Electronic Colloquium on Computational Complexity, Report No. 4 (2002)

A Note on the Power of Extra Queries to Membership Comparable Sets

Till Tantau[*]

Technische Universität Berlin
Fakultät für Elektrotechnik und Informatik
10623 Berlin, Germany
tantau@cs.tu-berlin.de

November 2, 2001

Abstract

A language is called k-membership comparable if there exists a polynomial-time algorithm that excludes for any k words one of the 2^k possibilities for their characteristic string. It is known that all membership comparable languages can be reduced to some P-selective language with polynomially many adaptive queries. We show however that for all k there exists a $(k+1)$-membership comparable set that is neither truth-table reducible nor sublinear Turing reducible to any k-membership comparable set. In particular, for all $k > 2$ the number of adaptive queries to P-selective sets necessary to decide all k-membership comparable sets is $\Omega(n)$ and $\mathcal{O}(n^3)$. As this shows that the truth-table closure of P-sel is a proper subset of P-mc(log), we get a proof of Sivakumar's conjecture that $\mathcal{O}(\log)$-membership comparability is a more general notion than truth-table reducibility to P-sel.

Keywords: P-selective, membership comparable, reduction.

Introduction

Ogihara [12] introduced a hierarchy of classes of *polynomial-time membership comparable sets.* For well-behaved functions $f\colon \mathbb{N} \to \mathbb{N}$ a set A is in the class P-mc(f) if there is a deterministic polynomial-time machine that for any input words $x_1, \dots, x_{f(n)}$ of length at most n outputs a bit string $b \in \{0,1\}^{f(n)}$ that is not the characteristic string of the words.

Ogihara showed that P-mc(f) is always a proper subset of P-mc($f+1$), and thus a fine-grained hierarchy of classes of membership comparable sets

[*] Work done in part while visiting the University of Rochester, New York. Supported by the TU Berlin Erwin-Stephan-prize grant.

ISSN 1433-8092

can be build. He also showed that P-mc(poly) is a subset of P/poly – more precisely $\text{P-mc}(f) \subseteq \text{P}/\,\mathcal{O}\big(f(n)n^2\big)$ – but proving that it is a proper subset would show $\text{P} \neq \text{NP}$. Ogihara's results show that the hierarchy of membership comparable sets nicely snuggles into the class P/poly. This invites us to try proving that $\text{NP} \subseteq \text{P-mc}(f)$ implies P = NP for larger and larger functions f. The state of the art result [12, 5, 1] is that $\text{NP} \subseteq \text{P-mc}\big(c \log n\big)$ for $c < 1$ implies P = NP.

It is an open problem whether $\text{NP} \subseteq \text{P-mc(log)}$ implies P = NP. Here P-mc(log) denotes $\bigcup_{c\in\mathbb{N}} \text{P-mc}(c \log n)$. A partial answer to this was obtained by Sivakumar [15] who showed that $\text{NP} \subseteq \text{P-mc(log)}$ implies NP = RP. He conjectured that this was an improvement over the previously known result [17, 4] that $\text{NP} \subseteq \text{R}^{\text{P}}_{\text{tt}}(\text{P-sel})$ implies RP = NP. The reason he only conjectured that it was an improvement was that $\text{R}^{\text{P}}_{\text{tt}}(\text{P-sel})$ was known to be a subset of P-mc(log) by a result of Ogihara, but was not known to be a proper subset. Ogihara did however show that $\text{R}^{\text{P}}_{\text{tt}}(\text{P-sel})$ is a proper subset of P-mc(poly). Theorem 10 will show that, indeed, $\text{R}^{\text{P}}_{\text{tt}}(\text{P-sel}) \subsetneq \text{P-mc(log)}$, thus improving on Ogihara's result and proving Sivakumar's conjecture.

Theorem 10 is a corollary of our main result, Theorem 1 below. It concerns the question how powerful extra queries to membership comparable sets are. It is known [13, 14, 10] that all sets in P/poly are Turing reducible to a P-selective set. A rough inspection of the proof shows that languages in P/f can be reduced with $\mathcal{O}\big(f(n)n\big)$ adaptive queries to a P-selective set. Hence all languages in P-mc(f) can be reduced with $\mathcal{O}(f(n)n^3)$ adaptive queries to a P-selective set. We show that starting with P-mc(3) the number of queries cannot drop below linear. More generally, we show that if $k < t$ there is a language in the class P-mc(t) that is not sublinear Turing reducible to P-mc(k). The main result can also be seen as improving Ogihara's result that $\text{P-mc}(k+1) \not\subseteq \text{P-mc}(k)$.

Theorem 1 (Main Result). *Let $t > k \geq 2$ and let $c < \frac{t-k}{k-1}$. Then*

$$\text{P-mc}(t) \not\subseteq \text{R}^{\text{P}}_{cn\text{-T}}\big(\text{P-mc}(k)\big).$$

This paper is organised as follows. In *Section 1* we review some basic results concerning the relationship of selectivity and membership comparability. In *Section 2* we give a proof of Theorem 1. In *Section 3* we apply this theorem to P-selective sets.

1 Selectivity versus Membership Comparability

In this section we review the notions of P-selectivity and membership comparability and state some basic properties. The notion of P-selectivity is due to Selman [13]. The notion of membership comparability is due to Ogihara [12].

Definition 2 ([13]). A language L is P-*selective* if there exists a function $g \in \mathrm{FP}$ such that for all words x, y we have $g(x,y) \in \{x,y\}$ and furthermore if $x \in L$ or $y \in L$, then $g(x,y) \in L$. The class of P-selective sets is denoted P-sel.

Definition 3 ([12]). Let $f\colon \mathbb{N} \to \mathbb{N}$ be a function. A language L is f-*membership comparable* if there exists a function $g \in \mathrm{FP}$ that on input of any $f(n)$ many words $x_1, \dots, x_{f(n)}$ of length at most n yields a bit string $b \in \{0,1\}^{f(n)}$ with $b \neq \big(\chi_L(x_1), \dots, \chi_L(x_{f(n)})\big)$. The class of all f-membership comparable languages is denoted P-mc(f).

Here $\chi_L(x)$ denotes the characteristic value of x with respect to L. The different kinds of reductions used in the following fact are defined in the usual way, see [11] for an introduction and detailed definitions.

Fact 4 ([12, 7]).

1. P-sel $\subsetneq$ P-mc(2).
2. P-mc$(k) \subsetneq$ P-mc$(k+1)$ *for all* $k \in \mathbb{N}$.
3. $\mathrm{R}^{\mathrm{P}}_{f(n)\text{-tt}}(\text{P-sel}) = \mathrm{R}^{\mathrm{P}}_{\log f(n)\text{-T}}(\text{P-sel}) \subseteq \text{P-mc}\big((1+\epsilon)\log f(n)\big)$.
4. $\mathrm{R}^{\mathrm{P}}_{\mathrm{tt}}(\text{P-sel}) \subsetneq \text{P-mc(poly)}$.

In our proof of the main theorem we will be needing the following lemma, which has been rediscovered repeatedly by different authors.

Fact 5 ([2, 3, 8, 6]). *Let* $P \subseteq \{0,1\}^n$ *have the property that for all indices* $i_1, \dots, i_k \in \{1, \dots, n\}$ *we have*

$$\big|\{\, b_{i_1} \dots b_{i_k} \mid b_1 \dots b_n \in P \,\}\big| < 2^k.$$

Then

$$|P| \le S(n,k) := \sum_{i=0}^{k-1} \binom{n}{i}.$$

2 Proof of the Main Theorem

To prove Theorem 1 we first need a lemma that shows how the function $S(n,k)$ reacts to an increase of its first versus its second argument. Essentially the lemma states that it reacts much more dramatically to an increase of its second argument than to an increase of the first.

Lemma 6. *Let* $t > k \ge 2$. *Let* $p\colon \mathbb{N} \to \mathbb{N}$ *be any function and let* $q\colon \mathbb{N} \to \mathbb{N}$ *be a strictly increasing function. Then*

$$\lim_{n\to\infty} \frac{p(n)^{k-1}}{q(n)^{t-k}} = 0 \quad \textit{implies} \quad \lim_{n\to\infty} \frac{S\big(p(n)q(n),k\big)}{S\big(q(n),t\big)} = 0.$$

Proof. Let us abbreviate $a := p(n)$ and $b := q(n)$. In the following calculation $c_1 := (t-1)!$ and $c_2 := (t-1)!k$ are constants.

$$\begin{aligned}
&\frac{S(ab,k)}{S(b,t)} = \frac{\sum_{i=0}^{k-1}\binom{ab}{i}}{\sum_{i=0}^{t-1}\binom{b}{i}} \le \frac{\sum_{i=0}^{k-1}\binom{ab}{i}}{\binom{b}{t-1}} \\
&\le c_1 \sum_{i=0}^{k-1} \frac{(ab)!\,(b-t+1)!}{(ab-i)!\,b!} \le c_2 \frac{(ab)!\,(b-t+1)!}{(ab-k+1)!\,b!} \\
&= c_2 \frac{\prod_{i=0}^{k-2}(ab-i)}{\prod_{i=0}^{t-2}(b-i)} = c_2 \frac{1}{\prod_{i=k-1}^{t-2}(b-i)} \, \frac{\prod_{i=0}^{k-2}(ab-i)}{\prod_{i=0}^{k-2}(b-i)} \\
&\le c_2 \frac{1}{(b-k+1)^{t-k}} \left(\frac{ab}{b-k+2}\right)^{k-1} \le c_2 \frac{a^{k-1}}{b^{t-k}} \left(\frac{b}{b-k+1}\right)^{t-1}
\end{aligned}$$

As $b = q(n)$ is strictly increasing, the last expression in brackets tends to 1 as n tends to infinity. As $\lim_{n\to\infty} a^{k-1}/b^{t-k} = 0$ by assumption, we get the claim. □

Proof of Theorem 1. We construct a supersparse language $A \in \text{P-mc}(t) \setminus \text{R}^{\text{P}}_{cn\text{-T}}\big(\text{P-mc}(k)\big)$ using a standard diagonalisation, see [9] for an example. Let $M_0, M_1, \dots$ be a standard enumeration of Turing machines that could serve as membership comparing machines. Let $R_0, R_1, \dots$ be an enumeration of Turing reduction machines. Let the time bounds of M_i and R_i be $n^i + i$.

Let $\ell\colon \mathbb{N} \to \mathbb{N}$ be a quickly growing function. The set $A = \bigcup_{s\in\mathbb{N}} A_s$ is constructed in stages. Each A_s contains only words of length $\ell(s)$. We define $\ell(0)$ appropriately large, such that the first stage of the diagonalisation works. We furthermore require that the function ℓ grows fast enough such that for inputs from any stage we can easily simulate all constructions for the words from earlier stages.

Each A_s will contain at most $t-1$ many words. We now argue that we then have $A \in \text{P-mc}(t)$ via some machine M. Whenever we are given t different words of length $\ell(s)$ it cannot be the case that all of them are in A. Hence M can simply output 1^t in this case. If we are given words from different lengths, by possibly simulating the construction for earlier stages we can easily directly decide at least one of the input words, say the i-th one. Then M can output any bit string that disagrees on the i-th position with the value that M knows to be correct. Finally, if the same word is given as input twice, say on positions i and j, M can simply output any bit string that is 0 at the i-th position and 1 and the j-th. This shows $A \in \text{P-mc}(t)$.

We must explain how we can setup A_s in stage $s = \langle m, r\rangle$ such that A is not reducible via R_r to any language L for which M_m is a k-membership comparing machine. If R_r asks more than $c\ell(s)$ queries for any input of length $\ell(s)$ we can skip the stage s and set $A_s := \emptyset$.

Let $n := \ell(s)$. For each word w of length n compute all queries the machine R_r asks in its query tree. There are at most 2^{cn} many queries. Let

Q contain all queries R_r asks in its query tree for any word $w \in \Sigma^n$. Then the size of Q is limited by $2^{cn}2^n$.

Let $P \subseteq \{0,1\}^{2^{cn}2^n}$ be the set of all bit strings that could possibly be characteristic strings of the words in Q with respect to some language for which M_m is a membership comparing machine. Then by Fact 5 the size of P is at most $S(2^{cn}2^n, k)$. Hence, there are also only $S(2^{cn}2^n, k)$ possibilities for the characteristic string of the words of length n with respect to the language A that are consistent with the machines M_m and R_r.

There are $S(2^n, t)$ many ways in which we can arrange A_s. Let $p(n) := 2^{cn}$ and let $q(n) := 2^n$. As $p(n)^{k-1} = 2^{c(k-1)n} = 2^{(t-k-\epsilon)n}$ for some $\epsilon > 0$, we have $\lim_{n\to\infty} p(n)^{k-1}/q(n)^{t-k} = 0$. By Lemma 6 we get

$$\lim_{n\to\infty} \frac{S\big(2^{cn}2^n, k\big)}{S\big(2^n, t\big)} = 0.$$

In particular, starting from some n_0 we have for all $n > n_0$

$$S\big(2^{cn}2^n, k\big) < S\big(2^n, t\big).$$

Thus, we can always choose A_s in such a way that M_m and R_r are fooled. □

Corollary 7. *If $k \geq 2$ then*

$$\text{P-mc}(k+1) \not\subseteq \mathrm{R}^{\mathrm{P}}_{\mathrm{tt}}\big(\text{P-mc}(k)\big).$$

Proof. We just repeat the proof. Only this time the function $p(n)$ limits the number of queries that can be asked by the truth-table reduction R_r. It is limited by $n^s + s \leq n^{\log^* n} + \log^* n$. Clearly, $\lim_{n\to\infty} p(n)^{k-1}/q(n) = 0$. □

3 Application to P-Selective Sets

In this section we present two applications of Theorem 1.

Theorem 8. *Let $c < t-2$. Then* $\text{P-mc}(t) \not\subseteq \mathrm{R}^{\mathrm{P}}_{cn\text{-T}}(\text{P-sel})$.

Proof. Applying the main theorem with $k = 2$ and $c < t - 2 = (t-2)/(2-1)$ yields $\text{P-mc}(t) \not\subseteq \mathrm{R}^{\mathrm{P}}_{cn\text{-T}}\big(\text{P-mc}(2)\big)$. As every P-selective language is 2-membership comparable, we get the claim. □

This theorem should be contrasted with the fact that all k-membership comparable sets *are* Turing reducible to a P-selective set with $\mathcal{O}(n^3)$ many queries. Thus

$$\text{P-mc}(\text{const}) \subseteq \mathrm{R}^{\mathrm{P}}_{\mathcal{O}(n^3)\text{-T}}(\text{P-sel}), \text{ but}$$

$$\text{P-mc}(\text{const}) \not\subseteq \mathrm{R}^{\mathrm{P}}_{cn\text{-T}}(\text{P-sel}) \text{ for all } c.$$

In [16] the notion of P-*selective query complexity* is introduced. The P-selective query complexity of a set (a class of sets) is the minimum number of queries that need to be asked to any P-selective oracle in order to decide the set (every sets in the class). Phrased in terms of this notion, the above result now reads as follows.

Theorem 9. *The* P-*selective adaptive query complexity of* P-mc(const) *is* $\Omega(n)$ *and* $\mathcal{O}(n^3)$.

Theorem 10. $\mathrm{R}^{\mathrm{P}}_{\mathrm{tt}}(\text{P-sel}) \subsetneq \text{P-mc}(\log)$.

Proof. By Fact 4 we have $\mathrm{R}^{\mathrm{P}}_{\mathrm{tt}}(\text{P-sel}) = \mathrm{R}^{\mathrm{P}}_{\mathcal{O}(\log n)\text{-T}}(\text{P-sel})$ and $\mathrm{R}^{\mathrm{P}}_{\mathrm{tt}}(\text{P-sel}) \subseteq \text{P-mc}(\log)$. □

The claim of the above theorem is exactly a conjecture made by Sivakumar [15]. It improves on Ogihara's result that $\mathrm{R}^{\mathrm{P}}_{\mathrm{tt}}(\text{P-sel}) \subsetneq \text{P-mc}(\text{poly})$.

Acknowledgments

I would like to thank Lane Hemaspaandra and Leen Torenvliet for helpful discussions.

References

[1] M. Agrawal and V. Arvind. Polynomial time truth-table reductions to P-selective sets. In *Proc. Ninth Annual Structure in Complexity Theory Conference*, pages 24–30. IEEE Computer Society Press, 1994.

[2] R. Beigel. *Query-limited reducibilities.* PhD thesis, Stanford University, Stanford, USA, 1987.

[3] R. Beigel. A structural theorem that depends quantitatively on the complexity of SAT. In *Proc. 2nd Annual IEEE Conference on Structure in Complexity Theory*, pages 28–32. IEEE Computer Society Press, 1987.

[4] R. Beigel. Np-hard sets are p-superterse unless R = NP. Technical Report TR 4, Dept. of Computer Science, Johns Hopkins University, 1988.

[5] R. Beigel, M. Kummer, and F. Stephan. Approximable sets. *Inform. and Computation*, 120(2):304–314, 1995.

[6] R. Beigel, M. Kummer, and F. Stephan. Quantifying the amount of verboseness. *Inform. and Computation*, 118(1):73–90, Apr. 1995.

[7] H.-J. Burtschick and W. Lindner. On sets Turing reducible to p-selective sets. *ACM Trans. Comput. Syst.*, 30(2):135–143, 1997.

[8] S. Clarke, J. C. Owings, Jr., and J. Spriggs. Trees with full subtrees. In *Proc. of the Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing*, pages 169–172, Winnipeg, Canada, 1975.

[9] L. A. Hemaspaandra, A. Hoene, and M. Ogihara. Reducibility classes of P-selective sets. *Theoretical Comput. Sci.*, 155(2):447–457, 1996.

[10] K.-I. Ko. On self-reducibility and weak P-selectivity. *J. Comput. Syst. Sci.*, 26:209–221, 1983.

[11] R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial time reducibilities. *Theoretical Comput. Sci.*, 1(2):103–123, Dec. 1975.

[12] M. Ogihara. Polynomial-time membership comparable sets. *SIAM J. Comput.*, 24(5):1068–1081, Oct. 1995.

[13] A. L. Selman. P-selective sets, tally languages, and the behavior of polynomial time reducibilities on NP. *Math. Systems Theory*, 13:55–65, 1979.

[14] A. L. Selman. Reductions on NP and P-selective sets. *Theoretical Comput. Sci.*, 19:287–304, 1982.

[15] D. Sivakumar. On membership comparable sets. *J. of Computer and System Sci.*, 59(2):270–280, 1999.

[16] T. Tantau. On the power of extra queries to selective languages. Technical Report TR00-077, Electronic Colloquium on Computational Complexity, 2000.

[17] S. Toda. On polynomial-time truth-table reducibility of intractable sets to p-selective sets. *Math. Systems Theory*, 24:69–82, 1991.