The Isomorphism Conjecture Holds and One-way Functions Exist Relative to an Oracle

John Rogers*
Department of Computer Science
The University of Chicago
1100 East 58th Street
Chicago, Illinois 60637

November 23, 1994

Abstract

In this paper we demonstrate an oracle relative to which there are one-way functions but every paddable 1-li-degree collapses to an isomorphism type, thus yielding a relativized failure of the Joseph-Young Conjecture (**JYC**) [JY85].

We then use this result to construct an oracle relative to which the Isomorphism Conjecture (**IC**) is true but one-way functions exist, which answers an open question of Fenner, Fortnow, and Kurtz [FFK92]. Thus, there are now relativizations realizing every one of the four possible states of affairs between the **IC** and the existence of one-way functions.

1 Introduction

Berman and Hartmanis [BH76, BH77] showed that if two languages A and B are equivalent to one another under polynomial-time many-to-one reductions and if they are both *paddable* then they are polynomial-time isomorphic. After surveying all of the then-known **NP**-complete languages and discovering that each was indeed paddable, they posed:

The Isomorphism Conjecture (IC) *Every* **NP**-*complete language is isomorphic to* **SAT**.

This conjecture has been neither proven nor refuted and, because there are oracles relative to which it fails [Kur83, KMR89, HH91] and holds [FFK92], doing so will probably require new proof techniques.

In the meantime, we can try to demonstrate relationships between the **IC** and other complexity-theoretic propositions. For example, do the **IC** and the proposition $\mathbf{P} \neq \mathbf{UP}$ have anything to do with another? Grollmann and Selman [GS88] show that $\mathbf{P} \neq \mathbf{UP}$ if and

*Email: rogers@cs.uchicago.edu. Some of this work was done while being partially supported by NSF grant CCR 92-53582.

only if one-way functions exist, that is, one-to-one, honest polynomial-time functions that are not polynomial-time invertible. So, we will phrase the question as:

> *What is the relationship (if any) between the* **IC** *and the existence of one-way functions?*

Before dealing with this question, we will rephrase the **IC** in a slightly different language.

Let r be a class of reductions having transitive closure, that is, if a language A is r-reducible to a language B and B is r-reducible to C then A is r-reducible to C. Two languages are r-equivalent if each is r-reducible to the other. This induces an equivalence relation for which, using the terminology of recursion theory, we call the equivalence classes *r-degrees*. Let s also be a class of reductions having transitive closure. We say that an r-degree **a** *collapses* to an s-degree **b** if **b** is contained in **a** and every pair of languages in **a** is s-equivalent.

In this paper, we consider reductions realized by polynomial-time functions and the associated degrees. We consider reductions that are: many-to-one (m-reductions); one-to-one and length-increasing (1-li-reductions), that is, reductions for which the output is longer than the input; 1-li and invertible (1-li-inv-reductions), that is, 1-li-reductions f for which there is a polynomial-time reduction g such that, for all x, $g(f(x)) = x$; and isomorphisms (one-to-one, onto, and invertible reductions). We refer to an isomorphism degree as an isomorphism type and, when a degree collapses to an isomorphism type, we simply say that the degree collapses.

Because the m-degree of **SAT** contains all of the **NP**-complete languages, the **IC** can be phrased as:

The Isomorphism Conjecture (IC) *The m-degree containing* **SAT** *collapses.*

In this form, natural variants spring to mind. For example, one might pose:

The Isomorphism Conjecture for the 1-li-degree ($\mathbf{IC}_{1-\mathrm{li}}$) *The complete 1-li-degree of* **SAT** *collapses.*

Of course, this degree may *not* contain all of the **NP**-complete sets but it does contain **SAT**, which is 1-li (in fact, 1-li-invertible) complete.

And now we can return to one-way functions. If one-way functions do not exist then every 1-li function is invertible, that is, every 1-li-degree is a 1-li-inv-degree and Berman and Hartmanis [BH77] showed that every 1-li-inv-degree collapses. On the other hand, Ko, Long, and Du [KLD86] showed that if one-way functions *do* exist then length-increasing one-way functions also exist and that there is a nonpaddable 1-li-degree in exponential time that does *not* collapse. Could this failure of collapse happen to the 1-li-degree of **SAT**?

This question was first treated in depth when Joseph and Young [JY85] defined the k-creative languages K_f^k, where $k \geq 1$ and f is a length-increasing, polynomial-time function. If f is one-way, it was not (and is not) obvious that all of the resulting languages, which are **NP**-complete, are paddable. They posed:

The Joseph-Young Conjecture (JYC) *There is a one-way length-increasing function f such that, for some k, K_f^k is not paddable.*

Isomorphisms preserve paddability so **SAT**, which *is* paddable, and K_f^k would be 1-li-equivalent but not isomorphic. This led Selman [Sel92] to observe that the **JYC** implies a simpler conjecture:

The Encrypted Complete Set Conjecture (ECSC) *There is a one-way function f such that* **SAT** *and* $f(\mathbf{SAT})$ *are not polynomial-time isomorphic.*

Once again, these conjectures have been neither proven nor refuted. About all we know is that the following chain of implications holds:

$$\mathbf{JYC} \Rightarrow \mathbf{ECSC} \Rightarrow \neg\mathbf{IC}_{1-\mathrm{li}} \Rightarrow \neg\mathbf{IC}.$$

In fact, we do not know whether *any* one-way functions exist and, because there are oracles relative to which they do and do not exist [Rac82, GG86], establishing this will probably be very difficult.

So what can we do? One approach is to construct relativized universes in which one-way functions of some sort do or do not exist and the **IC** (or $\mathbf{IC}_{1-\mathrm{li}}$) does or does not hold. Previous work has yielded oracles relative to which three of the four possible states of affairs have been realized.

In the first of these results, Kurtz, Mahaney, and Royer [KMR89] showed that if one-way functions called *scrambling functions* exist then the **IC** fails. A scrambling function is a one-way function whose image is not paddable. They then showed that, relative to a random oracle R, scrambling functions exist. Indeed, they showed that an *annihilating* function exists, which is a one-way function having the property that every polynomial-time decidable subset of its image is sparse and hence not paddable. Because length-increasing annihilating functions also exist relative to R, the $\mathbf{IC}_{1-\mathrm{li}}$ fails as well.

What if there are no one-way functions? Is it still possible for the **IC** to fail? The answer is yes: Hartmanis and Hemachandra [HH91] demonstrated an oracle C relative to which there are no one-way functions but the **IC** still fails because the m-degree of $\mathbf{SAT}^C$ does not collapse to a 1-degree. However, relative to C, the $\mathbf{IC}_{1-\mathrm{li}}$ *does* hold.

What about an oracle relative to which the **IC** is true? This eluded researchers for quite a while. Finally, Fenner, Fortnow, and Kurtz [FFK92] proved that, relative to a *symmetric perfect generic* oracle A, the **IC** holds. They do this by showing that the m-degree of $\mathbf{SAT}^A$ collapses to a 1-li-degree and then, because they also show that one-way functions do not exist relative to A, the 1-li-degree collapses to an isomorphism type.

In this paper, we demonstrate an oracle relative to which there are one-way functions but *every* paddable 1-li-degree collapses. Thus, for the first time, we have a relativized world where one-way functions exist but the Joseph-Young Conjecture fails: All of the k-creative languages K_k^f are isomorphic to **SAT**.

We then combine this result with a modified version of the proof of Fenner, Fortnow, and Kurtz to derive an oracle relative to which the **IC** holds but one-way functions exist. This answers an open question posed by Fenner, Fortnow, and Kurtz [FFK92] and completes the line of research whose history is sketched above. Collectively, these results show that *any* proof of a relationship between the **IC** and the existence of one-way functions cannot be relativizable. As most complexity theory proofs relativize, it seems we will need new techniques to attack this problem.

We should mention that, despite the results here and in [FFK92], most researchers in this area believe that the **ECSC** is true and so that the **IC** is false.

2 Definitions

We assume familiarity with the function class **FP** and the complexity classes **P**, **UP**, **FewP**, **NP**, **PSPACE**, **EXP** and **NEXP**. The definitions that follow are standard or are taken from [FFK92, FFKL93, FR93].

Let $\Sigma = \{0,1\}$. Languages and oracles are subsets of Σ^*. Σ^n denotes the set of all strings of length n. For two oracles A and B, $A \oplus B$ denotes the *join* of A and B, that is, the language $\{x0 : x \in A\} \bigcup \{x1 : x \in B\}$. An oracle S is *sparse* if there is a polynomial p such that $|S \cap \Sigma^n| \leq p(n)$. Let $L(M)$ denote the language accepted by Turing machine M.

A function $f \in \mathbf{FP}$ from Σ^* to Σ^* is a *reduction* from a language A to a language B ($f : A \leq B$) if $x \in A \iff f(x) \in B$. It is *one-to-one and honest* (1-h) if it is one-to-one and there is a polynomial p such that $p(|f(x)|) > |x|$. It is *one-to-one and length-increasing* (1-li) if it is one-to-one and $|f(x)| > |x|$. It is *invertible* if it is one-to-one and there is a $g \in \mathbf{FP}$ from Σ^* to Σ^* such that $g(f(x)) = x$. It is an *isomorphism* if it is one-to-one, onto, and invertible. It is *one-way* if it is one-to-one, honest, and not invertible. Note that one-way functions exist if and only if $\mathbf{P} \neq \mathbf{UP}$ [GS88].

If a type of reduction possesses transitive closure (as all of the above do), we can define an equivalence relation under which two languages are equivalent if each is reducible to the other by that type of reduction. We call the equivalence classes *degrees*. If the reductions are isomorphisms, we call the degree an isomorphism type. We say that a degree $\mathbf{a}$ of one sort *collapses* to a degree $\mathbf{b}$ of a different sort if $\mathbf{b} \subset \mathbf{a}$ and every pair of languages in $\mathbf{a}$ is also in $\mathbf{b}$. If $\mathbf{b}$ is an isomorphism type, we simply say that $\mathbf{a}$ collapses.

A language A is *paddable* iff there exists $p(\cdot,\cdot)$, a polynomial-time padding function, that is 1-li, invertible in both arguments, and, for all x and y, $x \in A \iff p(x,y) \in A$. A degree is paddable if it contains a paddable language.

Let g be the function from integers to integers with the following recursive definition: $g(0) = 2$, $g(n+1) = 2^{g(n)}$. A language A is *gappy* iff, whenever $x \in A$, $|x| = g(n)$, for some $n \in \omega$. We will call those lengths equal to $g(n)$ for some n *allowed lengths*.

A *Cohen condition* is a partial characteristic function from Σ^* to Σ whose domain is finite. A condition σ *extends* another condition τ ($\sigma \supseteq \tau$) iff, for all $x \in \mathrm{dom}(\tau)$, $\sigma(x) = \tau(x)$. Two conditions σ and τ are *consistent* iff, for all $x \in \mathrm{dom}(\sigma) \cap \mathrm{dom}(\tau)$, $\sigma(x) = \tau(x)$. They *conflict* otherwise. A **UP** *condition* σ is a Cohen condition whose domain is gappy and such that, for all n, $|\{y \in \Sigma^n : \sigma(y) = 1\}| \leq 1$.

A sequence $\{a\}_{i\in\omega}$ of integers forms an *iterated-polynomial* sequence if there exists a polynomial p such that $p(n) \geq n^2$ for all n, $a_0 \geq 2$, and $a_{i+1} = p(a_i)$ for all i. A *symmetric perfect forcing condition* (*sp-condition*) σ is a partial characteristic function from Σ^* to Σ for which there is an iterated-polynomial sequence $\langle a_i \rangle_{i\in\omega}$ such that

$$(\bigcup_{i\in\omega} \Sigma^{a_i}) \cap \mathrm{dom}(\sigma) = \emptyset$$

In other words $\sigma(x)$ is undefined for all x such that $|x| = a_i$ for some $i \in \omega$. Note that σ may be undefined elsewhere as well.

A set of sp- or **UP**-conditions S is *dense* if, for every sp- or **UP**-condition σ, there is a string τ in S that extends σ. An oracle G is *sp- or* **UP***-generic* if it meets all dense, definable sets of sp- or **UP**-conditions. That sp- and **UP**-generic sets exist follows from [FFK92] and [FFKL93].

3 Results

In this section, we construct an oracle relative to which the Isomorphism Conjecture is true and there are one-way functions. The proof is in three major parts.

We first show in theorem 3.2 and corollary 3.4 that, relative to $D \oplus G$, where D is any oracle relative to which one-way functions do not exist and G is $\mathbf{UP}^D$-generic, one-way functions exist but every paddable 1-li-degree collapses to an isomorphism type. We then show in theorem 3.9 that, relative to $A \oplus S$, where A is an sp-generic oracle and S is any sparse oracle, the m-degree of **SAT** collapses to a 1-li-degree.

Combining these yields the main theorem:

Theorem 3.1 *There is an oracle relative to which the Isomorphism Conjecture holds but there are one-way functions.*

Proof. Let $C = A \oplus G$, where A is an sp-generic and G is a $\mathbf{UP}^A$-generic. G is sparse so, by theorem 3.9, the m-degree of $\mathbf{SAT}^C$ collapses to a 1-li-degree. Fenner, Fortnow, and Kurtz [FFK92] showed that $\mathbf{P}^A = \mathbf{UP}^A$ so, by corollary 3.4, $\mathbf{P}^C \neq \mathbf{UP}^C$ and every paddable 1-li-degree collapses. Because the m-degree of $\mathbf{SAT}^C$ is a 1-li-degree and $\mathbf{SAT}^C$ is paddable, the m-degree of $\mathbf{SAT}^C$ collapses. ■

3.1 Every paddable 1-li-degree collapses and $\mathbf{P} \neq \mathbf{UP}$

To get this result, we use a **UP**-generic oracle G, relative to which one-way functions exist [FR93]. G is sparse so, relative to $A \oplus G$, where A is sp-generic, the m-degree of $\mathbf{SAT}^{A\oplus G}$ is a 1-li-degree. But how do these one-way functions affect the collapse of this 1-li-degree? By [KLD86], they are sufficient to prevent the collapse of some 1-li-degree. As the following shows, though, they cannot prevent the collapse of *paddable* 1-li-degrees.

Theorem 3.2 *Assume that* $\mathbf{P} = \mathbf{UP}$*. Then relative to a* $\mathbf{UP}$*-generic oracle* G*, there are one-way functions but every paddable 1-li-degree collapses to an isomorphism type.*

Proof. Fix G, a $\mathbf{UP}$-generic. Fortnow and Rogers [FR93] showed that $\mathbf{P}^G \neq \mathbf{UP}^G$. Fix a language S that is paddable with respect to G. In fact, we may assume that S has two padding functions, $p_{S,0}$ and $p_{S,1}$, with disjoint ranges. (Given a padding function p_S for S, let $p_{S,i}(x, y) = p_S(x, yi)$.) Fix a language T that is 1-li-equivalent to S relative to G and let $f \in \mathbf{FP}^G$ 1-li-reduce S to T and $g \in \mathbf{FP}^G$ 1-li-reduce T to S.

Fix a pair of inputs u and q. For f and any input x, there is at most one string in G that can affect the invertibility of that computation. All other strings in G are either exponentially shorter, and so can be enumerated by a function trying to invert $f(x)$, or exponentially longer, and so cannot be queried by $f(x)$. We call that string, if it exists, the "cookie."

Knowing the "cookie" for a particular computation $f(x)$ allows us to invert the computation. An inverting function enumerates the shorter strings in the oracle and thus knows every string in the oracle that can affect $f(x)$. It then asks the question "Relative to this finite initial segment of the oracle, what is the inverse of $f(x)$?" This question is in unrelativized $\mathbf{UP}$ which, by assumption, is equal to $\mathbf{P}$.

We will now construct a padding function p_T for T by showing how to compute $p_T(u, q)$ and then demonstrate that it is, indeed, a padding function. Let $v = g(u)$, $v' = p_{S,0}(v, q)$, and $x = f(v')$. (Please see figure 1 on page 7.) Let c be the "cookie," if it exists. There are two cases:

1. The computation $f(v')$ does not query c in G. Then let $p_T(u, q) = x$.

2. The computation $f(v')$ *does* query c in G. Let $y = g(x)$. There are two subcases:

   (a) The computation $f \circ p_{S,1}(y, \epsilon)$ queries c in G. Then let $p_T(u, q) = x$.

   (b) The computation $f \circ p_{S,1}(y, \epsilon)$ does not query c in G. Let c' be the unique proper prefix of c such that $f \circ p_{S,1}(y, c')$ does not query c in G but at least one of the computations $f \circ p_{S,1}(y, c'0)$ or $f \circ p_{S,1}(y, c'1)$ does, if such a prefix exists. Otherwise, let $c' = c$. Then let $p_T(u, q) = f \circ p_{S,1}(y, c')$.

Because p_T is the composition of reductions and padding functions, for all x and y, $x \in T \iff p_T(x, y) \in T$.

Claim 1. p_T is 1-li.

Proof of claim. The cases above are mutually exclusive and exhaustive so every pair of inputs falls into exactly one case. On all pairs of inputs u and q that fall into case 1 or case 2a, $p_T(u, q)$ is $f \circ p_{S,0}(g(u), q)$, which is clearly 1-li. On all pairs of inputs that fall into case 2b, $p_T(u, q)$ is $f \circ p_{S,1}(g \circ f \circ p_{S,0}(g(u), q), c')$, which is also clearly 1-li.

Because the ranges of $p_{S,0}$ and $p_{S,1}$ are disjoint, the range of p_T on elements in cases 1 and 2a is disjoint from the range of p_T on elements in case 2b. ■Claim 1.

Claim 2. p_T is invertible.

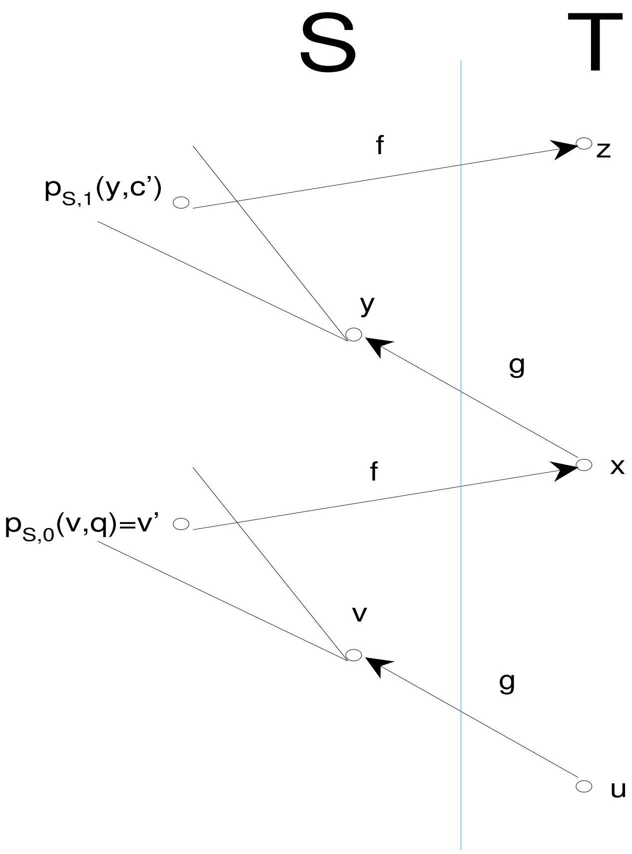

Figure 1: The chains and padding trees used in building p_T (See proof of theorem 3.2).

Proof of claim. Let w be in the range of p_T. Let $y' = f^{-1}(w)$. If $f(y') = w$ and the computation $f(y')$ does not query c then we are either in case 1 or case 2b.

If $y' = p_{S,0}(y,q)$, for some y and some q, then we are in case 1 so $w = p_T(g^{-1}(y), q)$.

If $y' = p_{S,1}(y,c')$, for some y and some c', then we are in case 2b so c' is a prefix of c. Let $x = g^{-1}(y)$. Now, either $c' = c$ or we can run f on $p_{S,1}(y, c'0)$ and $p_{S,1}(y, c'1)$ to discover c. Knowing c allows us to compute $f^{-1}(x)$, which will be of the form $p_{S,0}(v,q)$ and so $w = p_T(g^{-1}(v), q)$.

If $f(y') \neq w$ or the computation $f(y')$ queried c then we are in case 2a. So running f with the input $p_{S,1}(g(w), \epsilon)$ will find c. Knowing c now allows us to calculate $f^{-1}(w)$ correctly. ■Claim 2.

Because S and T both have padding functions and are in the same 1-li-degree, they are isomorphic [BH76]. ■

For the first time, we now have that:

Corollary 3.3 *There is an oracle relative to which there are one-way functions but the Joseph-Young Conjecture fails.*

Because the proof of theorem 3.2 relativizes, we have:

Corollary 3.4 *For every oracle A and $\mathbf{UP}^A$-generic oracle G, if $\mathbf{P}^A = \mathbf{UP}^A$ then, relative to $A \oplus G$, every paddable 1-li-degree collapses.*

This corollary and the fact that $\mathbf{P}^G \neq \mathbf{UP}^G$ have some interesting implications and we will digress briefly to investigate them.

In [KLD87], they show that if one-way functions exist then there is a 1-li-degree that does not collapse. Theorem 3.2 implies that there is no relativizable way to extend their technique (which relativizes) to show that the noncollapsing degree is paddable.

We also have:

Corollary 3.5 *There is an oracle relative to which the complete m-degree of* **EXP** *collapses and there are one-way functions.*

Proof. Berman [Ber77] showed that the m-degree of **EXP** collapses absolutely to a paddable 1-li-degree. Let $C = H \oplus G$, where H is an oracle making $\mathbf{P} = \mathbf{PSPACE}$ and G is a **UP**-generic oracle. Then the complete 1-li-degree of $\mathbf{EXP}^C$ collapses but there are still one-way functions. ■

With this corollary, we now have relativizations realizing all three possible states of affairs between the **IC** for **EXP** and the existence of one-way functions. There are only three states because the m-degree of **EXP** is a 1-li-degree so there cannot be an oracle relative to which there are no one-way functions but the **IC** fails for **EXP**.

Corollary 3.6 *Assume that $\mathbf{P} = \mathbf{PSPACE}$. Then relative to a* **UP**-*generic oracle G, there are one-way functions but every paddable 1-degree collapses to an isomorphism type.*

Proof sketch. Relative to G, one-way functions exist. Let S and T be languages such that S is paddable by $p(\cdot,\cdot)$ and let f and g be polynomial-time functions such that f 1-reduces S to T and g 1-reduces T to S relative to G. Because S is paddable, we may assume that g is 1-li-invertible.

To see that S is 1-li-reducible to T, fix a string x. Let y_0 be the least y such that $|f(p(x,y)| > |x|$. Such a y_0 must exist and be lexicographically less than or equal to $1^{|x|+1}$ because there are at most $2^{|x|+1} - 1$ strings of length $|x|$ or less and f is one-to-one. This procedure is in unrelativized **PSPACE** and so, by the assumption, can be done in polynomial time.

Now we can apply theorem 3.2 to collapse these 1-li-degrees in the presence of one-way functions. ■

Corollary 3.7 *There is an oracle relative to which the complete m-degrees of* **RE** *and* **NEXP** *collapse and there are one-way functions.*

Proof. Dowd [Dow] showed that the complete m-degree of **RE** collapses absolutely to a 1-degree and Ganesan and Homer [GH89] showed the same for **NEXP**. As these proofs relativize, applying corollary 3.6 yields the results. ■

3.2 The m-degree of SAT is a 1-li-degree

Here we show that the m-degree of $\mathbf{SAT}^C$ collapses to a 1-li-degree, where $C = A \oplus S$, A is an sp-generic oracle, and S is any sparse oracle. We do this by performing some straightforward modifications to the proof in [FFK92] that, relative to an sp-generic A, the m-degree of $\mathbf{SAT}^A$ collapses to a 1-li-degree. In that paper, they also show that there are no one-way functions relative to A so the 1-li-degree collapses to an isomorphism type.

In fact, they show that $\mathbf{P}^A = \mathbf{FewP}^A$. Their proof relies on this to get the m-degree to collapse to a 1-li-degree. As we *want* one-way functions, we cannot rely on this assumption and our proof shows that this assumption is not needed. This comes at a cost: Our proof relies heavily on the presence or absence of strings of a particular form in the oracle while the older proof does not.

Fix an m-reduction f and a language L such that f^C m-reduces $\mathbf{SAT}^C$ to L. As in [FFK92], we show in the following lemma that there exists a function $g \in \mathbf{FP}^C$ that also m-reduces $\mathbf{SAT}^C$ to L but in addition is length-increasing and many-to-one only on instances in $\mathbf{SAT}^C$ and even then that there is a polynomial bounding how many elements in $\mathbf{SAT}^C$ g maps to a particular element in L.

Lemma 3.8 *Let A be an sp-generic oracle and S any sparse oracle. Let $C = A \oplus S$. If f is a function in $\mathbf{FP}^C$ and M a machine in $\mathbf{NP}^C$ such that $f^C : \mathbf{SAT}^C \leq_m^p L(M^C)$, there exists a function $g \in \mathbf{FP}^C$ such that:*

1. *g^C m-reduces $\mathbf{SAT}^C$ to $L(M^C)$;*
2. *g^C is length-increasing;*
3. *If there exist $\varphi_0, \varphi_1 \in \mathbf{SAT}^C$ such that $\varphi_0 \neq \varphi_1$ and $g^C(\varphi_0) = g^C(\varphi_1) = q$ then*
   (a) *$||\{\psi : f^C(\psi) = q\}|| > 1$;*
   (b) *$q \in L(M^C)$;*
   (c) *$g^C(\varphi_0)$ queries at least one string of the form $\langle \varphi_1, w, y, 1\rangle$ or $\langle \varphi_1, w, y, 2\rangle$.*

Proof. Please see the Appendix.

Now we use lemma 3.8 twice to go from an m-reduction f to a 1-li-reduction $\mathbf{g}$.

Theorem 3.9 *Let A be an sp-generic oracle and S any sparse oracle. Let $C = A \oplus S$. The m-degree of $\mathbf{SAT}^C$ collapses to a 1-li-degree.*

Proof. Let f be a function in $\mathbf{FP}^C$ and M a machine in $\mathbf{NP}^C$ such that f m-reduces $\mathbf{SAT}^C$ to $L(M^C)$. Apply lemma 3.8 to get a g with the desired properties. Let

$$U = \{\varphi : (\exists \psi)\psi \neq \varphi \ \& \ g^C(\psi) = g^C(\varphi)\}$$

Claim. $U \in \mathbf{P}^C$.

Proof of claim. Fix a formula φ. Compute $g^C(\varphi)$ and record the output q and the list of all $\psi \neq \varphi$ such that $g^C(\varphi)$ makes a query of the form $\langle \psi, w, y, 1\rangle$ or $\langle \psi, w, y, 2\rangle$. Next, run g^C on each of these ψ. If any of these computations yields q then $\varphi \in U$. If none do then, by item 3c of lemma 3.8, there is no $\psi \neq \varphi$ such that $g^C(\psi) = q$ so $\varphi \notin U$. Clearly, this procedure is polynomial-time relative to C. ■Claim

Fix θ, a true formula in $\mathbf{SAT}^C$. Let $\hat{f}$ be the function defined by:

$$\hat{f}^C(\varphi) = \begin{cases} g^C(\theta) & \text{if } \varphi \in U \\ g^C(\varphi) & \text{otherwise} \end{cases}$$

By the definition of g and the claim $\hat{f}$ is clearly in $\mathbf{FP}^C$ and a reduction from $\mathbf{SAT}^C$ to $L(M^C)$.

Apply lemma 3.8 to $\hat{f}$ to get $\hat{g}$. By the definition of $\hat{f}$ and the properties of $\hat{g}$, the only element of $L(M^C)$ on which $\hat{g}$ is not one-to-one is $g^C(\theta) = q$. Because $\hat{g}$ is length-increasing, all of the strings that map to q are shorter than it. Let p be a padding function for $\mathbf{SAT}^C$. Let $\mathbf{g}^C(\varphi) = \hat{g}^C(p(\varphi, q))$. This has the effect of mapping every element into a region on which $\hat{g}$ is one-to-one. One can then see that $\mathbf{g}^C$ is a 1-li reduction from $\mathbf{SAT}^C$ to $L(M^C)$. ■

As noted above, there are no one-way functions relative to A so if S is an oracle relative to which there are no one-way functions the m-degree of $\mathbf{SAT}^C$ collapses, yielding a different proof than the one given in [FFK92].

4 Conclusions and open problems

The one-way functions considered here are extremely weak. The ones considered in [KMR89], scrambling and annihilating functions, are extremely powerful. The gap between them seems enormous. A natural question is: How much power must one-way functions possess to make the IC fails?

Here we have all paddable 1-li-degrees collapsing. Is it the case that if the 1-li-degree of **SAT** collapses then all of the paddable 1-li-degrees collapse? Also, if the Isomorphism Conjecture holds for **NP**, must it also hold for **EXP**?

Acknowledgements

The introduction of this paper owes much to the account in the introduction of [KMR89].

I especially thank Stuart Kurtz, my advisor, and Lance Fortnow for presenting this problem to me and engaging in numerous fruitful and (more importantly) encouraging discussions about it.

References

[Ber77] L. Berman. *Polynomial reducibilities and complete sets.* PhD thesis, Cornell University, 1977.

[BH76] L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. In *Proceedings of the 8th ACM Symposium on the Theory of Computing*, pages 30–40. ACM, New York, 1976.

[BH77] L. Berman and J. Hartmanis. On isomorphism and density of NP and other complete sets. *SIAM Journal on Computing*, 1:305–322, 1977.

[Dow] M. Dowd. On isomorphism. Unpublished manuscript, 1978.

[FFK92] S. Fenner, L. Fortnow, and S. Kurtz. The isomorphism conjecture holds relative to an oracle. In *Proceedings of the 33rd IEEE Symposium on Foundations of Computer Science*, pages 30–39. IEEE, New York, 1992.

[FFKL93] S. Fenner, L. Fortnow, S. Kurtz, and L. Li. An oracle builder's toolkit. In *Proceedings of the 8th IEEE Structure in Complexity Theory Conference*, pages 120–131. IEEE, New York, 1993.

[FR93] L. Fortnow and J. Rogers. Separability and one-way functions. Technical Report CS 93-14, University of Chicago Department of Computer Science, 1993.

[GG86] J. Geske and J. Grollmann. Relativizations of unambiguous and random polynomial time classes. *SIAM Journal on Computing*, 15(2):511–519, 1986.

[GH89] K. Ganesan and S. Homer. Complete problems and strong polynomial reducibilities. In *Proceedings of STACS '89*, volume 349 of *Lecture Notes in Computer Science*, pages 240–250. Springer, 1989.

[GS88] J. Grollmann and A Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17:309–355, 1988.

[HH91] J. Hartmanis and L. Hemachandra. One-way functions and the nonisomorphism of NP-complete sets. *Theoretical Computer Science*, 81(1):155–163, 1991.

[JY85] D. Joseph and P. Young. Some remakrs on witness functions for poynomial reducibilities 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*, pages 263–276, 1986.

[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.

[KMR89] S. Kurtz, S. Mahaney, and J. Royer. The isomorphism conjecture fails relative to a random oracle. In *Proceedings of the 21st ACM Symposium on the Theory of Computing*, pages 157–166. ACM, New York, 1989.

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

[Rac82] C. Rackoff. Relativized questions involving probablistic algorithms. *Journal of the ACM*, 29(1):261–268, 1982.

[Sel92] Alan Selman. A survey of one way functions in complexity theory. *Mathematical Systems Theory*, 25:203–221, 1992.

Appendix A: Proofs

Lemma 3.8. *Let A be an sp-generic oracle and S any sparse oracle. Let $C = A \oplus S$. If f is a function in $\mathbf{FP}^C$ and M a machine in $\mathbf{NP}^C$ such that $f^C : \mathbf{SAT}^C \leq_m^p L(M^C)$, there exists a function $g \in \mathbf{FP}^C$ such that:*

1. *$g^C : \mathbf{SAT}^C \leq_m^p L(M^C)$;*
2. *g^C is length-increasing;*
3. *If there exist $\varphi_0, \varphi_1 \in \mathbf{SAT}^C$ such that $\varphi_0 \neq \varphi_1$ and $g^C(\varphi_0) = g^C(\varphi_1) = q$ then*
   - *(a) $||\{\psi : f^C(\psi) = q\}|| > 1$;*
   - *(b) $q \in L(M^C)$;*
   - *(c) $g^C(\varphi_0)$ queries at least one string of the form $\langle \varphi_1, w, y, 1\rangle$ or $\langle \varphi_1, w, y, 2\rangle$.*

To understand this lemma and its proof, we refer to a number of notions and objects defined in [FFK92] and which we briefly review here.

1. For any sp-condition τ_0, there is an iterated polynomial sequence $\{a_i\}_{i\in\omega}$ on which it is not defined. When we extend it in proofs below to another sp-condition σ_0, we derive two iterated polynomial subsequences from τ_0. The first we call $\{b_i\}_{i\in\omega}$ and the second $\{d_i\}_{i\in\omega}$. In creating σ_0, we only perform coding on the strings whose lengths fall into the d_i sequence. Strings whose lengths fall into the b_i sequence are left undefined and so this becomes the iterated polynomial sequence for σ_0.

2. Let $\langle\cdot\rangle$ be a multi-arity pairing functions whose range is only strings whose length is some d_i.

3. Whenever we say $x \in A$, relative to an sp-generic joined to another oracle S, we mean $x0 \in C$.

4. Let h, r, and s be the following functions on relativized propositional formulae:

   (a) $h(\varphi, w) = (\varphi \;\&\; \exists y\langle\varphi, w, y, 1\rangle \in A) \;\vee\; \exists y\langle\varphi, y, 0\rangle \in A$;

   (b) $r(\varphi) = \exists w(\exists y\langle\varphi, w, y, 1\rangle \in A \;\&\; \mathbf{f}^C(h(\varphi, w))$ is good);

   (c) $s(\varphi) = (\varphi \;\&\; r(\varphi)) \;\vee\; \exists y\langle\varphi, y, 0\rangle \in A$.

   Note that none of these functions rely on the oracle.

We need to rely on the following technical lemma. A version whose item (a.) does not refer to relativizations to sparse oracles is proven in [FFK92] as Lemma 5.3.

Lemma. *Let S be a sparse oracle. There is a way to set σ_0 on the strings of length $\langle d_j\rangle_{j\in\omega}$ such that*

a. *σ forces "For every formula φ, $r(\varphi)$ is true relative to S."*

b. *For every φ and w there is exactly one y such that $\sigma(\langle\varphi, w, y, 1\rangle) = 1$.*

c. *For every φ and y, $\sigma(\langle\varphi, y, 0\rangle) = 0$.*

d. *For all φ, y, and w, $\sigma(\langle\varphi, w, y, 1\rangle) = \sigma(\langle\varphi, w, y, 2\rangle)$.*

The proof in [FFK92] does not refer to the sparse oracle but the proof can easily be adapted because the Kolmogorov argument used to prove item (a.) there can be slightly changed to take into account a sparse number of additional strings at every length. ■

Proof of lemma 3.8. Items 1, 2, 3a, and 3b can be proven in essentially the same way they were proven in [FFK92] because they only rely on the fact that the above technical lemma is true.

Item 3c. $g^C(\varphi_0)$ queries at least one string of the form $\langle\varphi_1, w, y, 1\rangle$ or $\langle\varphi_1, w, y, 2\rangle$. Recall that $g^C(\varphi_0) = g^C(\varphi_1) = q$.

Assume that $g^C(\varphi_0)$ does not query any string of the form $\langle\varphi_1, w_1, y_1, 1\rangle$ or $\langle\varphi_1, w_1, y_1, 2\rangle$.

1. $g^C(\varphi_0) = \mathbf{f}^C \circ h(\varphi_0, w_0) = q = g^C(\varphi_1) = \mathbf{f}^C \circ h(\varphi_1, w_1)$: Find a y such that neither $g^C(\varphi_0)$ nor $g^C(\varphi_1)$ queries $\langle\varphi_0, y, 0\rangle$. Let B be the oracle formed by adding $\langle\varphi_0, y, 0\rangle$ and removing all strings of the form $\langle\varphi_1, w_1, y_1, 1\rangle$. Clearly B extends τ.

   We know that $q = \mathbf{f}^C \circ h(\varphi_0, w_0)$. By assumption, $g^C(\varphi_0)$ does not query any of the strings that have been removed so $\mathbf{f}^C \circ h(\varphi_0, w_0)$ does not either. Thus, $\mathbf{f}^C \circ h(\varphi_0, w_0) = \mathbf{f}^B \circ h(\varphi_0, w_0)$.

   As $g^C(\varphi_0)$ does not query any string of the form $\langle\varphi_1, w, y, 2\rangle$, neither does $\mathbf{f}^B \circ h(\varphi_0, w_0)$. So $f^B \circ h(\varphi_0, w_0)$ does not query any string of the form $\langle\varphi_1, w, y, 1\rangle$. Thus, $\mathbf{f}^B \circ h(\varphi_0, w_0) = f^B \circ h(\varphi_0, w_0)$ and so $f^B \circ h(\varphi_0, w_0) = q$ and $h(\varphi_0, w_0)$ is true relative to B.

We also know that $q = \mathbf{f}^C \circ h(\varphi_1, w_1)$. By the definition of A, g, and $\mathbf{f}$, $\mathbf{f}^C \circ h(\varphi_1, w_1)$ is good so $\mathbf{f}^C \circ h(\varphi_1, w_1) = \mathbf{f}^B \circ h(\varphi_1, w_1)$ and $\mathbf{f}^B \circ h(\varphi_1, w_1) = f^B \circ h(\varphi_1, w_1)$. So $f^B \circ h(\varphi_1, w_1) = q$ and $h(\varphi_1, w_1)$ is false relative to B.

But now we have B, an oracle extending τ, relative to which f is not a reduction, a contradiction.

2. $g^C(\varphi_0) = \mathbf{f}^C \circ h(\varphi_0, w_0) = q = g^C(\varphi_1) = f^C \circ s(\varphi_1)$: Find a y such that neither $g^C(\varphi_0)$ nor $g^C(\varphi_1)$ queries $\langle \varphi_0, y, 0\rangle$. Let S be the set computed in step 1 of the computation for $g^C(\varphi)$. Let B be the oracle formed by adding $\langle \varphi_0, y, 0\rangle$ and removing all strings of the form $\langle \varphi_1, w_1, y_1, 1\rangle$, such that $w_1 \notin S$.

   Using the same argument as above, we get that $f^B \circ h(\varphi_0, w_0) = q$ and $h(\varphi_0, w_0)$ is true relative to B.

   We know that $f^C \circ s(\varphi_1) = q$. Assume that $r(\varphi_1)$ (and so $s(\varphi_1)$) is false relative to B. Because $f^C \circ s(\varphi_1)$ does not query any string of the form $\langle \varphi_1, w_1, y_1, 1\rangle$ for $w_1 \notin S$, $f^C \circ s(\varphi_1) = f^B \circ s(\varphi_1)$. So we have that $f^B \circ s(\varphi_1) = q$ and $s(\varphi_1)$ is false relative to B.

   Assume that $r(\varphi)$ is true relative to B. Then, for some $w \in S$, $\mathbf{f}^B \circ h(\varphi_1, w)$ is good. But then, because we did not remove any strings of the form $\langle \varphi_1, w', y, 2\rangle$ to create B, $\mathbf{f}^C \circ h(\varphi_1, w)$ is also good. But this contradicts the assumption that $g^C(\varphi_1) = f^C \circ s(\varphi_1)$.

   We either get a contradiction about g's behavior or, as above, we find a way of extending τ that forces f not to be reduction, also a contradiction.

3. $g^C(\varphi_0) = f^C \circ s(\varphi_0) = q = g^C(\varphi_1) = \mathbf{f}^C \circ h(\varphi_1, w_1)$.

4. $g^C(\varphi_0) = f^C \circ s(\varphi_0) = q = g^C(\varphi_1) = f^C \circ s(\varphi_1)$.

   These last two cases are handled similarly to the previous two.

■