



UvA-DARE (Digital Academic Repository)

Semi-Membership Algorithms: Some Recent Advances

Denny-Brown, D.; Han, Y.; Hemaspaandra, L.; Torenvliet, L.

Publication date
1994

Published in
SIGACT News

[Link to publication](#)

Citation for published version (APA):

Denny-Brown, D., Han, Y., Hemaspaandra, L., & Torenvliet, L. (1994). Semi-Membership Algorithms: Some Recent Advances. *SIGACT News*, 25(3), 12-23.

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

SIGACT News Complexity Theory Column 6

Lane A. Hemaspaandra
Dept. of Computer Science, University of Rochester
Rochester, NY 14627, USA lane@cs.rochester.edu

Introduction to Complexity Theory Column 6

I just attended the 9th Structure in Complexity Theory Conference, which was in Amsterdam this year. 100% of the first three papers in the proceedings ;-) were devoted to the study of semi-membership algorithms! In fact, during the last half-decade, there has been a marked surge of interest in semi-membership algorithms. The article below surveys some of the recent results from this research area. Though it is hard to pinpoint what triggers research “surges,” my own off-hand guess is that, if one had to put one’s finger on a single paper that restarted the interest in semi-membership algorithms, the paper one would finger would be Seinosuke Toda’s wonderful 1991 paper [Tod91], which set forth tricks (oops... *techniques*) that are used in many of the subsequent papers.

Guest Column: Semi-Membership Algorithms: Some Recent Advances¹

*Derek Denny-Brown*² *Yenjo Han*² *Lane A. Hemaspaandra*^{2,3} *Leen Torenvliet*⁴

Abstract

A semi-membership algorithm for a set A is, informally, a program that when given any two strings determines which is logically more likely to be in A . A flurry of interest in this topic in the late seventies and early eighties was followed by a relatively quiescent half-decade. However, in the 1990s there has been a resurgence of interest in this topic. We survey recent work on the theory of semi-membership algorithms.

1 Introduction

A *membership algorithm* M for a set A takes as its input any string x and decides whether $x \in A$. Informally, a *semi-membership algorithm* M for a set A takes as its input any strings x and y and decides which is “no less likely” to belong to A in the sense that if exactly one of the strings is in A , then M outputs that one string. Semi-membership algorithms have been studied in a number of settings. Recursive semi-membership algorithms (and the associated semi-recursive sets—those sets having recursive semi-membership algorithms) were introduced in the 1960s by Jockush [Joc79].

¹Supported in part by NSF grant CCR-8957604, NSF/JSPS grant INT-9116781/ENGR-207, HC&M grant ERB4050PL93-0516, and an NSF REU supplement.

²Department of Computer Science, University of Rochester, Rochester, NY, 14627.

³Work done in part while visiting the Tokyo Institute of Technology and the University of Amsterdam.

⁴Departments of Mathematics and Computer Science, University of Amsterdam, 1018 TV Amsterdam.

Deterministic polynomial-time semi-membership algorithms (and the associated P-selective or semi-feasible sets) were introduced in the 1970s by Selman [Sel79]. Nondeterministic polynomial-time semi-membership algorithms, both partial and total (and the associated NPSV_p-selective and NP-selective sets), were introduced in the 1990s by, respectively, Hemaspaandra, Naik, Ogihara, and Selman [HNOS94] and Hemaspaandra, Hoene, Ogihara, Selman, Thierauf, and Wang [HHO⁺93].

One telling question one can ask about abstract theoretical notions is, “Do they have any applications?” In the case of semi-membership algorithms, one can ask whether the extensive work done on sets having semi-membership algorithms yields any results that don’t explicitly refer to sets having semi-membership algorithms. Until recently, it would have been woefully hard to answer “yes” to this question. However, Section 2 discusses a recent application of semi-membership algorithms—that is, an instance where they resolve a question that was not thought to have any connection to the theory of semi-membership algorithms.

The application regards the following question: Is there a single-valued (partial) NP function that, whenever given a satisfiable formula as input, outputs a satisfying assignment? As an application of their results on nondeterministic semi-membership algorithms, Hemaspaandra et al. [HNOS94] have shown that if such a function exists, then the polynomial hierarchy collapses. This result is somewhat nonintuitive—especially as it is easy to see that NP functions can find *all* satisfying assignments for SAT. Thus, SAT seems to be a problem for which finding *one* solution is harder than finding *all* solutions! (This is not paradoxical. One cannot “get all solutions and then select the smallest one,” as the outputs from NP functions are so diffuse (in the computation tree) that a given output path has no obvious way of detecting whether or not its output is the smallest output value in the computation tree.) Section 2 also surveys related results on nondeterministic semi-membership algorithms, and their connections to nonuniform complexity and the extended low hierarchy.

Sections 4 through 6 survey recent results on the theory of sets having semi-membership algorithms computable in deterministic polynomial time. One unifying theme of these sections is their emphasis on the interrelations between P-selective sets and various polynomial-time reducibilities. Among the results surveyed are a result of Buhrman, van Helden, and Torenvliet [BvHT93] that P is exactly the class of sets that are both P-selective and Turing self-reducible, a result of Buhrman, Torenvliet, and van Emde Boas [BTvEB93] (respectively, of Ogihara, and Agrawal and Arvind, and Beigel, Kummer, and Stephan [Ogi94,AA94,BKS94]) that if NP has a positive-Turing-hard (respectively, bounded-truth-table-hard) P-selective set then P = NP, a result of Cai, Naik, and Selman [CNS94] that if NP has a truth-table-hard P-selective set then NP falls into a surprisingly small deterministic time class, a result of Hemaspaandra, Hoene, and Ogihara [HHO94] that more flexible reducibilities to P-selective sets provably accept larger language classes, and results of Hemaspaandra, Naik, Ogihara, and Selman [HNOS93] on the relationship between P-selective sets and “left cuts.”

2 Nondeterministic Semi-Membership Algorithms: Collapsing the Polynomial Hierarchy via Unique Solutions

Let us cut to the chase.

Hypothesis \mathcal{U} (see [Sel94]) There exists an NPSV function (that is, a single-valued NP function in the standard sense [BLS84]—the output from an NP machine for which each accepting path has an output, and all outputs on a given input are the same) h

such that for each Boolean formula F , it holds that $h(F)$ is a satisfying assignment of formula F .

That is, Hypothesis \mathcal{U} says that NP functions can find one satisfying assignment when given a satisfiable formula as input. This sounds innocuous, yet we have the following result.

Theorem 2.1 ([HNOS94]) If Hypothesis \mathcal{U} holds, then the polynomial hierarchy collapses to NP^{NP} .

Since we believe that the polynomial hierarchy does not collapse, in light of Theorem 2.1 we must conclude that Hypothesis \mathcal{U} is unlikely to hold. Before Theorem 2.1 was proven, the strongest known consequence of the truth of Hypothesis \mathcal{U} was a certain nice result of Selman [Sel94] regarding separability of NP-Turing-complete sets, but that result was not then (and still is not) known to imply the collapse of the polynomial hierarchy.

Though Theorem 2.1 does not mention semi-membership algorithms at all, its proof is deeply based on the theory of nondeterministic semi-membership algorithms, and indeed provides perhaps the first *application* of any notion of semi-membership algorithm in the sense discussed in the introduction. Hemaspaandra et al. in fact define semi-membership algorithms with respect to almost any function class (even, for the first time, multi-valued or partial function classes).

Definition 2.2 ([HNOS94]) Let \mathcal{FC} be any class of functions (possibly multivalued and/or partial). A set A is \mathcal{FC} -selective if there is a function $f \in \mathcal{FC}$ such that for every x and y , it holds that

$$f(x, y) \subseteq \{x, y\}, \text{ and} \\ \text{if } \{x, y\} \cap A \neq \emptyset, \text{ then } f(x, y) \neq \emptyset \text{ and } f(x, y) \subseteq A.$$

In a slight abuse of notation (using the same term both for the class of sets having the property and for the property—the particular context will make clear which use is intended), let \mathcal{FC} -selective also denote the class of sets that are \mathcal{FC} -selective.

The key lemma underpinning their proof is the following, which can be viewed as a strengthening of Ko’s [Ko83] result on the lowness of sets having total, deterministic semi-membership algorithms, though the proofs are quite different.

Lemma 2.3 ([HNOS94]) If $A \in \text{NP}$ and A is NPSV-selective, then $\text{NP}^{\text{NP}^A} = \text{NP}^{\text{NP}}$.

Given this lemma (whose proof is a bit tricky, and thus is not included here), Theorem 2.1 can be obtained as follows. SAT is trivially NPMV-selective. It is not hard to see that any NPSV “refinement” (that is, a function having the same domain, and having values always a (perhaps non-proper) subset of the function being refined) of an NPMV-selector for a set A in fact is an NPSV-selector for A . It is known [Sel94] that Hypothesis \mathcal{U} is equivalent to the statement that all NPMV functions have NPSV refinements. So if Hypothesis \mathcal{U} holds, SAT satisfies the hypothesis of the above lemma, and thus $\text{NP}^{\text{NP}^{\text{SAT}}} = \text{NP}^{\text{NP}}$, thus collapsing the polynomial hierarchy.

Open Question 2.4 Suppose Hypothesis \mathcal{U} is relaxed to allow h to be 2-valued (or even polynomially-valued), rather than single-valued. Does this relaxed hypothesis still collapse the polynomial hierarchy to NP^{NP} ? This question is currently open (and interesting!). Watanabe [Wat94] has taken a first step towards a resolution. He shows that one may relax the hypothesis to polynomially-valued functions if one adds a certain constraint on the behavior of h .

Below, we quickly summarize some of the other main results of Hemaspaandra et al. [HNOS94].

Definition 2.5 1. [KL80] For any class of sets \mathcal{C} , \mathcal{C}/poly denotes the class of sets L for which there exist a set $A \in \mathcal{C}$ and a polynomially length-bounded function $h : \Sigma^* \rightarrow \Sigma^*$ such that for every x , it holds that

$$x \in L \text{ if and only if } \langle x, h(0^{|x|}) \rangle \in A.$$

2. [BBS86] Let ExtendedLow_2 denote $\{L \mid \text{NP}^{\text{NP}^L} = \text{NP}^{\text{SAT} \oplus L}\}$, and let ExtendedLow_3 denote $\{L \mid \text{NP}^{\text{NP}^{\text{NP}^L}} = \text{NP}^{\text{NP}^{\text{SAT} \oplus L}}\}$.

The following two results show that NPSV-selective sets are of low nonuniform complexity.

Theorem 2.6 ([HNOS94]) $\text{NPSV-selective} \cap \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly}$.

Theorem 2.7 ([HNOS94]) $\text{NPSV-selective} \subseteq \text{NP}/\text{poly} \cap \text{coNP}/\text{poly}$.

The optimal number of bits of advice needed for nonuniform acceptance of selective sets has recently been established [HT94].

The following result shows that sets of relatively low nonuniform complexity are in the extended low hierarchy. Theorem 2.8 should be contrasted with the result of Köbler [Köb93] that $(\text{NP} \cap \text{coNP})/\text{poly}$ is “theta three extended low”; the two results are incomparable.

Theorem 2.8 ([HNOS94]) $(\text{NP}/\text{poly}) \cap (\text{coNP}/\text{poly})$ is ExtendedLow_3 .

From Theorems 2.7 and 2.8, it follows that the NPSV-selective sets are extended low.

Corollary 2.9 ([HNOS94]) The NPSV-selective sets are ExtendedLow_3 .

The above results all regard (partial) single-valued NP functions, which seems to be the most natural of the standard versions of NP functions, and which is the version that yields the result that unique solutions collapse the polynomial hierarchy. Readers interested in multivalued NP functions (respectively, total single-valued NP functions) can find more information on these in [HNOS94] (respectively, [HHO⁺93]). Wang [Wan] has recently defined probabilistic semi-membership algorithms, and has given a direct proof that $\text{PPF-selective} \subseteq \text{PP}/\text{poly}$, a result that is also implied by a relatively general meta-theorem, namely [HHO⁺93, Theorem 3.16].

3 Reductions to P-Selective Sets, and Two Puzzling Results

In the sense of Definition 2.2, consider the $\text{PF}_{\text{single-valued, total}}$ -selective sets. This class is commonly referred to as the P-selective sets (and we will also use this shorthand), and was first studied by Selman [Sel79]. In Section 4 of this paper, we will survey a line of research asking what consequences follow if, e.g., NP has a bounded-truth-table-hard P-selective set. It is now known (see Theorem 4.6) that this hypothesis implies $\text{P} = \text{NP}$. However, arriving at that result took a long time. On the other hand, as early as the 1970s it was known that if NP had a many-one-hard P-selective set, then $\text{P} = \text{NP}$. So if it were the case that every set that bounded-truth-table reduced to a P-selective set necessarily many-one reduced to some (perhaps different) P-selective set, then the recent bounded-truth-table result in fact would be an immediately corollary of the many-one result, and you, gentle reader, could happily skip much of Section 4 of this paper. Thus, one motivation for studying

whether the sets reducible to P-selective sets are themselves necessarily P-selective is simply to understand what extensions are meaningful, and which are already implicit based on known results about P-selective sets (see Corollary 4.2 for an example of this “result already implicit” effect in action).

More generally, in computer science we like to view polynomial-time reductions as being relatively innocuous. Does the class of P-selective sets have the property that different reductions to P-selective sets yield only P-selective sets? Though some classes—for example, P, $\text{NP} \cap \text{coNP}$, BPP, and PSPACE—do have this property of being “closed downwards under Turing reductions,” others—for example, the class of sparse sets [BK88]—do not.

Recently, Hemaspaandra, Hoene, and Ogihara [HHO94] have studied the relationships of different reducibilities (and equivalences) to P-selective sets, and their results show that, in the sense discussed in the previous paragraph, the P-selective sets are more like the sparse sets than like the BPP sets. On the other hand, the most striking feature of their paper is the contrast between their results and the known results for sparse sets.

In particular, for P-selective sets, both the separations and the collapses are more dramatic and unconditional than for sparse sets. For example, the theorem below states that one-truth-table reduction to P-selective sets yields the same class as one-truth-table equivalence to P-selective sets. In contrast, the same result is known for sparse sets only under the (rather strong) additional assumption that $\text{P} = \text{NP}$ [AHOW92]. In the course of proving the theorem below, [HHO94] in fact proves that $\text{R}_{2\text{-}tt}^p(\text{P-selective}) - \text{E}_{\mathcal{T}}^p(\text{P-selective})$ is non-empty. In contrast, it is known that proving the analogous result for sparse sets would immediately establish that $\text{P} \neq \text{NP}$ [AHOW92].

Adopting the standard notation in the literature, for any already-defined reducibility \leq_r^p , let $\text{R}_r^p(\text{P-selective})$ denote $\{A \mid (\exists L \in \text{P-selective}) [A \leq_r^p L]\}$, and let $\text{E}_r^p(\text{P-selective})$ denote $\{A \mid (\exists L \in \text{P-selective}) [A \leq_r^p L \text{ and } L \leq_r^p A]\}$.

- Theorem 3.1** ([HHO94])
1. $\text{P-selective} \stackrel{\zeta}{\sim} \text{R}_{1\text{-}\mathcal{T}}^p(\text{P-selective}) = \text{R}_{1\text{-}tt}^p(\text{P-selective}) = \text{E}_{1\text{-}\mathcal{T}}^p(\text{P-selective}) = \text{E}_{1\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{R}_{2\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots \stackrel{\zeta}{\sim} \text{R}_{k\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{R}_{(k+1)\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots$
 2. $\text{P-selective} \stackrel{\zeta}{\sim} \text{R}_{1\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{R}_{2\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots \stackrel{\zeta}{\sim} \text{R}_{k\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{R}_{(k+1)\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots$
 3. $\text{P-selective} \stackrel{\zeta}{\sim} \text{E}_{1\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{E}_{2\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots \stackrel{\zeta}{\sim} \text{E}_{k\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{E}_{(k+1)\text{-}tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots$
 4. $\text{P-selective} \stackrel{\zeta}{\sim} \text{E}_{1\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{E}_{2\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots \stackrel{\zeta}{\sim} \text{E}_{k\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{E}_{(k+1)\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \dots$
 5. $\text{E}_{btt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{E}_{tt}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{E}_{\mathcal{T}}^p(\text{P-selective})$.
 6. For every $k \geq 1$ and every P-selective set A it holds that $\text{R}_{k\text{-}\mathcal{T}}^p(A) = \text{R}_{(2^k-1)\text{-}tt}^p(A)$. In particular, for every $k \geq 1$ it holds that $\text{R}_{k\text{-}\mathcal{T}}^p(\text{P-selective}) = \text{R}_{(2^k-1)\text{-}tt}^p(\text{P-selective})$. For every $k \geq 2$ it holds that $\text{E}_{k\text{-}\mathcal{T}}^p(\text{P-selective}) \stackrel{\zeta}{\sim} \text{E}_{(2^k-1)\text{-}tt}^p(\text{P-selective})$.

In contrast to the above results on reductions to P-selective sets, one can also study the closure properties of the P-selective sets. The contrast here is a bit counter-intuitive. For example, it is known that the P-selective sets are closed downwards under disjunctive reductions, and yet it is

also known that the P-selective sets are not closed under union. For a typical complexity class, such a result would be impossible to obtain, as clearly, for any class closed under marked union (sometimes also called the “join” operation) closure under disjunctive reductions implies closure under union. The resolution of this puzzle is, of course, that the P-selective sets (in contrast to almost all standard complexity classes) are *not* closed under marked union! A discussion of the Boolean closure properties of the P-selective sets—in particular, the fact that for each k they fail to possess $2^{2^k} - 2k - 2$ of the k -ary Boolean closure properties—can be found in [HJ]. However, even though the fact that a set is (for example) the union of two P-selective sets does not perforce imply that it is P-selective, it does imply that the set is contained in certain of the recently defined generalizations of the P-selective sets (for example, the membership-comparable sets [Ogi94] and the multiselective sets [HJRW]), and thus is subject to the many results proving that these generalized classes contain only structurally simple sets.

Hemaspaandra, Jiang, Rothe, and Watanabe [HJRW] establish a similarly at-first-puzzling result. They prove that there exist two sets whose marked union (join) is easier than either of the sets, in the sense that both sets are not in the second level of the extended low hierarchy (see Definition 2.5) yet their join is in the second level! The reason this result should seem strange is that every set that many-one reduces to a set A also, for every set B , reduces to A joined with B . So joining two sets, intuitively, should never lower their complexity. The solution to this puzzle is simply that extended lowness is a measure of complexity orthogonal to the standard reduction-based measures of complexity, and thus one should not assume that it is closed downwards under various reductions. Indeed, it is known that the levels of the extended low hierarchy are not closed downwards under many-one reductions [AH92, Ver94]. In fact, informally stated, extended lowness is about the number of quantifiers required to extract information from a set—that is, it is a measure of a set’s organizational complexity, rather than of its conventional computational complexity.

4 Which Sets Reduce to P-Selective Sets?

As Toda [Tod91] remarked, the interesting reductions to P-selective sets are the non-positive reductions. Indeed, Buhrman, Torenvliet, and van Emde Boas [BTvEB93] show that the class of sets that positive-Turing reduce to P-selective sets is the class of P-selective sets itself. The best previously known result along these lines was the analogous result for positive-*truth-table* reductions, which was obtained by Selman [Sel79] over a decade earlier!

Theorem 4.1 ([BTvEB93]) For any set A and any P-selective set B , if $A \leq_{pos-T}^p B$ then $A \leq_m^p B$, and thus A is P-selective.

Corollary 4.2 ([BTvEB93]) If all NP sets \leq_{pos-T}^p -reduce to P-selective sets then $P=NP$.

The more interesting hunt is to find not just which sets reduce to P-selective sets, but which *interesting* sets reduce to P-selective sets. Results are often of a conditional sort: “If some set reduces to a P-selective set, then some unlikely collapse happens.” Toda [Tod91] showed the following important result. (R, UP, and FewP denote, respectively, random polynomial time, unambiguous polynomial time, and polynomial-bounded-ambiguity nondeterministic polynomial time (see, e.g., [Joh90]).)

Theorem 4.3 ([Tod91]) 1. If all sets in UP are \leq_{tt}^p -reducible to P-selective sets then $P = UP$.

2. If all sets in NP are \leq_{tt}^p -reducible to P-selective sets then $P = FewP$ and $R = NP$.

3. If all sets in P^{NP} are \leq_{tt}^p -reducible to P-selective sets then $P = \text{NP}$.

To prove these theorems, Toda introduces for each fixed NP machine M the set MINPATH , where $\langle x, i \rangle \in \text{MINPATH}$ if and only if the encoding of the i th bit on the minimum accepting path equals 1. A bit-string $\chi_{\text{MINPATH}}(\langle x, 1 \rangle) \dots \chi_{\text{MINPATH}}(\langle x, p(n) \rangle)$ can easily be checked to see whether it encodes an accepting path (by simulating the machine on the path obtained). If the set MINPATH is truth-table reducible to some P-selective set, then the strings $\langle x, 1 \rangle, \dots, \langle x, p(n) \rangle$ are connected to a polynomial number of queries, which can be sorted according to the quasi-ordering induced by the P-selector, to reveal a *polynomial* number of possible settings for $\chi_{\text{MINPATH}}(\langle x, 1 \rangle) \dots \chi_{\text{MINPATH}}(\langle x, p(n) \rangle)$. These possibilities can then all be checked in turn to find out if an accepting path exists.

Toda's absolute result that "there exists a set in exponential time that does *not* truth-table reduce to any P-selective set" was recently extended to Turing reducibility—albeit with a linear number of queries—by Burtchick and Lindner [BL93].

Theorems of the form "If some class reduces to a P-selective set then pigs can fly" tend to make use of some property other than P-selectivity of the set. Disjunctive self-reducibility has been a very central property in the long line of research on whether NP has sparse complete sets with respect to various reducibilities (the current state of this line can be seen in [AHH⁺93], and slightly outdated surveys of the line as a whole can be found in [HOW92, You92]), and has reappeared in the study of selectivity. SAT is a well-known disjunctive self-reducible set and it has long been known [Sel79, Ko83] that disjunctive self-reducible P-selective sets (in fact positive truth-table self-reducible sets) are in P. This result was recently extended by Buhrman, Torenlvliet, and van Helden [BvHT93].

Theorem 4.4 ([BvHT93]) Any Turing self-reducible P-selective set is in P.

We include a version of the proof of Theorem 4.4, rendering it as a story. With luck, this is more understandable than a formal proof, though it is obviously less explicit.

Let's say you have some great expert (Larry) who will solve a problem (namely, whether a given input x is in a certain fixed P-selective Turing self-reducible set A) that has been bugging you for a while, but needs to repeatedly question (yes or no) another expert (Moe). Now this other expert is really expensive, and you would like to avoid spending the money on having to call him multiple times. Fortunately, you happen to know that the questions Larry will ask Moe are about the same set as your original question. Knowing this, you might wonder "why not just *ask* the original question?" but that tempting option is precluded by the rules of Turing self-reducibility—and anyway, you have this great function that will tell you which of the two things is "stronger" (we use stronger to mean that it is more likely to be in the set, according to the selector function), so you want to get some use out of it. Here's what you do. You let Larry work and think and do whatever he does, and when he comes to talk to Moe, you use your comparison function and compare your original query x with Larry's query q . If x is stronger than q you respond no, otherwise you respond yes. Finally once Larry has given you an answer, you talk to Moe. There are only two queries to worry about. The strongest query that you answered no (y_1) and the weakest query you answered yes (y_2). First note that if the answers you gave to these two queries were correct then the answers you gave to *all* the queries were correct, and thus so was Larry's answer. If either of the answers to these two queries were incorrect, then you could immediately infer the answer to x from knowing which one was incorrect. But you can do even better! Suppose Larry's answer is yes. Then if the answer to y_2 is no then so is the answer to x because of the ordering, but if the answer to y_2 is yes then the answer to x cannot be no since otherwise the answer to y_1 would be no because of the ordering and the fact that in this case all the answers we have in Moe's place would have been

correct and so Larry’s answer “yes” would have to be correct! By the same reasoning the answer to x must be the same as the answer to y_1 in case where Larry’s answer was no.

The above story-proof proves that every Turing self-reducible P-selective set is many-one reducible. However, as observed by Ko [Ko83, p. 211], it is trivially true that every many-one self-reducible set (with or without the additional assumption that the set is P-selective) is in P. Thus, Theorem 4.4 is established.

Wang [Wan] observed that the same proof applies to well-behaved time classes larger than polynomial.

Buhrman et al. proved an extension in the direction of reductions to P-selective sets by showing:

Theorem 4.5 ([BvHT93]) If A is Turing self-reducible, B is P-selective, and $A \leq_{1-tt}^p B$, then $A \in P$.

On the other hand, under the assumption that $E \neq UE$, Buhrman [Buh93, Theorem 7.29] proves the existence of a disjunctive self-reducible set in NP that is Turing reducible to a P-selective set yet is not in P. Beigel, Kummer, and Stephan [BKS94, Theorem 7.1] observe that Theorem 4.5 cannot be extended to 2-truth-table reductions via any relativizable technique. Beigel et al. [BKS94], Ogihara [Ogi94], and Agrawal and Arvind [AA94] independently returned to the more restrictive domain of disjunctive self-reducibility, and within that restricted domain extended the type of truth-table reducibility from the reducibility found in Theorem 4.5.

Theorem 4.6 ([Ogi94, AA94, BKS94]) If all sets in NP are \leq_{bt}^p -reducible to P-selective sets then $P = NP$.

In fact both Ogihara’s and Beigel et al.’s results are more general since they deal with (provable) generalizations of P-selectivity called, respectively, “membership comparable sets” and “approximable sets.”

It is open whether Theorem 4.6 can be extended to truth-table reductions. The best known result along that line is Theorem 4.7 below. However, Hemaspaandra et al. [HHO⁺93, Proposition 3.9] prove that Theorem 4.6 cannot be extended to Turing reductions via any proof technique that relativizes.

Cai, Naik and Selman, using a result by Jenner and Torán [JT93], prove that if NP sets are truth-table reducible to P-selective sets, then the *deterministic* time complexity of SAT is surprisingly low.

Theorem 4.7 ([CNS94]) If there exists a P-selective set that is truth-table-hard for NP then, for all $k > 0$, $SAT \in DTIME[2^{n/\log^k n}]$.

5 Constructing P-Selective Sets

After having discussed P-selective sets, of course one wants to construct some of them. In this section, we mention first the classic construction technique of Selman, and then mention some new work that provides a new construction technique.

Selman [Sel82] gave the following straightforward method of producing P-selective sets. Let r be a real number written in binary and let r_n denote its n th bit. The *standard left cut* of r is defined as

$$L(r) = \{w \in \{0, 1\}^* \mid w \leq r_0 r_1 \dots r_{|w|}\},$$

where the \leq ordering is the dictionary ordering on strings.

For any given r , r 's standard left cut, $L(r)$, can easily be seen to be P-selective, since given any two strings x and y , the smaller one in dictionary order is more likely to be in *any* standard left cut. Standard left cuts have another interesting property. A real number $r \in [0, 1]$ can also be viewed as the characteristic string of a tally set $T(r) = \{0^n \mid r_n = 1\}$. It is easy to see that such a characteristic sequence can be recovered in polynomial time (by binary search) from $L(r)$ and so, since strings in $(L(r))^{\neq n}$ can be recovered in polynomial time from the information in $r_0 \dots r_n$, every standard left cut is polynomial-time Turing equivalent to a tally set. A moment's thought reveals that the reduction $L(r) \leq_T^p T(r)$ is even a positive reduction.

As every r.e. truth-table degree has tally sets, every r.e. truth-table degree has P-selective sets, so P-selective sets can be very complex. Are they all essentially left cuts? This question was recently answered to some extent. The answer is tied to the very hard question $P = PP$?

Theorem 5.1 ([HNOS93]) If $P = PP$ then for every non-empty P-selective set A there exists a standard left-cut $L(r)$ such that $A \equiv_m^p L(r)$.

From this theorem plus the above observation about positive reductions mentioned above, we have the following.

Theorem 5.2 ([HNOS93]) If $P = PP$ then for every P-selective set A there exists a Tally set T such that $A \leq_{pos-T}^p T$ and $T \leq_T^p A$.

Every standard left-cut is positive-truth-table reducible to a tally set, and every tally set is Turing reducible to a standard left-cut as we observed. An interesting question is whether this relation is as tight as possible. It is, as the following theorem shows.

Theorem 5.3 ([HNOS93]) There exists a standard left cut $L(r)$ such that for all tally sets T , $L(r) \not\equiv_{tt}^p T$.

Indeed, a tally set that is not \leq_{tt}^p -reducible to any P-selective set can even be found in $UP - P$, if we assume that $UE \neq E$ [HNOS93].

As we mentioned earlier in the paper, there is a long line of research studying whether *sparse* sets can be NP-hard with respect to various types of reductions. The results in this line are quite strong. One might naturally be tempted to wonder: Can the results about the consequences of having NP-hard P-selective sets with respect to various types of reductions be derived easily from the powerful known results about sparse sets? To preclude this, it would be nice to show that there is some P-selective set that does not reduce to any sparse set via, for example, positive-Turing reductions (or, even more to the point, bounded-truth-table reductions). However, Theorem 5.2 suggests that current techniques lack the power to establish this result for the positive-Turing reduction case; this is because proving this would immediately imply that $P \neq PP$ —a result that is probably true but is also thought to be beyond current techniques.

The following results are worth mentioning because they involve P-selective sets, although the results are also related to the study of sparse sets. Rao [Rao94] defines the class of P-selective-close sets as the class of sets that have a sparse symmetric difference with a P-selective set. He proves the following result, which obtains in a unified way the previously known results that no \leq_m^p -hard set for E can be either sparse or P-selective.

Theorem 5.4 ([Rao94]) No \leq_m^p -hard set for E is P-selective-close.

Fu and Li [FL93], extending a result of Ogihara and Watanabe [OW91], prove the following result about “weakly P-selective sets [Ko83]” and NP-hardness.

Theorem 5.5 ([FL93]) If there exists a weakly P-selective set A , an NP-hard set H , and a sparse set S , such that $H - A \leq_{btt}^p S$, then $P = NP$.

6 Search Reducing To Decision

An important question in the study of NP sets is the question of deciding the membership in a set vs. the hardness of obtaining an answer. A typical example is that to the question “Is 945032975230405 a prime number?,” we would like from an algorithm an answer richer than merely “no.” It is known that for any disjunctive self-reducible set, an algorithm deciding the set can easily be transformed into an algorithm producing a witness for membership in the set. This property, known as “search reduces to decision,” is the central theme of the paper of Hemaspaandra et al. [HNOS93], and as it turns out the question is related to reducibility to P-selectivity. They prove the following result.

Theorem 6.1 ([HNOS93]) If $L \in \text{NP}$ is P-selective and search nonadaptively reduces to decision for L then $L \in \text{P}$.

Assuming search reduces to decision for a language $L \in \text{NP}$, an even more general form of reduction can be used.

Theorem 6.2 ([HNOS93]) If $L \in \text{NP}$ is \leq_{1-tt}^p -reducible to a P-selective set and search nonadaptively reduces to decision for L then $L \in \text{P}$.

On the other hand, search adaptively reducing to decision and search nonadaptively reducing to decision seem quite different, as shown by the contrast between Theorem 6.1 and the following result.

Theorem 6.3 ([HNOS93]) If $\text{E} \neq \text{NE}$ then there exists a P-selective set $L \in \text{NP} - \text{P}$ for which search reduces to decision.

Acknowledgments

We are grateful to M. Cierniak and A. Selman for enjoyable discussions. All errors and opinions of course are the responsibility of the authors.

References

- [AA94] M. Agrawal and V. Arvind. Polynomial time truth-table reductions to P-selective sets. In *Proceedings of the 9th Structure in Complexity Theory Conference*, pages 24–30. IEEE Computer Society Press, June/July 1994.
- [AH92] E. Allender and L. Hemachandra. Lower bounds for the low hierarchy. *Journal of the ACM*, 39(1):234–250, 1992.
- [AHH⁺93] V. Arvind, Y. Han, L. Hemachandra, J. Köbler, A. Lozano, M. Mundhenk, M. Ogiwara, U. Schöning, R. Silvestri, and T. Thierauf. Reductions to sets of low information content. In K. Ambos-Spies, S. Homer, and U. Schöning, editors, *Complexity Theory*, pages 1–45. Cambridge University Press, 1993.
- [AHOW92] E. Allender, L. Hemachandra, M. Ogiwara, and O. Watanabe. Relating equivalence and reducibility to sparse sets. *SIAM Journal on Computing*, 21(3):521–539, 1992.
- [BBS86] J. Balcázar, R. Book, and U. Schöning. Sparse sets, lowness and highness. *SIAM Journal on Computing*, 15(3):739–746, 1986.
- [BK88] R. Book and K. Ko. On sets truth-table reducible to sparse sets. *SIAM Journal on Computing*, 17(5):903–919, 1988.

- [BKS94] R. Beigel, M. Kummer, and F. Stephan. Approximable sets. In *Proceedings of the 9th Structure in Complexity Theory Conference*, pages 12–23. IEEE Computer Society Press, June/July 1994.
- [BL93] H. Burtschick and W. Lindner. On sets Turing reducible to P-selective sets. Technical Report 1993-38, TU-Berlin, Fachbereich Informatik, 1993.
- [BLS84] R. Book, T. Long, and A. Selman. Quantitative relativizations of complexity classes. *SIAM Journal on Computing*, 13(3):461–487, 1984.
- [BTvEB93] H. Buhrman, L. Torenvliet, and P. van Emde Boas. Twenty questions to a P-selector *Information Processing Letters*, 48(4), 1993.
- [Buh93] H. Buhrman. *Resource Bounded Reductions*. PhD thesis, University of Amsterdam, Amsterdam, The Netherlands, June 1993.
- [BvHT93] H. Buhrman, P. van Helden, and L. Torenvliet. P-selective self-reducible sets: A new characterization of P. In *Proceedings of the 8th Structure in Complexity Theory Conference*, pages 44–51. IEEE Computer Society Press, May 1993.
- [CNS94] J. Cai, A. Naik, and A. Selman. A note on P-selective sets and on adaptive versus nonadaptive queries to NP. Technical Report 94-02, State University of New York at Buffalo, Department of Computer Science, Buffalo, NY, 1994.
- [FL93] B. Fu and H. Li. On symmetric differences of NP-hard sets with weakly P-selective sets. *Theoretical Computer Science*, 120(2):279–291, 1993.
- [HHO⁺93] L. Hemaspaandra, A. Hoene, M. Ogiwara, A. Selman, T. Thierauf, and J. Wang. Selectivity. In *Proceedings of the 5th International Conference on Computing and Information*, pages 55–59. IEEE Computer Society Press, 1993.
- [HHO94] L. Hemaspaandra, A. Hoene, and M. Ogiwara. Reducibility classes of P-selective sets. Technical Report TR-524, University of Rochester, Department of Computer Science, Rochester, NY, July 1994.
- [HJ] L. Hemaspaandra and Z. Jiang. P-selectivity: Intersections and indices. In *Journal of Computing and Information*, 1(1), Special Issue: *Proceedings of the 6th International Conference on Computing and Information*. To appear.
- [HJRW] L. Hemaspaandra, Z. Jiang, J. Rothe, and O. Watanabe. Multiselectivity. In preparation.
- [HNOS93] E. Hemaspaandra, A. Naik, M. Ogiwara, and A. Selman. P-selective sets, and reducing search to decision vs. self-reducibility. Technical Report 93-21, State University of New York at Buffalo, Department of Computer Science, Buffalo, NY, 1993.
- [HNOS94] L. Hemaspaandra, A. Naik, M. Ogiwara, and A. Selman. Computing solutions uniquely collapses the polynomial hierarchy. In *Proceedings of the 5th International Symposium on Algorithms and Computation*. Springer-Verlag *Lecture Notes in Computer Science*, August 1994. To appear.
- [HOW92] L. Hemachandra, M. Ogiwara, and O. Watanabe. How hard are sparse sets? In *Proceedings of the 7th Structure in Complexity Theory Conference*, pages 222–238. IEEE Computer Society Press, June 1992.
- [HT94] L. Hemaspaandra and L. Torenvliet. Optimal advice. Manuscript, July 1994.
- [Joc79] C. Jockusch. Recursion theory: Its generalizations and applications. In *Proceedings of the Logic Colloquium, Leeds*, pages 140–157. Cambridge University Press, 1979.
- [Joh90] D. Johnson. A catalog of complexity classes. In J. Van Leeuwen, editor, *Handbook of Theoretical Computer Science*, chapter 2, pages 67–161. MIT Press/Elsevier, 1990.
- [JT93] B. Jenner and J. Torán. Computing functions with parallel queries to NP. In *Proceedings of the 8th Structure in Complexity Theory Conference*, pages 280–291. IEEE Computer Society Press, May 1993.

- [KL80] R. Karp and R. Lipton. Some connections between nonuniform and uniform complexity classes. In *Proceedings of the 12th ACM Symposium on Theory of Computing*, pages 302–309, April 1980. An extended version has also appeared as: Turing machines that take advice, *L’Enseignement Mathématique*, 2nd series 28, 1982, pages 191–209.
- [Ko83] K. Ko. On self-reducibility and weak P-selectivity. *Journal of Computer and System Sciences*, 26:209–221, 1983.
- [Köb93] J. Köbler. Locating P/poly optimally in the extended low hierarchy. In *Proceedings of the 10th Annual Symposium on Theoretical Aspects of Computer Science*, pages 28–37. Springer-Verlag *Lecture Notes in Computer Science #665*, February 1993.
- [Ogi94] M. Ogiwara. Polynomial-time membership comparable sets. In *Proceedings of the 9th Structure in Complexity Theory Conference*, pages 2–11. IEEE Computer Society Press, June/July 1994.
- [OW91] M. Ogiwara and O. Watanabe. On polynomial-time bounded truth-table reducibility of NP sets to sparse sets. *SIAM Journal on Computing*, 20(3):471–483, June 1991.
- [Rao94] R. Rao. On P-selectivity and closeness. Technical Report TR-499, University of Rochester, Department of Computer Science, Rochester, NY, 1994.
- [Sel79] A. Selman. P-selective sets, tally languages, and the behavior of polynomial time reducibilities on NP. *Mathematical Systems Theory*, 13:55–65, 1979.
- [Sel82] A. Selman. Analogues of semirecursive sets and effective reducibilities to the study of NP complexity. *Information and Control*, 52:36–51, 1982.
- [Sel94] A. Selman. A taxonomy of complexity classes of functions. *Journal of Computer and System Sciences*, 48(2):357–381, 1994.
- [Tod91] S. Toda. On polynomial-time truth-table reducibilities of intractable sets to P-selective sets. *Mathematical Systems Theory*, 24:69–82, 1991.
- [Ver94] N. Vereshchagin, January 1994. Personal Communication.
- [Wan] J. Wang. Selectivity and self-reducibility: New characterizations of complexity classes. In *Journal of Computing and Information*, 1(1), Special Issue: *Proceedings of the 6th International Conference on Computing and Information*. To appear.
- [Wat94] O. Watanabe, May 1994. Personal Communication.
- [You92] P. Young. How reductions to sparse sets collapse the polynomial-time hierarchy: A primer. *SIGACT News*, 1992. Part I (#3, pages 107–117), Part II (#4, pages 83–94), and Corrigendum to Part I (#4, page 94).