JOURNAL OF COMPUTER AND SYSTEM SCIENCES 26, 209–221 (1983)

On Self-Reducibility and Weak *P*-Selectivity*

KER-I KO

Department of Computer Science, University of Houston, Houston, Texas 77004

Received July 9, 1982; revised July 1982

Self-reducible sets and some low sets, including p-selective sets, and weakly p-selective sets are studied. Several different formulations of self-reducible sets are given and compared with each other. A new characterization of p-selective sets is found, and weakly p- selective sets are introduced as a generalization of p-selective sets based on this characterization. It is proved that self-reducible sets are not polynomial-time Turing reducible to these sets. As a consequence, $\leqslant_m^p$-completeness and $\leqslant_T^p$-completeness in NP are not likely to be distinguished by weakly p-selective sets.

I. INTRODUCTION

Recent development in the study of intractable problems has revealed interesting structural properties of sets in NP. The works of Berman [6], Berman and Hartmanis [7], Mahaney [15], and Meyer and Paterson [16] study the relationship between density and completeness of sets in NP and *P*SPACE. They used the self-reducibility property of NP-complete sets to show that sparse sets cannot be polynomial-time many-one complete in NP unless $P = \text{NP}$. Thus sparseness and self-reducibility appear to be two incompatible properties. Assume that deterministic and nondeterministic exponential-time computable languages do not coincide. Then there exist sparse sets in $\text{NP} - P$, and these sparse sets are not self-reducible. Similar results on the relationship between NP-completeness and other structural properties have been found under different motivations. *P*-selective sets (definitions in Section 3) are introduced to distinguish polynomial-time many-one reducibility from polynomial-time Turing reducibility in NP, and are shown to be not NP-complete unless $P = \text{NP}$ [19]. The study of the computational complexity of real numbers shows that NP real numbers cannot be NP-complete unless $P = \text{NP}$ [11].

In recursion theory, many complexity-theoretic properties, such as speedability and levelability, and recursion-theoretic properties, such as creativity and simplicity, have been characterized by the "information content" of the sets. Let the nth jump $A^{(n)}$ of a set A be defined as in [17]. Then a hierarchy of high and low recursively enumerable (r.e.) sets can be defined: An r.e. set A is $high_n$ if $A^{(n)}$ is Turing equivalent to $\varnothing^{(n+1)}$, and A is low_n if $A^{(n)}$ is Turing equivalent to $\varnothing^{(n)}$. Using a

* This research was supported in part by the National Science Foundation under Grant MCS-8103479.

0022-0000/83 $3.00

notion of weak jumps, Bennison and Soare [3, 4, 22] showed that effective speedability and subcreativity are highness properties, while nonspeedability is a lowness property. Analogous definitions of high and low sets in the NP theory have been given by Schöning [18]. The analog of the jump operator in the NP theory is called a K operator. Characterizations of sets in the lower levels of the hierarchy have been found. The $p\text{-high}_0$ sets are NP-complete sets; $p\text{-high}_1$ sets are strong NP Turing complete sets; $p\text{-low}_0$ sets are those in P; and $p\text{-low}_1$ sets are those in NP $\cap$ co-NP. The mentioned studies on the structure of NP sets seem to suggest that self-reducibility is a highness property, while sparseness and p-selectivity are lowness properties.[1]

The idea that sparseness and p-selectivity are lowness properties will be elaborated in a subsequent paper [12]. In this paper, we examine self-reducibility more closely and introduce a new class of low sets called weakly p-selective sets. This class is a generalization of both the p-selective structure and the real number structure. We show that weakly p-selective sets are not self-reducible and hence are not NP-complete unless $P = \text{NP}$. Selman [20] asked for new constructions of p-selective sets to distinguish polynomial time m-completeness from T-completeness in NP. We show that weakly p-selective sets (and hence p-selective sets) cannot distinguish polynomial-time m-completeness from T-completeness in NP unless the polynomial-time hierarchy collapses to Σ_2^p.

Our notations are standard: P (NP) is the class of deterministic (nondeterministic) polynomial-time computable languages; P SPACE is the class of polynomial space computable languages; $\leqslant_m^p$ ($\leqslant_T^p$) is the polynomial-time many-one (Turing) reducibility; Σ is a fixed alphabet of at least two letters; and Σ^* is the set of all finite strings of letters from Σ. We use $|x|$ to denote the length of the string x. We call a set A *sparse* if there exists a polynomial p such that for each $n \in N$, the set $A_n = \{x \in A : |x| \leqslant n\}$ has $\leqslant p(n)$ elements. We use the logical symbols $\vee$ and $\wedge$ to denote the Boolean operators "or" and "and," respectively.

II. Self-Reducible Sets

Following Meyer and Paterson [16], we first define the polynomially related orderings on Σ^*.

Definition 1. A partial ordering $\prec$ on Σ^* is *polynomially well-founded and length-related* (abbr. *polynomially related*) if there is a polynomial p such that

(a) "$x \prec y$?" can be determined in $p(|x| + |y|)$ steps,

(b) $x \prec y$ implies $|x| \leqslant p(|y|)$ for all x, y in Σ^*, and

(c) the length of a $\prec$-decreasing chain is shorter than p of the length of its maximum element.

[1] A warning must be given that all sets in P (which, of course, are low) are self-reducible.

Informally a set L is self-reducible if the membership problem of an element x is (polynomial-time) reducible to the membership problems of smaller elements. Since the various reducibilities among sets of strings have been carefully studied [14], it is natural to borrow them to define self-reducible sets. Let χ_L be the characteristic function of the set L.

DEFINITION 2. A set $L \subseteq \Sigma^*$ is *tt-self-reducible* if there is a polynomially related ordering $\prec$ on Σ^*, a polynomial-time computable function f, and a polynomial p such that for all $x \in \Sigma^*$

(a) $f(x)$ is a *tt*-condition $\langle \alpha, \langle x_1,..., x_k \rangle \rangle$, where α is a k-ary Boolean function which can be evaluated in time $p(|x|)$ and $x_i \prec x$ for all $i = 1, 2,..., k$, and

(b) $x \in L$ iff $\alpha(\chi_L(x_1),..., \chi_L(x_k)) = 1$.

DEFINITION 3. (a) A set $L \subseteq \Sigma^*$ is *ptt-self-reducible* if it is *tt*-self-reducible and the Boolean function α produced in a *tt*-condition is always positive, i.e.,

$$[\alpha(\sigma_1,..., \sigma_k) = 1 \ \& \ (\forall i = 1,..., k)\ [\sigma_i = 1 \Rightarrow \tau_i = 1]] \quad \text{implies} \quad \alpha(\tau_1,..., \tau_k) = 1.$$

(b) A set $L \subseteq \Sigma^*$ is *c-self-reducible* if L is *tt*-self-reducible and the Boolean function α is always conjunctive, i.e.,

$$\alpha(\sigma_1,..., \sigma_k) = 1 \quad \text{iff} \quad \sigma_1 = \sigma_2 = \cdots = \sigma_k = 1.$$

(c) A set $L \subseteq \Sigma^*$ is *d-self-reducible* if L is *tt*-self-reducible and the Boolean function α is always disjunctive; i.e.,

$$\alpha(\sigma_1,..., \sigma_k) = 0 \quad \text{iff} \quad \sigma_1 = \sigma_2 = \cdots = \sigma_k = 0.$$

DEFINITION 4. A set $L \subseteq \Sigma^*$ is *T-self-reducible* if there is a polynomially related ordering $\prec$ on Σ^*, and a polynomial time oracle Turing machine (TM) M such that $M^{L_x}(x) = \chi_L(x)$ for all $x \in \Sigma^*$, where $L_x = \{y \in L: y \prec x\}$.

It is immediate that *c*- or *d*-self-reducibility implies *ptt*-self-reducibility, and that *tt*-self-reducibility implies *T*-self-reducibility.

Note that we did not define *m*-self-reducibility because a natural definition of *m*-self-reducibility would imply that *m*-self-reducible sets are just polynomial time computable sets.

We can also get easily some upper bounds for the complexity of other types of self-reducibilities.

THEOREM 1. (a) *If a set $L \subseteq \Sigma^*$ is T-self-reducible, then $L \in P$* SPACE.

(b) *If a set $L \subseteq \Sigma^*$ is d-self-reducible, then $L \in$* NP.

(c) *If a set $L \subseteq \Sigma^*$ is c-self-reducible, then $L \in$* co-NP.

Proof. (a) Assume that the oracle TM M computes L in the sense that $M^{L_x}(x) =$

$\chi_L(x)$ for all $x \in \Sigma^*$, and that $M^{L,x}(x)$ always halts in $q(|x|)$ steps for some polynomial q. We construct a self-reducing tree for each $x \in \Sigma^*$ as follows:

The root of the tree is x.

For each node y, its children are the "smaller" strings $z_1,\ldots, z_k$ about which M successively queried during the computation of $M^{L,y}(y)$ (assuming that correct answers are always given).

Each path of this self-reducing tree is a $\prec$-decreasing chain and hence has a length $\leqslant p(|x|)$ for some polynomial p. Thus a deterministic machine which computes the value $\chi_L(x) = M^{L,x}(x)$ by simulating the self-reducing tree of x in a depth-first manner uses only $p(|x|) \cdot q(p(|x|))$ cells.

(b) A self-reducing tree for every $x \in \sum^*$ can be constructed similar to that in (a).

The root of the tree is x.

Each node y has children $z_1,\ldots, z_k$, where $z_1,\ldots, z_k$ are the strings produced by the *tt*-condition generator for L.

This tree has the property that for each node y, $y \in L$ iff one of its children is in L. Moreover, $x \in L$ iff one of the node in the self-reducing tree of x is in L. Since the height of the tree is bounded by a polynomial of $|x|$, a natural nondeterministic algorithm which guesses, at each level, a child whose membership in L is the same as that of the root works in polynomial-time.

The proof of (c) is symmetric to that of (b) ∎

Let SAT be the set of all satisfiable Boolean formulas, and B_ω the set of all closed quantified true sentences. It is well known that SAT is NP-complete and B_ω is PSPACE-complete [8, 23].

It is easy to see that SAT is *d*-self-reducible, because a Boolean formula $F(x)$ with at least one Boolean variable x can be reduced to $F(0) \vee F(1)$, where $F(\alpha)$, $\alpha = 0, 1$, is the formula obtained from $F(x)$ by replacing x in $F(x)$ by a constant α. It is also not hard to see that B_ω is *ptt*-self-reducible. First, a formula F can be reorganized into an equivalent formula in a "normal" form in which all quantifiers precede other logical symbols. Then, a formula $F_1 = (\exists x)\, F_1'(x)$ can be reduced to $F_1'(0) \vee F_1'(1)$ and a formula $F_2 = (\forall x)\, F_2'(x)$ can be reduced to $F_2'(0) \wedge F_2'(1)$. Both of these reductions are positive. Therefore B_ω is *ptt*-self-reducible.

Whether all NP-complete sets are *d*-self-reducible or not is not known. However, we do know that if the Berman–Hartmanis conjecture [7] that all NP-complete problems are *p*-isomorphic is true, then all NP-complete sets are *d*-self-reducible. Indeed, if f is a polynomial-time isomorphism of Σ^* such that $f(A) = B$ and the membership of x in A is *d*-reduced to the memberships of $x_1,\ldots, x_k$ in A, then the membership of $f(x)$ in B is *d*-reduced to the memberships of $f(x_1),\ldots, f(x_k)$ in B. Therefore, all known NP-complete problems are *d*-self-reducible since all known NP-complete problems are *p*-isomorphic to SAT [7]. Furthermore, an exhibition of a non-*d*-self-reducible NP-complete set will refute the Berman–Hartmanis conjecture. Meyer and Paterson [16] pointed out the *d*-self-reducibility of some problems in NP which are not known to be in P or NP-complete.

These observations give us immediately the following relationships between different types of self-reducibility:

COROLLARY 1. (a) *There is a d-self-reducible set which is not c-self-reducible iff* NP $\neq$ co-NP.

(b) *There is a ptt-self-reducible set which is not m-self-reducible iff* $P \neq PSPACE$.

(c) *There is a ptt-self-reducible set which is neither c-self-reducible nor d-self-reducible unless* NP $= PSPACE$.

Therefore, assuming NP $\neq$ co-NP $\neq PSPACE$, the classes of *c*-, *d*-, and, *ptt*-self-reducible sets are different. The relationship among *T*-, *tt*-, and, *ptt*-self-reducibilities is not clear. Furthermore, whether *ptt*-self-reducibility in NP coincides with *d*-self-reducibility is not known.

III. P-SELECTIVE SETS AND WEAKLY P-SELECTIVE SETS

The P-selective sets were introduced by Selman [19] as the polynomial-time analog of the semirecursive sets. He used them to distinguish polynomial-time *m*- and *T*-reducibilities.

DEFINITION 5. A set $A \subseteq \Sigma^*$ is *p-selective* if there is a polynomial-time computable function f such that for given $x, y \in \sum^*$,

(a) $f(x, y) = x$ or $f(x, y) = y$, and

(b) if $x \in A$ or $y \in A$, then $f(x, y) \in A$.

The function f in Definition 5 is called a *p-selector* for A. Intuitively, A is *p*-selective if the elements in A are "less than" the elements in $\bar{A}$, and the *p*-selector f selects, in polynomial-time, the "smaller" one of the two given elements. That is, f acts like a partial ordering. Let $\prec$ denote a linear ordering on Σ^*. Call a set $A \subseteq \Sigma^*$ an *initial segment* of the linear ordering $(\Sigma^*, \prec)$ if $x \in A$ and $y \prec x$ implies $y \in A$. Selman [21] showed that an initial segment of a polynomial-time computable linear ordering is *p*-selective. Naturally, the function $f(x, y) = \min\{x, y\}$ (with respect to $\prec$) is a *p*-selector for A. In the following we make this notion more precise by giving a necessary and sufficient condition for *p*-selectivity. We will call a binary relation R a *preorder* if it is reflexive and transitive.

DEFINITION 6. A preorder R on Σ^* is *partially polynomial-time computable* if there is a polynomial-time computable function f such that

(a) $f(x, y) = f(y, x) = x$, if xRy but not yRx,

(b) $f(x, y) = f(y, x) \in \{x, y\}$, if xRy and yRx, and

(c) $f(x, y) = \#$, if neither xRy nor yRx, where $\#$ is a special symbol not in Σ.

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 contains x), then R' is a partial ordering on Σ^*/S. We call S and R' the equivalence relation and the partial ordering *induced* by R, respectively.

Now we are ready to state the necessary and sufficient condition.

THEOREM 2. *A set $A \subseteq \Sigma^*$ is p-selective if and only if there is a partially polynomial time computable preorder R on Σ^* such that if S and R' are the induced equivalence relation and partial ordering as defined, then,*

(a) *R' is a linear ordering, and*

(b) *A is the union of an initial segment of $(\Sigma^*/S, R')$.*

Proof. $\Leftarrow$ If A is the union of an initial segment of $(\Sigma^*/S, R')$, then the function f which partially computes the relation R in polynomial-time (as defined in Definition 6) is a p-selector for A.

$\Rightarrow$ Let f be a p-selector for A. If there are some pairs of strings (x, y) such that $f(x, y) \neq f(y, x)$, then we can define a new p-selector g for A: For input (x, y), if $f(x, y) \neq f(y, x)$, then let $g(x, y) = g(y, x) = \min\{x, y\}$ with respect to the natural lexicographic order on Σ^*; if $f(x, y) = f(y, x)$, then let $g(x, y) = g(y, x) = f(x, y)$. Then g satisfies $g(x, y) = g(y, x)$ for all pairs x and y, and g is still a p-selector for A. So, we may assume that the p-selector f satisfies that $f(x, y) = f(y, x)$ for all x, y.

Define a binary relation R on Σ^* as follows: xRy if there exists a finite sequence $z_0 = x, z_1, \ldots, z_n, z_{n+1} = y$ of strings in Σ^* such that $f(z_i, z_{i+1}) = z_i$ for all $i = 0, 1, \ldots, n$. It is easy to check that R is reflexive and transitive. In addition, if xRy and not yRx, then $f(x, y) = x$ because f is a total function and $[f(x, y) = y \Rightarrow yRx]$. Therefore, R is partially polynomial-time computable (by f).

To see that A is the union of an initial segment of $(\Sigma^*/S, R')$, we need only to verify that $[xRy$ and $y \in A]$ implies $x \in A$. From the definition of R, xRy implies that there exists $z_0 = x, z_1, \ldots, z_n, z_{n+1} = y$ such that $f(z_i, z_{i+1}) = z_i$ for all $i = 0, \ldots, n$. Therefore, $y = z_{n+1} \in A \Rightarrow z_n \in A \Rightarrow \cdots \Rightarrow z_0 = x \in A$. This completes the proof. ∎

We use this characterization to generalize the notion of p-selectivity to weak p-selectivity.

DEFINITION 7. A partial ordering R on Σ^* is *p-linear* if for every $n \in N$, the set $\Sigma_n = \{x \in \Sigma^* : |x| \leqslant n\}$ can be decomposed into at most $p(n)$ many pairwisely disjoint subsets $B_1, \ldots, B_m$, $m \leqslant p(n)$, for some polynomial p such that

(a) if x and y are in the same set B_i, $1 \leqslant i \leqslant m$, then xRy or yRx, and

(b) if x and y are in two different sets, $x \in B_i$ and $y \in B_j$, $1 \leqslant i < j \leqslant m$, then neither xRy nor yRx.

DEFINITION 8. A set $A \subseteq \Sigma^*$ is called *weakly p-selective* if there is a partially

polynomial-time computable preorder R, with the induced equivalence relation S and partial ordering R', and a polynomial q such that

(a) R' is p-linear on Σ^*/S, and

(b) for every $n \in N$, $A_n = \{x \in A: |x| \leqslant n\}$ is the union of initial segments of at most $q(n)$ many R'-chains in $\Sigma_n = \{x \in \Sigma^*: |x| \leqslant n\}$.

It is obvious that p-selectivity implies weak p-selectivity.

Selman showed the existence of p-selective sets of arbitrarily high complexity [19]. His proof used, implicitly, the concept of the left cuts of real numbers. Let x be a real number between 0 and 1. Call the set of all dyadic rational numbers which are less than x the *standard left cut* of x [11]. Then the standard left cuts of real numbers are p-selective. (The function f, $f(y, z) =$ the smaller of y and z, serves as the p-selector function.) Let $y_1, y_2, \ldots$, be a sequence of dyadic rational numbers approximating a real number x in the sense that y_n has length n and $|x - y_n| \leqslant 2^{-n}$. Then we call the set of all dyadic numbers z which is less than $y_{|z|}$ a *general left cut* of the real number x. Then a general left cut of a real number must be weakly p-selective (the relation uRv iff $|u| = |v|$ and $u \leqslant v$ suffices.) Thus, from the existence of arbitrarily complex real numbers, we know that there exist arbitrarily complex p-selective and weakly p-selective sets. In [11, 19] it is proved that if the classes of deterministic and nondeterminictic exponential time computable sets do not coincide, then there exist p-selective and weakly p-selective sets in NP-P.

In the next section we will show that weakly p-selective sets cannot be $\leqslant_m^p$-hard in NP or PSPACE, unless $P =$ NP or $P = P$SPACE, respectively. Here we show some other evidence that weakly p-selective sets are low.

In [10] it is shown that a set with small circuits cannot be $\leqslant_T^p$-hard in NP unless the Stockmeyer–Meyer polynomial-time hierarchy collapses to the level Σ_2^p. For instance, Meyer [7] pointed out that sparse sets have small circuits and Adleman [1] showed that all random polynomial-time sets (the class R) have small circuits. Therefore, these sets are not NP-hard (with respect to $\leqslant_T^p$) unless $\bigcup_{i=0}^{\infty} \Sigma_i^p = \Sigma_2^p$.

Selman [20] showed that a left cut of a real number has small circuits and thus cannot be NP-hard unless $\bigcup_{i=0}^{\infty} \Sigma_i^p = \Sigma_2^p$. This result can be generalized to weakly p-selective sets.

DEFINITION 9. A set $A \subseteq \Sigma^*$ is in P/poly if there exists a function $h: N \to \Sigma^*$, and a set $B \in P$, such that

(a) $\lambda n[|h(n)|]$ is a polynomial function, and

(b) $(\forall x)$ $[x \in A$ iff $\langle h(|x|), x\rangle \in B]$.

Karp, Lipton and Sipser [10] proved that NP $\subseteq P$/poly implies $\bigcup_{i=0}^{\infty} \Sigma_i^p = \Sigma_2^p$.

THEOREM 3. *If A is a weakly p-selective set, then $A \in P$/poly.*

Proof. Let R be a preorder on Σ^*, and S and R' are the induced equivalence relation and partial ordering such that Definition 8(a) and (b) are satisfied. Also let f be a polynomial-time computable function which partially computes R (as defined in Definition 6).

We first state

LEMMA 3.1. *Let $\bar{x}$ be an equivalence class in Σ^*/S with n elements. Then there exists a sequence of at most $[\log_2 n]$ elements $y_1,\ldots, y_m$ in $\bar{x}$ such that for all y in $\bar{x}$, $f(y, y_i) = y$ for some i, $1 \leqslant i \leqslant m$.*

Proof of Lemma 3.1. Similar to the proof of Theorem 2, we may assume that $f(y, z) = f(z, y)$ for all y and z. Since $\bar{x}$ is an equivalence class, $f(y, z) = y$ or z, for all $y, z \in \bar{x}$. Consider the relation defined by f as a directed graph G_0 of n nodes and $\binom{n}{2}$ arcs. Each node in the graph represents a string y in $\bar{x}$ and an arc $\langle y, z\rangle$ in the graph means $f(y, z) = y$. We can successively define $y_1, y_2,\ldots$ as follows.

Let y_1 be the node in G_0 with the greatest indegree, and B_1 the set of all nodes from which there are arcs to y_1. Consider the subgraph $G_1 = G_0 - (B_1 \cup \{y_1\})$. Because G_0 has $n(n-1)/2$ arcs and only n nodes, the size of B_1 is at least $(n-1)/2$ and G_1 has at most $(n-1)/2$ nodes.

Define y_i, B_i, and G_i, $i > 1$, successively as the node with the greatest indegree in G_{i-1}, the set of all nodes in G_{i-1} from which there are arcs to y_i, and $G_i = G_{i-1} - (B_i \cup \{y_i\})$, respectively, whenever $G_{i-1} \neq \emptyset$. The size of each G_i is at most half of that of G_{i-1}. So, this procedure produces at most $[\log_2 n]$ many y_i's and these y_i's satisfy the condition we want.

Let us call these y_i's *representatives* of the equivalence class $\bar{x}$.

(Continuation of the proof of Theorem 3.) For each n, $A_n = \{x \in A : |x| \leqslant n\}$ is the union of initial segments of R'-chains. Let us take, for each R'-chain, the representatives of the "greatest" equivalence class which is in A_n. Then, the total number of the representatives is polynomially bounded because the number of R'-chains is polynomially bounded and the size of an equivalence class is $\leqslant 2^{p(n)}$ for some polynomial p. Let $y_1,\ldots, y_k$ be all these representatives. Then $z \in A_n$ iff $f(z, y_i) = z$ for some $1 \leqslant i \leqslant k$.

Now, let $h(n) = y_1 \# y_2 \# \cdots \# y_k$, and $B = \{\langle w_1 \# \cdots \# w_m, z\rangle : \exists j \leqslant m, f(w_j, z) = z\}$. Then h is polynomial-length-bounded and $B \in P$. Also, $z \in A$ iff $<h(|z|), z > \varepsilon B$. Thus, we have proved that weakly p-selective sets are in P/poly. ∎

COROLLARY 2. *No weakly p-selective set can be $\leqslant_T^p$-hard in* NP *unless* $\bigcup_{i=0}^{\infty} \Sigma_i^p = \Sigma_2^p$.

Since a p-selective set is also weakly p-selective, this corollary shows that p-selectivity cannot distinguish $\leqslant_m^p$-completeness from $\leqslant_T^p$-completeness in NP unless $P \neq$ NP and $\bigcup_{i=0}^{\infty} \Sigma_i^p = \Sigma_2^p$ (cf., [20]).

IV. Distinguishing Self-Reducible Sets from Low Sets

In this section we show that weakly-p-selective sets, like sparse sets, are not higher than d-self-reducible sets. We first restate results about sparse sets.

THEOREM 4 [6, 16]. *If L is T-self-reducible, and $L \leqslant_m^p A, \bar{L} \leqslant_m^p B$ for some sparse sets A and B, then $L \in P$.*

The proof of Theorem 4 uses a depth-first search over the self-reducing trees and deletes the redundant nodes. A node is redundant if its membership in L or $\bar{L}$ is known to be the same as that of some other nodes in the tree. The polynomially bounded density of A and B guarantees that the pruned tree has only polynomially bounded many nodes.

Since $B_\omega \leqslant_m^p \bar{B}_\omega$ and B_ω is T-self-reducible, we have immediately

COROLLARY 3 [16]. *No sparse set can be $\leqslant_m^p$-hard in* PSPACE *unless* $P = P\text{SPACE}$.

If we only know that L is T-self-reducible and $L \leqslant_m^p A$ for some sparse set A, it does not appear to guarantee that $L \in P$. However, if we know that L is c-self-reducible, then we need only to control the nodes in L (because the existence of a node not in L implies that the root node is not in L) and only $L \leqslant_m^p A$ for some sparse A suffices.

THEOREM 5 [9]. *If L is c-self-reducible and $L \leqslant_m^p A$ for some sparse set A, then $L \in P$.*

COROLLARY 4. *No sparse set can be $\leqslant_m^p$-hard in* co-NP *unless* $P = \text{NP}$.

A clever nondeterministic guess of the census function of the sparse set A can help to show a similar result on NP.

THEOREM 6 [15]. *No sparse set can be $\leqslant_m^p$-hard in* NP *unless* $P = \text{NP}$.

However, the proof of Theorem 6 uses the fact that the sparse set to which SAT is reduced is $\leqslant_m^p$-hard in NP. This technique does not apply to other d-self-reducible sets.

Theorem 7 appears in [21]. We reprove it here using our characterization of p-selective sets (Theorem 2).

THEOREM 7. *If L is ptt-self-reducible and $L \leqslant_m^p A$ for some p-selective set A, then $L \in P$.*

Proof. Assume that R is a partially polynomial-time computable preorder on Σ^* which induces an equivalence relation S on Σ^* and a linear ordering R' on Σ^*/S

such that A is the union of an initial segment of $(\Sigma^*/S, R')$. Also assume that f is a polynomial-time computable function which reduces L to A.

For any $x \in \Sigma^*$, we first, in polynomial-time, compute the *tt*-condition $\langle \alpha, \langle x_1,..., x_n \rangle \rangle$. If α is identical to 1 or 0, then we may determine the membership of x in L accordingly. Therefore, we may assume that α is not trivial. Then, we compute $f(x_1),..., f(x_n)$ and "partially sort" them as follows: Assume that g is a polynomial-time computable function which partially computes R. Then we have $g(x, y) = x \Rightarrow xRy$. Sort $f(x_1),..., f(x_n)$ as if g defined a partial ordering. We then have a rearrangement $x_{i_1},..., x_{i_n}$ of $x_1,..., x_n$ such that $f(x_{i_j}) R f(x_{i_{j+1}})$ for all $j = 1,..., n-1$. (It is possible that $f(x_{i_j}) R f(x_{i_k})$ for some $k < j$, too.) This partial sort can be done in polynomial-time. The new ordering of x_i's satisfies the property that $f(x_{i_{j+1}}) \in A \Rightarrow f(x_{i_j}) \in A$ for $j = 1,..., n-1$. This means, equivalently, $x_{i_{j+1}} \in L \Rightarrow x_{i_j} \in L$ for $j = 1,..., n-1$.

Without loss of generality, let us assume that $i_j = j$ for all $j = 1,..., n$, i.e., $f(x_1) R f(x_2) R \cdots R f(x_n)$. All we need to do now is to perform a binary search to find a j, $1 \leqslant j \leqslant n$, such that

$$\alpha(\underbrace{1, 1,..., 1}_{(j-1) \text{ many } 1\text{'s}}, 0,..., 0) = 0$$

and

$$\alpha(\underbrace{1, 1,..., 1}_{j \text{ many } 1\text{'s}}, 0,..., 0) = 1.$$

By the positivity of α, we have found x_j such that $x \in L$ iff $x_j \in L$ since $x_j \in L$ and $i < j$ implies $x_i \in L$. That is, we have reduced x to a smaller element x_j. Since the size of an R-decreasing chain is polynomially bounded, we need only to perform the reduction polynomially bounded many times to reach a trivial case. ∎

Since both B_ω and SAT are *ptt*-self-reducible, we have

COROLLARY 5 [12]. *No p-selective sets can be* $\leqslant_m^p$*-hard in* NP (*PSPACE*), *unless* $P = \text{NP}$ (*or, respectively,* $P = PSPACE$).

Whether the condition *ptt*-self-reducibility on L can be weakened to *tt*- or *T*-self-reducibility is not known.

As for weakly *p*-selective sets we can only prove that these sets cannot be higher than *d*-self-reducible sets.

THEOREM 8. *If L is d-self-reducible and $L \leqslant_m^p A$ for some weakly p-selective set A, then $L \in P$.*

Proof. Assume that R is a partially polynomial-time computable preorder on Σ^* which induces S and R' such that R' is *p*-linear and A is the union of some initial

segments of R'-chains as described in Definition 8. Also assume that $L \leqslant_m^p A$ via g, a polynomial-time computable function.

Consider the self-reducing tree of a string $x \in \Sigma^*$. This tree has the property that any node y is in L iff x is in L. Since all the nodes are of length bounded by a polynomial of $|x|$, we may calculate their g-values and "partially" sort these g-values into polynomially bounded many R-chains in polynomial-time. In each chain, we need only to retain the smallest one because $g(y)\, R\, g(z)$ implies $[y \in L \Rightarrow z \in L]$.

We perform this pruning procedure in a width-first manner; i.e., at each level of the tree, perform this pruning procedure once to keep the width of the tree bounded by a polynomial of $|x|$. Thus, the pruning procedure can be done in polynomial-time and the size of the pruned tree is bounded by a polynomial of $|x|$. This pruned tree gives a polynomial time algorithm for finding the membership of x in L. ∎

COROLLARY 6. *No weakly p-selective sets can be* $\leqslant_m^p$*-hard in* NP *or* $\leqslant_m^p$*-hard in* co-NP, *unless* $P = \text{NP}$.

The width-first pruning technique used in Theorem 8 does not apply to *ptt*-self-reducible sets. The reason is that it is no longer sufficient to select just the smallest element in each R-chain. As a matter of fact, the choice of a critical element in an R-chain may depend on the choice in another R-chain. In addition, the set of these critical elements (probably one in each R-chain) is not necessarily unique. However, we can directly prove that if $B_\omega \leqslant_m^p A$ for some weakly p-selective set A, then $B_\omega \in P$. The proof is essentially the same as the one used in [11] to prove that if $B_\omega \leqslant_m^p L$ for some left cut L, then $B_\omega \in P$. We sketch it in the following.

For a given formula F whose membership in B_ω is to be determined, we first arrange F in a normal form that quantifiers precede other logical symbols. Now we describe the self-reducing tree of F as follows:

The root is F.

Each node F' has the form $G_1 \wedge G_2 \wedge \cdots \wedge G_m$, where each G_i is a formula obtained by replacing some variables in F by constants 0 or 1.

A node F' with no quantifiers is a terminal node. A nonterminal node may have two children or just one child according to its leftmost quantifier of the leftmost longest term G_i of F'. (A term G_i in F' is *longest* if it has the largest number of quantifiers.)

Without loss of generality, let G_1 be the leftmost longest term in F'.

Case 1. $F' = (\forall x)\, G(x) \wedge G_2 \wedge \cdots \wedge G_m$. Then F' has a single child $G(0) \wedge G(1) \wedge G_2 \wedge \cdots \wedge G_m$.

Case 2. $F' = (\exists x)\, G(x) \wedge G_2 \wedge \cdots \wedge G_m$. Then, F' has two children: $G(0) \wedge G_2 \wedge \cdots \wedge G_m$ and $G(1) \wedge G_2 \wedge \cdots \wedge G_m$.

Now this tree becomes a d-self-reducing tree in which the root F is true iff any node in the tree is true. Note that this does not mean that B_ω is d-self-reducible because a node F' may have exponentially many terms. However, each node

$F' = G_1 \wedge \cdots \wedge G_m$ has the conjunctive property that F' is true iff every term G_i in F' is true. Thus, we may prune the tree by first deleting redundant terms in each node then deleting redundant nodes at each level of the tree. Each deletion procedure is similar to that in the proof of Theorem 8 in which we calculate the g-values of the terms (or the nodes) and partially sort them and delete all but the largest one (or, the smallest one, respectively).

Finally, we observe that the height of the pruned tree is bounded by a polynomial of the length of the root formula because of our choice of reducing the *longest* term first. Therefore, we have proved

THEOREM 9. *No weakly p-selective sets can be* $\leqslant_m^p$*-hard in* PSPACE *unless* $P = P\text{SPACE}$.

V. DISCUSSION

We have studied some low sets which are not $\leqslant_m^p$-complete in NP unless $P = \text{NP}$. They are also known to have small circuits and hence not likely $\leqslant_m^p$-complete in NP. Are there other low sets which can be used to distinguish $\leqslant_m^p$-completeness from $\leqslant_T^p$-completeness in NP? Let us consider some candidates.

A set has an APT (*almost polynomial time*) algorithm if that algorithm runs in polynomial time on all inputs but a sparse set. Meyer and Paterson [16] showed that APT sets are not high in NP. A set B is *weakly sparse* if the cardinality of the set $B_n = \{x \in B : |x| \leqslant n\}$ is bounded by a polynomial of n for infinitely many n. A *weakly* APT *set* is a set with polynomial time algorithm on all inputs except a weakly sparse set. Meyer and Paterson [16] conjectured that these weakly sparse and weakly APT sets are also not high.

Another well-known class of sets is the class of p-immune sets. A set is *p-immune* if it is infinite and does not have an infinite subset in P. Berman [5] showed that no p-immune set can be $\leqslant_m^p$-complete in EXP, the class of exponential-time computable sets. Bennett and Gill [2] pointed out that p-immune sets cannot be $\leqslant_m^p$-complete in NP if all NP-complete sets are p-isomorphic. It is interesting to note that Ko and Moore [13] have used p-immunity to distinguish $\leqslant_m^p$-completeness from $\leqslant_{tt}^p$-completeness in EXP. Whether a p-immune set can be $\leqslant_m^p$-, or $\leqslant_T^p$-complete in NP is an interesting open question.

REFERENCES

1. L. ADLEMAN, Two theorems on random polynomial time, *in* "Proceedings, 19th IEEE Symposium on Foundations of Computer Science," pp. 75–83, 1978.
2. C. H. BENNETT AND J. GILL, Relative to a random oracle A, $P^A \neq \text{NP}^A \neq \text{co-NP}^A$ with probability 1, *SIAM J. Comput.* **10** (1981), 96–113.
3. V. L. BENNISON, Some lowness properties and computational complexity sequences, *Theoret. Comput. Cci.* **6** (1978), 233–254.

4. V. L. BENNISON, Information content characterizations of complexity theoretic properties, *in* "Proceedings, 4th GI Conference on Theoretical Computer Science," Lecture Notes in Computer Science, No. 67, Springer-Verlag, Berlin/New York, pp. 58–66, 1979.
5. L. BERMAN, On the structure of complete sets: Almost everywhere complexity and infinitely often speed up, *in* "Proceedings, 17th Symposium on Foundations of Computer Science," pp. 76–80, 1976.
6. P. BERMAN, Relationship between density and deterministic complexity of NP-complete languages, *in* "Proceedings, 5th International Colloquium Automata, Languages and Programming, pp. 63–71, Lecture notes in Computer Science, No. 62, Springer-Verlag, Berlin/New York, 1978.
7. L. BERMAN AND J. HARTMANIS, On isomorphism and densities of NP and other complete sets, *SIAM J. Comput.* **6** (1977), 305–322.
8. S. A. COOK, The complexity of theorem-proving procedures, *in* "Proceedings, 3rd ACM Symposium on Theory of Computing," pp. 151–158, 1971.
9. S. FORTUNE, A note on sparse complete sets, *SIAM J. Comput.* **8** (1979), 431–433.
10. R. KARP AND R. LIPTON, Some connections between nonuniform and uniform complexity classes, *in* "Proceedings, 12th ACM Symposium on Theory of Computing," pp. 302–309, 1980.
11. K. KO, The maximum value problem and NP real numbers, *J. Comput. System Sci.* **24** (1982), 15–35.
12. K. KO, A note on circuit-size complexity and the low hierarchy in NP, *SIAM J. Comput.*, to appear.
13. K. KO AND D. J. MOORE, Completeness, approximation and density, *SIAM J. Comput.* **10** (1981), 787–796.
14. R. LADNER, N. LYNCH, AND A. SELMAN, A comparison of polynomial time reducibilities, *Theoret. Comput. Sci.* **1** (1975), 103–213.
15. S. R. MAHANEY, Sparse complete sets for NP: Solution of a conjecture by Berman and Hartmanis, *in* "Proceedings, 21st IEEE Symposium on Foundations of Computer Science," pp. 54–60, 1980.
16. A. MEYER AND M. PATERSON, "With What Frequency Are Apparently Intractable Problem Difficult?" MIT Tech. Rep., MIT/LES/TM-126, 1979.
17. H. ROGERS, JR., "Theory of Recursive Functions and Effective Computability," McGraw–Hill, New York, 1967.
18. U. SCHÖNING, A low and a high hierarchy within NP, *J. Comput. System Sci.*, to appear.
19. A. L. SELMAN, P-selective sets, tally languages and the behavior of polynomial time reducibilities on NP, *Math. Systems Teory* **13** (1979), 55–65.
20. A. L. SELMAN, Some observations on NP real numbers and p-selective sets, *J. Comput. System Sci.* **23** (1981), 326–332.
21. A. L. SELMAN, Reductions on NP and p-selective sets, *Theoret. Comput. Sci.* **19** (1982), 287–304.
22. R. I. SOARE, Computational complexity, speedable and levelable sets, *J. Symbolic Logic* **42** (1977), 545–563.
23. L. J. STOCKMEYER AND A. R. MEYER, Word problems requiring exponential time, *in* "Proceedings, 5th ACM Symposium on Theory of Computing," pp. 1–9, 1973.