whether there are complexity theoretic characterizations of the collapse/noncollapse of any complete m-degrees. Watanabe [Wat85] conjectured the converse of Proposition 24(a). Machtey, Winklmann, and Young [MWY78, p. 51] in effect conjectured the converse of Proposition 24(b). (Their actual conjecture was an analogous statement for acceptable programming systems for the class of partial recursive functions.) Theorem 25 is a very partial confirmation of these two conjectures. The only characterization of the collapse/noncollapse of a complete m-degree is the following result due to Ganesan and Homer.

Theorem 26 ([Gan89]) *The complete m-degree of EXP is noncollapsing if and only if there exist C , an m-complete set for EXP, and a one-way function f for which there is no p-invertible function g such that $g(C) \subseteq f(C)$ and $g(\overline{C}) \subseteq f(\overline{C})$.*

Theorem 26 is not a “complexity theoretic” characterization of the collapse of EXP’s complete m-degree in the sense that the converse of Proposition 24(a) would be. The theorem is more of an analysis which shows, if this complete degree fails to collapse, how the failure must occur. (Watanabe [Wat88] has results related to this.)

Proof Sketch of Theorem 26 If for each C , an m-complete set for EXP, and each 1-1, length increasing f there is a p-invertible g such that $g(C) \subseteq f(C)$ and $g(\overline{C}) \subseteq f(\overline{C})$, then, by a straightforward application of

Theorems 8 and 17, we have that the complete degree of EXP collapses. Thus, the \implies direction follows.

To show the \impliedby direction, first suppose that C and f are as in the hypothesis. If C is not paddable, we are done. So, suppose that C is paddable. By a diagonalization argument one can construct A , an m-complete set for EXP such that (i) $f(C) \subseteq A$, (ii) $f(\overline{C}) \subseteq \overline{A}$, and (iii) for any f' that 1-li-reduces C to A , it is the case that both $f'(C) - A$ and $f'(\overline{C}) - \overline{A}$ are finite. (We leave the details of the construction to the reader.) Suppose by way of contradiction that there is a p-invertible reduction from C to A . Using C 's paddability, it follows that there must exist g , a length increasing, p-invertible reduction of C to A . Hence, $g(C) - f(C)$ and $g(\overline{C}) - f(\overline{C})$ are finite. Using C 's paddability again, it follows that there is a length increasing, p-invertible g' such that $g'(C) \subseteq f(C)$ and $g'(\overline{C}) \subseteq f(\overline{C})$, a contradiction. \square

1.6 Degree Structure

One of many things left open by the work of the previous section is the general question of which of the many potential structures of degrees actually occur. For example, are there *any* m-degrees that collapse—much less complete ones? There are two main motivations for construction of concrete examples of degrees with a particular structural property: (i) to see what sort of hypotheses (if any) are required for such degrees to exist, and (ii) to possibly obtain hints on how to show that some complete degree has the property in question. Taking the example of collapsing degrees again, at first blush it is conceivable that the existence of collapsing degrees might require a hypothesis like $P = NP$ or $P = UP$. If this were the case, then the collapse of any m-degree would be highly suspect. Well, this is not the case as shown by

Theorem 27 ([KMR88]) *Collapsing degrees exist. Moreover, there is a collapsing degree that is 2-tt-complete²⁴ in EXP.*

The proof of this theorem is a finite injury priority argument which is too involved to sketch here, see [KMR88] for the details. One of our (thoroughly naïve) motivations for working on collapsing degrees was to make progress

²⁴A set A is *2-truth-table (2-tt) reducible to B* if and only if there exists polynomial-time computable f such that (i) for each x , $f(x)$ codes both a binary boolean function α and a pair of numbers (x_1, x_2) , and (ii) for all x , $x \in A$ if and only if $\alpha([x_1 \in B?], [x_2 \in B?])$. **N.B.** The relation of 2-tt-reducibility is *not* transitive. Hence, it is an abuse of terminology to call “2-tt-reducibility” a reducibility. Furthermore, while the notion of 2-tt-complete makes perfect sense, the notion of a 2-tt-degree does not!

toward a proof that the complete m-degree of EXP does collapse. However, in our constructions of collapsing degrees, 2-tt-complete for EXP is as close to m-complete for EXP as we have been able to manage. Another of our motivations for showing Theorem 27 was to provide a counterpart for the following beautiful result of Ko, Long, and Du.

Theorem 28 ([KLD87]) *Suppose one-way functions exist. Then, there is a noncollapsing 1-li-degree, i.e., there are 1-li-equivalent sets that are not p -isomorphic. Moreover, there are such sets that are also 2-tt-complete for EXP.*

As discussed in §1.4.1, the existence of one-way functions is a necessary condition for the existence of noncollapsing 1-li-degrees, and, Theorem 28 shows the condition is also sufficient. (See the discussion around Theorem 9 above.) One of Ko, Long, and Du's goals was to try to confirm Watanabe's conjecture that the complete m-degree of EXP collapses if and only if one-way functions exist. However, as with our Theorem 27, 2-tt-complete was as close they could get to m-complete. Pushing closer to m-complete than 2-tt-complete for either of Theorems 27 or 28 seems to be a very hard and will probably require radical, new techniques.

The proof of Theorem 28 builds on Berman and Hartmanis's proof of Theorem 8 and introduces some important new ideas.

Proof Sketch of Theorem 28 Suppose one-way functions exist. Then, by [KLD87] there exists t , a *length increasing* one-way function. We define $f: N \rightarrow N'$ by the following two equations.

$$f(2x) = 4t(x) + 1. \quad f(2x + 1) = 4x + 3.$$

Let g have the same definition as f except that we regard g as a function from N' to N . Clearly, f and g are 1-1 and length increasing.

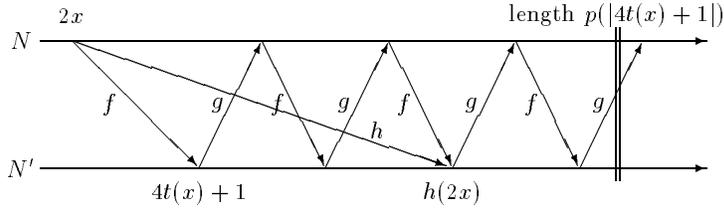
Terminology. A function $h: N \rightarrow N'$ *crosses an f, g -chain C* if and only if for some x , an N vertex of C , $h(x)$ is not an N' vertex of C .

Lemma *Suppose $h: N \rightarrow N'$ is p -invertible. Then, h crosses infinitely many f, g -chains.*

Proof of the Lemma Let p be a nondecreasing polynomial such that, for all x , $|h(x)| \leq p(|x|)$. For each y , let A_y be the set of N' vertices of the f, g -chain of $(4y + 1)'$ that are of length $\leq p(|4y + 1|)$. Since f and g are 1-1, length increasing, polynomial-time computable functions, there are fewer than $p(|4y + 1|)$ many elements of A_y , and, in fact, there is an obvious polynomial-time procedure that, given y , lists all the elements of A_y . By our definitions of f and g , we have that, for all x ,

$$h(2x) \text{ is in the same chain as } 2x \iff h(2x) \text{ is in } A_{t(x)}. \quad (9)$$

See Figure 1.3.


 FIGURE 1.3. $h(2x)$ lands in $A_{t(x)}$.

Now, suppose by way of contradiction that the lemma is false. Then, it follows from our definitions of f and g that, for all but finitely many x , $2x$ and $h(2x)$ are in the same chain. Let

$$y_0 = \max(\{t(x) : 2x \text{ and } h(2x) \text{ are in distinct chains}\}).$$

Then, by (9) and our choice of y_0 ,

$$(\forall y > y_0)[t^{-1}(y) \text{ is defined} \iff (\exists z' \in A_y)[h(2t^{-1}(y)) = z']]. \quad (10)$$

Observe that:

$$\begin{aligned} h(2t^{-1}(y)) = z' \\ \iff t^{-1}(y) = \frac{1}{2}h^{-1}(z') \end{aligned} \quad (11)$$

$$\iff t\left(\frac{1}{2}h^{-1}(z')\right) = y. \quad (12)$$

Since t and h^{-1} are polynomial-time computable, given y and z' , one can in polynomial (in $|y| + |z'|$) time check whether $h(2t^{-1}(y)) = z'$ using (12), and, if $h(2t^{-1}(y)) = z'$, compute $t^{-1}(y)$ using (11). Since one can list all the elements of A_y in polynomial (in $|y|$) time, it follows by (10) that, for each $y > y_0$, one can determine $t^{-1}(y)$ in polynomial in $|y|$ time. Therefore, t is p-invertible, a contradiction. \square **Lemma**

Using the lemma, we noneffectively construct 1-li-equivalent sets $A \subseteq N$ and $B \subseteq N'$ that are such that no p-invertible function m-reduces A to B . The construction is in stages $0, 1, \dots$. In each stage, the construction “paints” a finite number of f, g -chains blue or red. A chain painted blue has its N vertices in A and its N' vertices in B , and a chain painted red has its N vertices in \bar{A} and its N' vertices in \bar{B} . Since A and B will be constructed to respect f, g -chains, we shall have that f 1-li-reduces A to B and g 1-li-reduces B to A . The construction eventually paints all chains and never repaints a chain. Initially, all chains are unpainted.

Stage i . First, paint red each unpainted chain that has a vertex less than i . Next, if ψ_i is not p-invertible, go on to stage $i + 1$.

Otherwise, choose the least x such that C , the chain of x , is unpainted and $\psi_i(x)$ is in a chain C' distinct from C . (By the lemma and the fact that each stage paints only finitely many chains, such an x must exist.) If C' is painted, then paint C the opposite color. If C' is unpainted, paint C blue and C' red. (In either case, we now have $x \in A \iff \psi_i(x) \notin B$.)

Clearly, A and B are as required.

It is fairly straightforward to make the construction of A and B effective and with careful programming the construction can be made to produce A and B in EXP. Making A and B in addition 2-tt-complete for EXP is a simple, clever trick which we refer the reader to [KLD87] for the details. \square

By Theorem 17, if one-way functions exist, there are two possible structures of the complete m-degree for EXP: either the degree collapses or it contains sets that are 1-li-equivalent but not p-isomorphic. By Theorems 27 and 28, if one-way functions exist, both possible degree structures are realized within the sets 2-tt-complete for EXP.²⁵

By Theorems 16 and 18 the m-degrees of both RE and NEXP collapse to 1-degrees. However, at present it seems possible that these degrees may contain sets that are not even m-honest-equivalent. Fenner has shown that, if $P \neq PSPACE$, there are 1-degrees that have this structure.

Theorem 29 ([Fen89] [FKR89]) *Suppose $P \neq PSPACE$. Then there is a noncollapsing 1-degree. In fact, there exist 1-equivalent sets that fail to be m-honest-equivalent. Moreover, there are such sets that are also 2-tt-complete for EXP.*

The proof of this theorem is based in part on ideas from the Ko, Long, and Du construction and on Bennett's work on reversible Turing Machines [Ben89].

In related work, Fenner, Kurtz, and Royer show that, if $P \neq PSPACE$, then there are 1-degrees that have a very strange failure of collapse.

Theorem 30 ([FKR89]) *Suppose $P \neq PSPACE$. Then there is a noncollapsing p-invertible degree, i.e., there exist p-invertible-equivalent sets that fail to be p-isomorphic. Moreover, there are such sets that are also 2-tt-complete for EXP.*

At present essentially nothing is known about the complete m-degrees of NP and PSPACE. It is possible that these degrees contain sets that are

²⁵Theorem 28 shows the existence of a noncollapsing 1-li-degree provided one-way functions exist. We suspect that by combining the techniques of the proofs of Theorems 27 and 28 one can show that, if one-way functions exist, then there is an m-degree that collapses to a 1-li-degree, but not to a p-isomorphism type.

not 1-equivalent. M-degrees that contain sets that fail to be 1-equivalent do exist in “small” complexity classes as shown by

Theorem 31 ([KMR87a]) (a) *Suppose t is fully time constructible (see [HU79] for the definition) and $P \subset \text{DTIME}(t(n))$. Then, there exists a noncollapsing m -degree in $\text{DTIME}(t(n)) - P$.*

(b) *There exists a 2-tt-complete m -degree in EXP that contains infinitely many distinct 1-degrees.*

Proof Sketch Terminology. A set A is p -subset-immune if and only if A is infinite and it contains no infinite, polynomial-time decidable subsets. A is p -enumeration-immune if and only if A is infinite and for each 1-1, polynomial-time computable g , we have $\text{range}(g) \not\subseteq A$.

It is easy to show that if an m -degree contains a p -subset-immune set, then the m -degree is noncollapsing, and if the m -degree contains a p -enumeration-immune set, then the degree is made up of infinitely many different 1-degrees. It follows by a result of Geske, Huynh, and Seiferas [GHS89, Theorem 4] that, for each t as in the hypothesis of part (a), there is a p -subset-immune set in $\text{DTIME}(t(n)) - P$. Hence, part (a) follows. By a fairly straightforward diagonalization one can construct a p -enumeration-immune set that is 2-tt-complete for EXP. Hence, part (b) follows also. \square

The above results have been concerned with constructing degrees that exhibit a certain amount of collapsing. For each of the noncollapsing cases we have been content to simply build two sets that witness the form of non-collapse of interest, e.g., two non-1-li-equivalent sets in the case of Theorem 28. One can also consider the problem of describing the internal structure of noncollapsing degrees. Mahaney [Mah81] showed that every noncollapsing m -degree contains an $\omega + 1$ chain of sets ordered under 1-li-reductions none of which sets are p -isomorphic to any of the others. Mahaney and Young [MY85] later extended this result to

Theorem 32 ([MY85]) *In each noncollapsing m -degree, any countable partial ordering can be realized as a collection of pairwise non- p -isomorphic sets ordered under 1-li-reductions.*

1.7 Relativization Results

Thus far there has been little substantive said about degrees, complete or otherwise, in NP and PSPACE. This is because there is not much to report. Results about such degrees seem very hard to come by and seem to be beyond conventional techniques. Relativizations can be used to give a partial explanation of why this is the case.

The purpose of relativization results is to informally establish that a given property is independent of the standard diagonalization and simulation techniques of recursion and complexity theories, see [BGS75]. The idea is this. The aforementioned techniques seem to be indifferent to the presence of oracles in models of computation. That is, if with these techniques one can prove some property P of a standard model of computation, say Turing machines, then it seems to be the case that, one can also prove that P holds for Turing machines with an arbitrary oracle. Thus, if there is an oracle A for which *not* P holds relative to A , it seems unlikely that these standard techniques can provide a proof of P in the unrelativized setting. Baker, Gill and Solovay [BGS75] illustrate this with oracles A and B such that (i) relative to A we have $P = NP$ and (ii) relative to B we have $P \neq NP$. The interpretation of these two results is that the resolution of the P versus NP question is beyond the scope of the standard diagonalization and simulation techniques. However, since we have not precisely defined what these standard techniques are, relativization results are only an *informal* method of independence, and, thus, we cannot formally prove that all such methods will relativize. On the other hand, most proofs using these methods do indeed relativize.

Another use of relativization results is to establish the plausibility of certain hypotheses. One can interpret computability relative to a given oracle as a computational “possible world.” Arguing the plausibility of some fact based on an oracle result is usually a pretty tenuous proposition. However, when the oracle in a relativization result is drawn from certain special subclasses, arguing plausibility from an oracle result has somewhat better support. We discuss this issue for the classes of sparse and random oracles below.

For relativization results about the structure of m -degrees one needs be careful about which machines (i.e., those for language acceptors, m -reductions, and isomorphisms) have access to the oracle. Relativized settings in which both language acceptors and machines computing reductions have access to the oracle are called *full* relativizations and those settings in which just the language acceptors have access to the oracle are called *partial* relativizations [Rog67, §9.3]. Partial relativizations are of interest when studying the properties of *actual* m -reductions and p -isomorphisms. For “independence” results as discussed above, full relativizations seem to be the appropriate setting as machines accepting languages and computing reductions are treated alike. All the relativization results stated below are full relativizations.

The first relativization result pertaining to the isomorphism conjecture was due to Kurtz [Kur83] who constructed an oracle relative to which the isomorphism conjecture failed. Recently this result was improved to

Theorem 33 ([Kur88]) *Relative to a generic oracle,²⁶ the complete m -degree of NP is made up of multiple 1-degrees.*

Building on the ideas in [Kur83], Hartmanis and Hemachandra showed

Theorem 34 ([HH87]) *There is an oracle relative to which $P = UP$ and the complete m -degree of NP consists of multiple 1-degrees.*

This is a charming result in that it provides a relativized world in which both the isomorphism and the encrypted complete set conjectures fail. The constructions for both Theorem 33 and 34 make the isomorphism conjecture fail by building an oracle relative to which there is a “gappy” NP-complete set A . By this we mean that there are infinitely many n such that $\{x \in A : n \leq |x| \leq 2^n\}$ is empty. The existence (in the unrelativized world) of such a gappy NP-complete set runs counter to commonly held intuitions.

There is evidence that sparse oracles do not distort relationships among complexity classes. For example, it has been shown that the unrelativized polynomial-time hierarchy collapses if and only if there exists a sparse oracle relative to which the polynomial-time hierarchy collapses [LS86] [BBS86]. However, there is no evidence as to whether sparse oracle relativizations preserve fine details like the structure of the complete m -degree for NP. Be that as it may, the proofs of Theorems 17, 27, 28, and 31 can be modified to obtain

Theorem 35 ([KMR87b] [Lon88]) *There exists a sparse oracle relative to which the following holds:*

- *the complete m -degree for NP is a 1-li-degree;*
- *there is a collapsing degree that is 2- tt -complete for NP;*
- *there is a noncollapsing 1-li-degree that is 2- tt -complete for NP; and*
- *there is an m -degree that is 2- tt -complete for NP and that is made up of multiple 1-degrees.*

Goldsmith [Gol88] has related results obtained by somewhat different techniques.

If one dropped the sparsity condition on the oracle in the above theorem, then the result can be obtained trivially by choosing an oracle that makes $NP = EXP$, in which case Theorems 17, 27, 28, and 31 would apply at NP. However, it follows from [LS86, Theorem 3.2] that relative to a sparse oracle, $NP = EXP$ if and only if in the unrelativized case $NP = EXP$.

Until recently there was no known complexity class \mathcal{C} for which there were oracles A and B such that (i) relative to A the complete m -degree for \mathcal{C} collapsed and (ii) relative to B the complete m -degree for \mathcal{C} failed

²⁶See [Rog67] and [Joc80] for a discussion of generic sets.

to collapse. The breakthrough on this problem was made by Homer and Selman.

Theorem 36 ([HS89]) (a) *There exists an oracle relative to which the complete m -degree of Σ_2^P collapses.*

(b) *There exists an oracle relative to which the complete m -degree of Σ_2^P fails to collapse.*

The proof of part (b) is based on Kurtz's proof of an early version of Theorem 33. To show part (a), Homer and Selman cleverly construct an oracle A relative to which $\Sigma_2^P = \text{EXP}$ and $P = \text{UP}$, and thus, by Theorems 8 and 17, relative to A the complete m -degree of Σ_2^P collapses.

Shortly after Homer and Selman established Theorem 36, we showed

Theorem 37 ([KMR89]) *Relative to a random oracle²⁷ the complete 1-li-degrees of each of NP, PSPACE, EXP, NEXP, and RE all fail to collapse.*

To establish the theorem, we show that scrambling functions exist relative to random oracles and then apply Theorem 25 above. The proof that scrambling functions exist relative to random oracles involves an excursion into measure theory which we spare the reader in this survey. See [KMR89] for full details.

Putting together Proposition 24 and Theorems 36 and 37 we obtain

Corollary 38 (a) *There is an oracle relative to which the complete m -degrees of each of NP, PSPACE, EXP, NEXP, and RE all fail to collapse.*

(b) *For each of PSPACE, EXP, NEXP, and RE, there is an oracle relative to which the complete m -degree of the class collapses.*

Proof Sketch Part (a) follows directly from Theorem 37. The PSPACE portion of part (b) follows from Homer and Selman's proof of Theorem 36(a). The rest of part (b) follows from Proposition 24 and the existence of an oracle that makes $P = \text{NP}$. \square

An oracle that is notable for its absence in Corollary 38 is one that makes the original Berman and Hartmanis isomorphism conjecture true.

²⁷We say that a relativized statement T^X holds measure one if and only if the set $\{R : T^R\}$ has measure one. We say a set is *random* if and only if it satisfies all arithmetically definable properties of measure one. Thus, to show an arithmetically definable property holds relative to a random oracle, it suffices to show that the property holds measure one. Computability relative to a random oracle (very) roughly models computability under the hypothesis that strong, polynomial-time computable, pseudo-random functions exist. If one believes that such functions do exist, then random oracle results may be indicative of what is true about unrelativized computability.

Note that the notion of random set defined above is distinct from Chaitin's which is based on *algorithmic incompressibility*. There are Chaitin-random sets that are not random in the sense defined above.

The question of whether there is such an oracle is open and seems very difficult. When it was originally put forth, the isomorphism conjecture embodied some of the clearest insights into the structure of the NP-complete sets. It is ironic, then, that it seems so hard to obtain even a relativized confirmation of the conjecture.

Acknowledgements: Eric Allender made a number of very helpful suggestions on the first draft of this paper. Paul Young called us to task for an earlier inaccurate title. We would also like to thank Alan Selman for sharing with us his yet-unpublished research on the Joseph-Young conjecture.

Most of the work on this paper was done while the second author was at AT&T Bell Laboratories, Murray Hill and the third author was at the University of Chicago. The first author was supported in part by NSF Grant DCR-8602562. The third author was supported in part by NSF Grants DCR-8602991 and CCR-89011154.

1.8 REFERENCES

- [All88] E. Allender. Isomorphisms and 1-L reductions. *Journal of Computer and System Sciences*, 36:336–350, 1988.
- [BBS86] J. Balcázar, R. Book, and U. Schöning. The polynomial-time hierarchy and sparse oracles. *Journal of the ACM*, 33:603–617, 1986.
- [Ben89] C. Bennett. Time space tradeoffs for reversible computation. *SIAM Journal on Computing*, 1989. To appear.
- [Ber77] L. Berman. *Polynomial Reducibilities and Complete Sets*. PhD thesis, Cornell University, 1977.
- [Ber78] P. Berman. Relationship between density and deterministic complexity of NP-complete languages. In *Proceedings of the 5th International Colloquium on Automata, Languages, and Programming*, pages 63–71, Springer-Verlag, 1978. Lecture Notes in Computer Science No. 62.
- [BGS75] T. Baker, J. Gill, and R. Solovay. Relativizations of the $P = ?$ NP question. *SIAM Journal on Computing*, 4:431–442, 1975.
- [BH77] L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing*, 1:305–322, 1977.
- [Can55] G. Cantor. *Contributions to the Founding of the Theory of Transfinite Numbers*. Dover Publications, 1955.

- [Cut80] N. Cutland. *Computability: An Introduction to Recursive Function Theory*. Cambridge University Press, 1980.
- [Dow78] M. Dowd. On isomorphism. 1978. Unpublished manuscript.
- [Dow82] M. Dowd. *Isomorphism of Complete Sets*. Technical Report LCSR-TR-34, Laboratory for Computer Science Research, Busch Campus, Rutgers University, 1982.
- [DW83] M. Davis and E. Weyuker. *Computability, Complexity, and Languages*. Academic Press, 1983.
- [Fen89] S. Fenner. *A Complexity Theoretic Failure of the Cantor-Bernstein Theorem*. Technical Report 89-007, Department of Computer Science, University of Chicago, 1989.
- [FKR89] S. Fenner, S. Kurtz, and J. Royer. Every polynomial-time 1-degree collapses iff $P = PSPACE$. In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, pages 624–629, 1989.
- [For79] S. Fortune. A note on sparse complete sets. *SIAM Journal on Computing*, 431–433, 1979.
- [Gan89] K. Ganesan. *Complete Problems, Creative Sets and Isomorphism Conjectures*. PhD thesis, Boston University, 1989.
- [GH89] K. Ganesan and S. Homer. Complete problems and strong polynomial reducibilities. In *Proceedings of STACS '89*, pages 240–250, 1989. Lecture Notes in Computer Science No. 349.
- [GHS89] J. Geske, D. Huyhn, and J. Seiferas. A note on almost-everywhere-complex sets and separating deterministic-time-complexity classes. *Information and Computation*, 1989. To appear.
- [GJ79] M. Garey and D. Johnson. *Computers and Intractability*. W. H. Freeman and Company, 1979.
- [GJ86] J. Goldsmith and D. Joseph. Three results on the polynomial isomorphism of complete sets. In *Proceedings of the 27th Annual IEEE Symposium on Foundations of Computer Science*, pages 390–397, 1986.
- [Gol88] J. Goldsmith. *Polynomial Isomorphisms and Near-Testable Sets*. PhD thesis, University of Wisconsin at Madison, 1988. Available as: Technical Report Number 816, Computer Sciences Department, University of Wisconsin at Madison.

- [GS84] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. In *Proceedings of the 25th Annual IEEE Symposium on Foundations of Computer Science*, pages 495–503, 1984.
- [GS88] J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17:309–335, 1988.
- [Har78a] J. Hartmanis. *Feasible Computations and Provable Complexity Properties*. Society for Industrial and Applied Mathematics, 1978.
- [Har78b] J. Hartmanis. On log-tape isomorphisms of complete sets. *Theoretical Computer Science*, 273–286, 1978.
- [HH87] J. Hartmanis and L. Hemachandra. One-way functions, robustness, and the non-isomorphism of NP-complete sets. In *Proceedings of the 2nd Annual IEEE Structure in Complexity Theory Conference*, 1987.
- [HIM81] J. Hartmanis, N. Immerman, and S. Mahaney. One-way log-tape reductions. In *Proceedings of the 19th Annual IEEE Symposium on Foundations of Computer Science*, pages 65–72, 1981.
- [HS89] S. Homer and A. Selman. Oracles for structural properties. In *Proceedings of the 4th Annual IEEE Structure in Complexity Theory Conference*, pages 3–14, 1989.
- [HU79] J. Hopcroft and J. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, 1979.
- [Joc80] C. Jockusch, Jr. Degrees of generic sets. In F. R. Drake and S. S. Wainer, editors, *Recursion Theory: Its Generalizations and Applications*, pages 110–139, Cambridge University Press, 1980.
- [JY85] D. Joseph and P. Young. Some remarks on witness functions for polynomial reducibilities in NP. *Theoretical Computer Science*, 39:225–237, 1985.
- [KLD87] K. Ko, T. Long, and D. Du. A note on one-way functions and polynomial-time isomorphisms. *Theoretical Computer Science*, 47:263–276, 1987.
- [KMR87a] S. Kurtz, S. Mahaney, and J. Royer. *Noncollapsing Degrees*. Technical Report 87-001, Department of Computer Science, University of Chicago, 1987.

- [KMR87b] S. Kurtz, S. Mahaney, and J. Royer. Progress on collapsing degrees. In *Proceedings of the 2nd Annual IEEE Structure in Complexity Theory Conference*, pages 126–131, 1987.
- [KMR88] S. Kurtz, S. Mahaney, and J. Royer. Collapsing degrees. *Journal of Computer and System Sciences*, 37:247–268, 1988.
- [KMR89] S. Kurtz, S. Mahaney, and J. Royer. The isomorphism conjecture fails relative to a random oracle. In *Proceedings of the 21st annual ACM Symposium on Theory of Computing*, pages 157–166, 1989.
- [Ko85] K. Ko. On some natural complete operators. *Theoretical Computer Science*, 37:1–30, 1985.
- [Koz80] D. Kozen. Indexings of subrecursive classes. *Theoretical Computer Science*, 11:277–301, 1980.
- [Kur83] S. Kurtz. A relativized failure of the Berman-Hartmanis conjecture. 1983. Unpublished manuscript.
- [Kur88] S. Kurtz. *The Isomorphism Conjecture Fails Relative to a Generic Oracle*. Technical Report 88-018, Department of Computer Science, University of Chicago, 1988.
- [Lon88] T. Long. One-way functions, isomorphisms, and complete sets. *Abstracts of the AMS*, 9:125, 1988.
- [LS86] T. Long and A. Selman. Relativizing complexity classes with sparse oracles. *Journal of the ACM*, 33:618–627, 1986.
- [Mah81] S. Mahaney. On the number of p-isomorphism classes of NP-complete sets. In *Proceedings of the 22th Annual IEEE Symposium on Foundations of Computer Science*, pages 271–278, 1981.
- [Mah82] S. Mahaney. Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis. *Journal of Computer and System Sciences*, 25:130–143, 1982.
- [Mah89] S. Mahaney. The isomorphism conjecture and sparse sets. In J. Hartmanis, editor, *Computational Complexity Theory*, American Mathematical Society, 1989.
- [Moo82] G. Moore. *Zermelo's Axiom of Choice: Its Origins, Development, and Influence*. Springer-Verlag, 1982.
- [MS72] A. Meyer and L. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential time. In *Proceedings of the 13th Annual IEEE Symposium on Switching and Automata Theory*, pages 125–129, 1972.

- [MWY78] M. Machtey, K. Winklmann, and P. Young. Simple Gödel numberings. *SIAM Journal on Computing*, 7:39–60, 1978.
- [MY78] M. Machtey and P. Young. *An Introduction to the General Theory of Algorithms*. North-Holland, 1978.
- [MY85] S. Mahaney and P. Young. Reductions among polynomial isomorphism types. *Theoretical Computer Science*, 39:207–224, 1985.
- [Myh55] J. Myhill. Creative sets. *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik*, 1:97–108, 1955.
- [Myh59] J. Myhill. Recursive digraphs, splinters and cylinders. *Mathematische Annalen*, 138:211–218, 1959.
- [Pos44] E. Post. Recursively enumerable sets of positive integers and their decision problems. *Bulletin of the AMS*, 50:284–316, 1944.
- [RC87] J. Royer and J. Case. *Intensional Subrecursion and Complexity Theory*. Technical Report 87-007, Department of Computer Science, University of Chicago, 1987.
- [Rog58] H. Rogers. Gödel numberings of the partial recursive functions. *Journal of Symbolic Logic*, 23:331–341, 1958.
- [Rog67] H. Rogers. *Theory of Recursive Functions and Effective Computability*. McGraw-Hill, 1967. Reprinted. MIT Press. 1987.
- [Rus86] D. Russo. Optimal approximations of complete sets. In *Proceedings of the Structure in Complexity Theory Conference*, pages 311–324, Springer-Verlag, 1986.
- [Sch75] C. Schnorr. Optimal enumerations and optimal Gödel numberings. *Mathematical Systems Theory*, 8:182–191, 1975.
- [Wat85] O. Watanabe. On one-one polynomial time equivalence relations. *Theoretical Computer Science*, 38:157–165, 1985.
- [Wat88] O. Watanabe. A note on p-isomorphism conjecture. 1988. Unpublished manuscript.
- [You66] P. Young. Linear orderings under one-one reducibility. *Journal of Symbolic Logic*, 31:70–85, 1966.