Theoretical Computer Science 120 (1993) 279–291 Elsevier 279

Note

On symmetric differences of NP-hard sets with weakly P-selective sets*

Bin Fu**

Department of Computer Science, Beijing Computer Institute, 100044 Beijing, People's Republic of China, and Beijing Laboratory of Cognitive Science, The University of Science and Technology of China

Hong-zhou Li***

Department of Mathematics, Yunnan Education College, 650031 Kunning, People's Republic of China

Communicated by R.V. Book Received May 1992 Revised November 1992

Abstract

Fu, B. and H.-z. Li, On symmetric differences of NP-hard sets with weakly-P-selective sets, Theoretical Computer Science 120 (1993) 279-291.

The symmetric differences of NP-hard sets with weakly-P-selective sets are investigated. We show that if there exist a weakly-P-selective set A and an NP- \leq_{m}^{p} -hard set H such that $H - A \in P_{btt}(sparse)$ and $A - H \in P_{m}(sparse)$ then P = NP. So no NP- \leq_{m}^{p} -hard set has sparse symmetric difference with any weakly-P-selective set unless P = NP. The proof of our main result is an interesting application of the tree prunning techniques (Fortune 1979; Mahaney 1982). In addition, we show that there exists a P-selective set which has exponentially dense symmetric difference with every set in $P_{btt}(sparse)$.

Correspondence to: B. Fu, Beijing Computer Institute, 100044 Beijing, People's Republic of China. * This research is supported in part by HTP863.

** Department of Computer Science, Beijing Computer Institute, Beijing, 100044, P.R. China & Beijing Laboratory of Cognitive Science, The University of Science and Technology of China.

*** This research was performed while this author was visiting Beijing Computer Institute. Department of Mathematics, Yunnan Education College, Kunming, 650031, P.R. China.

0304-3975/93/\$06.00 © 1993-Elsevier Science Publishers B.V. All rights reserved

1. Introduction

The low sets (such as sparse sets, P-selective sets, cheatable sets, etc.) play very important roles in the study of the structures of hard sets in complexity theory. The study of what happens when hard sets can be reducible to sparse sets has long and rich history. The most notable early result is due to Mahaney [10], who proved that if $NP \subseteq P_m$ (sparse) then P = NP. Ogiwara and Watanabe [11] improved Mahaney's result by showing that if $NP \subseteq P_{bit}(sparse)$ then P = NP. Similar results on relationships between NP-hard sets and other low sets have been found. P-selective sets were introduced by Selman [13, 15] as polynomial-time analogue of the semirecursive sets [7]. He used them to distinguish polynomial-time m-reducibility from Turing-reducibility in NP under the assumption $E \neq NE$, and proved that if every set in NP is \leq_{ptt}^{p} -reducible to P-selective set, then P=NP. Weakly-P-selective sets were introduced by Ko [8] as a generalization of the P-selective sets. He showed that (1) weakly-P-selective sets cannot distinguish polynomial-time m-completeness from T-completeness in NP unless the polynomial-time hierarchy collapses to Σ_2^p , and (2) there exist sets in NP that are not \leq_{dtt}^{P} -reducible to a weakly-P-selective set unless P = NP. Toda [17] studied the truth table reducibility of intractable set to P-selective sets. He proved that (1) if UP is polynomial time truth table reducible to P-selective sets, then P = UP and (2) if NP is polynomial time truth table reducible to P-selective sets, then P = FewP and R = NP.

In this paper, we investigate the structural properties of NP- \leq_{m}^{P} -hard sets by combining weakly-P-selective sets with sparse sets.

Yesha [18] first considered the symmetric difference between NP- \leq_{m}^{P} -hard sets and the sets in P. He proved that no NP- \leq_m^P -hard sets has O(log log n) dense symmetric difference with any set in P unless P = NP. Schöning [12] showed that no paddable NP- \leq_{m}^{P} -hard sets has sparse symmetric difference with any set in P unless P=NP. Ogiwara and Watanabe [11] proved that $NP \subseteq P_{btt}$ (sparse) $\Rightarrow P = NP$ and a more simpler proof of this important theorem was given by Homer and Longpré [6]. From Ogiwara and Watanabe's [11] theorem, we know no NP-hard set has sparse symmetric difference with any set in P unless P = NP. Fu [4] investigated lower bounds of closeness between many complexity classes. He showed that if an NP- $\leq \frac{P}{m}$ -hard set is the union of a set in $P_{\text{btt}}(\text{sparse})$ with set A then $NP \subseteq P_{\text{dtt}}(A)$. Thus no NP-hard set can be the union of a set in P_{btt} (sparse) and a set in co-NP (FewP) unless NP = co-NP (NP = FewP). Recently Fu and Li [5] showed that if an NP-hard set has sparse symmetric difference with the set A then NP $\subseteq P_{ptt}(A)$. Since both co-NP and R are closed under positive truth-table reductions, thus no NP- \leq_m^P -hard set has sparse symmetric difference with any set in co-NP (R) unless NP=co-NP (NP=R). The symmetric difference between E-hard sets and subexponential-time-computable sets were studied by Tang et al. [16]. They proved that the symmetric difference of an $E \le m^{P}$ -hard set and a subexponential-time-computable set is still $E \le m^{P}$ -hard.

The symmetric differences of NP- \leq_{m}^{P} -hard sets with weakly-P-selective sets are investigated in this paper. We show that if there exist an NP- \leq_{m}^{P} -hard set H and

a weakly-P-selective set A such that $H - A \in P_{btt}(sparse)$ and $A - H \in P_m(sparse)$ then P = NP. The tree prunning methods are used very carefully in the proof of the result. This makes it of special interest. In the last section, we separate P-selective sets from $P_{btt}(sparse)$ by constructing a P-selective set that has exponentially dense symmetric difference with any set in $P_{btt}(sparse)$.

2. Preliminaries

We fix $\Sigma = \{0, 1\}$ as our alphabet. By a "string" we mean an element of Σ^* . For a string x in Σ^* , |x| denotes the length of x. Let $S \subseteq \Sigma^*$, the cardinality of S is denoted by ||S||, set $S^{\leq n}(S^{\leq n})$ consists of all words of length $= n(\leq n)$ in S. In particular, let $\Sigma^n = \{x | x \in \Sigma^* \text{ and } |x| = n\}$ and $\Sigma^{\leq n} = \{x | x \in \Sigma^* \text{ and } |x| \leq n\}$. For any $u \in \Sigma^*$ and $A \subseteq \Sigma^*$, $uA = \{ux | x \in A\}$. We use λ to denote the null string. N represents the set $\{0, 1, \ldots\}$.

We use the pairing function $\langle .,. \rangle : \Sigma^* \times \Sigma^* \to \Sigma^*$. It is convenient to assume for any x, y in $\Sigma^*, |\langle x, y \rangle| \leq 2(|x|+|y|)$.

Our computation model is the Turing machine. P (resp. NP) denotes the class of languages accepted by deterministic (resp. nondeterministic) Turing machines in polynomial time. PF denotes the class of polynomial-time-computable functions. We now define some notions of polynomial-time reducibilities.

A \leq_{m}^{P} -reduction from A to B is a polynomial-time-computable function f such that for each $x \in \Sigma^{*}$, $x \in A \Leftrightarrow f(x) \in B$.

A \leq_{tt}^{P} -reduction from A to B is a pair $\langle f,g \rangle$ of polynomial-time-computable functions such that the following hold for each $x \in \Sigma^*$, (1) $f(x) = \langle x_1, ..., x_k \rangle$ is an ordered k-tuple of strings, (2) g(x) is a polynomial-time-computable circuit with k inputs: $\{0, 1\}^k \rightarrow \{0, 1\}$, (3) $x \in A \Leftrightarrow g(x)(\chi_B(x_1), ..., \chi_B(x_k)) = 1$.

A \leq_{btt}^{P} -reduction from A to B is a pair $\langle f,g \rangle$ of polynomial-time-computable functions such that $A \leq_{tt}^{P} B$ is witnessed by $\langle f,g \rangle$ and there exists a constant k_0 such that for all $x \in \Sigma^*$, the number of inputs of g(x) is not more than k_0 .

A \leq_{dtt}^{P} -reduction of A to B is polynomial-time-computable function f such that for each $x \in \Sigma^*$, $f(x) = \langle x_1, ..., x_k \rangle$ and $x \in A \Leftrightarrow x_i \in B$ for some $i \leq k$.

Let \leq_r^p be one of the kinds of reductions defined above and C be a class of languages. We say language H is $C - \leq_r^p$ -hard if each language in C is \leq_r^p -reducible to H.

Let $A, B \subseteq \Sigma^*$; we say A is sparse if there exists a polynomial p such that $||A^{\leq n}|| \leq p(n)$ for all $n \in N$. We define $A \bigtriangleup B = (A - B) \cup (B - A)$. The function $\operatorname{dist}_{A,B}: N \to N$ is called the distance function of A and B, where $\operatorname{dist}_{A,B}(n) = ||(A \bigtriangleup B)^{\leq n}||$.

A set A is weakly-P-selective if there is a polynomial-time-computable function $f: \Sigma^* \times \Sigma^* \to \Sigma^* \cup \{\#\}$ and a polynomial q(n) such that for each integer n, (1) $\Sigma^{\leq n}$ is the disjoint union of $m_n < q(n)$ sets: $\Sigma^{\leq n} = C_{n,1} \cup C_{n,2} \cdots \cup C_{n,m_n}$; (2) if x, y are in $C_{n,i}$, then $f(x, y) \in \{x, y\}$; (3) if $x \in C_{n,i}$ and $y \in C_{n,j}$, $i \neq j$, then f(x, y) = #; (4) if $x, y \in C_{n,i}$ and

 $(x \in A \text{ or } y \in A)$ then $f(x, y) \in A$. f is called the selector function for A and $C_{n,i}$ is called a chain obtained from f in $\Sigma^{\leq n}$.

Ko [8] involved "polynomial time computable linear order" and "partially polynomial time computable partial order" to characterize P-selective sets and weakly-P-selective sets respectively.

A binary relation R is a preorder if R is reflexive and transitive. Let R be a preorder on Σ^* . Define xSy iff xRy and yRx. Then S is an equivalence relation on Σ^* . If we define R' on Σ^*/S (the set of equivalence classes defined by S) by $\bar{x}R'\bar{y}$ iff xRy (\bar{x} is the equivalence class in Σ^*/S which contain x), then R' is a partial order induced by R.

Let f be the selector function for weakly-P-selective set A. We define $xR_f y$ iff there exists a finite sequence $z_0 = x, z_1, ..., z_n, z_{n+1} = y$ of strings in Σ^* such that $f(z_i, z_{i+1}) = z_i$ for all $i \leq n$. It is easy to verify that R_f is a preorder. Let S_f, \leq_f be the equivalence relation and partial order induced by R_f , respectively. $A^{\leq n}$ is the union of initial segments of at most polynomial \leq_f -chains on Σ^n/S_f (see [8]). If A is P-selective and f is the selector function, then \leq_f is a linear order on Σ^*/S_f and A is an initial segment of Σ^*/S_f using order \leq_f (see [8]). For convenient consideration, we use $x \leq_f y$ instead of $\bar{x} \leq_f \bar{y}$.

By the definition, if f is the selector function for a weakly-P-selective set, determining whether two strings are in the same chain is just to determine whether $f(x, y) \in \{x, y\}$. Let all elements of $\{x_1, ..., x_t\}$ be in the same chain. Since f(x, y) = ximplies $x \leq_f y$, we only need to calculate function f t - 1 times to obtain an element x in $\{x_1, ..., x_t\}$ such that $x \leq_f x_i$ for all $i \leq t$.

If the reader cannot understand the above paragraphs clearly, he can read Ko's paper [8].

We assume all polynomials involve in this paper have nonnegative coefficients.

3. Symmetric difference between NP-hard sets and weakly-P-selective sets

In this section we study the symmetric difference between an NP- \leq_m^P -hard set and a weakly-P-selective set. The main result (Theorem 3.6) is obtained from a result in [4] and Lemma 3.1.

The proof of Lemma 3.1 is a generalization of Fortune's [3] proof that if $\overline{SAT} \in P_m(sparse)$ then P = NP.

Lemma 3.1. Let H be NP- \leq_{dut}^{P} -hard. If there exist a weakly-P-selective set A and a set $B \in P_m(sparse)$ such that H = A - B, then P = NP.

Proof. Let *H* be NP- \leq_{m}^{P} -hard, *A* be weakly-P-selective, and $g \in PF$ be the selector function for *A*. Let $B \leq_{m}^{P} S$ via $h_1 \in PF$, where *S* is a sparse set. Since *H* is NP- \leq_{dtt}^{P} -hard, let SAT $\leq_{dtt}^{P} H$ via $h_2 \in PF$. For each $x \in \Sigma^*$, $h_2(x)$ is considered as a subset of Σ^* .

Let p(n) be a polynomial such that $||S^{\leq n}|| \leq p(n), g, h_1, h_2 \in \text{DTIME}(p(n))$ and $\Sigma^{\leq n}$ can be partitioned into at most p(n) chains by the selector function g.

For a boolean formula f, in order to determine the satisfiability of f we use breadth-first search to prune a binary tree formed from self-reduction of f. The tree will be prunned so that each level contains at most polynomial formulas and at least a satisfiable formula if f is satisfiable.

For set L whose elements are in the same chain, Algorithm 1 provides a method to select polynomial elements subset L' from L such that $L \cap H \neq \emptyset \Leftrightarrow L' \cap H \neq \emptyset$.

Algorithm 1

Input a set L and let $n = Max\{|x| | x \in L\}$.

If not (all elements in L are in the same chain) then exit (Note: two strings u, v are in the same chain iff $g(u, v) \in \{u, v\}$).

L is partitioned into the blocks: M_1, M_2, \dots which satisfy the two conditions as follows.

(1) For every $x, y \in L$, x, y are in the same block if and only if $h_1(x) = h_1(y)$.

(2) $m_1 \leq_g m_2 \leq_g \cdots$, where m_i is the least element (with respect to order \leq_g) of M_i . (Note: if there are more than one least elements in a block we choose one arbitrarily.) Let $L' = \{m_s | s \leq p(p(n)) + 1\}$.

Output L'.

End of the algorithm

Claim 3.2. (1) Algorithm 1 will stop in q(n+m) steps for some polynomial q, where $n = Max\{|x| | x \in L\}$ and m = ||L||.

(2) If all of the elements of L are in the same chain (with respect to order \leq_g) and L' is the output of Algorithm 1 with input L, then $L \cap H \neq \emptyset \iff L' \cap H \neq \emptyset$ and $||L'|| \leq p(p(n)) + 1$, where $n = Max\{|x||x \in L\}$.

Proof. (1) Since $g, h_1 \in PF$, it is easy to verify.

(2) Assume $L \cap H \neq \emptyset$. Let $y \in L \cap H$ and $y \in M_s$.

Case 1: $s \leq p(p(n)) + 1$.

Because m_s is the least element of M_s , $m_s \leq_g y$. Since $y \in H$ and H = A - B. So $m_s \in A$ (for A is weakly-P-selective and y, m_s are in the same chain). Because both m_s and y are in M_s , $h_1(m_s) = h_1(y) \notin S$. Thus m_s is in A - B = H. Since $s \leq p(p(n)) + 1$, $m_s \in L'$. So $L' \cap H \neq \emptyset$.

Case 2: s > p(p(n)) + 1.

In this case for each $t \leq p(p(n)) + 1$, $m_t \leq_g m_s \leq_g y$. Since A is weakly-P-selective and y, m_s, m_t are in the same chain, thus $m_t \in A$. On the other hand if $t \neq t'$ then $h_1(m_t) \neq h_1(m_{t'})$. The strings in L are of length $\leq n$. The strings in $\{h_1(m_1), h_1(m_2), \ldots\}$ are of length $\leq p(n)$. Since $||S^{\leq p(n)}|| \leq p(p(n))$. Therefore, there exists a $t_0 \leq p(p(n)) + 1$ such that $h_1(m_{t_0}) \notin S$. So $m_{t_0} \in A - B = H$. So $L' \cap H \neq \emptyset$.

From the definition of L', it is easy to see $||L'|| \le p(p(n)) + 1$, where $n = Max\{|x| | x \in L\}$. \Box

Algorithm 2 is to prune the self-reduction tree of f and determine its satisfiability.

Algorithm 2

Input formula f with length n. Let $F_0 = \{f\}$ and i = 0. Repeat Let $C_i = \bigcup_{x \in F_i} h_2(x)$. Partition C_i into following blocks: $L_{i,1}, L_{i,2}, \dots$ such that for $u, v \in C_i, u, v$ are in the same block if and only if u, v are in the same chain $(g(u, v) \in \{u, v\})$. Let n_i be the number of blocks partitioned from C_i . For each $L_{i,j}$, $j \leq n_i$, let $L'_{i,j} = \{m_{i,j,1}, \dots, m_{i,j,n_{i,j}}\}$ be the output of Algorithm 1 with input $L_{i, i}$. Let $f_{i,j,s}$ be a formula in F_i such that $m_{i,j,s} \in h_2(f_{i,j,s})$. $G_{i,j} = \{f_{i,j,s} \mid s \leq n_{i,j}\}.$ $G_i = \bigcup_{j=1}^{n_i} G_{i,j}.$ $F_{i+1} = \{g_1, g_2 | g_1, g_2 \text{ are obtained by fixing one variable of } g \in G_i \text{ to } 0, 1$ respectively}. i = i + 1. **Until** all formulas in F_i are of length ≤ 5 . Let i_0 be the value *i* after executing the above cycle. Accept x if and only if one of the formulas in F_{i_0} is satisfiable.

End of the algorithm.

Claim 3.3. (1) For each $i < i_0$, $n_i \le p(p(n))$. (2) For each $i < i_0$, $||F_{i+1}|| \le 2||G_i|| \le 2(p(p(p(n))) + 1)^2$.

Proof. (1) Since $h_2 \in \text{DTIME}(p(n))$, so $C_i \subseteq \Sigma^{\leq p(n)}$. $\Sigma^{\leq p(n)}$ can be partitioned into at most p(p(n)) chains by the selector function g. So, $n_i \leq p(p(n))$.

(2) Since $L_{i,j} \subseteq C_i \subseteq \Sigma^{\leq p(n)}$, by Claim 3.2 $||L'_{i,j}|| \leq p(p(p(n))) + 1$. So $||G_{i,j}|| \leq p(p(p(n))) + 1$, therefore $||F_{i+1}|| \leq 2||G_i|| \leq 2n_i \cdot (p(p(p(n))) + 1) \leq 2(p(p(p(n))) + 1)^2$. \Box

Claim 3.4. For each $i \leq i_0$, there exists a satisfiable formula in $F_i \Leftrightarrow$ there exists a satisfiable formula in G_i .

Proof. We assume a formula x in F_i is satisfiable. Thus there exists an element y in $h_2(x)$ having $y \in H$ (for SAT $\leq_{dit}^{P} H$ via h_2). Let $y \in L_{i,j}$. Therefore $L_{i,j} \cap H \neq \emptyset$.

Since $L'_{i,j}$ is the output of Algorithm 1 with input $L_{i,j}$, by Claim 3.2 we have $L'_{i,j} \cap H \neq \emptyset$. Therefore, $G_{i,j}$ contains at least one satisfiable formulas. Thus, there exists a satisfiable formula in G_i . \Box

Since initially $F_0 = \{f\}$, by the above claim f is satisfiable if and only if there exists a satisfiable formula in F_{i_0} . It is easy to see that the algorithm will stop in polynomial steps. We have SAT \in P, hence P = NP.

284

Lemma 3.5 (Fu [4]). Let H be NP- \leq_m^P -hard set and $A \subseteq \Sigma^*$. If there exists $B \in P_{\text{but}}(sparse)$ such that $H = A \cup B$, then NP $\subseteq P_{\text{dut}}(A)$.

Theorem 3.6. If there exist an NP- \leq_m^P -hard set H and a weakly-P-selective set A such that $H - A \in P_{btt}(sparse)$ and $A - H \in P_m(sparse)$ then P = NP.

Proof. Let H and A satisfy the conditions of the theorem. Let $H' = H \cap A$. Thus $H' \cup (H-A) = H$ is NP- \leq_{m}^{P} -hard. By Lemma 3.5 we have NP $\subseteq P_{dtt}(H')$. So H' is NP- \leq_{dtt}^{P} -hard. Since A is weakly-P-selective and $A - H = A - H' \in P_{m}$ (sparse), so we have P = NP by Lemma 3.1. \Box

Under the assumption $P \neq NP$, we show that the symmetric difference of a NP- \leq_{m}^{P} -hard set and a weakly-P-selective set is complicate. So, it is not easy to approximate a NP- \leq_{m}^{P} -hard set by weakly-P-selective sets if $P \neq NP$.

Corollary 3.7. Let H be NP- \leq_{m}^{P} -hard. If there exists a weakly-P-selective set A such that $A \bigtriangleup H$ is sparse, then P = NP.

4. Separating P-selective sets from P_{btt}(sparse)

Ko [8] showed that for each weakly-P-selective set belongs to $P_{tt}(sparse)$, the following theorem gives a lower bound for the number of queries to the sparse sets that may be required by such a reduction. In particular, we show that there are weakly-P-selective sets A such that $A \notin P_{btt}(sparse)$. This implies that Theorem 3.6 is not a trivial consequence of Ogiwara and Watanabe's theorem. Since A has exponentially dense symmetric difference with every set in $P_{btt}(sparse)$, this tells us that A is not easy to be approximated by the sets in $P_{btt}(sparse)$. The techniques used here are from [2, 4].

Let $\langle i, j \rangle, \langle i', j' \rangle \in N \times N$, we say $\langle i, j \rangle \leq \langle i', j' \rangle$ if (i < i') or $(i = i' \text{ and } j \leq j')$; if $\langle i, j \rangle \leq \langle i', j' \rangle$ and $\langle i, j \rangle \neq \langle i', j' \rangle$, then we say $\langle i, j \rangle < \langle i', j' \rangle$. Let strings $s_1, s_2 \in \Sigma^*$, we say $s_1 \subset s_2$ if $s_2 = s_1 x$ for some string x with |x| > 0. The proof of Theorem 4.1 will employ ordinary dictionary ordering \leq_d of binary strings with $0 \leq_d 1$. Let x and y belong to $\{0, 1\}^*$, $x = x_1 \dots x_m$ and $y = y_1 \dots y_n$, $x \leq_d y$ if and only if

(1) m = n and $\exists i \leq m \forall j < i [x_j = y_j \text{ and } x_i = 0 \text{ and } y_i = 1]$ or

(2) m < n and $x \leq_d y_1 \dots y_m$, or

(3) m > n and $(x_1 \dots x_n \leq_d y \land x_1 \dots x_n \neq y)$.

For strings $x, y \in \Sigma^*$, we say $x <_d y$ if $(x \leq_d y)$ and $(x \neq y)$.

Let $f: N \to N$. We say A is of dense bound f(n) if $||A^{\leq n}|| \leq f(n)$ for all large n.

 $A \leq_{\log \log - tt}^{P}$ -reduction from A to B is a pair of polynomial-time-computable functions $\langle f, g \rangle$ such that $A \leq_{tt}^{P} B$ is wittnessed by $\langle f, g \rangle$ and for each $x \in \Sigma^*$, the number of inputs of g(x) is not more than $\log \log |x|$ (Note: in the proof of Theorem 4.1, g(x) is considered as a truth table). **Theorem 4.1.** There exists a P-selective set A such that for any $B \in P_{\log \log - ti}(sparse)$, $dist_{A, B}(n) > 2^{n^{1/5}}$ for all large n.

Proof. Let $\langle f_1, g_1 \rangle, \langle f_2, g_2 \rangle, ...$ be an effective enumeration of all $\leq_{\log \log - tt}^{P}$ -reductions. For each reduction $\langle f_i, g_i \rangle, f_i, g_i$ are computable functions under the time bound $n^{\log i} + \log i$ and for each $x \in \Sigma^*, f_i(x) = \langle x_1, ..., x_k \rangle$ with $k \leq \log \log |x|, g(x)$ is a k-argument truth table.

In the following construction, we will construct a set A which is an initial segment of Σ^* with respect to the order \leq_d and make dist_{A,B}(n) have exponential lower bound for every B which is log log-tt-reducible to a sparse set via reduction $\langle f_i, g_i \rangle$. The construction at stage $\langle n, i \rangle$ will guarantee that there are at least $2^{n^2/2}$ elements in $(A \triangle B) \cap D_{n,i}$ for all sufficiently large n, where $D_{n,i} \subseteq \Sigma^{n^4 + in^2}$ and will be defined in the construction.

In order to guarantee that A is P-selective, we construct a series of strings $d_{n,i}$ $(1 \le i \le n)$ for all large n such that if $\langle n, i \rangle < \langle n', i' \rangle$ then $d_{n,i}$ is an initial segment of $d_{n',i'}$ $(d_{n,i} \subset d_{n',i'})$. A is defined to be the set $\{x \mid x \le d_{n,i} \text{ for some } d_{n,i}\}$. Thus, there exists an infinite string s such that each $d_{n,i}$ is the initial segment of s. For each $x \in \Sigma^* x \in A$ iff $x \le_d s$ (comparing x with s is just to follow the definition of \le_d and let $|s| = \infty$). So A is an initial segment of Σ^* and s is the boundary.

At stage $\langle n, i \rangle$, we consider the strings in $d_{n,i-1} \Sigma^{n^2}$. One of the following two cases will be obtained at the stage.

(1) For each S of dense bound $n^{\log n}$, there exists a exponentially dense subset F_0 of $d_{n,i}\Sigma^{n^2}$ such that for every $x, y \in F_0$, $g_i(x) = g_i(y)$ and $\langle \chi_S(x_1), \ldots, \chi_S(x_r) \rangle = \langle 0, \ldots, 0 \rangle$, where $f_i(x) = \langle x_1, \ldots, x_r \rangle$.

(2) There exist an integer $e \leq 5 \log \log n$ and string $u_1, u_2, ..., u_{e-1}, y_e, z_e(y_e \neq z_e)$ in Σ^n such that for each S of dense bound $n^{\log n}$, there exist two sets $F_e^{(0)} \subseteq d_{n,i-1}u_1 \dots u_{e-1}y_e \Sigma^{(n-e)n}$ and $F_e^{(1)} \subseteq d_{n,i-1}u_1 \dots u_{e-1}z_e \Sigma^{(n-e)n}$ such that for any x, y in $F_e^{(0)} \cup F_e^{(1)}, g_i(x) = g_i(y)$ and $\langle \chi_S(x_1), \dots, \chi_S(x_r) \rangle = \langle \chi_S(y_1), \dots, \chi_S(y_r) \rangle$, where $f_i(x) = \langle x_1, \dots, x_r \rangle$ and $f_i(y) = \langle y_1, \dots, y_r \rangle$.

If case 1 is obtained (subcase 2.1), then let

$$d_{n,i} = \begin{cases} d_{n,i-1} 0^{n^2} & \text{if } t_0(0,\ldots,0) = 1, \\ d_{n,i-1} 1^{n^2} & \text{if } t_0(0,\ldots,0) = 0. \end{cases}$$

So, either $(F_0 \subseteq B \land d_{n,i-1} \Sigma^{n^2} \cap A = \{d_{n,i-1} 0^{n^2}\})$ or $(d_{n,i-1} \Sigma^{n^2} \subseteq A \land F_0 \cap B = \emptyset)$. So, $F_0 - \{d_{n,i-1} 0^{n^2}\} \subseteq A \land B$.

If case 2 is obtained (subcases 1.2 and 2.2), then let

$$d_{n,i} = \begin{cases} d_{n,i-1}u_1 \dots u_{e-1} y_e 1^{(n-e)n} & \text{if } y_e <_{d} z_e, \\ d_{n,i-1}u_1 \dots u_{e-1} z_e 1^{(n-e)n} & \text{otherwise.} \end{cases}$$

So, either $(F_e^{(0)} \subseteq A \land F_e^{(1)} \cap A = \emptyset)$ or $(F_e^{(0)} \cap A = \emptyset \land F_e^{(1)} \subseteq A)$. On the other hand, either $(F_e^{(0)} \cup F_e^{(1)} \subseteq B)$ or $(F_e^{(0)} \cup F_e^{(1)}) \cap B = \emptyset$, thus either $F_e^{(0)} \subseteq A \bigtriangleup B$ or $F_e^{(1)} \subseteq A \bigtriangleup B$. Therefore, $A \bigtriangleup B$ can be guaranteed to be exponentially dense. In the following we give the formal proof of the theorem.

Let function $d(n) = n^{\log n}$ which is subexponential and dominates all polynomials. Every sparse set is of dense bound d.

Construction

Let n_0 be the least number such that for all $n > n_0$: $(\log \log n^5) \cdot n^5 < 2^{n^{1/2}}$, $\log \log n^5 \cdot d(((n^5)^{\log n} + \log n) < 2^{n^{1/2}}$, and $3(3 \log \log n^5 + 1) < n^{1/2}$.

 $d_{n_0, n_0} = 0^{n_0^4}$.

For an integer pair $\langle n, i \rangle$, we say $\langle n, i \rangle$ is active if $(n_0 < n)$ and $(1 \le i \le n)$. Stage $\langle n, i \rangle$ will be processed in the construction if and only if $\langle n, i \rangle$ is active. For two active pairs $\langle n, i \rangle$, $\langle n', i' \rangle$, stage $\langle n, i \rangle$ will be processed before stage $\langle n', i' \rangle$ if and only if $\langle n, i \rangle < \langle n', i' \rangle$.

Stage $\langle n, i \rangle$

Let $\sigma = \frac{1}{3(3 \log \log n^5 + 1)}$. If i = 1 then let $d_{n,0} = d_{n-1,n-1} 0^{n^4 - |d_{n-1,n-1}|}$. For each $x \in \Sigma^*$, let x_r be the *r*th element of $f_i(x)$, where $f_i(x) = \langle x_1, ..., x_k \rangle$. Let $D_{n,i} = d_{n,i-1} \Sigma^{n^2}$. Let t_0 be one of the truth tables *t* such that $|| \{x | x \in D_{n,i} \land g_i(x) = t\} ||$ is the largest. Let r_0 be the dimension of t_0 . Define two sets $G_0^{(0)}, G_0^{(1)}$: $G_0^{(0)} = G_0^{(1)} = \{x | x \in D_{n,i} \land g_i(x) = t_0\}$. $e = 1, J_0 = \phi$

Substage e

Case 1: There exist $v \in \Sigma^*$, $r \in \{1, ..., r_0\} - J_{e-1}$ and $b \in \{0, 1\}$ such that $\|\{x \mid x \in G_{e-1}^{(b)} \land x_r = v\}\| \ge 2^{(n-(e-1)-3e\sigma)n} \dots$

(1)

Fix such v, r and b, let $H_e = \{x \mid x \in G_{e-1}^{(b)} \land x_r = v\}$. If e > 1 then let

$$u_{e-1} = \begin{cases} y_{e-1} & \text{if } b = 0, \\ z_{e-1} & \text{if } b = 1. \end{cases}$$

 $J_e = J_{e-1} \cup \{r\}.$

Let y_e be a $y \in \Sigma^n$ such that $||H_e \cap d_{n,i-1}u_1 \dots u_{e-1}y\Sigma^{(n-e)n}||$ is the largest and z_e be a $z \in \Sigma^n - \{y_e\}$ such that $||H_e \cap d_{n,n-1}u_1 \dots u_{e-1}z\Sigma^{(n-e)n}||$ is the largest. Let

$$G_e^{(0)} = H_e \cap d_{n, i-1} u_1 \dots u_{e-1} y_e \Sigma^{(n-e)n},$$

$$G_e^{(1)} = H_e \cap d_{n, i-1} u_1 \dots u_{e-1} z_e \Sigma^{(n-e)n}.$$

Subcase 1.1: $e < r_0$

e = e + 1 and enters the next substage.

Subcase 1.2: $e = r_0$

$$d_{n,i} = \begin{cases} d_{n,i-1}u_1 \dots u_{e-1}y_e 1^{(n-e)n} & \text{if } y_e <_d z_e, \\ d_{n,i-1}u_1 \dots u_{e-1}z_e 1^{(n-e)n} & \text{otherwise.} \end{cases}$$

Case 2: There exist no v, r and b to satisfy inequality (1), Subcase 2.1: e = 1

$$d_{n,i} = \begin{cases} d_{n,i-1} 0^{n^2} & \text{if } t_0(0,\ldots,0) = 1, \\ d_{n,i-1} 1^{n^2} & \text{if } t_0(0,\ldots,0) = 0. \end{cases}$$

Subcase 2.2: *e*>1

$$d_{n,i} = \begin{cases} d_{n,i-1}u_1 \dots u_{e-2}y_{e-1} 1^{(n-(e-1))n} & \text{if } y_{e-1} <_d z_{e-1}, \\ d_{n,i-1}u_1 \dots u_{e-2}z_{e-1} 1^{(n-(e-1))n} & \text{otherwise.} \end{cases}$$

End of stage $\langle n, i \rangle$.

We define the set A as follows.

 $x \in A \Leftrightarrow x \leq_d d_{n,i}$ for some active integer pair $\langle n, i \rangle$.

We shall show that for every $B \leq_{\log \log - ti}^{P} S$ via $\langle f_i, g_i \rangle$, where S is of dense bound d(n), $||(A \triangle B) \cap D_{n,i}|| > 2^{n^2/2}$ for all large n and A is P-selective.

We only consider the stage $\langle n, i \rangle$ in the construction. We assume *n* is sufficiently large and $\langle n, i \rangle$ is active. Claims 4.1 and 4.2 can be verified easily from the construction. The detailed proofs are omitted here.

Claim 4.2. If stage $\langle n, i \rangle$ ends at substage e_0 , then for each $e < e_0$ we have the following facts:

- (1) $H_e \subseteq d_{n,i-1} u_1 \dots u_{e-1} \Sigma^{(n-(e-1))n}$.
- (2) $G_e^{(0)} \subseteq d_{n,i-1}u_1 \dots u_{e-1} y_e \Sigma^{(n-e)n}$
- (3) $G_e^{(1)} \subseteq d_{n,i-1} u_1 \dots u_{e-1} z_e \Sigma^{(n-e)n}$
- (4) For any $x, x' \in H_e$, $x_r = x'_r$ for all $r \in J_e$.
- (5) $G_e^{(0)}, G_e^{(1)} \subseteq H_e$.
- (6) $J_e \subseteq \{1, 2, ..., r_0\}$ and $||J_e|| = e$.

(7)
$$H_e, G_e^{(0)}, G_e^{(1)} \subseteq D_{n,i}$$
.

(8) If the condition of case 1 is true at substage e_0 , then (1)–(7) still hold when e_0 replaces e.

Claim 4.3. (1) For two active integer pairs $\langle n,i \rangle$, $\langle n',i' \rangle$, if $\langle n,i \rangle < \langle n',i' \rangle$, then $d_{n,i} \subset d_{n',i'}$.

(2) For each $x \in D_{n,i}$, $x \in A \Leftrightarrow x \leq_{d} d_{n,i}$.

(3)
$$d_{n,i} \in D_{n,i} \subseteq \Sigma^{n^4 + in^2} \subseteq \Sigma^{\leq n^5}$$

288

Claim 4.4. At stage $\langle n, i \rangle$,

(1) If the condition of case 1 is satisfied at substage e, then $||G_e^{(b)}|| \ge 2^{(n-e-(3e+1)\sigma)n}$ for each $b \in \{0, 1\}$... (2)

(2) (2) is also true for e=0.

Proof of Claim 4.4. At stage $\langle n, i \rangle$, (1) $D_{n,i} \subseteq \Sigma^{\leq n^5}$ (by Claim 4.3(3)) and (2) initially t_0 is one of the truth tables t with dimension $\leq \log \log n^5$ such that $\|\{x \mid x \in D_{n,i} \land g_i(x) = t\}\|$ is the largest. Hence $G_0^{(0)} = G_0^{(1)} = \{x \mid x \in D_{n,i} \land g_i(x) = t_0\}$.

The number of truth tables with dimension $\leq \log \log n^5$ is not more than $(\log \log n^5)$. $2^{2^{\log \log n^5}} = (\log \log n^5) \cdot n^5 \leq 2^{n\sigma}$. So

$$\|G_0^{(0)}\| = \|G_0^{(1)}\| \ge \frac{\|D_{n,i}\|}{2^{n\sigma}} = \frac{2^{n^2}}{2^{n\sigma}} = 2^{(n-\sigma)n}.$$

Thus, (2) holds for e = 0.

We consider e > 0. At substage e there exist v, r and b such that: $||H_e|| \ge 2^{(n-(e-1)-3e\sigma)n}$, where $H_e = \{x \mid x \in G_{e-1}^{(b)}$ and $x_r = v\}$. Since $G_e^{(0)} = H_e \cap d_{n,i-1}u_1 \dots u_{e-1}y_e \Sigma^{(n-e)n}$, $G_e^{(1)} = H_e \cap d_{n,i-1}u_1 \dots u_{e-1}z_e \Sigma^{(n-e)n}$, where y_e is such a $y \in \Sigma^n$ that $||H_e \cap d_{n,i-1}u_1 \dots u_{e-1}y \Sigma^{(n-e)n}||$ is the largest, and z_e is such a $z \in \Sigma^n - \{y_e\}$ that $||H_e \cap d_{n,i-1}u_1 \dots u_{e-1}z \Sigma^{(n-e)n}||$ is the largest.

Since $H_e \subseteq d_{n,i-1}u_1 \dots u_{e-1} \Sigma^{(n-(e-1))n}$ (by Claim 4.2(1)), we have the following:

$$\|G_e^{(0)}\| = \|H_e \cap d_{n,i-1}u_1 \dots u_{e-1}y_e \Sigma^{(n-e)n}\| \ge \frac{\|H_e\|}{\|\Sigma^n\|} \ge \frac{2^{(n-(e-1)-3e\sigma)n}}{2^n}$$
$$= 2^{(n-e-3e\sigma)n} > 2^{(n-e-(3e+1)\sigma)n}.$$

$$\|G_{e}^{(1)}\| = \|H_{e} \cap d_{n,i-1}u_{1} \dots u_{e-1}z_{e}\Sigma^{(n-e)n}\| \ge \frac{\|H_{e} - d_{n,i-1}u_{1} \dots u_{e-1}y_{e}\Sigma^{(n-e)n}\|}{\|\Sigma^{n}\|}$$
$$\ge \frac{2^{(n-(e-1)-3e\sigma)n} - 2^{(n-e)n}}{2^{n}} > 2^{(n-e-(3e+1)\sigma)n}.$$

Claim 4.5. If stage $\langle n, i \rangle$ ends at subcase 1.2 of substage e, then $||(A \triangle B) \cap D_{n,i}|| > 2^{n^2/2}$.

Proof of Claim 4.5. We know for each $x \in D_{n,i}$, $x \in A \Leftrightarrow x \leq_d d_{n,i}$ (by Claim 4.3(2)).

$$G_{r_0}^{(0)} \subseteq d_{n,i-1} u_1 \dots u_{r_0-1} y_{r_0} \Sigma^{(n-r_0)n}, \qquad G_{r_0}^{(1)} \subseteq d_{n,i-1} u_1 \dots u_{r_0-1} z_{r_0} \Sigma^{(n-r_0)n}$$

(by Claim 4.2(2), (3)). By the definition of $d_{n,i}$ at substage 1.2 all of the strings in $G_{r_0}^{(b)}$ belong to A and none of the strings of $G_{r_0}^{(1-b)}$ are in A, where

$$b = \begin{cases} 0 & \text{if } y_{r_0} <_{\mathrm{d}} z_{r_0}, \\ 1 & \text{otherwise.} \end{cases}$$

On the other hand, for any x, y in $G_{r_0}^{(0)} \cup G_{r_0}^{(1)}$, $\langle f_i(x), g_i(x) \rangle = \langle f_i(y), g_i(y) \rangle$ by Claim 4.2(4)-(6)). Hence, either all of the strings in $G_{r_0}^{(0)} \cup G_{r_0}^{(1)}$ are in B, or none of them

are in *B*. Therefore, $||(A \triangle B) \cap D_{n,i}|| \ge Min(||G_{r_0}^{(0)}||, ||G_{r_0}^{(1)}||) \ge 2^{(n-r_0-(3r_0+1)\sigma)n}$ (by Claim 4.4) $\ge 2^{n^2/2}$. \Box

Claim 4.6. If stage $\langle n,i \rangle$ ends at subcase 2.1 or 2.2 for some *e*, then $||(A \triangle B) \cap D_{n,i}|| \ge 2^{n^2/2}$.

Proof of Claim 4.6. At substage *e* of stage $\langle n, i \rangle$, for every $v \in \Sigma^*$, $r \in \{1, ..., r_0\} - J_{e-1}$ and $b \in \{0, 1\} \| \{x | x \in G_{e-1}^{(b)} \text{ and } x_r = v\} \| < 2^{(n-(e-1)-3e\sigma)n}$.

Because S is of dense bound d(n), $f_i, g_i \in DTIME(n^{\log i} + \log i)$ and $G_{e^{-1}}^{(b)} \subseteq \Sigma^{\leq n^5}$ there are at most $r_0 \cdot d((n^5)^{\log i} + \log i) \cdot 2^{(n-(e-1)-3e\sigma)n} < 2^{\sigma n} \cdot 2^{(n-(e-1)-3e\sigma)n} = 2^{(n-(e-1)-(3e-1)\sigma)n}$ strings x in $G_{e^{-1}}^{(b)}$ ($b \in \{0, 1\}$) having $x_r \in S$ for some $r \in \{1, ..., r_0\} - J_{e^{-1}}$, where $f_i(x) = \langle x_1, ..., x_{r_0} \rangle$. By Claim 4.4, $||G_{e^{-1}}^{(b)}|| \ge 2^{(n-(e-1)-(3(e^{-1})+1)\sigma)n}$ for each $b \in \{0, 1\}$, hence in $G_{e^{-1}}^{(b)}$ ($b \in \{0, 1\}$) there are at least

$$2^{(n-(e-1)-(3(e-1)+1)\sigma)n} - 2^{(n-(e-1)-(3e-1)\sigma)n} \ge 2^{(n-(e-1)-((3e-1)+2)\sigma)n}$$
$$= 2^{(n-(e-1)-(3e-1)\sigma)n}$$

strings x having $x_r \notin S$ for every $r \in \{1, ..., r_0\} - J_{e-1}$.

Let $F_{e-1}^{(b)} = \{x \mid x \in G_{e-1}^{(b)} \text{ and } x_r \notin S \text{ for all } r \in \{1, \dots, r_0\} - J_{e-1}\}$. So $||F_{e-1}^{(b)}|| \ge 2^{(n-(e-1)-(3e-1)\sigma)n}$.

It is easy to see that for any $x, y \in F_{e^{-1}}^{(0)} \cup F_{e^{-1}}^{(1)} g_i(x) = g_i(y) = t_0$ and $\langle \chi_S(x_1), \dots, \chi_S(x_{r_0}) \rangle = \langle \chi_S(y_1), \dots, \chi_S(y_{r_0}) \rangle$ (By Claim 4.2 (4)-(6) and the above discussion).

Let

$$c = \begin{cases} 0 & \text{if } e = 1 \text{ or } y_{e-1} <_{d} z_{e-1}, \\ 1 & \text{otherwise.} \end{cases}$$

If the stage $\langle n, i \rangle$ ends at subcase 2.1 then (a) $t_0(0, ..., 0) = 0 \rightarrow \text{all of the strings}$ in $F_0^{(c)}$ belong to A and none of them are in B and (b) $t_0(0, ..., 0) = 1 \rightarrow \text{all of the}$ strings in $F_0^{(c)} - \{d_{n,i}0^{n^2}\}$ belong to B and none of them are in A. So $\|(A \triangle B) \cap D_{n,i}\| \ge \|F_0^{(c)}\| - 1 \ge 2^{n^2/2}$.

If the stage $\langle n, i \rangle$ ends at subcase 2.2 of substage *e*. It is easy to see that all of the strings in $F_{e^{-1}}^{(c)}$ are in *A* and none of the strings are in $F_{e^{-1}}^{(1-c)}$ are in *A*. On the other hand, either all of the strings in $F_{e^{-1}}^{(0)} \cup F_{e^{-1}}^{(1)}$ are in *B* or none of them are in *B*. $\|(A \bigtriangleup B) \cap D_{n,i}\| \ge \operatorname{Min}(\|F_{e^{-1}}^{(0)}\|, \|F_{e^{-1}}^{(1)}\|) \ge 2^{n^{2}/2}$. \Box

Claim 4.7. A is P-selective.

Proof of Claim 4.7. By Claim 4.3(1) and the definition of A that $x \in A \Leftrightarrow x \leq_d d_{n,i}$ for some active integer pair $\langle n, i \rangle$, it is easy to verify this claim. \Box

By Claim 4.5 and Claim 4.6, it is easy to see that for all large n, $\operatorname{dist}_{A,B}(n^5) \ge \operatorname{dist}_{A,B}(n^4 + in^2) \ge ||(A \bigtriangleup B) \cap D_{n,i}|| \ge 2^{n^{2}/2}$. Hence, for almost every n, $\operatorname{dist}_{A,B}(n) \ge 2^{n^{1/3}}$.

290

Corollary 4.8. There exists a P-selective set A such that for any $B \in P_{but}$ (sparse), $dist_{A,B}(n) > 2^{n^{1/5}}$ for all large n.

Acknowledgment

We sincerely thank Prof. Shouwen Tang for his encouragement in this research. The first author would also like to thank Prof. Qiongzhang Li for his encouragement. We thank Prof. Ronald Book for his kind suggestions and the unknown referees for their help in improving our presentation.

References

- [1] J. Balcarzar, J. Diaz and J. Gabarro, Structural Complexity I, II (Springer, New York, 1988 and 1990).
- [2] R. Book and K. Ko, On sets truth-table reducible to sparse sets, SIAM J. Comput. 17 (1988) 903-919.
- [3] S. Fortune, A note on sparse complete sets, SIAM J. Comput. 8 (1979) 431-433.
- [4] B. Fu, On lower bounds of the closeness between complexity classes, Math. Systems Theory, to appear.
- [5] B. Fu and H. Li, On closeness of NP-hard sets to other complexity classes, in: Proc. 7th Ann. Conf. in Structural Complexity Theory (IEEE, New York, 1992) 243-248.
- [6] S. Homer and L. Longpré, On reductions of NP sets to sparse sets, in: Proc. 6th Ann. Conf. in Structural Complexity Theory (IEEE, New York, 1991) 79-88; J. Comput. System Sci., to appear.
- [7] C.G. Jocksuch, Semirecursive sets and positive reducibility, Trans. Amer. Math. Soc. 131 (1968) 420-436.
- [8] K. Ko, On self-reducibility and weakly-P-selectivity, J. Comput. System Sci. 26 (1983) 209-211.
- [9] K. Ko, Distinguishing bounded reducibility by sparse sets, in: Proc. 3rd Conf. on Structural Complexity Theory (IEEE, New York, 1988) 181-191.
- [10] S. Mahaney, Sparse complete sets for NP: solution of a conjecture of Berman and Hartmanis, J. Comput. System Sci. 25 (1982) 130-143.
- [11] M. Ogiwara and O. Watanabe, On polynomial-time bounded truth-table reducibility of NP sets to sparse sets, in: *Proc. 22nd ACM Symp. on Theory of Computing* (1990) 457-467.
- [12] U. Schöning, Complete sets and closeness to complexity classes, Math. Systems Theory 13 (1986) 55-65.
- [13] A.L. Selman, P-selective sets, Tally languages and the behavior of polynomial-time reducibility on NP, Math. Systems Theory 13 (1981) 326-332.
- [14] A.L. Selman, Some observation on NP real numbers and P-selective sets, J. Comput. Systems Sci. 19 (1981) 326-332.
- [15] A.L. Selman, Reductions on NP and P-selective sets, Theoret. Comput. Sci. 19 (1982) 287-304.
- [16] S. Tang, B. Fu and T. Liu, Exponential time and subexponential time sets, in: Proc. 6th Ann. Conf. in Structural Complexity Theory (IEEE, New York, 1991) 230-237.
- [17] S. Toda, On polynomial-time truth table reducibility of intractable sets to P-selective sets, *Math. Systems Theory* 24 (1991) 69-82.
- [18] Y. Yesha, On certain polynomial-time truth-table reducibilities of complete sets to sparse sets, SIAM J. Comput. 12 (1983) 411-425.