The Isomorphism Conjecture Fails Relative to a Random Oracle (Extended Abstract)

Stuart A. Kurtz*
University of Chicago

Stephen R. Mahaney
A. T. & T. Bell Laboratories

James S. Royer†
University of Chicago

Abstract

Berman and Hartmanis [BH77] conjectured that there is a polynomial-time computable isomorphism between any two languages m-complete ("Karp" complete) for NP. Joseph and Young [JY85] discovered a structurally defined class of NP-complete sets and conjectured that certain of these sets (the K_f^k's) are not isomorphic to the standard NP-complete sets for some one-way functions f. These two conjectures cannot both be correct.

We introduce a new family of strong one-way functions, the *scrambling* functions. If f is a scrambling function, then K_f^k is not isomorphic to the standard NP-complete sets, as Joseph and Young conjectured, and the Berman-Hartmanis conjecture fails. As evidence for the existence of scrambling functions, we show that much more powerful one-way functions—the *annihilating* functions—exist relative to a random oracle.

1 Introduction

The relationship between the Berman-Hartmanis isomorphism conjecture and existence of one-way functions has been the subject of considerable research and conjecture in recent years, e.g., [JY85,KLD86, KMR88,HH87].

We prove that the isomorphism conjecture is incompatible with the existence of *scrambling functions*, a type of powerful one-way function. To provide plausibility to the hypothesis that scrambling functions exist, we show that they exist relative to a random[1] oracle. As a corollary, we obtain that the isomorphism conjecture fails with respect to a random oracle.

The remainder of Section 1 consists of three parts: a historical survey, a precise statement of our results, and some possible directions for future research. Section 2 considers the structural consequences of the existence of scrambling functions, and Section 3 establishes the existence of scrambling functions (and still more powerful one-way functions called *annihilating functions*) relative to a random oracle.

1.1 A Brief Survey

In this section, we will briefly survey the research that lead to this work. The reader may wish to consult Young's excellent survey [You88] of structural research on isomorphisms, as well as [KMR88] and [Mah86]. In the text, we assume that the reader is familiar with the terminology and notation of [KMR88]. For readers unfamiliar with this earlier paper, we define our terms in the footnotes.

1.1.1 The Structural Approach

Berman and Hartmanis [BH77] conjectured that all m-complete languages for NP are polynomial time isomorphic to one another.[2] As evidence for this

*The first author was supported in part by NSF Grant DCR–8602562

†The third author was supported in part by NSF Grant DCR–8602991

[1] Our use of *random* is to be carefully distinguished from Chaitin's use of the same term. Chaitin uses random to mean *algorithmically incompressible*, whereas we use the term to mean *possessing all arithmetically definable properties of measure one.*

[2] A *language* is a set of *strings.*

conjecture, they modified the proof of the Schröder-Bernstein Theorem to show that paddable[3] NP-complete languages are isomorphic to one another. As the converse is immediate, it follows that the isomorphism conjecture is equivalent to the conjecture that all NP-complete languages are paddable. By surveying the literature of the time on NP-complete languages, Berman and Hartmanis established that all of the then-known NP-complete languages were paddable, thereby providing empirical evidence for their conjecture.

In the years immediately following the isomorphism conjecture, research centered not on the conjecture itself, but rather on structural predictions of the conjecture. For example, the isomorphism conjecture predicts that there are no sparse[4] NP-complete languages. This prediction was verified by Mahaney [Mah82] under the hypothesis that P $\neq$ NP.

Another direction pursued in the years immediately following the conjecture was to "relocate" it to other natural degrees. In their original article, Berman and Hartmanis conjectured not only that the NP-complete degree collapsed, but also that the PSPACE complete degree collapsed. Berman [Ber77] was able to obtain a number of important partial results, e.g., that the complete m-degree for EXP consists of a single 1-li degree.

A re-examination of the isomorphism conjecture began with Joseph and Young's [JY85] definition of a new class of NP-complete languages—the k-creative languages. Joseph-Young then constructed specific k-creative languages (the K_f^k's) from polynomial-time computable, honest[5] functions f. At present, it is only known how to pad a K_f^k when f is polynomial-time invertible. Joseph and Young conjectured that

---

If A and B are languages, then A is *polynomial-time many-one reducible* to B if there is a polynomial-time computable function $f: \Sigma^* \to \Sigma^*$ such that

$$x \in A \iff f(x) \in B.$$

This relation is denoted by $f: A \leq_m^p B$, or simply $A \leq_m^p B$. If $f: A \leq_m^p B$, and f is also one-one, then we say A is *polynomial-time one-one reducible* to B, and write $f: A \leq_1^p B$. If f can be chosen to be length-increasing as well as one-one, then we say A is *polynomial-time 1-li reducible* to B, and write $f: A \leq_{1\text{-li}}^p B$. As a general rule, we are only interested in (possibly relativized) polynomial-time reducibilities, and so we abbreviate *polynomial-time many-one reducible* by *m-reducible*, *polynomial-time one-one reducible* by *1-reducible*, and *polynomial-time 1-li reducible* by *1-li reducible*.

A language L is complete for a class C with respect to a reducibility $\leq_r$ if L is C, and for all $M \in$ C, $M \leq_r L$. In the literature, the term NP-*complete* is often used without specifying the intended reducibility. In the early literature, NP-*completeness* usually meant *with respect to log-space reductions*. In more recent literature, NP-*complete* has come to mean *with respect to m-reductions*. We use the term in this latter sense.

If $A \leq_m^p B$ and $B \leq_m^p A$, then we say A and B are *polynomial-time many-one equivalent*, and write $A \equiv_m^p B$. The notions of *1-equivalent* and *1-li equivalent* are defined analogously. The collection of languages equivalent to a language A is called the *degree* of A. Thus, the m-degree of A is $\{B : A \equiv_m^p B\}$. The set of NP-complete languages is an important example of an m-degree.

If $f: A \leq_m^p B$, where f is one-one, onto, and polynomial-time invertible, then we say that f is a *polynomial-time isomorphism* between A and B, and write $f : A \cong_p B$. We abbreviate *polynomial-time isomorphism* by *isomorphism*. We say that a degree *collapses* if and only if all of its members are isomorphic to one another. Notice that m-degrees and 1-degrees are always unions of isomorphism classes, but 1-li degrees need not be.

In our terminology, the Berman-Hartmanis isomorphism conjecture can be stated succinctly: the complete m-degree for NP collapses.

[3] A *padding* function $\langle\langle \cdot, \cdot \rangle\rangle$ is a polynomial-time computable one-one function from pairs of strings to strings that is polynomial-time invertible in both [MY85]. A language A is *paddable* [BH77] if for all x and y,

$$x \in A \iff \langle\langle x, y \rangle\rangle \in A.$$

The original definition of *padding function* given by Berman and Hartmanis only required polynomial-time invertibility in the second argument. However, if a set is paddable by a Berman-Hartmanis function, then it is paddable by our definition.

If a padding function $\langle\langle \cdot, \cdot \rangle\rangle$ is also *onto*, then we say $\langle\langle \cdot, \cdot \rangle\rangle$ is a *polynomial-time pairing function*. If a set A is paddable by a pairing function $\langle\langle \cdot, \cdot \rangle\rangle$, then A is a *cylinder*. Cylinders arise naturally as cartesian products, and so occur in many natural complete degrees.

Let $\langle x, y \rangle$ be the standard Rogers' pairing function ([Rog67, Page 64]: $\frac{1}{2}((x+y)^2 + x + 3y)$). It is easy to see that $\langle x, y \rangle$ is a polynomial-time pairing function according to our definitions; moreover, $\langle \cdot, \cdot \rangle$ is length-nondecreasing in both arguments. Let $B \times C$ denote $\{\langle b, c \rangle : b \in B \wedge c \in C\}$. If B is m-complete for NP, then $A = B \times \Sigma^*$ is 1-li complete for NP.

Most complexity classes are closed under $\times$, i.e., if $\mathcal{C}$ is a complexity class, and $A, B \in \mathcal{C}$, then $A \times B \in \mathcal{C}$. Moreover, most complexity classes contain Σ^*. For such complexity classes, the construction above yields a simple but important result: If B is m-complete for $\mathcal{C}$, then $B \times \Sigma^*$ is paddable and 1-li complete for $\mathcal{C}$.

[4] A language L is *sparse* if there is a polynomial p such that for every n there are $p(n)$ or fewer elements of L of length less than or equal to n.

[5] A function f is *honest* if there is a polynomial p such that for every $x \in \Sigma^*$, $|x| \leq p(|f(x)|)$. Every polynomial time invertible function is honest. It is generally believed that the converse is false.

one-way functions exist, and that some K_f^k is non-paddable.

This conjecture goes beyond asserting that the Berman-Hartmanis conjecture fails: it asserts that a language with a specific form will witness the failure. These sets, the K_f^k's, are not merely m-complete for NP, they are 1-li complete. Thus, the Joseph-Young conjecture predicts that the 1-li complete degree for NP fails to collapse. We refer to this possibly weaker prediction as the *encrypted set conjecture*, as it claims that there exists a one-way (encryption) function f such that f(SAT) is not is isomorphic to SAT.

At the time the Berman-Hartmanis and Joseph-Young conjectures were made, both predicted properties of the NP-complete degrees that were not known to hold for any degrees: in particular, the Berman-Hartmanis conjecture predicts that the complete m-degree for NP collapses, and yet no nontrivial collapsing m-degree was known; and the Joseph-Young conjecture predicts that the complete 1-li degree for NP does not collapse, and yet no noncollapsing 1-li degree was known to exist.

If one-way functions don't exist, then the Schröder-Bernstein-Berman-Hartmanis proof shows that every 1-li degree collapses. Therefore, a minimal hypothesis for the construction of a noncollapsing 1-li degree is the existence of a one-way function. Watanabe [Wat85] conjectured that the existence of a one-way function *is* an adequate hypothesis for the construction of a noncollapsing 1-li degree, and he was proven correct by Ko, Long, and Du [KLD86]. This validation of a prediction of the Joseph-Young conjecture is an important piece of evidence in its favor.

The following year, we [KMR88] showed that there are nontrivial collapsing m-degrees, providing analogous evidence in favor of the Berman-Hartmanis conjecture.

1.1.2 Relativizations

Relativizations have long been used in structural complexity theory to probe the limitations of our proof techniques. Indeed, the use of relativizations has been so successful that at times it seems that *any* reasonable complexity theoretic statement holds relative to *some* oracle. The various isomorphism conjectures are a notable exception to this trend: it has proven very difficult to produce oracles relative to which one can decide the various conjectures.

The one simple relativization is an oracle relative to which the complete m-degree for EXP collapses. By Berman's theorem that the m-complete for EXP consists of a 1-li degree, it suffices to take an oracle relative to which one-way functions fail to exist, for if one-way functions don't exist, then *all* 1-li degrees must collapse. The original Baker-Gill-Solovay oracle relative to which P = NP suffices.

In contrast, and in spite of widely perceived similarities between NP and EXP, progress has not been made in obtaining an oracle relative to which the complete degree for NP collapses.

Kurtz [Kur83] provided the first example of an oracle relative to which P $\neq$ NP and yet the isomorphism conjecture fails. Curiously, the failure of the isomorphism conjecture relative to Kurtz's oracle is different from that predicted by Joseph and Young, as it is obtained by splitting the m-complete degree for NP into several 1-degrees. Thus, while the Berman-Hartmanis and the Joseph-Young conjectures can not both be true, they can both be false. Hartmanis and Hemachandra [HH87], by combining Kurtz's construction with the Rackoff's [Rac82] construction of an oracle relative to which P = UP $\neq$ NP, construct an oracle relative to which both conjectures fail.

After publication of the Hartmanis-Hemachandra paper, we had the following view of oracles and isomorphisms: it was possible to make the complete degrees for higher classes such as EXP collapse, but we did not know how to make them fail to collapse; it was possible to make the complete degree for NP fail to collapse, but we could not make it collapse; there was no natural complexity class which we could both make collapse, and make fail to collapse; and while it was possible to make either or both of the Berman-Hartmanis and Joseph-Young conjectures fail, we could not make either succeed.

After [KLD86] and [KMR88] appeared, we hoped to break the impasse. We expected that the techniques of [KLD86] could be exploited in an oracle construction relative to which the Joseph-Young conjecture holds; we expected that the techniques of [KMR88] could be used to construct an oracle relative to which the Berman-Hartmanis conjecture holds.

We achieved [KMR87] limited success by constructing a sparse oracle relative to which there is a collapsing m-degree in NP. As sparse oracles seem less likely to distort structural relationships than unrestricted oracles[6], we take this as evidence for the proposition that some m-degree in NP collapses.

Homer and Selman [HS88] achieved the first breakthrough, producing an oracle relative to which the m-complete degree for Σ_2^p collapses, as well as an oracle relative to which it fails to collapse. By their efforts, the complete m-degree for Σ_2^p became the first natural degree to have both collapsing and noncollapsing relativizations.

[6] We defend this position in footnote 8.

In this paper, we show that the encrypted set conjecture holds relative to a random oracle. Relative to a random oracle, higher complexity classes such as PSPACE and EXP fail to collapse, and so we provide numerous examples of natural complexity classes that can be relativized in both directions.

This leaves, of the many questions about oracles and isomorphisms, only the original problem unsolved: to construct an oracle relative to which the Berman-Hartmanis conjecture holds.

1.1.3 Randomness

If T is a statement about complexity theory, e.g., P $\neq$ NP, it is not unusual for there to be oracles A and B such that T^A is true, and T^B is false. If only for this reason, unrestricted relativizations cannot be relied upon for insight into what is true in the unrelativized world.

In spite of this difficulty, it is possible to restrict the set of permissible oracles so that a coherent picture emerges. Two notable examples of such restrictions are to *random* and *generic* oracles.[7] Complexity theory relative to a random oracle *is* well defined, as is complexity theory relative to a generic oracle. Let $\mathcal{T}$ denote the set of true formulae in some fixed formalization of complexity theory, $\mathcal{T}^{\mathcal{R}}$ denote the formulae true relative to a random oracle, and $\mathcal{T}^{\mathcal{G}}$ denote the formulae true relative to a generic oracle.[8]

[7] These two classes of oracles have been studied fairly extensively by recursion-theorists. We direct the reader to [Joc80] for an introduction to generic oracles, and to [Kur81] for random oracles.

[8] A number of authors have studied mechanisms for restricting the notion of relativization so as to obtain "absolute" results. These restrictions come in two flavors: restricting the machine's ability to access the oracle, and restricting the class of oracles to be considered. The restrictions of interest to this program are those which preserve the validity of certain complexity theoretic statements.

A pertinent example of such a result is that all sparse oracles agree as to whether or not the polynomial-time hierarchy collapses [BBS86,LS86]. As the empty oracle is sparse, if a sparse oracle can be constructed relative to which one can determine whether or not the polynomial-time hierarchy collapses, then one has settled the unrelativized question as well.

We know of no complexity theoretic statements T such that for sparse oracles A and B, T^A is true but T^B is false. This suggests a "sparse oracle hypothesis." While we do not believe that the sparse oracle hypothesis is true, its validity in certain special cases provides evidence for our earlier claim that sparse oracles are less likely to distort relationships among complexity classes than unrestricted relativizations.

The relationship between these theories has been the focus of considerable research. Most known results about $\mathcal{T}$ are also true of $\mathcal{T}^{\mathcal{R}}$ and $\mathcal{T}^{\mathcal{G}}$: this merely reflects the fact that we have few tools for proving theorems about unrelativized complexity theory that do not relativize.

The theory $\mathcal{T}^{\mathcal{G}}$ is fairly well understood, as most oracle constructions that separate two classes can be modified to apply to generic oracles. For example, from Yao's proof that the polynomial time hierarchy (PH) separates relative to some oracle, it is not difficult to demonstrate that PH separates with respect to a generic oracle.

The theory $\mathcal{T}^{\mathcal{R}}$ is less well understood, in part because its measure theoretic arguments are more difficult than the Baire category theoretic arguments of $\mathcal{T}^{\mathcal{G}}$. For example, the proof that NP $\neq$ coNP relative to a generic oracle is a consequence of the original Baker-Gill-Solovay [BGS75] construction of an oracle that separates P and NP; while the proof that NP $\neq$ coNP relative to a random oracle is difficult and deep [BG81].

1.2 Overview of New Results

This section surveys the technical contributions of this paper. A one-way function (cf. Definition 2.1) is a polynomial-time computable, one-one, honest function that is not polynomial-time invertible. We have not been able to make progress on the Joseph-Young conjecture under the hypothesis that one-way functions exist. We have, however, been able to make considerable progress under a stronger hypothesis:

Definition 2.2 *A function f is a* scrambling function *if and only if f is a one-way function and range(f) does not contain a nonempty paddable set.*

First, we show that if scrambling functions exist, then the encrypted set conjecture holds:

Theorem 2.3 *If scrambling functions exist, the complete 1-li degree for* NP *fails to collapse.*

In fact, if scrambling functions exist, then the Joseph-Young conjecture holds, as the noncollapse can be witnessed by a K_f^k:

Theorem 2.4 *If f is a scrambling function, then K_f^k is a nonpaddable 1-li complete set for* NP.

This noncollapse of a 1-li degree is not specific to the NP-complete degree. We can show that a large number of other natural, complete degrees also all fail to collapse if scrambling functions exist.

Theorem 2.8 *If scrambling functions exist, then the complete 1-li degrees for* NP, PSPACE, EXP, NEXP, *and* RE *fail to collapse.*

In as much as a direct proof of the existence of scrambling functions seems to be beyond our immediate ability, as a surrogate, we looked for an oracle relative to which such functions exist. It was intuitively obvious that scrambling functions must exist relative to a random oracle. In fact, much more powerful one-way functions exist relative to a random oracle:

Definition 2.9 *A function f is an* annihilating *function if and only if f is a 1-way function such that all polynomial-time decidable subsets of range(f) are sparse.*

It is not difficult to see that an annihilating function is necessarily a scrambling function.

Theorem 3.6 *Annihilating functions exist relative to a random oracle.*

Combining Theorems 2.8 and 3.6 yields

Theorem 3.7 *Relative to a random oracle, the complete 1-li degrees for* NP, PSPACE, EXP, NEXP, *and* RE *do not collapse. In particular, the isomorphism conjecture fails relative to a random oracle.*

1.3 Further Questions

We see a number of opportunities for improving on our results of this paper.

A first opportunity is to weaken the structural hypotheses that suffice to prove the encrypted set conjecture. We do not believe that either the "vanilla" one-way functions of Grollmann and Selman, or our own more powerful scrambling functions, are the correct characterization.

A second opportunity is to explore additional structural consequences of the existence of scrambling and/or annihilating functions. It seems that the existence of annihilating functions ought to have profound structural consequences, and yet none of our structural theorems require this power. In particular, we would like to see proofs that the existence of annihilating functions implies the complete m-degree for NP consists of a single 1-li degree, or perhaps that the existence of annihilating functions implies that the polynomial-time hierarchy separates. In view Theorem 3.6, these structural consequences would immediately hold relative to a random oracle.

We would like to see structural hypotheses that are equivalent to the existence of these strong one-way functions, much as P $\neq$ UP is equivalent to the existence of one-way functions. This sort of structural taxonomy of one-way functions seems to have a great deal of promise.

A final opportunity is to look for more powerful structural properties that hold relative to random or generic oracles. We have found random oracles, in particular, to be a valuable "laboratory" for exploring the plausibility of various structural hypotheses. In particular, random oracles tend to be very good at separating deterministic and nondeterministic complexity classes, and at producing sets with very strong immunity properties.

2 Structural Theorems

In this section, we consider various strengthenings of the definition of a 1-way function.

Definition 2.1 *A function f is a* 1-way function *if and only if f is honest, one-one, polynomial-time computable, and* not *polynomial-time invertible.*

Our definition of 1-way function requires totality, which is not the case in all presentations. Grollmann and Selman [GS84,GS88] and Ko [Ko85] show that the existence of 1-way functions is equivalent to P $\neq$ UP. Ko, Long, and Du [KLD86] show that if 1-way functions exist, then length increasing 1-way functions exist.

We introduce two more powerful variants of the notion of a 1-way function, and show that if these functions exist, then the complete 1-li degree for NP (and for many other natural complexity classes) does not collapse.

Definition 2.2 *A function f is* a scrambling function *if and only if f is a one-way function and range(f) does not contain a nonempty paddable set.*

As with "vanilla" one-way functions [KLD86, Proposition 2.1], if scrambling functions exist, then length increasing scrambling functions exist.

The existence of scrambling functions implies that the encrypted set conjecture is valid.

Theorem 2.3 *If scrambling functions exist, then the complete 1-li degree for* NP *fails to collapse, and so the isomorphism conjecture fails*

Proof: Let f be a length increasing scrambling function and let A be paddable 1-li complete for NP.

Consider[9] $B = f''A$. It is easy to see that B is 1-li complete for NP.

As $B \subset \text{range}(f)$, B cannot be paddable. As paddability is an isomorphism invariant, A and B are not isomorphic.

□

It is natural to ask whether or not the existence of scrambling functions implies the Joseph-Young conjecture.

To this end, let φ_i denote the i-th nondeterministic Turing machine, and let Φ_i denote its running time. Joseph and Young define

$$K_f^k = \{f(i) : \Phi_i(f(i)) < |i| \cdot |f(i)|^k + |i|\}$$

for one-one, honest, polynomial-time computable f.

It is clear that K_f^k is a subset of range(f), and so is not paddable. By the analysis in [JY85], K_f^k will be 1-li complete for NP whenever f is a scrambling function.

We have

Theorem 2.4 *If f is a scrambling function, then K_f^k is a nonpaddable 1-li complete set for* NP.

Theorem 2.3 is far more general than it might initially appear. In particular, the hypothesis that A was 1-li complete for NP was only used to ensure that $B \leq_{\text{1-li}}^{\text{P}} A$. By isolating this hypothesis, we can extend the proof of Theorem 2.3 to obtain the non-collapse of many other 1-li degrees.

Definition 2.5 *A set A is* 1-li image complete *if and only if for every polynomial-time computable 1-li function f, $f''A \leq_{\text{1-li}}^{\text{P}} A$. Similarly, a set A is* m-image complete *if and only if for every honest, polynomial-time computable f, $f''A \leq_{\text{m}}^{\text{P}} A$.*

Image completeness is a property shared by the complete languages for most natural complexity classes containing NP. In particular, the complete languages for NP, PSPACE, EXP, NEXP, and RE are all image complete. The following proposition is trivial.

Proposition 2.6 *If A is 1-li image complete, then so is every set in the 1-li degree of A. If A is m-image complete, then so is every set in the m-degree of A.*

Proposition 2.6 enables us to extend the terminology of image completeness from sets to degrees.

[9] We use the set theoretic $f''A$ to denote $\{f(x) : x \in A\}$, rather than the more conventional $f(A)$. The later notation is ambiguous in situations where A may be in the domain of f.

Theorem 2.7 *If scrambling functions exist, then every image complete 1-li degrees with a paddable element does not collapse; and every image complete m-degree contains an image complete 1-li degree that does not collapse.*

Many natural classes contain m-image complete sets. Thus,

Theorem 2.8 *If scrambling functions exist, then the complete 1-li degrees for* NP, PSPACE, EXP, NEXP, *and* RE *fail to collapse.*

In Section 3, we will show that there are oracles relative to which scrambling functions exist, indeed, that much more powerful sorts of 1-way functions exist relative to random oracles.

Definition 2.9 *A function f is an* annihilating *function if and only if f is a 1-way function such that all polynomial-time decidable subsets of range(f) are sparse.*

As before, if annihilating functions exist, then length increasing annihilating functions exist.

Annihilating functions are, in one sense, the most powerful sort of one-way function possible, for the range of every polynomial-time computable one-one function must contain sparse sets with arbitrarily large polynomial census.

It is easy to see that every annihilating function is a scrambling function. The main result of the Section 3 is that annihilating functions exist relative to a random oracle.

3 Randomness

In this section we will show that annihilating functions exist relative to a random oracle.

3.1 Notation

We consistently identify sets with their characteristic functions. Thus, if $A \subseteq D$ and $x \in D$, then

$$A(x) = \begin{cases} 1, & \text{if } x \in A; \\ 0, & \text{if } x \notin A. \end{cases}$$

The cardinality of a set A is denoted by $\|A\|$.

If $\mathcal{A} \subseteq 2^\omega$, then we use $\mu(\mathcal{A})$ to denote the Lebesgue measure [Oxt80] of $\mathcal{A}$. In this paper, we will consider only 1st-order definable subsets of 2^ω. Definable subsets are explicitly Borel, and therefore are measurable. We will use the term *probability* as a synonym for *measure*. E.g., if we say that a random oracle

R is in $\mathcal{A}$ with probability ρ, this means that $\mathcal{A}$ has measure ρ.

A *tail set* is a subset $\mathcal{P}$ of 2^ω that is closed under finite variants, i.e., if X and Y are subsets of ω such that $X \triangle Y$ is finite, then $X \in \mathcal{P} \iff Y \in \mathcal{P}$. Kolmogorov's zero-one law [Oxt80, Theorem 21.3] states that a measurable tail set must have measure 0 or 1. Structural properties such as $\{X : \mathrm{P}^X \neq \mathrm{NP}^X\}$ are definable tail sets, and so have measure 0 or 1. Informally, this means that there is a well-defined "measure 1" theory. If $\mathcal{P}$ is a measure 1 subset of 2^ω, then we say $\mathcal{P}$ *holds relative to a random oracle*. In essence, this defines our use of the word *random*. It should be noted that this use of *random* [Kur81,Kur88] is more restrictive than Chaitin's use [Cha77,Cha87] of the same term. Thus, if we claim $\mathcal{P}$ holds relative to a random oracle, there may well be Chaitin random sets X such that $X \notin \mathcal{P}$. For example, the statement $\{X : X \text{ is not arithmetic}\}$ is a measure one property of 2^ω, and yet Chaitin's Ω *is* arithmetic.

An *operator* is a function from 2^ω to 2^ω. We often decurry an operator, and view it as a function from $2^\omega \times \omega$ to 2. If L is an operator, we will generally write $L^R(n)$ rather than $L(R,n)$ or $L(R)(n)$. As elements of 2^ω are identified with languages, an operator can be identified with a function from languages to languages. In this guise, operators are usually referred to as *reducibilities*. Occasionally, we view the argument to an operator as having been fixed, in which case we speak of *relativizations* or *oracle dependent languages*. It is helpful to realize that these notions, which are superficially quite different, are mathematically equivalent.

The most important classes of operators are the continuous and the partial recursive operators. A partial recursive operator need not be continuous, but all total recursive operators are. The polynomial-time computable operators are total, and therefore continuous. We refer the reader to [Rog67] for a mathematical introduction to operators.

3.2 Annihilating functions exist relative to a random oracle

We focus our attention on the following function:

$$\xi_R(x) = R(x1)R(x10)\ldots R(x10^{3|x|}).$$

Lemmas 3.1 and 3.5 show that ξ_R is an annihilating function with probability at least 1/2. By general measure theoretic principles (Theorem 3.6), annihilating functions exist relative to a random oracle.

It is easily seen that ξ_R maps strings of length n to strings of length $3n+1$. Therefore ξ_R is honest.

Lemma 3.1 *With positive probability, ξ_R is one-one.*

Proof: If $\xi_R(a) = \xi_R(b)$, then a and b must have the same length. We establish an upper-bound on the probability that two strings of length n have the same image, and then by summing over n, establish an upper-bound of 1/2 on the probability that ξ_R fails to be one-one.

If a and b are distinct elements of length n, then the probability that they have the same image under ξ_R is exactly $1/2^{3n+1}$. There are $\binom{2^n}{2}$ distinct pairs of elements of length n, and so the probability that there exist two strings of length n having the same image under ξ_R can be bounded above by

$$\begin{aligned}\binom{2^n}{2}\frac{1}{2^{3n+1}} &= \frac{2^{n-1}(2^n-1)}{2^{3n+1}} \\ &< \frac{2^{n-1}2^n}{2^{3n+1}} \\ &= \frac{1}{2^{n+2}}.\end{aligned}$$

We can now bound the probability that there are ξ_R is not one-one by summing this estimate over all n:

$$\sum_{n\in\omega}\frac{1}{2^{n+2}} = \frac{1}{2}.$$

As ξ_R is not one-one with probability at most 1/2, it is one-one with probability at least 1/2.

□

To show that ξ_R is an annihilating function with positive probability, we need to show for random R that if $L^R \subseteq \mathrm{range}(\xi_R)$, and if $\xi_R(x) \in L^R$, then $L^R(\xi_R(x))$ must depend on x for all but finitely many x. In fact, this really isn't an observation about computation, but rather about information.

Definition 3.2 *Let R and S be oracles. We say that R and S are x-variants if and only if $R \triangle S \subseteq \{x10^k : k \in 3n+1\}$. If R and S are x-variants, then we write $R \sim_x S$.*

Clearly $\sim_x$ is an equivalence relation for every string x.

Definition 3.3 *If L is an oracle-dependent language, then we say L^R* examined *x on argument y if and only if there is an S, $S \sim_x R$, such that $y \in L^R \triangle L^S$.*

The terminology *examined* is an artifact of viewing L as a Turing machine, where we say $L^R(y)$ examines a string x if L on input y queries R about a string

of the form $x10^k$. Notice that the definition of *examined* given in Definition 3.3 is more restrictive than the Turing machine definition, as a Turing machine may make queries whose answer does not affect the outcome of the computation.

Lemma 3.4 *Let U be a continuous operator such that for all x, y, and R, if $y = \xi_R(x) \in U^R$, then $U^R(y)$ does not examine x. The probability that U^R is an infinite subset of range(ξ_R) for a random R is zero.*

Proof: We establish a stronger result than we claim. We show that if U is a continuous operator, and if for all x, y, and R, $U^R(y)$ does not examine x whenever $y = \xi_R(x) \in U^R$ then the probability that U^R both contains 2^n or fewer elements of length 2^{3n+1} or less for every n, and has an infinite intersection with range(ξ_R), is zero.

Let $x \in 2^n$. Define

$$\mathcal{M}_n(x) = \{R : \xi_R(x) \in U^R \wedge \|U^R \bigcap 2^{3n+1}\| \leq 2^n\}$$

We claim

$$\mu(\mathcal{M}_n(x)) \leq 1/2^{2n+1}. \tag{1}$$

Consider a fixed language R. This R has exactly 2^{3n+1} equally probable x-variants. It suffices to show that at most 2^n of R's x-variants can be in $\mathcal{M}_n(x)$.[10]

Let $Y = \{y_i : i \in I\}$ be the collection of strings of length $3n+1$ in U^R that do not examine x. If S is an x-variant of R, then by the definition of "examine," we must have $Y \subseteq U^S$. If $\|Y\| > 2^n$, then none of R's x-variants are in $\mathcal{M}_n(x)$, and (1) holds.

Therefore, assume $\|Y\| \leq 2^n$. Let S be an x-variant of R, and let $y = \xi_S(x) \in U^S$. We claim that y must be one of the y_i's. If not, then U^S must examine x, but in this case $y \notin U^S$ by our hypothesis on U. Thus, the only variants of R which can be in $\mathcal{M}_n(x)$ are the variants S such that $\xi_S(x) = y_i$ for some i. There is one such variant for every $i \in I$, and therefore at most 2^n many such variants. Again, (1) holds, establishing our claim.

Let

$$\mathcal{R}(n) = \{R : (\exists k \geq n)(\exists x \in 2^k)[\xi_R(x) \in U^R \wedge \|U^R \bigcap 2^{3k+1}\| \leq 2^k]\}.$$

[10] Well, actually, this does not suffice. Technically, one has to extend the notion of x-variant to basic open intervals. Then, consider minimal basic open intervals σ such that $U^\tau(y)$ is determined for all $y \in 2^{3n+1}$ and $\tau \sim_x \sigma$. (It is at this point that we use the hypothesis of continuity.) These σ's form a finite partition of 2^ω. The argument which we state informally in terms of R can then be formally stated in terms of the σ's.

The set $\mathcal{R}(n)$ is merely the collection of oracles R relative to which for some $k \geq n$, U^R contains few enough elements of length $3k+1$ to fit within the range of ξ_R, and U^R has an element of length $3k+1$ in range(ξ_R).

We claim that for all n,

$$\mu(\mathcal{R}(n)) \leq 1/2^n. \tag{2}$$

By countable subadditivity,

$$\begin{aligned}
\mu(\mathcal{R}(n)) &\leq \sum_{k \geq n} \sum_{x \in 2^k} \mu(\{R : \xi_R(x) \in U^R \wedge \|U^R \bigcap 2^{3k+1}\| \leq 2^k\}) \\
&= \sum_{k \geq n} \sum_{x \in 2^k} \mu(\mathcal{M}_n(x)) \\
&\leq \sum_{k \geq n} \sum_{x \in 2^k} 1/2^{2k+1} \qquad \text{(by 1)} \\
&= \sum_{k \geq n} 1/2^{k+1} \\
&= 1/2^n
\end{aligned}$$

and therefore (2).

Now, if U^R is an infinite subset of range(ξ_R), then $R \in \mathcal{R}(n)$ for every n. The lemma follows, as $\mu(\mathcal{R}(n))$ can be made as small as desired by an appropriate choice of n.

□

Lemma 3.5 *With probability 1, if $L^R \subseteq$ range(ξ_R) is a polynomial-time computable set relative to R, then L^R is sparse.*

Proof: We begin by decomposing L^R into two disjoint sets: Q^R is the set of $y \in L^R$ such that $L^R(y)$ examined an x such that $\xi_R(x) = y$; and U^R is the set of $y \in L^R$ such that L^R did not examine such an x. It suffices to show that with probability 1, Q^R is sparse, and if U^R is a subset of range(ξ_R), then U^R is sparse.

By Lemma 3.4, if $U^R \subseteq$ range(ξ_R), then U^R is finite, and so it suffices to show that Q^R is sparse with probability 1.

For each string y of length $3n+1$, the probability that any given x of length n is a preimage of y is $1/2^{3n+1}$. As Q^R can examine at most $p(3n+1)$ potential preimages of y, the probability that Q^R will examine a preimage of y is at most $p(3n+1)/2^{3n+1}$.

Therefore, the expected number of elements of length $3n+1$ that Q^R will accept is bounded by $2^{3n+1}(p(3n+1)/2^{3n+1}) = p(3n+1)$.

We claim that the probability that Q^R can contain more than $n^2 p(3n+1)$ many elements is bounded

above by n^{-2}, otherwise the mass contributed to the expected number of elements of Q^R by these "large" sets would exceed the overall expectation. As Q^R can never have a negative number of elements of a given length, this cannot occur.

The probability that Q^R can have more than $k^2 p(3k+1)$ elements for some $k > n$ is therefore bounded by

$$\sum_{k>n} \frac{1}{k^2} < \frac{1}{n-1}.$$

The lemma follows immediately.

□

Theorem 3.6 *Annihilating functions exist relative to a random oracle.*

Proof: If an annihilating function exists with respect to an oracle R, an annihilating function exists with respect to all its finite variants. By Kolmogorov's zero-one law (cf. [Oxt80, Theorem 21.3]), the measure of the set of oracles R such that there is an annihilating function relative to R has measure 0 or 1. By Lemmas 3.1 and 3.5, we know that there is a set of positive measure on which ξ_R is an annihilating function. The theorem follows immediately.

□

The following theorem is an immediate consequence of Theorem 3.6, Theorem 2.8, and the fact that all annihilating functions are scrambling functions.

Theorem 3.7 *Relative to a random oracle, the complete 1-li degrees for* NP, PSPACE, EXP, NEXP, *and* RE *do not collapse. In particular, the isomorphism conjecture fails relative to a random oracle.*

4 Acknowledgments

We would like to acknowledge the contributions of a number of our colleagues. The following people commented on an earlier version of this paper: Joan Feigenbaum, Stephen Fenner, Jeffrey Legarias, Lane Hemachandra, Stephen Homer, Neil Immerman, Tim Long, Alan Selman, Janos Simon, and Osamu Watanabe. We would like to acknowledge several helpful discussions with Laszlo Babai. We would like to thank Alan Selman for sharing with us his yet-unpublished research on the Joseph-Young conjecture. Finally, we would like to thank the two gracious antagonists—Juris Hartmanis and Paul Young—whose differing insights have provided us with many fine problems to solve.

References

[BBS86] Jose L. Balcázar, Ronald V. Book, and Uwe Schöning. The polynomial-time hierarchy and sparse oracles. *Journal of the ACM*, 33:603–617, 1986.

[Ber77] L. Berman. *Polynomial Reducibilities and Complete Sets.* PhD thesis, Cornell University, 1977.

[BG81] Charles H. Bennett and John Gill. Relative to a random oracle A, $\mathbf{P}^A \neq \mathbf{NP}^A \neq \mathbf{co\text{-}NP}^A$ with probability 1. *SIAM Journal on Computing*, 10:96–113, February 1981.

[BGS75] Theodore Baker, John Gill, and Robert Solovay. Relativizations of the $\mathcal{P} =? \mathcal{NP}$ 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*, 6:305–322, June 1977.

[Cha77] Gregory J. Chaitin. Algorithmic information theory. *IBM Journal of Research and Development*, 21:350–359, 1977.

[Cha87] Gregory J. Chaitin. *Algorithmic Information Theory.* Cambridge University Press, Cambridge, 1987.

[GS84] Joachim Grollman and Alan L. Selman. Complexity measures for public-key cryptosystems. In *25th Annual Symposium on Foundations of Computer Science*, pages 495–503, Los Angeles, October 1984. IEEE Computer Society.

[GS88] Joachim Grollman and Alan L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17:309–335, April 1988.

[HH87] Juris Hartmanis and Lane A. Hemachandra. One-way functions, robustness, and the non-isomorphism of NP-complete sets. In *Structure in Complexity Theory, Second Annual Conference*, pages 160–174. IEEE Computer Society, 1987.

[HS88] Steven Homer and Alan L. Selman. Oracles for structural properties. In preparation, 1988.

[Joc80] Carl G. 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] Deborah Joseph and Paul Young. Some remarks on witness functions for nonpolynomial and noncomplete sets in NP. *Theoretical Computer Science*, 39:225–237, 1985.

[KLD86] Ker-I Ko, Timothy J. Long, and Ding-Zhu Du. On one-way functions and polynomial-time isomorphisms. *Theoretical Computer Science*, 47:263–276, 1986.

[KMR87] Stuart A. Kurtz, Stephen R. Mahaney, and James S. Royer. Progress on collapsing degrees (extended abstract). In *Proceedings of Structure in Complexity Theory, 2nd Annual Conference*, pages 126–131, 1987.

[KMR88] Stuart A. Kurtz, Stephen R. Mahaney, and James S. Royer. Collapsing degrees. *Journal of Computer System Science*, 1988. To appear.

[Ko85] Ker-I Ko. On some natural complete operators. *Theoretical Computer Science*, 37:1–30, 1985.

[Kur81] Stuart A. Kurtz. *Randomness and Genericity in the Degrees of Unsolvability*. PhD thesis, University of Illinois at Urbana-Champaign, 1981.

[Kur83] Stuart A. Kurtz. A relativized failure of the Berman-Hartmanis conjecture. Technical Report 83–001, University of Chicago, 1983.

[Kur88] Stuart A. Kurtz. A hierarchy of notions of randomness. *Abstracts of the AMS*, 9:126, January 1988. Abstract 839–68–395.

[LS86] Timothy J. Long and Alan L. Selman. Relativizing complexity classes with sparse oracles. *Journal of the ACM*, 33:618–627, 1986.

[Mah82] Stephen R. Mahaney. Sparse complete sets for NP: solution of a conjecture of Berman and Hartmanis. *Journal of Computer System Science*, 25:130–143, 1982.

[Mah86] Stephen R. Mahaney. Sparse sets and reducibilities. In Ronald V. Book, editor, *Studies in Complexity Theory*, pages 63–118. John Wiley & Sons, Inc., 1986.

[MY85] Stephen R. Mahaney and Paul Young. Reductions among polynomial isomorphism types. *Theoretical Computer Science*, 39:207–224, 1985.

[Oxt80] John C. Oxtoby. *Measure and Category*. Springer-Verlag, New York, 2nd edition, 1980.

[Rac82] C. Rackoff. Relativized questions involving probabilistic algorithms. *Journal of the ACM*, 29:261–268, 1982.

[Rog67] Hartley Rogers, Jr. *Theory of Recursive Functions and Effective Computability*. McGraw-Hill, New York, 1967.

[Wat85] Osamu Watanabe. On one-one polynomial time equivalence relations. *Theoretical Computer Science*, 38:157–165, 1985.

[You88] Paul Young. Juris Hartmanis: Fundamental contributions to isomorphism problems. In *Proceedings of the 3rd Annual Structural in Complexity Theory*, pages 138–154, 1988. Preliminary Version.