ISSN 1342-2812

Research Reports on Mathematical and Computing Sciences

One-Way Functions and the Isomorphism Conjecture

Manindra Agrawal and Osamu Watanabe

March 2009, C–260

Department of
Mathematical and
Computing Sciences
Tokyo Institute of Technology

SERIES C: Computer Science

One-Way Functions and the Isomorphism Conjecture

Manindra Agrawal[1] and Osamu Watanabe[2]
1. Dept. of Computer Science, IIT Kanpur, Kanpur (manindra@iitk.ac.in)
2. Dept. of Math. & Comp. Sci., Tokyo Inst. of Tech., Tokyo (watanabe@is.titech.ac.jp)

Research Report C-260

Abstract

We study the Isomorphism Conjecture proposed by Berman and Hartmanis. It states that all sets complete for NP under polynomial-time many-one reductions are P-isomorphic to each other. From previous research it has been widely believed that all NP-complete sets are reducible each other by one-to-one and length-increasing polynomial-time reductions, but we may not hope for the full p-isomorphism due to the existence of one-way functions. Here we showed two results on the relation between one-way functions and the Isomorphism Conjecture.

Firstly, we imporve the result of Agrawal [Agrawal, CCC'02] to show that if regular one-way functions exist, then all NP-complete sets are indeed reducible each other by one-to-one, length-increasing and P/poly-reductions. 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 NP-complete sets are reducible each other by one-one and length-increasing polynomial-time reductions but (as already shown by [Kurtz etal, JACM 95]) they are not P-isomorphic. Neverthless, we also conjecture that (different from the random oracle world) all one-way functions should have some dense easy parts, which we call P/poly-easy cylinders, where they are P/poly-invertible. Then as our second result we show that if regular one-way functions exist and furthermore all one-one, length-increasing and P/poly-computable functions have P/poly-easy cylinders, then all many-one complete sets for NP are P/poly-isomorphic.

1 Introduction

The Isomorphism Conjecture [BH77] states 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 [KMR90, You90]). On the positive side, Berman and Hartmanis showed [BH77] that NP-complete sets known at the time were all P-isomorphic to each other. Also, in [AAR98, Agr01] 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 [JY85] (also see [Wat91]) 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 [KMR95] 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 [Agr02] 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 P/poly-computable reductions.

In this paper, we show two results. Firstly, we improve the result of [Agr02]: instead of one-way *permutations* that cannot be inverted by 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 [KMR95]) 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 4). Then we show that if all one-one, length-increasing, and P/poly-computable functions have easy cylinders, then any one-one, length-increasing, and 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 P/poly.

The above two results show an interesting phenomenon: the Isomorphism Conjecture, in a slightly weaker form (isomorphisms are required to be 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 3 proves the first result and section 4 proves the second result.

2 Preliminaries

Throughout this paper, we use n to denote an integer ≥ 1. We fix our alphabet to $\Sigma = \{0, 1\}$, and we assume (unless explicitly stated otherwise) that all functions are total functions over Σ^* and that each function f is defined[1] as $f = \{f_n\}_{n\geq 1}$, for some $f_n : \Sigma^n \mapsto \Sigma^{\ell(n)}$ and some *length function* ℓ.

Definition 1. A function f is $s(\cdot)$*-secure* if the following holds for every polynomial-time randomized Turing machine M and for all sufficiently large n: $\Pr_{x\in_{\mathrm{U}}\Sigma^n}[\, M(x) = f_n(x)\,] < s(\ell(n))^{-1}$. In the above and throughout this paper, the probability (when a raondomized machine is involved) is also over random choices of M.

Definition 2. A function f is a $s(\cdot)$*-secure one-way function* if (1) f is a polynomial-time computable function and (2) its any inverse f', i.e., any function f' satisfying $f(f'(f(x))) = f(x)$ for all x, is $s(\cdot)$-secure.

[1] For simplifying our argument, we treat the null string separately and consider only strings of positive length.

Definition 3. 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: $|\Pr_{y \in_{\mathrm{U}} \Sigma^{\ell(n)}}[\,M(y) = 1\,] - \Pr_{x \in_{\mathrm{U}} \Sigma^n}[\,M(g_n(x)) = 1\,]\,| < s(n)^{-1}$.

We will make use of 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 [HILL98]. 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 $S \subseteq \Gamma$.

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

3 Many-one Complete Degrees Collapse

We begin this section by introducing some notations and notions on one-way functions. For any function f mapping elements in Σ^n to $\Sigma^{\ell(n)}$ 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. In the following, for any function f and any input x, we say that f *is one-to-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.

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

Based on this hypothesis, we prove the following collapsing result. (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.)

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

The remainder of this section is devoted to the proof of this theorem. 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 $0 \leq t_0(n) \leq n-1$, and the following holds for all $x \in \Sigma^n$.

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

In [HILL98], a pseudorandom generator is constructed from a one-way function. The following lemma captures the result of [HILL98].

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

3.1 Constructing a Nearly One-to-One One-way Function

We will transform f_0 to another one-way function that is nearly one-to-one. This construction is well-known, see, e.g., [Gol01]. We give details for the sake of completeness and also because our parameters are slightly different. (Throughout 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 $f_1 \in$ P/poly.

We first show that the function f_1 is almost one-to-one.

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

Proof. Fix n. 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

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

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

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

Therefore,

$$\frac{1}{2^{n+b(n)}} + \frac{K}{2^{2n+2b(n)}} \;\leq\; \Pr[\, f_1(X,R) = f_1(X',R')\,] \;\leq\; \frac{1}{2^{n+b(n)}} + \frac{T_0(n)}{2^{n+b(n)+a(n)}},$$

and hence,

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

□

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

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

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. Let X and R be random variables as previously defined, and let $V \in_{\mathrm{U}} \Sigma^{a(n)}$. We have $f_1(X,R) = f_0(X)R\mathrm{H}_{n,a(n)}(X,R)$. 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 $f_0(X)R\lfloor \mathrm{H}_{n,a(n)}(X,R) \rfloor_{t_0(n)-\Delta}$ 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, we have

$$\begin{aligned}
&\Pr[\, f_0(M'(f_0(X))) = f_0(X)\,] \\
&\quad\geq\ \Pr[\, f_1(M(f_0(X)RV)) = f_1(X,R)\,] \quad \text{(by definition of } M'\text{)} \\
&\quad\geq\ \frac{1}{2^{3n^{0.9\epsilon}+1}} \cdot \Pr\Big[\, \exists v' \,\big[\, |v'| = 3n^{0.9\epsilon} + 1 \ \wedge\ f_1(M(f_0(X)R\lfloor V\rfloor_{a(n)-3n^{0.9\epsilon}-1}v')) = f_1(X,R)\,\big]\ \Big] \\
&\quad\geq\ \frac{1}{2^{3n^{0.9\epsilon}+1}} \cdot \Bigg(\ \Pr\Big[\ \exists v' \Big[\, |v'| = 3n^{0.9\epsilon} + 1 \\
&\qquad\qquad\qquad \wedge\ f_1(M(f_0(X)R\lfloor \mathrm{H}_{n,a(n)}(X,R)\rfloor_{a(n)-3n^{0.9\epsilon}-1}v') = f_1(X,R)\,\Big]\ \Big] \\
&\qquad\qquad\qquad - \frac{1}{2^{n^{0.9\epsilon}-1}}\ \Bigg) \\
&\quad\geq\ \frac{1}{2^{3n^{0.9\epsilon}+1}} \cdot \frac{1}{2^{n^{0.9\epsilon}}} \ =\ \frac{1}{2^{4n^{0.9\epsilon}+1}} \ >\ \frac{1}{2^{n^{\epsilon}}}.
\end{aligned}$$

This contradicts the security of f_0. □

We now use the *hard-core bit* of f_1 [GL89] 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 $f_{\mathrm{hc}}(x,r,z) = f_2(x,r,z)\mathrm{dot}(xr,z)$, where $|z| = |x| + |r|$. Then the last bit of the output of the function f_{hc} is pseudorandom [GL89].

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 $B \in_{\mathrm{U}} \Sigma$.

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

The function f_{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: $f_{\mathrm{hc}}(u) = f_2(x,r,zz')\mathrm{dot}(xr,zz')$, where $u = xrzz'$ with x the largest prefix of u such that $2|x| + 2b(|x|) \leq |u|$, $|r| = b(|x|)$, $|z| = |x| + b(|x|)$, $|z'| = |u| - 2|x| - 2b(|x|)$, 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-to-oneness guaranteed by Lemma 4 holds for this new f_{hc} with a slightly larger non-one-to-one ratio $2^{-|xrzz'|^{\delta}}$ instead of $2^{-n^{0.9\epsilon}}$.)

3.2 Constructing a Length-Increasing and Almost One-to-One Reduction

Let A be a $\leq^{\mathrm{p}}_{\mathrm{m}}$-hard set for $\mathcal{C}$. Let $B \in \mathcal{C}$. We will use functions f_{hc}, g_{prg}, and H to construct a one-to-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-to-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 f_{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 f_{hc}.

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

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

Note that $f_{\rm hc}$ is length-increasing and $\mathcal{C}$ is closed under non-deterministic reductions; it follows that both B_1 and B_2 are in $\mathcal{C}$. Let $B_2 \le_{\rm m}^{\rm p} A$ via $h_{B_2 \cdot A}$. Notice that $f_{\rm hc}$ may not be a reduction from B_1 to B_2 since it may not be one-to-one. We show that for two random strings U and U' in $\Sigma^{2\widetilde{n}}$, the probability that $h_{B_2 \cdot A}(f_{\rm hc}(U)) = h_{B_2 \cdot A}(f_{\rm hc}(U'))$ is small. This allows us to construct a reduction $h_{B \cdot B_1}$ from B to B_1 such that $h_{B_2 \cdot A} \circ f_{\rm hc} \circ h_{B \cdot B_1}$ is a reduction from B to A with required properties. We use pseudorandomness of both $f_{\rm hc}$ and $g_{\rm prg}$ to obtain a bound on the probability of this collision. Now let

$$p \;=\; \Pr_{u,u' \in_{\rm U} \Sigma^{2\widetilde{n}}} [\; h_{B_2 \cdot A}(f_{\rm hc}(u)) = h_{B_2 \cdot A}(f_{\rm hc}(u')) \;].$$

This probability is very small.

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

Proof. Let $\ell_{\rm hc}$ be the length function for $f_{\rm hc}$; that is, $|f_{\rm hc}(u)| = \ell_{\rm hc}(2\widetilde{n})$ for any u, $|u| = 2\widetilde{n}$. Define machine M as follows: on input y, $|y| = \ell_{\rm hc}(2\widetilde{n})$, randomly pick $u' \in \Sigma^{2\widetilde{n}}$ and accept iff $h_{B_2 \cdot A}(y) = h_{B_2 \cdot A}(f_{\rm hc}(u'))$. Note that $p = \Pr_{u \in_{\rm U} \Sigma^{2\widetilde{n}}}[\, M(u) = 1 \,]$.

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

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

Define

$$\widehat{p} \;=\; \Pr[\, h_{B_2 \cdot A}(f_2(U)\overline{\mathrm{dot}(U)}) = h_{B_2 \cdot A}(f_{\rm hc}(U'))\,],$$

where $\overline{\mathrm{dot}(U)}$ denotes its complement; that is, $\overline{\mathrm{dot}(U)}$ is 0 if $\mathrm{dot}(U) = 1$ and 1 if $\mathrm{dot}(U) = 0$. Then we have

$$\begin{aligned}
&\Pr[\, M(f_2(U)B) = 1 \,] \\
&\quad = \;\; \Pr[\, h_{B_2 \cdot A}(f_2(U)B) = h_{B_2 \cdot A}(f_{\rm hc}(U'))\,] \\
&\quad = \;\; \Pr[\, h_{B_2 \cdot A}(f_2(U)B) = h_{B_2 \cdot A}(f_{\rm hc}(U')) \;\wedge\; B = \mathrm{dot}(U)\,] \\
&\qquad\quad + \Pr[\, h_{B_2 \cdot A}(f_2(U)B) = h_{B_2 \cdot A}(f_{\rm hc}(U')) \;\wedge\; B \ne \mathrm{dot}(U)\,] \;=\; \frac{1}{2}p + \frac{1}{2}\widehat{p}.
\end{aligned}$$

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

$$p \;\le\; \widehat{p} + 2^{-(2\widetilde{n})^{\delta}+1}. \tag{2}$$

To bound $\widehat{p}$, we define another machine M' that works as follows: on input u, $|u| = 2\widetilde{n}$, randomly pick a $u' \in \Sigma^{2\widetilde{n}}$ and accept iff $h_{B_2 \cdot A}(f_{\rm hc}(u)) = h_{B_2 \cdot A}(f_2(u')\overline{\mathrm{dot}(u')})$.

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

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

Hence, we have

$$\widehat{p} \;\le\; 2^{-(\widetilde{n})^{\gamma}} + \Pr[\, M'(g_{\mathrm{prg}}(S)) = 1 \,] \;\le\; 2^{-(\widetilde{n})^{\gamma}} + \Pr[\, h_{B_2\cdot A}(f_{\mathrm{hc}}(g_{\mathrm{prg}}(S))) = h_{B_2\cdot A}(f_2(U')\overline{\mathrm{dot}(U')}) \,].$$

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

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

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

We now use the universal hash function H to define reduction $h_{B\cdot B_1}$ from B to B_1. Let $m(n) = n^{\frac{2}{\delta}} - n$. Define a function h_0 by $h_0(x,r) = x\mathrm{H}_{|x|,m(|x|)}(x,r)$. A function $h_{B\cdot B_1}$ will be h_0 with its second component fixed to some specific value. We will choose this value so that $h_{B_2\cdot A} \circ f_{\mathrm{hc}} \circ h_{B\cdot B_1}$ is a length-increasing reduction from B to A that is one-to-one on Σ^n for all large enough n. The following lemma shows this can be done. Let $h = h_{B\cdot B_1} \circ f_{\mathrm{hc}} \circ h_0$.

Lemma 8. For all large enough n, there exists $r_n \in \Sigma^{(n+1)m(n)}$ that satsifies the following.
(1) For every string $x \in \Sigma^n$, we have $x \in B$ iff $h(x, r_n) \in A$ and $|h(x, r_n)| > n$ $(= |x|)$.
(2) For every $x \ne x' \in \Sigma^n$, we have $h(x, r_n) \ne h(x', r_n)$.

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

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

$$\begin{aligned}
\Pr[\, |h(X,R)| \le n \,] \;&=\; \sum_{y\in\Sigma^{\le n}} \Pr[\, h(X,R) = y \,] \;=\; \sum_{y\in\Sigma^{\le n}} \Pr[\, h_{B_2\cdot A}(f_{\mathrm{hc}}(U)) = y \,] \\
&\le\; \sqrt{\sum_{y\in\Sigma^{\le n}} (\Pr[\, h_{B_2\cdot A}(f_{\mathrm{hc}}(U)) = y \,])^2} \cdot \sqrt{\sum_{y\in\Sigma^{\le n}} 1} \\
&=\; \sqrt{\sum_{y\in\Sigma^{\le n}} \Pr[\, h_{B_2\cdot A}(f_{\mathrm{hc}}(U)) = y \,] \cdot \Pr[\, h_{B_2\cdot A}(f_{\mathrm{hc}}(U')) = y \mid h_{B_2\cdot A}(f_{\mathrm{hc}}(U)) = y \,]} \cdot \sqrt{\sum_{y\in\Sigma^{\le n}} 1} \\
&\le\; \sqrt{p} \cdot 2^{\frac{n+1}{2}} \;\le\; \frac{2^n}{2^{\frac{1}{2}(2\widetilde{n})^{\delta}}} \;\le\; \frac{1}{2^{\frac{1}{2}n^2 - n}} \;<\; \frac{1}{2^{n+2}} \quad \text{(since n is large enough).}
\end{aligned}$$

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

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

Next we show that f_{hc} is one-to-one on $h_0(\Sigma^n, r)$ for most of $r \in \Sigma^{(n+1)m}$. Again since n is large enough, we have

$$\begin{aligned}
&\Pr[\; \exists x \in \Sigma^n \,[\, f_{\mathrm{hc}} \text{ is not one-to-one on } h_0(x,R) \,] \;] \\
&\quad\le\; 2^n \cdot \Pr[\, f_{\mathrm{hc}} \text{ is not one-to-one on } h_0(X,R) \,] \\
&\quad=\; 2^n \cdot \Pr[\, f_{\mathrm{hc}} \text{ is not one-to-one on } U \,] \;\le\; \frac{2^n}{2^{(2\widetilde{n})^{\delta}}} \;\le\; \frac{1}{2^{n^2-n}} \;<\; \frac{1}{4}.
\end{aligned}$$

Similarly, most of r's ensure that $h_0(\Sigma^n, r)$ does not intersect with the range of g_{prg}. That is,

$$\begin{aligned}
&\Pr[\ \exists x \in \Sigma^n,\ \exists s \in \Sigma^{\widetilde{n}}\,[\,h_0(x,R) = g_{\mathrm{prg}}(s)\,]\ ] \\
&\quad \le\ 2^n \cdot \Pr[\exists s \in \Sigma^{\widetilde{n}}\,[\,h_0(X,R) = g_{\mathrm{prg}}(s)\,]\,]\ =\ 2^n \sum_{s\in\Sigma^{\widetilde{n}}} \Pr[\,h_0(X,R) = g_{\mathrm{prg}}(s)\,] \\
&\quad =\ 2^n \sum_{s\in\Sigma^{\widetilde{n}}} \Pr[\,U = g_{\mathrm{prg}}(s)\,]\ =\ 2^n \sum_{s\in\Sigma^{\widetilde{n}}} \frac{1}{2^{2\widetilde{n}}}\ =\ \frac{2^n}{2^{\widetilde{n}}}\ \le\ \frac{2^n}{2^{n^{\frac{2}{\delta}}}}\ \le\ \frac{1}{2^{n^2-n}}\ <\ \frac{1}{4}.
\end{aligned}$$

Finally, we bound the probability that h is not one-to-one on Σ^n. Again since n is large enough and $h_0(X,R)$ and $h_0(X',R)$ are pair-wise independent, we have

$$\begin{aligned}
&\Pr[\ \exists x \neq x' \in \Sigma^n\,[\,h(x,R) = h(x',R)\,]\ ]\ \le\ 2^{2n} \cdot \Pr[\,h(X,R) = h(X',R)\ \mid\ X \neq X'\,] \\
&\quad \le\ 2^{2n} \cdot \Pr[\,h_{B_2\cdot A}(f_{\mathrm{hc}}(U)) = h_{B_2\cdot A}(f_{\mathrm{hc}}(U'))\,]\ =\ 2^{2n} \cdot p\ \le\ 2^{-n^2+2n+2}\ <\ \frac{1}{4}.
\end{aligned}$$

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) f_{hc} is one-to-one on $h_0(\Sigma^n, r_n)$, (iii) $h_0(\Sigma^n, r_n)$ does not intersect range of g_{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

$$\begin{aligned}
x \in B\ &\Leftrightarrow\ h_0(x,r_n) \in B_1 \quad \text{(since } h_0(x,r_n) \text{ is not in range of } g_{\mathrm{prg}}) \\
&\Leftrightarrow\ f_{\mathrm{hc}}(h_0(x,r_n)) \in B_2 \quad \text{(since } f_{\mathrm{hc}} \text{ is one-to-one on } h_0(\Sigma^n, r_n)) \\
&\Leftrightarrow\ h_{B_2\cdot A}(f_{\mathrm{hc}}(h_0(x,r_n))) \in A \quad \text{(since } h_{B_2\cdot A} \text{ is a reduction from } B_2 \text{ to } A)
\end{aligned}$$

□

Finally, define a function $h_{B\cdot B_1}$ by $h_{B\cdot B_1}(x) = h(x, r_{|x|})$ 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 $h_{B\cdot B_1}(x)$ appropriately so that our requirements hold on $\Sigma^{<n_0}$.) Then $h_{B\cdot B_1}$ is in P/poly. Furthermore, by above lemma, $h_{B_2\cdot A} \circ f_{\mathrm{hc}} \circ h_{B\cdot B_1}$ is a reduction from B to A that is (i) length-increasing and (ii) one-to-one on Σ^n for all n.

3.3 Constructing a Length-Increasing and One-to-One Reduction

By Lemma 8, we have a length-increasing reduction from B to A that is one-to-one on Σ^n on all sufficiently large n. But it may be still the case that the reduction is not one-to-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.

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

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

For any x, let $|h_1(x)| \le q(|x|)$ for some polynomial q. Define a function k by $k(j) = q(k(j-1))$ and $k(1) = n_0$, where n_0 is the smallest number such that for all $n \ge n_0$, h_1 is length-increasing and one-to-one on Σ^n. 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-to-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-to-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-to-one on $\Sigma^{n'}$ and h_2 is one-to-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 is one-to-one. □

3.4 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 nondeterministic reductions, if A is $\leq^{\mathrm{p}}_{\mathrm{m}}$-hard for $\mathcal{C}$, then A is also $\leq^{\mathrm{p}}_{\mathrm{li,1\text{-}1}}$-hard for $\mathcal{C}$. (On the other hand, as shown in [KMR95], relative to a random oracle, there exists an A which is $\leq^{\mathrm{p}}_{\mathrm{m}}$-hard for $\mathcal{C}$ but not $\leq^{\mathrm{p}}_{\mathrm{li,1\text{-}1,inv}}$-hard.)

Proof. Impagliazzo [Imp96] showed that there exists a $2^{\sqrt{n}}$-secure pseudorandom generator relative to a random oracle R. Further, this generator is a one-to-one and length-increasing function.

It follows from Theorem 1 that any $\leq^{\mathrm{p}}_{\mathrm{m}}$-hard sets for $\mathcal{C}$ are $\leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}}$-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. □

4 Are NP-complete Sets Isomorphic?

Consider the class NP, and let usdiscuss the possibility of the Isomorphism Conjecture [BH77] holds. we argue that a weaker form of this conjecture may be true: all $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets for NP are P-isomorphic to each other via non-uniform reductions.

As shown above, under some plausible assumption, all $\leq^{\mathrm{p}}_{\mathrm{m}}$-complete sets for NP are $\leq^{\mathrm{p/poly}}_{\mathrm{li,1\text{-}1}}$-complete. The Isomorphism Conjecture states that these sets are all P-isomorphic to each other. The evidence against the Isomorphism Conjecture is that given a standard NP-complete set, say SAT, and a one-to-one, length-increasing one-way function f, the set $f(\mathrm{SAT})$ is NP-complete but there is no clear way to construct a polynomial-time invertible reduction of SAT to $f(\mathrm{SAT})$. In fact, as explained in the previous subsection, it was shown in [KMR95] that relative to a random oracle there exist very strong form of one-way functions for which $f(\mathrm{SAT})$ has only sparse polynomial-time computable subsets. This makes it impossible for a one-to-one, length-increasing, and P-invertible reduction to exist from SAT to $f(\mathrm{SAT})$.

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. If this property holds for all one-to-one and length-increasing one-way functions, and the corresponding dense subsets are easily identifiable, then we show that all $\leq_{\mathrm{m}}^{\mathrm{p}}$-complete sets for NP are isomorphic to each other via non-uniform polynomial-time reductions, i.e., P/poly-reductions.

For nonuniform complexity classes, we use the standard ones P/poly. Classes such as P/q are used to bound (more specifically) advice string size by some polynomial q. Here we fix one advice interpreter $I(\cdot,\cdot)$ and assume that for any advice u and input x, $I(a,x)$ is computable in $O((|a|+|x|)^2)$-time. 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 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-to-one and length increasing, and (ii) polynomial-time computable and invertible[2]. A function $e : \Sigma^* \mapsto \Sigma^*$ is called a P/poly-*embedding* if (i) e is one-to-one and length-increasing, and (ii) e is P/poly-computable.

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

Definition 4. Let f be a one-to-one, length-increasing function in P/poly. For any polynomial q, the function f has a *P/q-easy cylinder w.r.t.* π if there exist some P/poly-embedding e, and some length function $\ell(\cdot)$ such that for any n and for every string u with $|u| \geq \ell(n)$, there exists some $g_u \in \mathrm{P}/q$ such that $g_u(f(\pi(u, e(x)))) = x$ for all $x \in \Sigma^n$. In general a P/q-easy cylinder for some polynomial q is called a P/poly-easy cylinder.

Intuitively, a function f having a P/poly-easy cylinder w.r.t. π has a "parameterized" dense part in its domain on which it is easy to invert. Note that a P/poly-embedding e can be chosen depending on f and that one can define a P/q-computable function g_u for each parameter u. We believe that all one-to-one and length-increasing functions in P/poly have a 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-to-one and length-increasing functions in P/poly have a 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. Now we make the following conjecture.

> **Easy Cylinder Conjecture:** All one-to-one and length-increasing functions in P/poly have a P/poly-easy cylinder.

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

The known one-way functions all appear to have a P/poly-easy cylinder. Let us see some examples. First we fix our paring function π. Though a bit tricky, in order to simplify our explanation, here we define it as follows.

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

where $\mathrm{pre}(u)$ denotes a prefex-free code of u, and $(\cdots)^{\mathrm{rev}}$ is a mirror image of $\cdots$.

We here consider the following two functions, the former is from factorization and the latter is from RSA.

$$f_\times(x,y) \;=\; x \times y, \quad \text{and} \quad f_{\mathrm{rsa}}(m,e,n) \;=\; (m^e \,(\mathrm{mod}\, n), e, n).$$

Precisely speaking, e.g., $f_\times$ is a function from Σ^{2n} to Σ^{2n} and two numbers x and y are obtained from the first and the last half of a given input binary string. Similarly, we assume that m, e, and n (resp., m^e (mod n), e, and n) are of the same length and encoded as a single binary string. We believe that these functions are not polynomial-time invertible. Nevertheless, it is easy to see that they have P/poly-easy cylinders. To see this, for $f_\times$, we use an embedding function $e_1(x) = 0x$ and a length function $\ell(n) = n+1$. Then for any fixed $u \in \Sigma^{\geq \ell(n)}$, the first half bits of $\pi(u, e_1(x))$ is fixed for any x; that is, $\pi(u, e_1(x)) = u'x'$ with some u' and x' of length n', 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. On the other hand, for f_{rsa}, we use an embedding function $e_2(x) = 1x$ and a length function $\ell(n) = 2n+2$. Then similarly, each $u \in \Sigma^{\geq \ell(n)}$ 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).

We provide some more examples of functions believed to be one-way that have an easy cylinder.

Subset-sum. $f_{\mathrm{ss}}(x_1, x_2, \ldots, x_n, S) = (x_1, x_2, \ldots, x_n, \sum_{i \in S} x_i)$, $|x_1| = |x_2| = \cdots = |x_n| = n$. Use embedding function $e_2(x) = 1x$, and $\ell(n) = (n+1)^2$. Then for any fixed $u \in \Sigma^{\geq \ell(n)}$, the last $\ell(n)$ 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. $f_{\mathrm{ecc}}(M, x, e) = (M, xM + e)$ with $|M| = nm$ is an $n \times m$ matrix over F_2, x a $1 \times n$ vector, and e a $1 \times m$ error vector (with not too many 1's). Use embedding function $e_1(x) = 0x$ and $\ell(n) = (n+1)^2 + n + 1$. Then for any fixed $u \in \Sigma^{\geq \ell(n)}$, the first $\ell(n)$ 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. $f_{\exp}(g, e, p) = (g, g^e\,(\mathrm{mod}\, p), p)$ with $|g| = |e| = |p|$. 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 this way, we can easily show known one-way function candidates all have P/poly-easy cylinders. This may be a good support for our Easy Cylinder Conjecture. On the other hand, based on this conjecture, we can show that $\leq_{\text{li,1-1}}^{\text{p/poly}}$-reducibility implies $\leq_{\text{li,1-1,inv}}^{\text{p/poly}}$-reducibility. Our result is stated in terms of the following canonical NP-complete set.

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

Theorem 3. Suppose that Easy Cylinder Conjecture holds. Then for any set A, $K \leq_{\text{li,1-1}}^{\text{p/poly}} A$ implies $K \leq_{\text{li,1-1,inv}}^{\text{p/poly}} A$.

Proof. Consider any set A such that $K \leq_{\text{li,1-1}}^{\text{p/poly}} A$, and let f be a one-to-one, length-increasing, and P/poly-computable reduction from K to A. Then it follows from Easy Cylinder Conjecture that f has a P/q-easy cylinder w.r.t. some polynomial q, P/poly-embedding function e, and length function $\ell(\cdot)$. We may assume that e is P/r-computable for some polynomial r.

We define a 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_n that executes as follows on input $y = e(x)$ for each $x \in \Sigma^n$: Guess x and check whether $e(x)$ is indeed y; if not reject y, and if so, accept y if and only if x is in K. Here we note that the advice of size $r(n)$ for computing e on Σ^n is hardwired in M_n. On the other hand, from our assumption on the advise interpreter I, $M_n(y)$ halts in $O(r(n)^2 + |y|)$ steps. Thus, by letting p_n be a code of this machine M_n that is (with some padding) sufficiently long, we have M_{p_n} halts and accepts $e(x)$ in $|p_n e(x)|$ steps iff M_n accepts $e(x)$ iff $x \in K$ for all $x \in \Sigma^n$. We may assume that $\ell(n) \leq |p_n| \leq r'(n)$ for some polynomial r'.

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

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

Then it follows from the above that this is a reduction from K to K. Furthermore, h is P/$(r+r')$-computable.

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

Finally we summarize our discussion as follows.

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

References

[AAR98] 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.

[Agr01] M. Agrawal, The first order isomorphism theorem, in *Proceedings of Twenty First FST&TCS*, Lecture Notes in Comp. Sci. 2245, 70–82, 2001.

[Agr02] M. Agrawal, Pseudo-random generators and the structure of complete degrees, in *Proceedings of the Conference on Computational Complexity*, IEEE, 139–146, 2002.

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

[GL89] 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.

[Gol01] O. Goldreich, *Foundation of Cryptography I: Basic Tools*, Cambridge University Press, 2001.

[HILL98] 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.

[Imp96] R. Impagliazzo, Very strong one-way functions and pseudo-random generators exists relative to a random oracle, Manuscript, January 1996.

[JY85] D. Joseph and P. Young, Some remarks on witness functions for nonpolynomial and noncomplete sets in NP, *Theoret. Comput. Sci.*, 39:225–237, 1985.

[KMR90] S. Kurtz, S. Mahaney, and J. Royer, The structure of complete degrees, in *Complexity Theory Retrospective* (A. Selman, ed.), Springer-Verlag, 108–146, 1990.

[KMR95] 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.

[Wat91] O. Watanabe, On the p-isomorphism conjecture, *Theoret. Comput. Sci.*, 83:337–343, 1991.

[You90] P. Young, Juris Hartmanis: Fundamental contributions to isomorphism problems, in *Complexity Theory Retrospective* (A. Selman, ed.), Springer-Verlag, 28–58, 1990.