Unique Solutions Collapse Polynomial Hierarchy

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

December, 2016
We will show that if all NP functions can be refined to output at most one value across all paths of computation, then the polynomial-time hierarchy collapses. More formally,

**Theorem**

*If all NPMV functions have NPSV refinements, then $PH = NP^{NP}$.*
Definition

Define the **output set** of an NP Turing Machine N on an input x to be the set of strings y that remain on the N’s worktape at the end of computation along at least one computation path that halts and accepts. A multivalued function \( f \) is in **NPMV** if there exists an NP Turing Machine N such that for every input x, the set of outputs of \( f(x) \) and the output set of N are equal.
**Definition**

For a multivalued function $f$, define

\[ \text{set-}f(x) = \{a \mid a \text{ is an output of } f(x) \} . \]

**Definition**

NPSV is the set

\[ \{ f \mid f \in \text{NPMV and for every input } x, \|\text{set-}f(x)\| \leq 1 \} . \]
Definition

Let $F$ be a (possibly multivalued) class of functions. A set $L$ is **F-selective** if there exists a function 2-ary $f \in F$ such that

1. $(\forall x, y)\left[\text{set-f}(x, y) \subseteq \{x, y\}\right]$
2. $(\forall x, y)\left[(x \in L \lor y \in L) \implies \emptyset \neq \text{set-f}(x, y) \subseteq L\right]$.

Note: Later we will be using NPSV-sel.
Refinement

Definition

If \(f\) and \(g\) are multivalued functions, then \(g\) is a refinement of \(f\) if

1. \((\forall x)\left[\text{set-}g(x) = \emptyset \iff \text{set-}f(x) = \emptyset\right]\)
2. \((\forall x)\left[\text{set-}g(x) \subseteq \text{set-}f(x)\right]\).
\[ \Sigma^0_0 = P \]
\[ \Sigma^p_{i+1} = NP^{\Sigma^p_i} \]
\[ PH = \bigcup_i \Sigma^p_i \]
Cook’s Theorem

**Theorem**

Let $N_i$ be a standard enumeration of NPTMs that without loss of generality is such that $N_i$ runs in time $n^i + i$. There is a function $f_{\text{COOK}} \in \text{FP}$, mapping from strings to boolean formulas, such that

1. $(\forall i)(\forall x)[N_i(x) \text{ accepts } \iff f_{\text{COOK}}(N_i, x, 0|x|_i + i) \text{ is satisfiable}]

2. $(\exists g_{\text{COOK}} \in \text{FP})(\forall i)(\forall x)[g_{\text{COOK}}(f_{\text{COOK}}(N_i, x, 0|x|_i + i)) = \langle N_i, x \rangle]

3. $(\exists h_{\text{COOK}} \in \text{FP})(\forall i)(\forall x)(\forall a)$
   
   [if $a$ is a satisfying assignment of $f_{\text{COOK}}(N_i, x, 0|x|_i + i)$, then $h_{\text{COOK}}(N_i, x, a, 0|x|_i + i)$ outputs an accepting computation path of $N_i(x)$]

Note: This was proven in a previous lecture.
Lemma 3.23

The following are equivalent:

1. Every NPMV function has an NPSV refinement.

2. \((\exists f \in NPSV)(\forall F \in SAT) [the only element in set-f(F) is a satisfying assignment of F].\)
Proof (Lemma 3.23)

"⇒"

Assume (1) holds.
Consider \( h \in NPMV \) where
\[
\text{set-} h(F) = \{ a \mid a \text{ is a satisfying assignment of } F \}.
\]
By (1) \( h \) has an NPSV refinement. Note that this refinement satisfies (2).
Proof (Lemma 3.23)

"⇐"

Assume (2) holds. Meaning: \((\exists f \in \text{NPSV})(\forall F \in \text{SAT})[\text{the only element in set-}f(F) \text{ is a satisfying assignment of } F]\). Let \(\hat{f}\) be such a function.

Let \(g \in \text{NPMV}\), by the function-computing NPTM \(N_i\).

Let \(f_{\text{COOK}}\) and \(h_{\text{COOK}}\) be defined as in Cook’s Thm..

We will now build an NPTM \(N\) which will compute an NPSV refinement of \(g\).
Proof (Lemma 3.23)

Let $N$ on input $x$:

1. Deterministically compute $f_{\text{COOK}}(N_i, x, 0|x|^i+i)$
2. Nondeterministically guess a computation path of $\hat{f}(f_{\text{COOK}}(N_i, x, 0|x|^i+i))$. If $\hat{f}$ produces no output along this computation path, do not produce output. Otherwise suppose $\alpha = \hat{f}(f_{\text{COOK}}(N_i, x, 0|x|^i+i))$ along this computation path.
3. Check $\alpha$ is a satisfying assignment of $f_{\text{COOK}}(N_i, x, 0|x|^i+i)$, if not, produce no output along this path of computation.
4. Deterministically compute 'path' = $h_{\text{COOK}}(N_i, x, \alpha, 0|x|^i+i)$. Compute $N_i(x)$ along computation path determined by 'path', and output its value.

Note $N$ is an NPSV refinement of $g$. □
Lemma 3.25

\[ NPSV-sel \cap NP \subseteq (NP \cap coNP)/poly \]
Proof (Lemma 3.25)

Let $L \in \text{NPSV-sel} \cap \text{NP}$.
Since $L \in \text{NP}$, there exists an NP machine that accepts it. Let $N_L$ be this machine.
Since $L \in \text{NPSV-sel}$, there exists a selector function $f \in \text{NPSV}$ for $L$. Recall, without loss of generality we may assume
$$\forall x, y [\text{set-f}(x, y) = \text{set-f}(y, x)].$$
Consider the advice interpreter
$$A = \{ \langle x, \langle \langle a_1, a_2, \ldots, a_z \rangle, \langle w_1, w_2, \ldots, w_{z'} \rangle \rangle \rangle \mid z = z' \text{ and }$$
$$\forall i : 1 \leq i \leq z)[w_i \text{ is an accepting path of } N_L(a_i)] \text{ and }$$
$$\exists i : 1 \leq i \leq z)[x \in \text{set-f}(x, a_i)] \}$$
Note $A \in \text{NP}$. 
Proof (Lemma 3.25)

\[ A = \left\{ \langle x, \langle \langle a_1, a_2, \ldots, a_z \rangle, \langle w_1, w_2, \ldots, w_{z'} \rangle \rangle \rangle \mid z = z' \text{ and} \right. \]
\[ (\forall i : 1 \leq i \leq z)[w_i \text{ is an accepting path of } N_L(a_i)] \text{ and} \]
\[ (\exists i : 1 \leq i \leq z)[x \in \text{set-f}(x, a_i)] \]

Note the following NPTM N accepts \( \bar{A} \):

1. If input is malformed or \( z \neq z' \), accept.
2. Deterministically check if
\[(\forall i : 1 \leq i \leq z)[w_i \text{ is an accepting path of } N_L(a_i)] \text{ and accept if this fails for any } i.\]
3. Guess the element of set-f\((a_i, x)\) and the paths f takes to arrive at the output. Accept if only if for each \( i \) set-f\((a_i, x) = \{a_i\}\) and the path guessed was an output-producing path.

Thus \( \bar{A} \in NP \), so \( A \in coNP \). So, \( A \in NP \cap coNP \).
Proof (Lemma 3.25)

Let’s define an advice function $g$. Fix a length $n$, and consider $L^n$. Define a tournament on $L^n$ using the NPSV-sel function $f$. Recall there exists a set $H_n$, $\|H_n\| \leq n$, and $(\forall y \in L^n)$ either $y \in H_n$ or $(\exists h \in H_n)$ s.t. set-$f(y, h) = \{y\}$. Consider the advice $\langle\langle h_1, h_2, ..., h_z\rangle, \langle w_1, w_2, ..., w_z\rangle\rangle$ where $\langle h_1, h_2, ..., h_z\rangle = H_n$ and each $w_i$ is the encoding of an accepting path of $N_L(h_i))$.

Note the advice is polynomially bounded.
Looking at $A$ with advice $g$, we see $(\forall x), A(\langle x, g(|x|)\rangle)$ accepts iff $x \in L^{|x|}$. Thus, $L \in (NP \cap coNP)/poly$.
So, we have proven $\text{NPSV-sel} \cap \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly}$. \qed
Lemma 3.26

Lemma

$$NP \subseteq (NP \cap \text{coNP})/\text{poly} \Rightarrow PH = NP^{NP}$$
Proof (Lemma 3.26)

By Theorem 1.16 (Karp-Lipton) we know that 
$NP \subseteq P/poly \Rightarrow PH = NP^{NP}$. This relativizes* to 
$(\forall A)[NP^A \subseteq P^A/poly \Rightarrow PH^A = NP^{NP^A}]$
Proof (Lemma 3.26)

Assume that $NP \subseteq (NP \cap coNP)/poly$. This means that $SAT \in (NP \cap coNP)/poly$ by some set $B \in (NP \cap coNP)$. Using the relativized form of Theorem 1.16, we now have $NP^B \subseteq P^B/poly \Rightarrow PH^B = NP^{NP^B}$. 
Proof (Lemma 3.26)

Note that:

- $NP \subseteq NP^{B} \subseteq NP^{NP \cap coNP} = NP$
- $P^{B} \subseteq P^{NP \cap coNP} = NP \cap coNP$
- $PH^{B} = PH$

Substituting these into our previous equation yields our lemma.

$NP \subseteq (NP \cap coNP)/poly \Rightarrow PH = NP^{NP}$
Theorem

If all NPMV functions have NPSV refinements, then $PH = NP^{NP}$. 
Proof (Thm 3.20*)

Assume all NPMV functions have NPSV refinements. Consider multivalued function \( f_{SAT} \) where
\[
\text{set-} f_{SAT}(x, y) = \{x, y\} \cap SAT.
\]
f_{SAT} is in NPMV as it can be computed by NP TM by:

1. Nondeterministically choose \( x \) or \( y \).
2. Nondeterministically choose variable assignment to formula chosen in previous step.
3. If variable assignment is satisfying, output the chosen formula.

Since \( f_{SAT} \) is in NPMV, by assumption it has an NPSV refinement. Let \( g_{SAT} \) be an NPSV refinement for \( f_{SAT} \).
Proof (Thm 3.20*)

Note that $g_{SAT}$ is an NPSV-selector for SAT. Suppose $L \in NP$. Since SAT is NP-Complete $L \leq^p_m$ reduces to SAT. So there exists a polynomial function $\sigma$ such that $\sigma(x) \in SAT \iff x \in L$. Note that

$$set-f_L(x,y) = \begin{cases} 
\{x\} & g_{SAT}(\sigma(x), \sigma(y)) = \{\sigma(x)\} \\
\{y\} & g_{SAT}(\sigma(x), \sigma(y)) = \{\sigma(y)\}, \sigma(x) \neq \sigma(y) \\
\emptyset & \text{otherwise}
\end{cases}$$

is an NPSV-selector for $L$. So, $L \in \text{NPSV-sel}$. Thus $L \in \text{NPSV-sel} \cap NP$. So, $NP \subseteq \text{NPSV-sel} \cap NP$. 
Proof (Thm 3.20*)

From the previous slide we have $NP \subseteq NPSV$-sel $\cap NP$. By lemma 3.25, $NPSV$-sel $\cap NP \subseteq (NP \cap coNP)/poly$.

So, $NP \subseteq (NP \cap coNP)/poly$.

Recall lemma 3.26 which states $NP \subseteq (NP \cap coNP)/poly \Rightarrow PH = NP^{NP}$.

So, $PH = NP^{NP}$.
Definition

The class of languages **RP** is

$$RP = \{L \mid \text{there is a probabilistic polynomial-time TM M so that for every input } x:\$$

(1) if $$x \in L$$ then $$Pr[M(x) \text{ accepts}] \geq \frac{1}{2}$$

(2) if $$x \notin L$$ then $$Pr[M(x) \text{ accepts}] = 0$$

\}$$

The class of languages **coRP** = $$\{L \mid \bar{L} \in RP\}$$.

Definition

The class of languages **ZPP** = $$RP \cap coRP.$$
Lemma 3.27 and Thm 3.20

Lemma

\[ NP \subseteq (NP \cap \text{coNP})/\text{poly} \Rightarrow PH = ZPP^{NP} \]

Note that this resembles Lemma 3.26, but with ZPP instead of NP.

Theorem

If all NPMV functions have NPSV refinements, then

\[ PH = ZPP^{NP} \]

It turns out \( ZPP^A \subseteq NP^A \) for all A. So our Thm 3.20* is actually a corollary!
Open Questions

- Does $\text{UP} = \text{NP}$ imply the polynomial hierarchy collapses?
- $\text{P-sel} \subseteq \text{P}/\text{linear}$?
In this section we proved Theorem 3.20: if all NPMV functions have NPSV refinements, the polynomial hierarchy collapses to $\Sigma_2^p$. 