Theoretical Computer Science 38 (1985) 157-165
North-Holland

ON ONE-ONE POLYNOMIAL TIME EQUIVALENCE RELATIONS

Osamu WATANABE

Department of Information Science, Tokyo Institute of Technology, Ookayama, Meguroku, Tokyo, Japan

Communicated by R.V. Book
Received October 1983
Revised December 1984

Abstract. Two sets A and B are one-one polynomial time equivalent (one-one p-equivalent) if there are polynomial time one-one reductions from A to B and from B to A. In this paper we show that all EXPTIME complete sets are one-one p-equivalent by length increasing reductions. Moreover we show this result for many complexity classes which can be proved by a straightforward diagonalization to contain P properly.

We also obtain some nontrivial examples in EXPTIME − P which show the difference between one-one and many-one polynomial time equivalence relations.

1. Introduction

Many families of resource bounded recursive languages, such as P, NP or EXPTIME, have complete sets under polynomial time reductions. Let $\mathscr{L}$ be one of such families. Any complete sets for $\mathscr{L}$ are polynomial time reducible to each other, i.e. they are many-one polynomial time equivalent (many-one p-equivalent). This means that they have the same degree of difficulty under polynomial time reductions. Moreover we have an intuitive feeling that $\mathscr{L}$-complete sets have similar structure. Berman and Hartmanis defined this type of structural similarity between two sets by a existence of a polynomial time isomorphism (p-isomorphism), and conjectured (and also showed some evidence) that all NP complete (EXPTIME complete or PTAPE complete) sets are p-isomorphic.

In this paper we will consider one-one polynomial time equivalence (one-one p-equivalence) relations, i.e. the existence of polynomial time one-one reductions to each other, and we will show that all EXPTIME-complete sets are one-one p-equivalent. We also extend this result to many complexity classes which provably contain P properly.

Moreover we will also prove, at the same time, that all EXPTIME-complete sets are one-one p-equivalent by length increasing functions. So it follows from Theorem

1 of [3] that, if the inverse of each length increasing polynomial time injection is polynomial time computable, then all EXPTIME-complete sets are p-isomorphic.

We also consider the problem whether all the sets in EXPTIME − P having the same many-one degree are structurally similar or not. We introduce a notion called 'functional immunity' (f-immunity for short) that is another of the many possible analogues in complexity theory of the 'immunity'-notion in recursive function theory [8], and show that it is useful for the investigation of this problem.

2. Preliminaries

Let Σ denote a fixed finite alphabet which contains at least 0 and 1, and let Σ^* denote the set of all words on Σ. By a *language* we mean a subset of Σ^*. We shall consider languages encoded over Σ. We use $|x|$ to denote the length of string x and $\#S$ to denote the number of elements in a set S.

Our basic computation model is the *standard multi-tape Turing machine* (TM) acceptors and transducers [3, 4, 6]. Let P and NP denote the class of languages accepted by deterministic and nondeterministic polynomial time bounded TM acceptors, respectively, and let

$$\text{EXPTIME} = \bigcup_{c>0} \text{DTIME}(2^{cn}).$$

Let t_i denote the mapping from Σ^* to Σ^* computed by the ith polynomial time bounded TM transducer. We use $\mathcal{T}$ to denote $\{t_i\}_{i>0}$. We say that a function f is *length increasing* if for all w we have $|f(w)|>|w|$, and that f is (polynomial time) *invertible* if f is a one-one mapping (not necessarily onto) and f^{-1} is also computable in polynomial time. We define several reduction relations as follows.

Definition 2.1. Let $A, B \subseteq \Sigma^*$.

(1) A is *many-one* p-*reducible* to B ($A \leqslant_{\text{m}} B$) if there is a function $t_i \in \mathcal{T}$ such that $t_i(x) \in B$ iff $x \in A$.

(2) A is *one-one* p-*reducible* to B ($A \leqslant_1 B$) if $A \leqslant_{\text{m}} B$ by a one-one reduction.

(3) A is *length increasingly one-one* p-*reducible* to B ($A \leqslant_{1,1\text{e}} B$) if $A \leqslant_1 B$ by a length increasing reduction.

It is clear that $A \leqslant_{1.1\text{e}} B$ implies $A \leqslant_1 B$ and that $A \leqslant_1 B$ implies $A \leqslant_{\text{m}} B$. A set C is *complete* for $\mathcal{L}$, a class of languages, if $C \in \mathcal{L}$ and $A \leqslant_{\text{m}} C$ for all $A \in \mathcal{L}$.

Definition 2.2. Let $A, B \subseteq \Sigma^*$.

(1) A and B are *many-one* p-*equivalent* ($A \equiv_{\text{m}} B$) if $A \leqslant_{\text{m}} B$ and $B \leqslant_{\text{m}} A$.

(2) A and B are *one-one* p-*equivalent* ($A \equiv_1 B$) if $A \leqslant_1 B$ and $B \leqslant_1 A$.

(3) A and B are *pseudo* p-*isomorphic* ($A \equiv_{\text{p}} B$) if $A \leqslant_{1,1\text{e}} B$ and $B \leqslant_{1.1\text{e}} A$.

(4) A and B are p-*isomorphic* ($A \equiv B$) if $A \leqslant_{\text{m}} B$ by an invertible bijection f, that is, $A \leqslant_1 B$ by f and $B \leqslant_1 A$ by f^{-1}.

The following theorem shows the relation between pseudo p-isomorphism and p-isomorphism.

Theorem 2.3 ([3, Theorem 1]). *If $A \equiv_p B$ by invertible reductions, then $A \equiv B$.*

3. Pseudo p-isomorphism of complete sets

In this section we first show that all EXPTIME-complete sets are pseudo p-isomorphic. That is, we prove that all EXPTIME-complete sets are one-one p-equivalent and that these equivalence relation can be achieved by length increasing reductions.[1] Then we extend this result to other complexity classes and show that, for many deterministic complexity classes which can be proved to contain P properly, the same result holds.

In recursive function theory, a concept 'cylinder' is used to construct one-one reductions from many-one reductions. In [9] a set A is called p-*cylinder* if $A \equiv A \times \Sigma^*$. Here we show that EXPTIME-complete sets have a property very similar to this.

Theorem 3.1. *Let A be any* EXPTIME *complete set. Then $A \equiv_p A \times \Sigma^*$.*

It is clear that $A \leqslant_{1.1e} A \times \Sigma^*$. So we need to show that $A \times \Sigma^* \leqslant_{1.1e} A$.

Berman and Hartmanis constructed a set in EXPTIME whose reduction to any other set must be one-one almost everywhere [3]. Here we extend this idea to obtain a length increasing one-one p-reduction from $A \times \Sigma^*$ to A. First we define a set C by giving a description of a TM acceptor M_C that accepts C. The inputs to M_C must be of the form $\langle i, x, y\rangle$, where i is a positive integer, and x, y are words in Σ^*.

Let M_A denote an exponential time bounded TM acceptor that accepts A. On an input z, $z = \langle i, x, y\rangle$, M_C operates as follows (where n is used to denote $|z|$):

begin

(1) compute $u = t_i(\langle i, x, y\rangle)$ for 2^n actual steps. **If** the computation needs more than 2^n steps **then** go to step (4).

(2) **if** $|u| \leqslant |z|$ **then if** M_A accepts u **then** M_C rejects z
else M_C accepts z
else go to step (3).

(3) **for** all $\langle x', y'\rangle$ such that $\langle x', y'\rangle < \langle x, y\rangle$ in lexicographic order **do**

(a) compute $t_i(\langle i, x', y'\rangle)$ for 2^n actual steps.

(b) **if** the computation of (a) needs more than 2^n steps **then** go to step (4).

(c) **if** $u = t_i(\langle i, x', y'\rangle)$ **then if** M_A accepts x' **then** M_C rejects z
else M_C accepts z
else go to the next loop.

[1] The same result was independently shown by Dr. L. Berman in his Ph.D. Thesis (1977). We will state a more simple and easy proof here.

(4) M_C accepts z iff M_A accepts x.

end

In the following we will show several properties of the set C. It is easy to show that, for some $c>0$, the computation time of M_C is bounded by 2^{cn} steps.

Lemma 3.2. $C \in$ EXPTIME.

Lemma 3.3. *If C is* p*-reducible to A by some function $t_i \in \mathcal{T}$, then there exist $n_i > 0$ such that*

(1) $|t_i(\langle i, x, y\#^{n_i}\rangle)| > |\langle i, x, y\#^{n_i}\rangle|$.

(2) *For all $\langle x', y'\rangle$ and $\langle x, y\rangle$ such that $\langle x', y'\rangle \neq \langle x, y\rangle$, we have $t_i(\langle i, x', y'\#^{n_i}\rangle) \neq t_i(\langle i, x, y\#^{n_i}\rangle)$.*

(3) *For all x and y, we have $\langle i, x, y\#^{n_i}\rangle \in C$ iff $x \in A$.*

Proof. The acceptor M_C uses an ordinary universal TM transducer, M_T to compute each function t_j in $\mathcal{T}$. Since each t_j is polynomially computable, there exists a polynomial p_j such that for all x, $|x|<n$, M_T computes t_j within p_j steps. Let n_i be an integer such that $p_i < 2^n$ for all $n > n_i$.

(1) Suppose that there exist x and y such that $|t_i(\langle i, x, y\#^{n_i}\rangle)| < |\langle i, x, y\#^{n_i}\rangle|$. Since $t_i(\langle i, x, y\#^{n_i}\rangle)$ is computable within 2^n steps, the computation of M_C on input $\langle i, x, y\#^{n_i}\rangle$ reaches step (2). Thus

$$\begin{aligned}\langle i, x, y\#^{n_i}\rangle \in C &\Leftrightarrow M_C \text{ accepts } \langle i, x, y\#^{n_i}\rangle\\ &\Leftrightarrow M_A \text{ rejects } t_i(\langle i, x, y\#^{n_i}\rangle)\\ &\Leftrightarrow t_i(\langle i, x, y\#^{n_i}\rangle) \notin A.\end{aligned}$$

This contradicts the fact that t_i is a reduction from C to A.

(2) Suppose that there exist x and y such that for some $\langle x', y'\rangle$, $\langle x', y'\rangle < \langle x, y\rangle$, $t_i(\langle i, x', y'\#^{n_i}\rangle) = t_i(\langle i, x, y\#^{n_i}\rangle)$. Let $\langle x', y'\rangle$ be the smallest such pair by lexicographic order. Then it is easy to show that the execution of M_C on $\langle i, x', y'\#^{n_i}\rangle$ and on $\langle i, x, y\#^{n_i}\rangle$ terminate at step (4) and at step (3)(c) respectively. Thus

$$\begin{aligned}\langle i, x, y\#^{n_i}\rangle \in C &\Leftrightarrow M_C \text{ accepts } \langle i, x, y\#^{n_i}\rangle\\ &\Leftrightarrow M_A \text{ rejects } x'\\ &\Leftrightarrow \langle i, x', y'\#^{n_i}\rangle \notin C.\end{aligned}$$

But $t_i(\langle i, x', y'\#^{n_i}\rangle) = t_i(\langle i, x, y\#^{n_i}\rangle)$, which contradicts the fact that t_i is a reduction from C to A.

(3) From (1) and (2) we have that, for all x and y, the execution of M_C on input $\langle i, x, y\#^{n_i}\rangle$ reaches step (4). So $\langle i, x, y\#^{n_i}\rangle \in C$ if and only if $x \in A$. □

Proof of Theorem 3.1. Since $C \in$ EXPTIME and A is EXPTIME-complete, there

exists a p-reduction t_i from C to A. Then t_i satisfies the conditions of Lemma 3.3. So f, a one-one and length increasing p-reduction from $A \times \Sigma^*$ to A, is defined as follows:

$$f(\langle x, y\rangle) = t_i(\langle i, x, y\#^{n_i}\rangle). \qquad \square$$

Corollary 3.4. *Let A and B be any* EXPTIME*-complete sets. Then $A \equiv_p B$.*

Proof. Let f be a one-one and length increasing p-reduction from $B \times \Sigma^*$ to B. Since $A \in$ EXPTIME and B is EXPTIME-complete, there exists a p-reduction g from A to B. Then we can define h, a one-one and length increasing p-reduction from A to B, as follows:

$$h(x) = f(\langle g(x), x\rangle).$$

Thus we have $A \leqslant_{1.1e} B$. The proof of converse is analogous. $\square$

Let $\mathscr{L}$ be a class of languages accepted by resource bounded TM acceptors. It is obvious that if $\mathscr{L} \supseteq$ EXPTIME, then the same result as Corollary 3.4 also holds for $\mathscr{L}$. However, it is also easy to show the same result for many other resource bounded deterministic complexity classes by slightly modifying the definition of M_C.

A function $f(n)$ is said to be *more than polynomial* if for any polynomial $p(n)$, $f(n) > p(n)$ for almost all n.

Theorem 3.5. *Let $S(n)$ be a tape constructible function which is more than polynomial. Then all complete sets for* DTAPE($S(n)$) *are pseudo* p*-isomorphic.*

Proof. It is easy to modify M_C so that M_C is $S(n)$ tape bounded. Here we omit the proof since it is almost the same as those of Theorem 3.1 and Corollary 3.4. $\square$

The above theorem implies that for almost all tape bounded complexity classes which are provable to contain P properly by a usual diagonalization technique [4, 6], we have such one-one equivalence results. Unfortunately we need more restrictions on resource bounded functions when we consider time complexity.

For any $k > 0$, we define k-SUBEXPTIME by

$$k\text{-SUBEXPTIME} = \bigcup_{c>0} \text{DTIME}(2^{cn^{1/k}}).$$

Theorem 3.6. *Let $k > 0$. All complete sets for* k-SUBEXPTIME *are pseudo* p*-isomorphic.*

Proof. In order to make M_C $2^{cn^{1/k}}$ time bounded, we have to modify M_C so that it may not examine more than $2^{cn^{1/k}}$ different words in step 3. That is, M_C is constructed to ensure that if $\langle x', y'\rangle$ and $\langle x, y\rangle$ differ within the first $n^{1/k}$ bits, then $t_i(\langle i, x', y'\rangle) \neq$

$t_i(\langle i, x, y\rangle)$. We define a one-one and length increasing p-reduction from $A \times \Sigma^*$ to A as follows:

$$f(\langle x, y\rangle) = t_i(\langle i, x, y \# {}^{(|x|+|y|)^k+n_i}\rangle).$$

The rest of the proof is the same as that of Corollary 3.4. □

As a corollary of Theorem 3.1 we will show some structural property of EXPTIME-complete sets.

For each set $A \subseteq \Sigma^*$, define the *census function* C_A of A by $C_A = \#\{x \in A \mid |x| \leq n\}$. A set A has *exponential density* if there exists a polynomial p such that $C_A(p(n)) = \omega(2^n)$. Balcázar and Schöning show that, for every EXPTIME-complete set A, both A and A^c (the complement of the set A) must have exponential density [1]. An immediate corollary of Theorem 3.1 gives us this result.

Corollary 3.7. *Let A be any* EXPTIME*-complete set. Then both A and A^c have exponential density.*

4. Structural differences among many-one p-equivalent sets

From Corollary 3.4 we know that all EXPTIME-complete sets have similar structures. Now we have a question: Are all the sets in EXPTIME − P having the same many-one degree structurally similar? In this section we will consider this problem.

There are many sorts of 'structural similarity'. Among them 'similarity of density' is the lowest type of similarity and the easiest one to consider. It is easy to construct two sets in EXPTIME − P of a same many-one degree which do not have a similar density (e.g. one is sparse and the other is of exponential density). These two sets, of course, differ in higher types of similarity. So we have an answer to the above question. However, to get deeper understanding of the structural properties of the class EXPTIME, we need to consider higher types of similarity. Here we will investigate similarities such as one-one p-equivalence and pseudo p-isomorphism. For them, the above mentioned question becomes as follows: Are there any sets in EXPTIME − P which have the same many-one degree and a similar density, but do not have these types of similarity? We will also consider what concepts are useful for showing structural nonsimilarity of these types.

From the proof of Corollary 3.4, we know that if each set A in EXPTIME − P is one-one p-equivalent (respectively pseudo p-isomorphic) to its cylinderification $A \times \Sigma^*$ then any sets of the same many-one degree must be one-one p-equivalent (resp. pseudo p-isomorphic). Moreover any set A and its cylinderification $A \times \Sigma^*$ have a same many-one degree. This motivates us to consider the structural similarity relation between one set and its cylinderification.

In recursive function theory the concepts 'simpleness' and 'immunity' are introduced to study the difference between one-one and many-one reducibilities. These notions have been also introduced into computational complexity theory [1, 2, 3].

A set A is *immune* if it is infinite and for all B in P we have that $B \not\subset A$.

Recently Balcázar and Schöning have introduced a stronger notion 'strong bi-immunity' and have showed that there exist strongly bi-immune (so immune) sets in EXPTIME of any (reasonable) density [1]. So we have a set A_1 such that A_1 and A_1^c are of exponential density and that A_1 is immune. From this fact it is easy to show the following Proposition.

Proposition 4.1. *There exists a set* A_1 *in* EXPTIME$-$P *such that* A_1 *and* A_1^c *are of exponential density and that* $A_1 \times \Sigma^* \not\leq_{1.1e} A_1$ *(so* $A_1 \times \Sigma^* \not\equiv_p A_1$*).*

However, it seems to be difficult to get examples of non one-one p-equivalent sets using this type of immunity only. So we will introduce the following notion.

A set A is *functionally immune* (*f-immune* for short) if A and A^c (complement of A) are of exponential density and for all one-one polynomially computable function g we have $g(\Sigma^*) \not\subset A$.

Using a technique similar to that used in [1] we obtain an f-immune set in EXPTIME$-$P.

Theorem 4.2. *There exists an* f*-immune set* A_2 *in* EXPTIME$-$P.

Proof. We will construct the desired set A_2 by a stage construction. At stage n, for each string of length n we determine whether it is put into A_2 or not. For any string $x \in \Sigma^*$ let $\overline{0x} = 1x$ and $\overline{1x} = 0x$ respectively.

Stage 0: $A_2 \leftarrow \emptyset$ and $i \leftarrow 1$.

Stage $n > 0$:

Case (a) $t_i(x)$ is computable in 2^n steps for all x, $|x| \leq n$, **and** t_i is not one-one on $\{x \mid |x| \leq n\}$ **then**

$$A_2 \leftarrow A_2 \cup 0\,\Sigma^{n-1} \quad \text{and} \quad i \leftarrow i+1.$$

Case (b) $t_i(x)$ is computable in 2^n steps for all x, $|x| \leq n$, **and** there is a x such that $|x| \leq n$ and $|t_i(x)| = n$ **then**

$$A_2 \leftarrow A_2 \cup 0\,\Sigma^{n-1} \cup \{\overline{t_i(x)}\} - \{t_i(x)\} \quad \text{and} \quad i \leftarrow i+1.$$

Case (c) **Otherwise** $A_2 \leftarrow A_2 \cup 0\,\Sigma^{n-1}$.

Then it is easy to show that $A_2 \in$ EXPTIME and that A_2 is f-immune. Suppose that $A_2 \in$ P, then we can define the following polynomially computable one-one function f:

$$f(x) = \begin{cases} 0x & \text{if } 0x \in A_2, \\ 1x & \text{otherwise.} \end{cases}$$

But $f(\Sigma^*) \subseteq A_2$, which contradicts the f-immunity of A_2. □

This set A_2 satisfies our purpose.

Corollary 4.3. *There exists a set A_2 in* EXPTIME − P *such that A_2 and A_2^c are of exponential density and that $A_2 \times \Sigma^* \not\leq_1 A_2$ (so $A_2 \times \Sigma^* \not\equiv_1 A_2$).*

5. Conclusion

We will summarize our results and state related open problems.

We showed that all EXPTIME-complete sets are pseudo p-isomorphic (i.e. one-one p-equivalent by length increasing reductions). How can we extend this to other complexity classes? For the tape complexity measure, we can prove this result for almost all complexity classes which can be proved to contain P properly by a straightforward diagonalization technique. For the time complexity measure we can prove it for k-SUBEXPTIME (i.e. $\bigcup_{c>0} \mathrm{DTIME}(2^{cn^{1/k}})$) for any k. However, at present we can not prove it, for example, for classes such as $\bigcup_{c>0} \mathrm{DTIME}(2^{c \log^2 n})$. The following problems are interesting:

(1) Can we prove a pseudo p-isomorphic result for such classes as $\bigcup_{c>0} \mathrm{DTIME}(2^{c \log^2 n})$?

(2) Are all NP-complete sets pseudo p-isomorphic (or one-one p-equivalent) if P ≠ NP? Can we strengthen Mahaney's result [7]?

Although we proved that all EXPTIME-complete sets are pseudo p-isomorphic, it seems difficult to show that they are p-isomorphic. The main difficulty is the (polynomial time) invertibility of polynomial time computable one-one functions [9]. If each polynomial time computable function is invertible, then pseudo p-isomorphism is the same as p-isomorphism. So we have the following open problem:

(3) Find an example to show the difference between pseudo p-isomorphism and p-isomorphism assuming the existence of a noninvertible polynomial time one-one function.

From the above result we know that $\equiv_p$ and $\equiv_m$ (so $\equiv_1$ and $\equiv_m$) coincide on EXPTIME-complete sets. There also exist examples of sets on which $\equiv_p$ (respectively $\equiv_1$) differs from $\equiv_m$. A sparse (cosparse) set A and its cylinderification $A \times \Sigma^*$ are trivial examples since it is obvious that $A \equiv_m A \times \Sigma^*$ and that $A \not\equiv_1 A \times \Sigma^*$ (so $A \not\equiv_p A \times \Sigma^*$). We obtained such nontrivial examples. That is, we constructed a set A in EXPTIME − P such that both of A and A^c (complement of A) are exponential density and that $A \equiv_m A \times \Sigma^*$ but $A \not\equiv_1 A \times \Sigma^*$ (so $A \not\equiv_p A \times \Sigma^*$). It is interesting to consider the following problem:

(4) Are there such examples in NP − P (if P ≠ NP)? Note that it is difficult to show the existence of a sparse set in NP − P (if P ≠ NP) [5].

Acknowledgment

The author expresses his appreciation to Prof. Kojiro Kobayshi for his careful reading of the earlier version of this paper. He also thanks an anonymous referee for pointing out to him related works, and Prof. Ronald Book, Dr. Leonard Berman and Mr. Eric Allender for sending him copies of related papers.

References

[1] J. Balcázar and U. Schöning, Bi-immune sets for complexity classes, *Math. Systems Theory*, to appear.
[2] L. Berman. On the structure of complete sets, *Proc. 17th FOCS* (1976) 76-80.
[3] L. Berman and J. Hartmanis, On isomorphisms and density of NP and other complete sets, *SIAM J. Comput.* **6** (2) (1977) 305-322.
[4] J. Hartmanis, *Feasible Computations and Provable Complexity Properties* (SIAM, Philadelphia, 1978).
[5] J. Hartmanis, On sparse sets in NP−P, *Inform. Process. Lett.* **16** (1983) 55-60.
[6] J. Hopcroft and J. Ullman, *Introduction to Automata Theory, Language, and Computation* (Addison-Wesley, Reading, MA, 1979).
[7] S. Mahaney, Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis, *J. Comput. System Sci.* **25** (1982) 130-143.
[8] H. Rogers Jr., *Theory of Recursive Functions and Effective Computability* (McGraw-Hill, New York, 1967).
[9] P. Young, Some structural properties of polynomial reducibilities, *Proc. 15th STOC* (1983) 392-401.