P-sel \subseteq \text{NP}/n + 1 \text{ but } P-sel \not\subseteq \text{NP}/n

Colin Pronovost    David Thomas    Haichuan Yang    Maria Janczak    Shir Maimon    Brian Dickenson    Nathan Kent

November 29, 2016
A/f

For any set $A$ and any function $f$, $A/f$ denotes the class of all sets $L$ such that for some function $h$ satisfying $(\forall n)(|h(n)| = f(n))$ it holds that

$$L = \{ x \mid \langle x, h(|x|) \rangle \in A \}$$
For any class $C$ and any class of functions $\mathcal{F}$, $C/\mathcal{F}$ denotes the class of all sets $L$ such that

$$(\exists C \in C)(\exists f \in \mathcal{F})(L \in C/f)$$
P-sel = \{ L \mid (\exists \text{ polynomial-time 2-ary function } f) \cr (\forall x, y)(f(x, y) \in \{x, y\} \cr \wedge \{x, y\} \cap L \neq \emptyset \implies f(x, y) \in L)\}\}
The reachability function: $R_{i,G}(v)$

$R_{i,G}(v)$ is the set of vertices in graph $G$ that can be reached from vertex $v$ in at most $i$ steps. $R_{0,G}(v) = \{v\}$. 
Theorem 3.9: 2-reachability in a tournament

In a $k$-tournament $G$, there exists a vertex $v$ in $G$ such that all vertices in $G$ can be reached from $v$ in at most 2 steps. Formally, $(\forall k$-tournaments $G)(\exists v \in V_G)(R_{2,G}(v) = V_G)$
Proof of Theorem 3.9

The result obviously holds for 1-tournaments and 2-tournaments. Assume it holds for all $k$-tournaments. Consider some $k + 1$ tournament $G$. Let $v$ be a vertex in $G$, and let $G'$ be the $k$-tournament induced by the vertices of $G$ other than $v$. 
By induction, $(\exists u \in V_{G'}) (R_{2,G'}(u) = V_G)$. If $v \in R_{2,G}(u)$, then $R_{2,G}(u) = V_G$. Otherwise, for each vertex $w$ in $R_{1,G}(v)$, $(v, w) \in E_G$. Therefore $R_{2,G}(v) = V_G$. 
Theorem 3.10: $\text{P-sel} \subseteq \text{NP} / n + 1$
Let $f$ be the selector function and $g$ be the advice function, defined as

$$g(n) = \begin{cases} 1^{n+1} & L^n = \emptyset \\ 0w_n & \text{otherwise} \end{cases}$$

where $w_n \in L^n$ is the string from which all other strings in $L^n$ can be reached via paths of length at most 2 in the tournament induced on $L^n$ by $f$. By Theorem 3.9, such a string exists. Clearly, $|g(n)| = n + 1$. 
The advice interpreter set $A$ is defined as follows:

$$A = \{ \langle x, 0w \rangle \mid \text{there is a path of length at most 2 from } w \text{ to } x \text{ in the tournament induced by } f \text{ on } L^=n \}$$

$A \in \text{NP}$ (guess the path).
Because P-sel is closed under complementation,
\( \text{P-sel} \subseteq \text{NP} / \text{linear} \cap \text{coNP} / \text{linear} \).
Corollary: linear nondeterminism

Each semi-feasible set can be accepted with linear advice via an NP machine using linear nondeterminism.
Theorem 3.13: $P\text{-sel} \not\subseteq NP/n$
Proof sketch of Theorem 3.13

We define a semi-feasible set which cannot be accepted with only $n$ bits of advice for a length $n$ string. We use diagonalization to ensure that no NP machine accepts this set, regardless of what length $n$ advice it is given.
Properties of the set

Let $l_0 = 2$ and let $l_i = 2^{2^{l_{i-1}}}$ for each $i > 0$. Let $Q = \{l_0, l_1, \ldots\}$. We will construct our set to have the following three properties:

1. All strings in $L$ have lengths from $Q$.
2. At each length, if some string $w$ of that length is in $L$, then all strings of that length lexicographically less than $w$ are also in $L$.
3. $L \in \text{DTIME}[2^{2^n}]$.

We claim (and will prove) that any set with these properties is semi-feasible.
Sets with these properties are semi-feasible

Any set $L$ with the aforementioned properties is semi-feasible. Define the selector function $f$ as follows:

$$f(x, y) = \begin{cases} 
  x & |y| \not\in Q \\
  y & |x| \not\in Q \land |y| \in Q \\
  \min_{\text{lex}}\{x, y\} & |x| \in Q \land |y| \in Q \land |x| = |y| \\
  \min_{\text{lex}}\{x, y\} & |x| \in Q \land |y| \in Q \land |x| \neq |y| \land \min_{\text{lex}}\{x, y\} \in L \\
  \max_{\text{lex}}\{x, y\} & |x| \in Q \land |y| \in Q \land |x| \neq |y| \land \min_{\text{lex}}\{x, y\} \not\in L 
\end{cases}$$
Rightmost strings

Let $N_1, N_2, \ldots$ be an enumeration of nondeterministic polynomial-time Turing machines in which each machine appears infinitely often. At each $k \in Q$, we let $i = ||\{j \mid j \in Q \land j \leq k\}||$. That is, $k = l_{i-1}$.

We define $rightmost_y$ for each length $k$ string $y$ as follows:

\[
rightmost_y = \begin{cases} 
1^{k-1} & \text{if } X = \emptyset \\
\max_{\text{lex}} X & \text{otherwise}
\end{cases}
\]

Let $X = \{ x \mid |x| = k \land N_i(\langle x, y \rangle) \text{ accepts} \}$
Let $j_k = \min_{\text{lex}} \left( \left( \Sigma^k \cup \{1^{k-1}\} \right) - \{z \mid (\exists y \in \Sigma^k)(\text{rightmost}_y = z)\} \right)$

In other words, $j_k$ is the lexicographically minimal string that was not a rightmost string.

Let $L^{=k} = \{x \mid |x| = k \land x \leq_{\text{lex}} j_k\}$

That is, $L^{=k}$ is the set of all length $k$ strings which are lexicographically less than or equal to $j_k$. If the construction takes more than $2^{2^k}$ steps, set $L^{=k} = \emptyset$. By construction, the three properties mentioned in the previous section hold, therefore $L$ is semi-feasible.
Definitions

Theorem 3.9: $\text{P-sel} \subseteq \text{NP/}n + 1$

Theorem 3.13: $\text{P-sel} \not\subseteq \text{NP/}n$

Proof outline

Properties of the set

Construction of the set $L$

$L \not\in \text{NP/}n$

The construction eventually completes for all machines

For strings of length $k$, in order to perform the construction, we must loop over $2^k$ advice strings and $2^k$ input strings, and take time $(2^{bk^c})^2$ to simulate an NP machine with a brute-force EXP machine. Note that $b$ and $c$ are properties of the machine, not the input string. In total, the construction takes $2^k 2^k (2^{bk^c})^2 = 2^{2k+2bk^c}$ steps, which is less than $2^{2k}$ for sufficiently large $k$. Because each machine appears infinitely often in the enumeration, each machine will eventually be paired with a $k$ large enough for the construction to complete.
Let \( k \) be such that the construction completes. Let \( i \) be defined as above (\( k = l_{i-1} \)). By construction, none of the \( 2^k \) advice strings of length \( k \) can be given to \( N_i \) to yield \( L =^k \). There are two cases:
Case 1: $|j_k| = k - 1$

If $|j_k| = k - 1$ ($j_k = 1^{k-1}$), then $L^{=k} = \emptyset$. However, for each advice string $y$, there is an $x$ for which $N_i$ accepts $\langle x, y \rangle$. If there was some $y$ for which $N_i$ rejected $\langle x, y \rangle$ for all $x$, then rightmost$_y$ would equal $1^{k-1}$, and therefore $j_k$ could not equal $1^{k-1}$. Therefore $L \notin \text{NP} / n$. 
Case 2: $|j_k| = k$

If $|j_k| = k$, then for each advice string $y$, either $N_i$ rejects $\langle j_k, y \rangle$ or $N_i$ accepts $\langle z, y \rangle$ for some $z >_{\text{lex}} j_k$. If there was some $y$ for which $N_i$ accepted $\langle j_k, y \rangle$ but did not accept $\langle z, y \rangle$ for any string $z$ which is lexicographically greater than $j_k$, then $\text{rightmost}_y$ would equal $j_k$. However, $j_k$ is defined to be a string which is not $\text{rightmost}_y$ for any $y$. Therefore $L \notin \text{NP} / n$. 
