One-Way Functions and the Berman-Hartmanis Conjecture

Manindra Agrawal[†]
Dept. of Computer Science
IIT Kanpur
Kanpur, India
Email: manindra(at)iitk.ac.jp

Osamu Watanabe
Dept. of Math. & Comp. Sci.
Tokyo Inst. of Tech.
Tokyo, Japan
Email: watanabe(at)is.titech.ac.jp

***Abstract*—The Berman-Hartmanis conjecture states that all NP-complete sets are P-isomorphic each other. On this conjecture, we first improve the result of [3] and show that all NP-complete sets are $\le^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}}$-reducible to each other based on the assumption that there exist regular one-way functions that cannot be inverted by randomized polynomial-time algorithms. Secondly, we show that, besides the above assumption, if all one-way functions have some easy part to invert, then all NP-complete sets are P/poly-isomorphic to each other.**

***Index Terms*—average-case one-way function; P-isomorophism conjecture; P/poly-isomorophism in NP; one-way function with easy cylinder**

I. Introduction

Berman and Hartmanis [4] conjectured that all sets complete for NP under polynomial-time many-one reductions are P-isomorphic to each other. This conjecture has attracted a lot of attention with evidence available for both possible answers to it (see some good survey papers [12], [15]). On the positive side, Berman and Hartmanis showed [4] that NP-complete sets known at the time were all P-isomorphic to each other. Also, in [1], [2] it was shown that all complete sets for NP under AC^0-reductions are isomorphic to each other via AC^0-computable isomorphisms proving the conjecture for a weaker class of reductions. On the negative side, Joseph and Young [11] (also see [14]) argued, in essence, that for a one-one, length-increasing one-way function f, SAT and $f(\mathrm{SAT})$ are unlikely to be P-isomorphic since it is not clear how to construct an invertible reduction from SAT to $f(\mathrm{SAT})$. Also, Kurtz et al showed [13] that relative to a random oracle this is indeed true. On the whole, there is more belief that the conjecture is false. The reason is the widely believed existance of strong one-way functions coupled with the argument of Joseph and Young. Another interesting relationship between one-way functions and the structure of NP-complete degree was observed in [3] that used the existance of special kind of one-way functions (one-way *permutations*) to show that all many-one complete sets for NP are also one-one and length-increasing complete under $\mathrm{P/poly}$-computable reductions. (Note also that similar structural properties have been studied and in fact (partially) proved for higher classes such as EXP, and so on (see, e.g., [5] for a recent result). We, however, discuss in this paper mainly the P-isomorphism conjecture for NP-complete sets as proposed by Berman and Hartmanis; for this reason, we use the "Berman-Hartmanis Conjecture" for the title of this paper.)

In this paper, we show two results. Firstly, we improve the result of [3]: instead of one-way *permutations* that cannot be inverted by $\mathrm{P/poly}$-functions, we prove it is enough to assume the existence of *regular* one-way functions that cannot be inverted by randomized polynomial-time algorithms to obtain the same result. Regular one-way functions are a generalization of one-way permutations in which every image of a particular length has the same number of pre-images. (We can also show the same result from one-way functions whose pre-image size is polynomial-time computable.) A consequence of this result is the complete description of the structure of many-one complete sets of NP relative to a random oracle: all these sets are complete under one-one and length-increasing polynomial-time reductions but (as already shown in [13]) they are not P-isomorphic.

Our second result is on a certain easy structure of one-way functions. We first observe that the known one-way functions have *easy cylinders*: they all have small but dense subsets that are easily identifiable and on which the functions are easily invertible (a more formal definition will be given in section IV). Then we show that if all one-one, length-increasing, and $\mathrm{P/poly}$-computable functions have easy cylinders, then any one-one, length-increasing, and $\mathrm{P/poly}$-reduction from some canonical NP-complete set can be converted to a one-one and length-increasing reduction that is both computable and invertible in $\mathrm{P/poly}$.

The above two results show an interesting phenomenon: the Isomorphism Conjecture, in a slightly weaker form (isomorphisms are required to be $\mathrm{P/poly}$-computable instead of polynomial-time computable) is true if there exist one-way functions of a certain strength but no stronger. We conjecture that this is indeed the case, and hence, the weaker form of Isomorphism Conjecture is true.

The paper is organized as follows. The next section gives the definitions we use. Section III proves the first result and section IV proves the second result.

[†] This work was primarily done while visiting Tokyo Inst. of Tech. during summers 2008.

II. Preliminaries

Throughout this paper, we use n to denote an integer ≥ 0. We fix our alphabet to $\Sigma = \{0,1\}$, and we assume (unless explicitly stated otherwise) that all functions are total functions over Σ^*. Also we assume that input length determines output length; that is, each function f has some *length function* ℓ such that $|f(x)| = \ell(n)$ for all $n \geq 0$ and all $x \in \Sigma^n$. For any function f with length function ℓ, and for any $y \in \Sigma^{\ell(n)}$, by $f^{-1}(y)$ we mean the set of strings x such that $y = f(x)$ holds. The one-wayness notion considered in this paper is now defined precisely as follows.

Definition 1. A function f is a *$s(\cdot)$-secure one-way function* if (1) f is a polynomial-time computable function and (2) the following holds[1] for every polynomial-time randomized Turing machine M and for all sufficiently large n:

$$\Pr_{x \in_{\mathrm{U}} \Sigma^n}\left[\, M(f(x)) \in f^{-1}(f(x)) \cap \Sigma^n \,\right] \;<\; \frac{1}{s(n)}.$$

Definition 2. A function g is a *$s(\cdot)$-secure pseudo-random generator* if (1) g is polynomial-time computable, (2) its length function ℓ satisfies $\ell(n) > n$ for all n, and (3) the following holds for every polynomial-time randomized Turing machine M and for all sufficiently large n:

$$\left|\; \Pr_{y \in_{\mathrm{U}} \Sigma^{\ell(n)}}[\, M(y) = 1\,] - \Pr_{x \in_{\mathrm{U}} \Sigma^n}[\, M(g(x)) = 1\,] \;\right| \;<\; \frac{1}{s(n)}.$$

We will use a universal hash function family, and here we define the following standard one. Let $\mathcal{H} = \{\mathrm{H}_{n,m}\}_{n,m\geq 1}$, where $\mathrm{H}_{n,m} : \Sigma^n \times \Sigma^{(n+1)m} \mapsto \Sigma^m$, be defined as $\mathrm{H}_{n,m}(x,r) = x_+ \cdot r$, where r is a $(n+1) \times m$ matrix over F_2 (the Galois field of two elements), x_+ is a $1 \times (n+1)$ vector over F_2 obtained from x by padding 1 to its end, and $\cdot$ is the matrix multiplication operator. Let $s(n,m) = (n+1)m$, and we will identify each $(n+1) \times m$ matrix r with its corresponding string r of length $s(n,m)$. (In the following, we will sometimes use r longer than $s(n,m)$ bits, in which case we assume that its prefix of appropriate length is used.) Clearly this hash function family is polynomial-time computable and it satisfies the property required for a *pair-wise independent universal hash function family*. That is, the following holds.

Lemma 1. For any $n, m \geq 1$ and any fixed two $x \neq x'$, $|x| = |x'| = n$, two function values $\mathrm{H}_{n,m}(x,R)$ and $\mathrm{H}_{n,m}(x',R)$ defined by a random variable $R \in_{\mathrm{U}} \Sigma^{s(n,m)}$ are random variables that are independently and uniformly distributed over Σ^m.

From this property, we can also prove another important property of a pair-wise independent universal hash function family, which is usually referred as "Leftover Hash Lemma" of [9]. Here we state the property in a way suitable to our analysis. (The proof, which is essentially the same as the standard one, is omitted here.)

For any t and any string w, we will use $\lfloor w \rfloor_t$ to denote the first t bits of w.

Lemma 2. For any $n \geq 1$, let Γ be any subset of Σ^n of cardinarity $\geq 2^t$. For any parameters $t' \geq t$ and $\Delta > 0$, consider a random variable $R\lfloor \mathrm{H}_{n,t'}(X,R) \rfloor_{t-\Delta}$ defined with random variables $X \in_{\mathrm{U}} \Gamma$ and $R \in_{\mathrm{U}} \Sigma^{s(n,t')}$. Then this random variable is quite close to the uniform distribution over $\Sigma^{s(n,t')+t-\Delta}$. More specifically, we have the following difference from a random variable $Y \in_{\mathrm{U}} \Sigma^{s(n,t')+t-\Delta}$ for any $S \subseteq \Gamma$.

$$|\Pr[\, R\lfloor \mathrm{H}_{n,t'}(X,R) \rfloor_{t-\Delta} \in S \,] - \Pr[Y \in S]| \;\leq\; \frac{1}{2^{\Delta/2-1}}.$$

III. Many-one Complete Degrees Collapse

We begin this section by introducing some type of one-way functions. In the following, for any function f and any input x, we say that f *is one-one on* x if $f^{-1}(f(x)) = \{x\}$. A function f is called *regular* if $|f^{-1}(x)|$ is the same for all $x \in \Sigma^n$.

We will base on the following hypothesis that has been widely believed. (We can also show the same result from one-way functions whose pre-image size is P/poly-computable; but since the modification of the proof is easy, we leave it to the interest reader.)

> **Regular One-Way Hypothesis:** There exist 2^{n^ϵ}-secure regular one-way functions for some $\epsilon > 0$.

Based on this hypothesis, we show as our main result that the $\leq^{\mathrm{p}}_{\mathrm{m}}$-degree collapses to the $\leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}}$-degree in NP and in general in classes with a standard closure property under non-uniform polynomial-time reductions. Here by "a $\leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}}$-reduction", we mean a many-one reduction that is one-one, length-increasing, and P/poly-computable. Precisely, we prove the following theorem.

Theorem 1. (Main Theorem)
If Regular One-Way Hypothesis is true, then for every class $\mathcal{C}$ closed under non-uniform polynomial-time reductions, if A is $\leq^{\mathrm{p}}_{\mathrm{m}}$-hard for $\mathcal{C}$, then A is $\leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}}$-hard for $\mathcal{C}$.

The remainder of this section is devoted to the proof of this theorem. In the proof, we will make use of two one-way functions or more precisely pseudo-random generators g_{prg} and g_{hc}, both of which can be shown based on Regular One-way Hypothesis. In the following subsections, we first state those pseudo-random generators and then prove our main theorem.

A. Constructing Two Pseudo-random Generators

In [9], a pseudo-random generator is constructed from a one-way function, which is our first pseudo-random generator g_{prg}. The following lemma captures the result of [9].

Lemma 3. Assume (Regular) One-Way Hypothesis. Then there exists a 2^{n^γ}-secure pseudo-random generator g_{prg} for some $\gamma > 0$. Further, g_{prg} maps strings of length n to strings of length $2n$.

[1] For simplicity, let us assume here that the input length of f is also determined by its output length.

Next we consider the second pseudo-random generator $g_{\rm hc}$. For this we first define a nearly one-one one-way function. Assume Regular One-way Hypothesis. Let f_0 be a 2^{n^ϵ}-secure regular one-way function. Let ℓ_0 and t_0 be respectively the length function of f_0 and a function defined from the size of f_0's preimage as follows: $t_0(n) = \lfloor \log_2 |f_0^{-1}(f_0(x))| \rfloor$ for any $x \in \Sigma^n$. Then we may assume that $0 \le t_0(n) \le n-1$, and the following holds for all $x \in \Sigma^n$.

$$2^{t_0(n)} \ \le\ |f_0^{-1}(f_0(x))| \ \le\ 2^{t_0(n)+1}.$$

We transform f_0 to another one-way function that is nearly one-one. This construction is well-known, see, e.g., [7]. We give details for the sake of completeness and also because our parameters are slightly different. (In the rest of this subsection, we will use input length of f_0 as a size parameter, which is denoted by n.)

Let $a(n) = t_0(n) + n^{0.9\epsilon} + 1$ and $b(n) = (n+1)a(n)$. For any n and any string $x \in \Sigma^n$ and $r \in \Sigma^{b(n)}$, define

$$f_1(x,r) \ = \ f_0(x) r {\rm H}_{n,a(n)}(x,r).$$

Note that we may need some advice, namely, $t_0(n)$ for computing $f_1(x)$ for each $x \in \Sigma^n$; but it is easy to see that $f_1 \in {\rm P/poly}$.

We can show that the function f_1 is almost one-one.

Lemma 4. For every n, the number of strings in $\Sigma^{n+b(n)}$ on which f_1 is not one-one is bounded by $2^{n+b(n)}/2^{n^{0.9\epsilon}}$.

Proof. Fix n. For succinct expressions, we omit specifying n and $a(n)$ of ${\rm H}_{n,a(n)}$ in this proof. Let $T_0(n)$ be the size of preimage of $f_0(x)$ for each $x \in \Sigma^n$; that is, $T_0(n) = |f_0^{-1}(f_0(x))|$. We estimate probabilities based on random variables X, X', R, and R, where $X, X' \in_{\rm U} \Sigma^n$ and $R, R' \in_{\rm U} \Sigma^{b(n)}$.

We first note that

$$\begin{aligned}
&\Pr[\, f_1(X,R) = f_1(X',R')\,] \\
&\quad = \ \Pr[\, R = R' \\
&\qquad\qquad \wedge\ f_0(X) = f_0(X') \ \wedge\ {\rm H}(X,R) = {\rm H}(X',R')\,] \\
&\quad = \ \Pr[\, R = R'\,] \\
&\qquad \times \Pr[\, f_0(X) = f_0(X') \ \wedge\ {\rm H}(X,R) = {\rm H}(X',R)\,] \\
&\quad = \ \frac{1}{2^{b(n)}} \cdot \Pr[\, f_0(X) = f_0(X')\,] \\
&\qquad \times \Pr[\, {\rm H}(X,R) = {\rm H}(X',R) \mid f_0(X) = f_0(X')\,] \\
&\quad = \ \frac{1}{2^{b(n)}} \cdot \frac{T_0(n)}{2^n} \\
&\qquad \times (\, \Pr[X = X' \mid f_0(X) = f_0(X')] \\
&\qquad\quad + \Pr[\, {\rm H}(X,R) = {\rm H}(X',R) \mid \\
&\qquad\qquad\qquad X \neq X' \ \wedge\ f_0(X) = f_0(X')\,]\,) \\
&\quad = \ \frac{T_0(n)}{2^{n+b(n)}} \cdot \left(\frac{1}{T_0(n)} + \frac{1}{2^{a(n)}} \right) \\
&\quad = \ \frac{1}{2^{n+b(n)}} + \frac{T_0(n)}{2^{n+b(n)+a(n)}}.
\end{aligned}$$

On the other hand, letting K denote the number of strings in $\Sigma^{n+b(n)}$ on which f_1 is not one-one, we have

$$\Pr[\, f_1(X,R) = f_1(X',R')\,] \ \ge\ \frac{1}{2^{n+b(n)}} + \frac{K}{2^{2n+2b(n)}}.$$

Therefore,

$$\begin{aligned}
\frac{1}{2^{n+b(n)}} + \frac{K}{2^{2n+2b(n)}} \ &\le\ \Pr[\, f_1(X,R) = f_1(X',R')\,] \\
&\le\ \frac{1}{2^{n+b(n)}} + \frac{T_0(n)}{2^{n+b(n)+a(n)}},
\end{aligned}$$

and hence,

$$K \ \le\ \frac{2^{n+b(n)} \cdot T_0(n)}{2^{t_0(n)+n^{0.9\epsilon}+1}} \ \le\ \frac{2^{n+b(n)}}{2^{n^{0.9\epsilon}}}.$$

■

The following lemma makes sure that f_1 remains a one-way function.

Lemma 5. f_1 is a $2^{n^{0.9\epsilon}-2}$-secure one-way function.

Proof. Suppose not. Let M be a polynomial-time randomized machine such that

$$\Pr_{x \in_{\rm U} \Sigma^n, r \in_{\rm U} \Sigma^{b(n)}} [\, f_1(M(f_1(x,r))) = f_1(x,r)\,] \ \ge\ \frac{1}{2^{n^{0.9\epsilon}-2}}$$

for any n. Define another machine M' as follows: on input y, $|y| = \ell_0(n)$, randomly pick r, $|r| = b(n)$, and v, $|v| = a(n)$; compute the output, say xr, of the M on yrv; and output x iff $f_0(x) = y$.

We show that machine M' inverts f_0 on impossibly large fraction. Fix suffciently large n. Again in the following, we omit n and $a(n)$ from ${\rm H}_{n,a(n)}$. Let X and R be random variables as previously defined, and let $V \in_{\rm U} \Sigma^{a(n)}$. We have $f_1(X,R) = f_0(X)R{\rm H}(X,R)$. Here we use Leftover Hash Lemma (i.e., Lemma 2) for the following parameters of the lemma: $\Gamma = f_0^{-1}(f_0(X))$, $t = t_0(n)$, and $\Delta = 2n^{0.9\epsilon}$. Then the lemma guarantees that the distance between the distributions $f_0(X)R\lfloor {\rm H}(X,R) \rfloor_{t_0(n)-\Delta}$ and $f_0(X)R\lfloor V \rfloor_{t_0(n)-\Delta}$ is at most $2^{-(\Delta/2-1)} = 2^{-(n^{0.9\epsilon}-1)}$. Note that $t_0(n) - \Delta = a(n) - 3n^{0.9\epsilon} - 1$. Therefore, letting $n' = 3n^{0.9\epsilon} + 1$ and $a' = a(n) - n'$, we have

$$\begin{aligned}
&\Pr[\, f_0(M'(f_0(X))) = f_0(X)\,] \\
&\quad \ge\ \Pr[\, f_1(M(f_0(X)RV)) = f_1(X,R)\,] \\
&\qquad\qquad\qquad\qquad \text{(by definition of } M'\text{)} \\
&\quad \ge\ \frac{1}{2^{n'}} \cdot \Pr\left[\begin{array}{l} \exists v' \in \Sigma^{n'} \text{ s.t.} \\ f_1(M(f_0(X)R\lfloor V \rfloor_{a'} v')) = f_1(X,R) \end{array} \right] \\
&\quad \ge\ \frac{1}{2^{n'}} \\
&\qquad \times \left(\ \Pr\left[\begin{array}{l} \exists v' \in \Sigma^{n'} \text{ s.t.} \\ f_1(M(f_0(X)R\lfloor {\rm H}(X,R) \rfloor_{a'} v') = f_1(X,R) \end{array} \right] \right. \\
&\qquad\qquad\qquad\qquad\qquad \left. - \ \frac{1}{2^{n^{0.9\epsilon}-1}} \right) \\
&\quad \ge\ \frac{1}{2^{3n^{0.9\epsilon}+1}} \cdot \frac{1}{2^{n^{0.9\epsilon}}} \ =\ \frac{1}{2^{4n^{0.9\epsilon}+1}} \ >\ \frac{1}{2^{n^\epsilon}}.
\end{aligned}$$

This contradicts the security of f_0. ■

We now use the *hard-core bit* of f_1 [6] to define another one-way function. Let $\mathrm{dot}(c,d) = c \cdot d$, and define $f_2(x,r,z) = f_1(x,r)z$ and $g_{\mathrm{hc}}(x,r,z) = f_2(x,r,z)\mathrm{dot}(xr,z)$, where $|z| = |x| + |r|$. Then the last bit of the output of the function g_{hc} is pseudo-random [6].

Lemma 6. For all sufficiently large n, and for every polynomial-time randomized Turing machine M, the following holds, where the probabilities are defined on random variables $X \in_{\mathrm{U}} \Sigma^n$, $R \in_{\mathrm{U}} \Sigma^{b(n)}$, $Z \in_{\mathrm{U}} \Sigma^{n+b(n)}$, and $B \in_{\mathrm{U}} \Sigma$.

$$|\Pr[\, M(g_{\mathrm{hc}}(X,R,Z)) = 1\,] - \Pr[\, M(f_2(X,R,Z)B) = 1\,]\,| \le \frac{1}{2^{n^{0.8\epsilon}}}.$$

The function g_{hc} is defined only on inputs of size $2n+2b(n)$ for some n. We extend it to inputs u of all *even length* as follows: $g_{\mathrm{hc}}(u) = f_2(x,r,zz')\mathrm{dot}(xr,zz')$, where $u = xrzz'$ with x the largest prefix of u such that $2|x| + 2b(|x|) \le |u|$, $|r| = b(|x|)$, $|z| = |x| + b(|x|)$, $|z'| = |u| - 2|x| - 2b(|x|)$, and $\mathrm{dot}(xr,zz') = xr \cdot z$. This slightly increases the probability bound in above lemma; we choose a parameter δ so that the bound of the lemma holds with $2^{-|xrzz'|^\delta}$ istead of $2^{-n^{0.8\epsilon}}$. (We may also assume that the one-oneness guaranteed by Lemma 4 holds for this new g_{hc} with a slightly larger non-one-one ratio $2^{-|xrzz'|^\delta}$ instead of $2^{-n^{0.9\epsilon}}$.)

B. Constructing a Length-Increasing and Almost one-one Reduction

Let A be a $\le^{\mathrm{p}}_{\mathrm{m}}$-hard set for $\mathcal{C}$. Let $B \in \mathcal{C}$. We will use functions g_{hc}, g_{prg}, and H to construct a one-one and length-increasing reduction from B to A. This will be done in two steps. In the first step, we exhibit in this subsection a reduction from B to A that is (i) length-increasing and (ii) one-one on Σ^n for all n. (Throughout this subsection we will use n to denote input length of the reduction from B to A. Let γ and δ denote the constants for g_{prg} (Lemma 3) and g_{hc} (Lemma 6 and the comment after the lemma). We assume that $\delta = \gamma/2$.)

We define the following two intermediate sets based on B, g_{prg}, and g_{hc}.

$$\begin{aligned} B_1 &= \{\, u \mid u = xw \,\wedge\, |w| = |x|^{\frac{2}{\delta}} - |x| \,\wedge\, x \in B \,\} \\ &\quad \cup \{\, u \mid \exists s[\, g_{\mathrm{prg}}(s) = u \,] \}, \\ B_2 &= \{\, y \mid \exists u \,[\, u \in B_1 \,\wedge\, g_{\mathrm{hc}}(u) = y \,] \}. \end{aligned}$$

Recall that we assume that an input u of g_{hc} is a string of even length; let $\overline{n}$ denote $|u|/2$, i.e., $|u| = 2\overline{n}$, and we will use this $\overline{n}$ as a size parameter throughout this subsection.

Note that g_{hc} is length-increasing and $\mathcal{C}$ is closed under nondeterministic reductions; it follows that both B_1 and B_2 are in $\mathcal{C}$. Let $B_2 \le^{\mathrm{p}}_{\mathrm{m}} A$ via h_A. Here we cannot assume that the output length of h_A is determined by its input length. Notice also that g_{hc} may not be a reduction from B_1 to B_2 since it may not be one-one. We show that for two random strings u and u' in $\Sigma^{2\overline{n}}$, the probability that $h_A(g_{\mathrm{hc}}(u)) = h_A(g_{\mathrm{hc}}(u'))$ is small. This allows us to construct a reduction h_{B_1} from B to B_1 such that $h_A \circ g_{\mathrm{hc}} \circ h_{B_1}$ is a reduction from B to A with required properties. We use the pseudo-randomness of both g_{hc} and g_{prg} to obtain a bound on the probability of this collision.

Define

$$p \;=\; \Pr_{u,u' \in_{\mathrm{U}} \Sigma^{2\overline{n}}}[\, h_A(g_{\mathrm{hc}}(u)) = h_A(g_{\mathrm{hc}}(u')) \,].$$

As our key technical lemma, we show below that this probability is very small. Before the proof, we give some intuitive reasoning for this, which also explain why those intermediate sets B_1 and B_2 were introduced as above.

Suppose that p is not so small. Then by definition $g_{\mathrm{hc}}(u) = f_2(u)\mathrm{dot}(u)$ and by the pseudo-randomness of $\mathrm{dot}(u)$ w.r.t. $f_2(u)$, we can show that the following $\overline{p}$ is not so small either (here $\overline{\mathrm{dot}(u)}$ denotes the complement of $\mathrm{dot}(u)$; that is, $\overline{\mathrm{dot}(u)}$ is 0 if $\mathrm{dot}(u) = 1$ and 1 if $\mathrm{dot}(u) = 0$).

$$\overline{p} \;=\; \Pr_{u,u' \in_{\mathrm{U}} \Sigma^{2\overline{n}}}[\, h_A(f_2(u)\overline{\mathrm{dot}(u)}) = h_A(g_{\mathrm{hc}}(u')) \,],$$

On the other hand, this implies a similar bound for the following $\overline{p}'$ because of the pseudo-randomness of g_{prg}.

$$\overline{p}' \;=\; \Pr_{u \in_{\mathrm{U}} \Sigma^{2\overline{n}},\, s \in_{\mathrm{U}} \Sigma^{\overline{n}}}[\, h_A(f_2(u)\overline{\mathrm{dot}(u)}) = h_A(g_{\mathrm{hc}}(g_{\mathrm{prg}}(s))) \,].$$

Consider u such that $h_A(f_2(u)\overline{\mathrm{dot}(u)}) = h_A(g_{\mathrm{hc}}(g_{\mathrm{prg}}(s)))$ holds for some s. Note first that $g_{\mathrm{hc}}(g_{\mathrm{prg}}(s)))$ is in B_2 and hence $h_A(g_{\mathrm{hc}}(g_{\mathrm{prg}}(s)))$ is in A because h_A is a reduction from B_2 to A. Thus, $h_A(f_2(u)\overline{\mathrm{dot}(u)}) = h_A(g_{\mathrm{hc}}(g_{\mathrm{prg}}(s)))$ implies $f_2(u)\overline{\mathrm{dot}(u)} \in B_2$; this further implies that $f_2(u)\overline{\mathrm{dot}(u)} = f_2(u'')\mathrm{dot}(u'')$ for some u'' because B_2 is a subset of the range of g_{hc} and $g_{\mathrm{hc}}(u'') = f_2(u'')\mathrm{dot}(u'')$. But then $u \ne u''$ because $\overline{\mathrm{dot}(u)} = \mathrm{dot}(u'')$. Thus, for u, we have some $u'' \ne u$ such that $f_2(u'') = f_2(u)$. Therefore, if $\overline{p}'$ is not so small, then f_2 has not so small number of collision pairs, contradicting that f_2 is almost one-one.

Now we state this argument formally.

Lemma 7. $p \le 2^{-(2\overline{n})^\delta + 2} \le 2^{-n^2+2}$.

Proof. Let ℓ_{hc} be the length function for g_{hc}; that is, $|g_{\mathrm{hc}}(u)| = \ell_{\mathrm{hc}}(2\overline{n})$ for any u, $|u| = 2\overline{n}$. Define machine M as follows: on input y, $|y| = \ell_{\mathrm{hc}}(2\overline{n})$, randomly pick $u' \in \Sigma^{2\overline{n}}$ and accept iff $h_A(y) = h_A(g_{\mathrm{hc}}(u'))$. Note that $p = \Pr_{u \in_{\mathrm{U}} \Sigma^{2\overline{n}}}[\, M(u) = 1\,]$.

Again fix $\overline{n}$, and we discuss probabilities on random variables $U, U' \in_{\mathrm{U}} \Sigma^{2\overline{n}}$ and $B \in \Sigma$. First from Lemma 6 it follows

$$|\Pr[\, M(f_2(U)B) = 1\,] - \Pr[\, M(g_{\mathrm{hc}}(U)) = 1\,]\,| \;\le\; 2^{-(2\overline{n})^\delta}. \tag{1}$$

Then for $\overline{p}$ defined above, we have

$$\begin{aligned} &\Pr[\, M(f_2(U)B) = 1\,] \\ &\quad= \Pr[\, h_A(f_2(U)B) = h_A(g_{\mathrm{hc}}(U'))\,] \\ &\quad= \Pr[\, h_A(f_2(U)B) = h_A(g_{\mathrm{hc}}(U')) \,\wedge\, B = \mathrm{dot}(U)\,] \\ &\qquad + \Pr[\, h_A(f_2(U)B) = h_A(g_{\mathrm{hc}}(U')) \,\wedge\, B \ne \mathrm{dot}(U)\,] \\ &\quad= \frac{1}{2}p + \frac{1}{2}\overline{p}. \end{aligned}$$

Thus, the equation (1) becomes $|p+\overline{p}-2p| \le 2^{-(2\overline{n})^{\delta}+1}$, which gives the following bound on p in terms of $\overline{p}$.

$$p \ \le\ \overline{p} + 2^{-(2\overline{n})^{\delta}+1}. \qquad (2)$$

To bound $\overline{p}$, we define another machine M' that works as follows: on input u, $|u| = 2\overline{n}$, randomly pick a $u' \in \Sigma^{2\overline{n}}$ and accept iff $h_A(g_{\rm hc}(u)) = h_A(f_2(u')\overline{{\rm dot}(u')})$.

Now for the same $\overline{n}$, we continue our analysis of probabilities; here we consider random variables $U, U' \in_{\rm U} \Sigma^{2\overline{n}}$ and $S \in \Sigma^{\overline{n}}$. Note first that $\overline{p} = \Pr[M'(U) = 1]$. On the other hand, by pseudo-randomness of $g_{\rm prg}$, the following holds.

$$|\Pr[\,M'(U) = 1\,] - \Pr[\,M'(g_{\rm prg}(S)) = 1\,]| \ \le\ 2^{-(\overline{n})^{\gamma}}. \quad (3)$$

Hence, we have

$$\begin{aligned}\overline{p} &\le 2^{-(\overline{n})^{\gamma}} + \Pr[\,M'(g_{\rm prg}(S)) = 1\,]\\ &\le 2^{-(\overline{n})^{\gamma}} + \Pr[\,h_A(g_{\rm hc}(g_{\rm prg}(S))) = h_A(f_2(U')\overline{{\rm dot}(U')})\,].\end{aligned}$$

Fix any $s \in \Sigma^{\overline{n}}$. Since $g_{\rm prg}(s) \in B_1$, $g_{\rm hc}(g_{\rm prg}(s))$ is in B_2, and hence $h_A(g_{\rm hc}(g_{\rm prg}(s)))$ is in A. Now comes the key part of the argument: $h_A(g_{\rm hc}(g_{\rm prg}(s))) = h_A(f_2(u')\overline{{\rm dot}(u')})$ is possible for some u' only if $f_2(u')\overline{{\rm dot}(u')} \in B_2$ as h_A is a reduction from B_2 to A. Since B_2 is a subset of the range of $g_{\rm hc}$, this is possible only if $f_2(u')\overline{{\rm dot}(u')} = f_2(u''){\rm dot}(u'')$ for some $u'' \in \Sigma^{2\overline{n}}$ and $u'' \neq u'$. This implies $f_2(u'') = f_2(u')$. By Lemma 4, f_2 is not one-one on at most $\frac{2^{2\overline{n}}}{2^{(2\overline{n})^{\delta}}}$ strings. Therefore,

$$\overline{p} \ \le\ 2^{-(\overline{n})^{\gamma}} + 2^{-(2\overline{n})^{\delta}} \ \le\ 2^{-(2\overline{n})^{\delta}+1}.$$

This bound on $\overline{p}$ gives the required bound on p using equation (2). ■

We now use the universal hash function H to define reduction h_{B_1} from B to B_1. Let $m(n) = n^{\frac{2}{\delta}} - n$. Define a function H by $H(x, r) = x{\rm H}_{|x|,m(|x|)}(x, r)$. The reduction h_{B_1} will be H with its second component fixed to some specific value. We will choose this value so that $h_A \circ g_{\rm hc} \circ h_{B_1}$ is a length-increasing reduction from B to A that is one-one on Σ^n for all large enough n. The following lemma shows this can be done. Let $h = h_A \circ g_{\rm hc} \circ H$.

Lemma 8. *For all large enough n, there exists $r_n \in \Sigma^{(n+1)m(n)}$ that satsifies the following:*

(1) *$h(\cdot, r_n)$ is length-increasing on Σ^n (i.e., $|h(x, r_n)| > n$ for every $x \in \Sigma^n$);*

(2) *$h(\cdot, r_n)$ is one-one on Σ^n (i.e., $h(x, r_n) \neq h(x', r_n)$ for every $x \neq x' \in \Sigma^n$); and*

(3) *$h(\cdot, r_n)$ is a reduction from B to A on Σ^n (i.e., $x \in B$ iff $h(x, r_n) \in A$ for every $x \in \Sigma^n$).*

Proof. Fix a large enough n, and let $m = m(n)$ and $2\overline{n} = n + m$. We estimate probabilities on random variables $X, X' \in_{\rm U} \Sigma^n$, $R \in_{\rm U} \Sigma^{(n+1)m}$, and $U, U' \in_{\rm U} \Sigma^{2\overline{n}}$.

We show that $h(\cdot, R)$ is length increasing with high probability. For this we observe that

$$\begin{aligned}\Pr[\,|h(X,R)| \le n\,] &= \sum_{y\in\Sigma^{\le n}} \Pr[\,h(X,R) = y\,]\\ &= \sum_{y\in\Sigma^{\le n}} \Pr[\,h_A(g_{\rm hc}(U)) = y\,]\\ &\qquad \text{(since } {\rm H}_{n,m}(X,R) \text{ is uniformly distributed)}\\ &\le \sqrt{\sum_{y\in\Sigma^{\le n}} (\Pr[\,h_A(g_{\rm hc}(U)) = y\,])^2} \cdot \sqrt{\sum_{y\in\Sigma^{\le n}} 1}\\ &= \sqrt{\sum_{y\in\Sigma^{\le n}} \Pr[\,h_A \circ g_{\rm hc}(U) = h_A \circ g_{\rm hc}(U') = y\,]}\\ &\qquad\qquad \times \sqrt{\sum_{y\in\Sigma^{\le n}} 1}\\ &\le \sqrt{p} \cdot 2^{\frac{n+1}{2}} \ \le\ \frac{2^n}{2^{\frac{1}{2}(2\overline{n})^{\delta}}} \ \le\ \frac{1}{2^{\frac{1}{2}n^2-n}} \ <\ \frac{1}{2^{n+2}}.\\ &\qquad \text{(since } n \text{ is large enough)}\end{aligned}$$

From this we bound the probability that $h(\cdot, R)$ is not length-increasing as follows.

$$\begin{aligned}\Pr[\,\exists x \in \Sigma^n[\,|h(x,R)| \le n\,]\,] &\le \sum_{x\in\Sigma^n} \Pr[\,|h(x,R)| \le n\,]\\ &= 2^n \cdot \Pr[\,|h(X,R)| \le n\,] \ <\ \frac{1}{4}.\end{aligned}$$

Next we show that $g_{\rm hc}$ is one-one on all $y \in H(\Sigma^n, r)$ for most of $r \in \Sigma^{(n+1)m}$. Again since n is large enough, we have

$$\begin{aligned}&\Pr[\ \exists x \in \Sigma^n\,[\,g_{\rm hc} \text{ is not one-one on } H(x,R)\,]\ ]\\ &\quad\le\ 2^n \cdot \Pr[\,g_{\rm hc} \text{ is not one-one on } H(X,R)\,]\\ &\quad=\ 2^n \cdot \Pr[\,g_{\rm hc} \text{ is not one-one on } U\,]\\ &\quad\le\ \frac{2^n}{2^{(2\overline{n})^{\delta}}} \ \le\ \frac{1}{2^{n^2-n}} \ <\ \frac{1}{4}.\end{aligned}$$

Similarly we show that for most of r, $H(\Sigma^n, r)$ does not intersect with the range of $g_{\rm prg}$. That is,

$$\begin{aligned}&\Pr[\ \exists x \in \Sigma^n,\, \exists s \in \Sigma^{\overline{n}}\,[\,H(x,R) = g_{\rm prg}(s)\,]\ ]\\ &\quad\le\ 2^n \cdot \Pr[\,\exists s \in \Sigma^{\overline{n}}\,[\,H(X,R) = g_{\rm prg}(s)\,]\,]\\ &\quad=\ 2^n \sum_{s\in\Sigma^{\overline{n}}} \Pr[\,H(X,R) = g_{\rm prg}(s)\,]\\ &\quad=\ 2^n \sum_{s\in\Sigma^{\overline{n}}} \Pr[\,U = g_{\rm prg}(s)\,] \ =\ 2^n \sum_{s\in\Sigma^{\overline{n}}} \frac{1}{2^{2\overline{n}}}\\ &\quad=\ \frac{2^n}{2^{\overline{n}}} \ \le\ \frac{2^n}{2^{n^{\frac{2}{\delta}}}} \ \le\ \frac{1}{2^{n^2-n}} \ <\ \frac{1}{4}.\end{aligned}$$

Finally, we bound the probability that h is not one-one on Σ^n. Again since n is large enough and $H(X, R)$ and

$H(X', R)$ are pair-wise independent, we have

$$\begin{aligned}
&\Pr[\ \exists x \neq x' \in \Sigma^n\, [\, h(x,R) = h(x',R)\,]\ ] \\
&\quad \leq \quad 2^{2n} \cdot \Pr[\, h(X,R) = h(X',R) \mid X \neq X'\,] \\
&\quad = \quad 2^{2n} \cdot \Pr[\, h_A \circ g_{\rm hc} \circ H(X,R) = h_A \circ g_{\rm hc} \circ H(X',R) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \mid X \neq X'\,] \\
&\quad \leq \quad 2^{2n}\left(1 + \frac{1}{2^n - 1}\right) \Pr[\, h_A(g_{\rm hc}(U)) = h_A(g_{\rm hc}(U'))\,] \\
&\quad \leq \quad 2^{2n+1} \cdot p \ \leq\ 2^{-n^2+2n+3} \ <\ \frac{1}{4}.
\end{aligned}$$

Therefore there exists an $r_n \in \Sigma^{(n+1)m}$ satisfying (i) $|h(x, r_n)| > n$ for all $x \in \Sigma^n$, (ii) $g_{\rm hc}$ is one-one on all $y \in H(\Sigma^n, r_n)$, (iii) $H(\Sigma^n, r_n)$ does not intersect range of $g_{\rm prg}$, and (iv) $h(x, r_n) \neq h(x', r_n)$ for all $x \neq x' \in \Sigma^n$. For this r_n, $h(\cdot, r_n)$ is also a reduction from B to A on Σ^n. To see this, consider any $x \in \Sigma^n$; then it holds that

$$\begin{aligned}
& x \in B \\
&\quad \Leftrightarrow \quad H(x, r_n) \in B_1 \quad (\text{since } H(x, r_n) \notin g_{\rm prg}(\Sigma^{\overline{n}})) \\
&\quad \Leftrightarrow \quad g_{\rm hc}(H(x, r_n)) \in B_2 \\
&\qquad\qquad (\text{since } g_{\rm hc} \text{ is one-one on } H(x', r_n) \text{ for } \forall x' \in \Sigma^n) \\
&\quad \Leftrightarrow \quad h_A(g_{\rm hc}(H(x, r_n))) \in A \quad (\text{since } B_2 \leq_{\rm m}^{\rm p} A \text{ via } h_A).
\end{aligned}$$

■

Finally, define a function h_0 by $h_0(x) = h(x, r_{|x|})$ for any x with $|x| > n_0$ for some sufficiently large n_0. (For each x in the finite set $\Sigma^{<n_0}$, we define $h_0(x)$ appropriately so that our requirements hold on $\Sigma^{<n_0}$.) Then h_0 is in P/poly. Furthermore, by above lemma, h_0 is a reduction from B to A that is (i) length-increasing and (ii) one-one on Σ^n for all n.

C. Constructing a Length-Increasing and one-one Reduction

By Lemma 8, we have a length-increasing reduction from B to A that is one-one on Σ^n on all n. But it may be still the case that the reduction is not one-one because two strings of *different* lengths could be mapped to the same string by the reduction. Here we get around this by using a standard padding trick.

Define set B_3 as follows.

$$B_3 \ =\ \{\, x01^m \mid x \in B \ \wedge\ m \geq 0\,\}.$$

Again by Lemma 8, we can define some $\leq_{\rm m}^{\rm p/poly}$-reduction from B_3 to A that is length-increasing and one-one on Σ^n for all n. Let us denote it as h_1.

For any x, let $|h_1(x)| \leq q(|x|)$ for some polynomial q. Define a function k by $k(j) = q(k(j-1))$ and $k(1) = 0$. Now define a function h_2 by $h_2(x) = x01^{k(j_n)-n-1}$, where $n = |x|$ and j_n is the smallest number such that $k(j_n) > n$. Clearly, h_2 is a length-increasing and one-one reduction from B to B_3 mapping strings of length n to strings of length $k(j_n)$. Finally, define $h_3 = h_1 \circ h_2$. Clearly, h_3 is a length-increasing reduction from B to A. We now show that this is what we want.

Lemma 9. The function h_3 is one-one.

Proof. Consider $y_1 = h_3(x_1)$ $(= h_1(h_2(x_1)))$ and $y_2 = h_3(x_2)$ $(= h_1(h_2(x_2)))$ for $x_1 \neq x_2$. If $|h_2(x_1)| = |h_2(x_2)| = n'$, we immediately have $y_1 \neq y_2$ since h_1 is one-one on $\Sigma^{n'}$ and h_2 is one-one. On the other hand, if $|h_2(x_1)| = k(j_{n_1}) > |h_2(x_2)| = k(j_{n_2})$, then we have $|h_1(h_2(x_2))| \leq q(|h_2(x_2)|) = q(k(j_{n_2})) = k(j_{n_2}+1)$ (by the definition of k) $\leq k(j_{n_1}) < |h_1(h_2(x_1))|$. Thus, again we have $y_1 \neq y_2$. Therefore, h_3 is one-one. ■

D. Structure of Complete Sets Relative to a Random Oracle

Our main theorem allows us to completely describe the structure of complete degrees relative to a random oracle.

Theorem 2. Relative to a random oracle, for every class $\mathcal{C}$ closed under polynomial-time non-deterministic reductions, if A is $\leq_{\rm m}^{\rm p}$-hard for $\mathcal{C}$, then A is also $\leq_{\rm li,1\text{-}1}^{\rm p}$-hard for $\mathcal{C}$. (On the other hand, as shown in [13], relative to a random oracle, there exists an A which is $\leq_{\rm m}^{\rm p}$-hard for $\mathcal{C}$ but not $\leq_{\rm li,1\text{-}1,inv}^{\rm p}$-hard.)

Proof. Impagliazzo [10] showed that there exists a $2^{\sqrt{n}}$-secure pseudo-random generator relative to a random oracle R. Further, this generator is a one-one and length-increasing function.

It follows from Theorem 1 that any $\leq_{\rm m}^{\rm p}$-hard sets for $\mathcal{C}$ are $\leq_{\rm li,1\text{-}1}^{\rm p/poly}$-hard relative to R. We can eliminate the non-uniformity by querying the random oracle to get the "right" value of the string r_n. To ease the analysis, this querying must be done at locations which are not accessed otherwise. This is easily achievable by querying strings of the form $x10^t$ on input x for t larger than running time of the reduction h. ■

IV. Are NP-complete Sets Isomorphic?

The previous section shows that many-one complete sets for NP and other classes are likely to be also one-one, length-increasing complete under non-uniform reductions. The Isomorphism Conjecture [4] says that these sets are also p-isomorphic to each other. Doubts have been raised about the truth of this conjecture due to existance of one-way functions of the kind we assumed in the previous section: if f is a one-one, length-increasing one-way function, then $f(\text{SAT})$ is also NP-complete but it is not clear how to construct a reduction of SAT to $f(\text{SAT})$ that is also polynomial-time invertible (which is required for constructing a p-isomorphism between SAT and $f(\text{SAT})$). By its definition, f is not invertible almost everywhere! Moreover, as explained in the previous subsection, it was shown in [13] that relative to a random oracle there exist very strong form of one-way functions for which $f(\text{SAT})$ has only sparse polynomial-time computable subsets. This makes it impossible for a one-one, length-increasing, and P-invertible reduction to exist from SAT to $f(\text{SAT})$.

In the real world, however, no examples of such strong one-way functions are known. In fact, for the known one-way functions, it is generally easy to identify small, but dense, subsets on which they are invertible via non-uniform polynomial-time computable functions. Therefore, the evidence provided against the conjecture by the random oracle result is not very strong. But is the property of having easily identifiable dense invertible subsets enough to guarantee ismorphism? Below, we answer in affirmative, provided there is a collection of easily parameterizable and easily identifiable dense invertible subsets.

For nonuniform complexity classes, we use the standard ones $\mathrm{P/poly}$. Classes such as P/q are used to bound (more specifically) advice string size by some polynomial q. Language classes are extended to function classes naturally by extending the role of the interpreter from a recognizer to a transducer. Any function $f \in \mathrm{P/poly}$ is called a $\mathrm{P/poly}$-computable function.

Now we formalize the property that we need from one-way functions. A *polynomial-time computable pairing function* (or a *polynomial-time computable padding function*) is a function $\pi : \Sigma^* \times \Sigma^* \mapsto \Sigma^*$ that is (i) one-one and length increasing, and (ii) polynomial-time computable and invertible[2]. A function $e : \Sigma^* \mapsto \Sigma^*$ is called a $\mathrm{P/poly}$-*embedding* if (i) e is one-one and length-increasing, and (ii) e is $\mathrm{P/poly}$-computable.

Fix any polynomial-time computable pairing function π. We first define the notion of "$\mathrm{P/poly}$-easy cylinder w.r.t. π."

Definition 3. Let f be a one-one, length-increasing function in $\mathrm{P/poly}$. For any polynomial q, the function f has a $\mathrm{P/poly}$-*easy cylinder w.r.t.* π if there exists polynomials $q(\cdot)$, $q'(\cdot)$, and $\ell(\cdot)$ with $\ell(n) \geq 2q(2q'(n)+n)$, and a P/q-embedding e, $e(y)$ computable in time $\leq q(|e(y)|)$, such that for any n and for every string u of length $\ell(n)$, there exists some $g_u \in \mathrm{P/poly}$ and s_u, $|s_u| \leq q'(n)$, such that $g_u(f(\pi(u, e(\pi(s_u, x))))) = x$ for all $x \in \Sigma^n$.

Intuitively, a function f having a $\mathrm{P/poly}$-easy cylinder w.r.t. π has a parameterized (on u) dense subset in its domain on which it is easy to invert and the dense subset depends on the parameter in a simple way (via the string s_u). Note that the $\mathrm{P/poly}$-computable function g_u can be chosen depending on f as well as u but the embedding function e must be independent of u.

We believe that all one-one and length-increasing functions in $\mathrm{P/poly}$ have a $\mathrm{P/poly}$-easy cylinder w.r.t. π. Notice here that the choice of the pairing function π is not essential; the following relation is easy to show.

Proposition 1. All one-one and length-increasing functions in $\mathrm{P/poly}$ have a $\mathrm{P/poly}$-easy cylinder w.r.t. *some* polynomial-time computable pairing function if and only if it holds w.r.t. *any* polynomial-time computable pairing function.

Thus, in the following, we fix one polynomial-time computable pairing function, and the reference to the pairing function is omitted. We now show that if SAT reduces to a set via a reduction that has an easy cylinder, then the set is $\mathrm{P/poly}$-isomorphic to SAT. Our result is stated in terms of the following canonical NP-complete set.

$$\begin{aligned} K \;=\; \{ \quad & \pi(p,y) \mid \\ & \quad p \text{ is a code of a machine } M_p \text{ such that} \\ & \quad M_p \text{ accepts } y \text{ in at most } |py| \text{ steps} \}. \end{aligned}$$

Theorem 3. Let A be such that $K \leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}} A$ via f and f has a $\mathrm{P/poly}$-easy cylinder. Then $K \leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1,inv}} A$.

Proof. Suppose f has a $\mathrm{P/poly}$-easy cylinder with P/q-embedding function e.

We define a $\mathrm{P/poly}$-computable reduction h from K to K such that f is easy to invert on the range of h. Fix any n, and consider a nondeterministic Turing machine M that executes as follows on input $\pi(u, y)$: Guess x, s, $|x| = n$ $|s| \leq q'(n)$, and check whether $e(\pi(s, x))$ equals y; if not, reject; if yes, accept if and only if x is in K. Here we note that the advice of size $q(2q'(n)+n)$ for computing e on $\Sigma^{2q'(n)+n}$ is hardwired in M. Further, from the time complexity of e, $M(y)$ halts within $q(2q'(n) + n)$ steps. Thus, by letting p_n be a code of this machine M that is (with some padding) of size $\ell(n) \geq 2q(2q'(n) + n)$, we have M_{p_n} halts and accepts $\pi(p_n, e(\pi(s, x)))$ in $|p_n e(\pi(s, x))|$ steps iff M accepts $e(\pi(s, x))$ iff $x \in K$ for all $x \in \Sigma^n$.

With these machine codes p_n for all n, the reduction h is defined as follows for each n and each $x \in \Sigma^n$.

$$h(x) \;=\; \pi(p_n, e(\pi(s_{p_n}, x))).$$

Then it follows from the above that this is a reduction from K to K. Furthermore, h is $\mathrm{P/poly}$-computable.

Now we define $\widehat{f} = f \circ h$ and claim that $K \leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1,inv}} A$ via $\widehat{f}$. Clearly, it is a $\leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}}$-reduction from K to A. To complete the proof, observe that $\{\pi(p_n, e(\pi(s_{p_n}, x)))\}_{x \in \Sigma^n}$ satisfies the condition of a $\mathrm{P/poly}$-easy cylinder. Thus, from our assumption, for each n, we have some g_n in $\mathrm{P/poly}$ such that $x = g_n(f(\pi(p_n, e(\pi(s_{p_n}, x))))) \; (= g_n(\widehat{f}(x)))$ for all $x \in \Sigma^n$. That is, $\widehat{f}$ is $\mathrm{P/poly}$-invertible. ■

A. Easy Cylinder Conjecture

Here we discuss the following conjecture.

> **Easy Cylinder Conjecture:** All one-one and length-increasing functions in $\mathrm{P/poly}$ have a $\mathrm{P/poly}$-easy cylinder.

The following corollary is immediate from Theorems 1 and 3:

Corollary 4. If both Regular One-Way Hypothesis and Easy Cylinder Conjecture hold, then all $\leq^{\mathrm{p/poly}}_{\mathrm{m}}$-complete sets for NP are isomorphic under $\mathrm{P/poly}$-reductions.

We give some evidence supporting this conjecture. First, the known one-way functions all appear to have a $\mathrm{P/poly}$-easy cylinder. We give several examples.

First we fix our paring function π. Though a bit tricky, in order to simplify our explanation, here we define it as follows.

$$\pi(u, z) \;=\; \begin{cases} 10\,\mathrm{pre}(u)\,z, & \text{if } z \in 0\Sigma^*, \text{ and} \\ 11\,(\mathrm{pre}(u)\,z)^{\mathrm{rev}}, & \text{otherwise,} \end{cases}$$

[2] The following argument holds by extending the polynomial-time computability to the $\mathrm{P/poly}$-computability. But we leave this extension to the interest reader.

where $\mathrm{pre}(u)$ denotes a prefex-free code of u, and $(\cdots)^{\mathrm{rev}}$ is a mirror image of $\cdots$. We can assume that $|\mathrm{pre}(u)| = 2|u|$.

We consider the following five functions.

- **Multiplication:** For all $|x| = |y|$, define
$$f_\times(x, y) \;=\; x \times y.$$
Let $|x| = n$. We use embedding function $e_1(x) = 0x$ and polynomial $q(n) = \frac{1}{2}(n+1)$. The string $s_n = \epsilon$ for all these five examples. Then for any fixed $u \in \Sigma^{n+1}$, the first half bits of $\pi(u, e_1(x))$ are fixed for any x; that is, $\pi(u, e_1(x)) = u'x'$ with some $|u'| = |x'|$, and u' is fixed whereas x' varies depending on x. Then clearly, by using u as an advice, it is easy to invert $f_\times(\pi(u, e_1(x)))$ to obtain x.
- **RSA Function:** For all $|m| = |e| = |n|$, define
$$f_{\mathrm{rsa}}(m, e, n) \;=\; (m^e \,(\mathrm{mod}\, n), e, n).$$
Let $|x| = t$. We use the embedding function $e_2(x) = 1x$ and polynomial $q(t) = \frac{1}{2}(t+2)$. Then, each $u \in \Sigma^{t+2}$ determines e and n in $(m, e, n) = \pi(u, e_2(x))$ whereas m depends on x. Hence it is again easy to invert $f_{\mathrm{rsa}}(\pi(u, e_2(x)))$ to obtain x (since e and n are fixed, we can non-uniformly supply $d = e^{-1} \,(\mathrm{mod}\, \phi(n))$ to g_u).
- **Subset-sum:** For all $|x_1| = |x_2| = \cdots = |x_n| = n$, define
$$f_{\mathrm{ss}}(x_1, x_2, \ldots, x_n, S) \;=\; (x_1, x_2, \ldots, x_n, \sum_{i \in S} x_i).$$
Let $|x| = n$. Use embedding function $e_2(x) = 1x$, and $q(n) = \frac{1}{4}(n+1)^2$. Then for any fixed $u \in \Sigma^{\frac{1}{2}(n+1)^2}$, the last $(n+1)^2$ bits in $\pi(u, e_2(x)) = (x_1, x_2, \ldots, x_n, S)$ are fixed and so only x_1 depends on x. Knowing u, inverting f_{ss} on such inputs is trivial.
- **Linear Error Correcting Codes over F_2:** For all $n \times m$ matrix M, $1 \times n$ vector x, $1 \times m$ error vector e with not so many 1's (all over F_2), define
$$f_{\mathrm{ecc}}(M, x, e) \;=\; (M, xM + e).$$
Let $|x| = n$. Use embedding function $e_1(x) = 0x$, and $q(n) = \frac{1}{4}((n+1)^2 + n + 1)$. Then for any fixed $u \in \Sigma^{\frac{1}{2}((n+1)^2+n+1)}$, the first $(n+1)^2 + n + 1$ bits of $\pi(u, e_1(x)) = (M, x, e)$ are fixed and so only e depends on x. Inverting f_{ecc} on such inputs is trivial with the help of u.
- **Exponentiation in Finite Fields:** For all $|g| = |e| = |p|$, define
$$f_{\exp}(g, e, p) \;=\; (g, g^e \,(\mathrm{mod}\, p), p).$$
As before, using embedding e_2, we can fix e and p in the input, and on this, $f_{\exp}$ is trivial to invert.

In addition to these special one-way functions, we can show that the following class of functions have an easy cylinder.

Theorem 5. Let f be any one-one, length-increasing computed by a constant depth circuit family. Then f has a $\mathrm{P/poly}$-easy cylinder.

Proof. Fix n. Consider the circuit C computing f on inputs of size $3n+2$. We use the embedding $e(x) = 0x'$ with $|e(x)| = n$ and $|x| = m$, m and x' to be determined later. Let $q(m) = \frac{1}{2}n$, $q'(n) = 0$ (as before), and fix any u, $|u| = n$. For any x, $\pi(u, e(x)) = 10u'e(x)$, where u' is completely determined by u and $|u'| = 2n$. Consider the circuit C' which equals C with input of the form $10u'0y$, $|y| = n - 1$. In [1] it is shown that any constant depth circuit reduces, via a random restriction, to a *superprojection* — a constant depth circuit C'' whose every input bit is mapped directly to an output bit, perhaps after negation. Further, the random restriction leaves n^ϵ bits unset for some $\epsilon > 0$. Fix any such restriction. Letting $m = n^\epsilon$, we can now define the embedding $e(x) = 0y$ where x is mapped to those positions of y that remaing unset in C'' and other positions of y set according to the fixed restriction. It is clear that f is invertible on $10u'e(x)$ as the string x is written (after complementing some bits) in the output of f.

There is a problem with this reduction, however. The embedding e depends on the string u as the random rescrition depends on the circuit C' which, in turn, depends on u. This is not allowed in the definition of easy cylinder. We solve this problem using the result in [2] that shows that the random restrictions for C' can be generated from a very small $(= O(\log n))$ length seed. Moreover, a careful observation of the proof reveals that the seed can be made a part of the random restrictions. Define the embedding function e as one that takes as input the seed as well as x and outputs the random restriction generated according to the seed filling in x in the unset positions. Now e is independent of u. It is also 1-1, and invertible due to the presence of entire input (including the seed) in fixed output positions. Define polynomial $q'(n)$ to be equal to the seed length, and choose s_u to be that setting of the seed which generates a good random restriction for the circuit C'. All the required properties are satisfied now. ■

It is not clear if the class of functions with $\mathrm{P/poly}$-easy cylinders is closed under composition. Emphasizing this is a very recent note by Oded Goldreich [8] in which he constructs a one-way function that is of the form f^n (f composed with itself n times) with f having an easy cylinder. He conjectures that this function does not have an easy cylinder which implies that the Easy Cylinder Conjecture is false. In fact, closure under polynomially many compositions of functions with easy cylinders is central to a resolution of the Easy Cylinder Conjecture: if the closure does not hold, the Conjecture is false; and if the closure holds then it is most likely true as any one-way function can be viewed as a composition of polynomially many functions that have an easy cylinder (e.g., those computed by constant depth circuits).

References

[1] M. Agrawal, E. Allender, and S. Rudich, Reductions in circuit complexity: An isomorphism theorem and a gap theorem, *J. Comput. Sys. Sci.*, 57:127–143, 1998.

[2] M. Agrawal, The first order isomorphism theorem, in *Proceedings of Twenty First FST&TCS*, Lecture Notes in Comp. Sci. 2245, 70–82, 2001.

[3] M. Agrawal, Pseudo-random generators and the structure of complete degrees, in *Proceedings of the Conference on Computational Complexity*, IEEE, 139–146, 2002.

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

[5] K. Ganesan, One-way functions and isomorphism conjecture, *Theoret. Comput. Sci.*, 129:309–321, 1994.

[6] O. Goldreich and L. A. Levin. A hardcore predicate for all one-way functions, in *Proceedings of Annual ACM Symposium on the Theory of Computing*, ACM, 25–32, 1989.

[7] O. Goldreich, *Foundation of Cryptography I: Basic Tools*, Cambridge University Press, 2001.

[8] O. Goldreich, A candidate counterexample to the Easy Cylinder Conjecture, TR09-028, ECCC report, http://eccc.hpi-web.de/eccc-reports/2009/TR09-028/index.html, 2009.

[9] J. Håstad, R. Impagliazzo, L. Levin, and M. Luby, A pseudo-random generator from any one-way function, *SIAM Journal on Computing*, 221–243, 1998.

[10] R. Impagliazzo, Very strong one-way functions and pseudo-random generators exists relative to a random oracle, Manuscript, January 1996.

[11] D. Joseph and P. Young, Some remarks on witness functions for non-polynomial and noncomplete sets in NP, *Theoret. Comput. Sci.*, 39:225–237, 1985.

[12] S. Kurtz, S. Mahaney, and J. Royer, The structure of complete degrees, in *Complexity Theory Retrospective* (A. Selman, ed.), Springer-Verlag, 108–146, 1990.

[13] S. Kurtz, S. Mahaney, and J. Royer, The isomorphism conjecture fails relative to a random oracle, *Journal of the ACM*, 42(2):402–420, 1995.

[14] O. Watanabe, On the p-isomorphism conjecture, *Theoret. Comput. Sci.*, 83:337–343, 1991.

[15] P. Young, Juris Hartmanis: Fundamental contributions to isomorphism problems, in *Complexity Theory Retrospective* (A. Selman, ed.), Springer-Verlag, 28–58, 1990.