# Simpler proofs of the power of one query to a p-selective set *

David Eisenstat
Department of Computer Science
University of Rochester
Rochester, NY 14627 USA

Univ. of Rochester Comp. Sci. Dept. Technical Report TR-2005-883
October 5, 2005

**Abstract**

We eliminate some special cases from the proofs of two theorems in which a machine instantiating a many-query reduction to a p-selective set is made to use only one query. The first theorem, originally proved by Buhrman, Torenvliet, and van Emde Boas [BTvEB93], states that any set that positively reduces to a p-selective set has a many-one reduction to that same set. The second, originally proved by Buhrman and Torenvliet [BT96], states that self-reducible p-selective sets are in P.

The p-selective sets were introduced by Selman [Sel79] as a complexity-theory analog of semirecursive sets, which were introduced by Jockusch [Joc68]. This note assumes that the reader is familiar with basic complexity theory but presents definitions and basic propositions from the theory of p-selective sets. Interested readers are advised to consult the original papers [BTvEB93, BT96] and also Hemaspaandra and Torenvliet's monograph [HT02] on semifeasible algorithms.

A set $B \subseteq \Sigma^*$ is *p-selective* [Sel79] iff there exists a (total, deterministic) polynomial-time function $f : \Sigma^* \times \Sigma^* \to \Sigma^*$ such that for all $w, x \in \Sigma^*$,

1. $f(w, x) \in \{w, x\}$, and
2. $\overline{f}(w, x) \in B \to f(w, x) \in B$,

where $\overline{f}$ is defined according to the rule

$$\overline{f}(w, x) := \begin{cases} x, & \text{if } f(w, x) = w \\ w, & \text{otherwise.} \end{cases}$$

$f$ is a *p-selector* for $B$. This definition, although nonstandard, captures the same class of sets as the usual one while highlighting its duality under complementation. For example, the following proposition is a direct consequence of the contrapositive form of the condition $\overline{f}(w, x) \in B \to f(w, x) \in B$.

**Proposition 1.** *If $B$ is p-selective via p-selector $f$, then $\overline{B}$ is p-selective via p-selector $\overline{f}$.*

*Supported in part by NSF grant NSF-CCF-0426761. Retyped with minor corrections on November 22, 2011.

Given a p-selector $f$, we can extend $f$ to finite nonempty sets by repeated application of $f$. for all finite nonempty $W \subseteq \Sigma^*$ we define

$$f(W) := \begin{cases} w_1, & \text{if } |W| = 1 \\ f(f(\ldots f(w_1, w_2), w_3), \ldots, w_n), & \text{otherwise,} \end{cases}$$

where $w_1, \ldots, w_n$ is an enumeration of $W$ in increasing lexicographic order. This extension of $f$ has properties similar to those of a p-selector.

**Proposition 2** ([BTvEB93]). *Let $B$ be p-selective via p-selector $f$ and let $W \subseteq \Sigma^*$ be a finite nonempty set.*

1. *Given a reasonable encoding of finite sets, the extension of $f$ is a polynomial-time function.*
2. *$f(W) \in W$.*
3. *$\overline{f}(W) \in B \rightarrow W \subseteq B$.*
4. *$f(W) \in \overline{B} \rightarrow B \subseteq \overline{W}$.*

Next we consider the set of strings $x$ whose inclusion in a p-selective set $B$ is "obviously" entailed by the inclusion of a given string $w$. Formally, given a p-selective set $B$ with p-selector $f$, we define for all $w \in \Sigma^*$ the set $B_f^+(w)$ according to the rule

$$B_f^+(w) := \{x \in \Sigma^* \mid f(w, x) = x\}.$$

Buhrman, Torenvliet, and van Emde Boas call this set $B^+(w)$; we add a subscript $f$ to reflect the dependence of this definition on $f$. These sets either contain $B$ or are contained in $B$, depending on whether $w \in B$.

**Proposition 3** ([BTvEB93]). *Let $B$ be a p-selective set with p-selector $f$. For all $w \in \Sigma^*$,*

1. *$B_f^+(w)$ is in P.*
2. *$w \in B \rightarrow B_f^+(w) \subseteq B$, and*
3. *$w \in \overline{B} \rightarrow B \subseteq B_f^+(w)$.*

Now we define various reducibilities. These involve an oracle (Turing) machine $M$; we say $M$ is *polynomial-time* iff there exists a polynomial $p$ such that for all oracles $O \subseteq \Sigma^*$ and inputs $w \in \Sigma^*$, the computation $M^O(w)$ halts within $p(|w|)$ steps, where $|w|$ denotes the length of $w$. $L(M^O)$ is the set of strings accepted by $M$ with oracle $O$. An oracle machine $M$ is *positive* iff for all oracles $O \subseteq O' \subseteq \Sigma^*$, $L(M^O) \subseteq L(M^{O'})$.

Let $A, B \subseteq \Sigma^*$ be sets. $A$ is *positively reducible* to $B$, denoted $A \leq_{pos}^p B$, iff there exists a positive polynomial-time oracle machine $M$ such that $A = L(M^B)$. We say $A \leq_{\widehat{m}}^p B$ iff $A \leq_{pos}^p B$ via oracle machine $M$ such that for all oracles $O \subseteq \Sigma^*$ and inputs $w \in \Sigma^*$, $M$ makes at most one query during the computation $M^O(w)$. $\leq_{\widehat{m}}^p$-reducibility, first introduced by Ambos-Spies [AS89], is a variant of many-one reducibility that avoids trivial corner cases: $A \leq_{\widehat{m}}^p B$ if and only if $A$ is many-one reducible to $B$ or $A$ is in P.

A set $B \subseteq \Sigma^*$ is *self-reducible* [MP79] iff $B \leq_T^p B$ via oracle machine $M$ such that for all oracles $O \subseteq \Sigma^*$ and inputs $w \in \Sigma^*$, $M$ queries only strings shorter than $w$. $B$ is *many-one self-reducible* iff it is self-reducible via an oracle machine that instantiates $B \leq_{\widehat{m}}^p B$.

We can now prove the theorems about the power of one query to a p-selective set.

**Theorem 4** ([BTvEB93])**.** *Suppose a set $A \subseteq \Sigma^*$ is positively reducible to a p-selective set $B$. Then $A \leq^p_{\widehat{m}} B$.*

*Proof.* Let $M$ be an oracle machine that instantiates $A \leq^p_{pos} B$, and let $B$ have p-selector $f$. We specify the behavior of another oracle machine $N$ and show that it instantiates $A \leq^p_{\widehat{m}} B$.

Given oracle $O \subseteq \Sigma^*$ and input $w \in \Sigma^*$, $N$ computes $M^C(w)$, where $C := \{x \in \Sigma^* \mid M^{B^+_f(x)}(w) \text{ rejects}\}$, recording the set of queries $Q_{yes}$ answered affirmatively and the set of queries $Q_{no}$ answered negatively. If $M^C(w)$ accepts, $N$ accepts iff $Q_{yes}$ is empty or $\overline{f}(Q_{yes}) \in O$. Otherwise, $N$ accepts iff $Q_{no}$ is nonempty and $f(Q_{no}) \in O$. If $N$ does not accept, it halts and rejects.

$N$ is a positive polynomial-time oracle machine that queries $O$ at most once. To show that $A = L(N^B)$, fix $w \in \Sigma^*$; it suffices to show that $N^B(w)$ accepts if and only if $M^B(w)$ accepts. Assume first that $M^C(w)$ accepts. This entails that $M^{Q_{yes}}(w)$ also accept. If $Q_{yes}$ is empty, then $N^B(w)$ accepts, and $Q_{yes} \subseteq B$. Since $M$ is positive, $M^B(w)$ accepts as well. Otherwise, let $x := \overline{f}(Q_{yes})$. If $x \in B$, then $N^B(w)$ accepts, $Q_{yes} \subseteq B$, and $M^B(w)$ accepts. If $x \in \overline{B}$, then $N^B(w)$ rejects and $B \subseteq B^+_f(x)$. Since $x \in C$, $M^{B^+_f(x)}(w)$ rejects, and thus $M^B(w)$ rejects. The case when $M^C(w)$ rejects is exactly dual. □

**Theorem 5** ([BT96])**.** *Suppose $B \subseteq \Sigma^*$ is p-selective and self-reducible. Then $B$ is many-one self-reducible.*

*Proof.* Let $M$ be an oracle machine via which $B$ is self-reducible, and let $B$ have p-selector $f$. We specify the behavior of another oracle machine $N$ via which $B$ is many-one self-reducible.

Given oracle $O \subseteq \Sigma^*$ and input $w \in \Sigma^*$, $N$ computes $M^{B^+_f(w)}(w)$, recording the set of queries $Q_{yes}$ answered affirmatively and the set of queries $Q_{no}$ answered negatively. If this computation accepts, $N$ accepts iff $Q_{yes}$ is empty or $\overline{f}(Q_{yes}) \in O$. Otherwise, $N$ accepts iff $Q_{no}$ is nonempty and $f(Q_{no}) \in O$. If $N$ does not accept, it halts and rejects.

$N$ is a positive polynomial-time oracle machine such that for all oracles $O \subseteq \Sigma^*$ and inputs $w \in \Sigma^*$, $N$ queries at most one string during the computation $N^O(w)$, and this string, if extant, is shorter than $w$. To show that $A = L(N^B)$, fix $w \in \Sigma^*$; it suffices to show that $N^B(w)$ accepts if and only if $w \in B$. Assume first that $M^{B^+_f(w)}(w)$ accepts. This entails that $M^{Q_{yes}}(w)$ also accept. When $Q_{yes}$ is nonempty, let $x := \overline{f}(Q_{yes})$. If $Q_{yes}$ is empty or $x \in B$, then $N^B(w)$ accepts, and $Q_{yes} \subseteq B$. It follows that $w \in B$, since if $y \in B \cap Q_{no}$, $f(w, y) = w$ and $y \in B$ implies that $w \in B$; otherwise $M^B(w)$ and $M^{Q_{yes}}(w)$ behave identically. If $x \in \overline{B}$, then $N^B(w)$ rejects and $w \in \overline{B}$, since $f(w, x) = w$. The case when $M^{B^+_f(w)}(w)$ rejects is exactly dual. □

The latter theorem has the following immediate corollary, via iteration.

**Corollary 6** ([BT96])**.** *$B$ is in P if and only if $B$ is p-selective and self-reducible.*

The author thanks Lane Hemaspaandra for helpful comments and for proofreading an earlier draft.

## References

[AS89] Klaus Ambos-Spies. Honest polynomial time reducibilities and the P=?NP problem. *Journal of Computer and System Sciences*, 39(3):250–281, December 1989.

[BT96] Harry Buhrman and Leen Torenvliet. P-selective self-reducible sets: a new characterization of P. *Journal of Computer and System Sciences*, 53(2):210–217, October 1996.

[BTvEB93] Harry Buhrman, Leen Torenvliet, and Peter van Emde Boas. Twenty questions to a p-selector. *Information Processing Letters*, 48(4):201–204, November 1993.

[HT02] Lane A. Hemaspaandra and Leen Torenvliet. *Theory of semi-feasible algorithms*. Springer, December 2002.

[Joc68] Carl G. Jockusch. Semirecursive sets and positive reducibility. *Transactions of the American Mathematical Society*, 131(2):420–436, May 1968.

[MP79] Albert R. Meyer and Mike Paterson. With what frequency are apparently intractable problems difficult? Technical Report MIT-LCS-TM-126, Massachusetts Institute of Technology Laboratory for Computer Science, February 1979.

[Sel79] Alan L. Selman. P-selective sets, tally languages, and the behavior of polynomial time reducibilities on NP. *Mathematical Systems Theory*, 13:55–65, 1979.