The Tournament Divide and Conquer Technique

Daniel Rubery
Georgiy Platonov
Mohammad Rafayet Ali
Xiong Zhang
Lecture 3

Unique solutions collapse the Polynomial Hierarchy
Motivation

Looking at functions that give a satisfying assignment of clauses. We want some kind of function such that for any \( F \) in SAT, \( f(F) \) is a satisfying assignment of \( F \).

If there is a deterministic polynomial time function \( f \), then \( P=NP \).

There definitely exists an FP function with NP oracle.

We will define a weaker function, between FP and FP\(^{NP}\), whose existence implies \( \text{PH} = \text{NP}^{NP} \).
Definitions

1) Let $f$ be a multivalued function. $\text{set}-f(x)$ denotes the set of all values that are an output of $f(x)$. If $f(x)$ has no output then $\text{set}-f(x)$ is the empty set.

2) We consider any given nondeterministic polynomial-time machine $N$ to implicitly compute a (potentially partial) multivalued function, namely, the function $f_N$ defined by the set $\text{set}-f_N(x) = \{ y \mid \text{some computation path of } N(x) \text{ outputs } y \}$. $\text{NPMV}$ denotes the class of functions computed in this sense by nondeterministic polynomial-time machines.
More definitions

3) A (potentially partial) multivalued function $f$ is said to be single-valued if $\forall x(||\text{set-f}(x)|| \leq 1)$. NPSV denotes the class of all single-valued NPMV functions.

4) Given a multivalued functions $f$ and $g$, we say that $g$ is a refinement of $f$ if
   a. $\forall x(\text{set-g}(x) \subseteq \text{set-f}(x))$, and
   b. $\forall x(\text{set-g}(x) = \emptyset \Rightarrow \text{set-f}(x) = \emptyset)$. 
Yet more definitions

5) Let $F$ be any (possibly partial, possibly multivalued) function class. We say a set $L$ is $F$-selective if there is a multivalued function $f \in F$ such that

a. $\forall x, y (\text{set-f}(x, y) \subseteq \{x, y\})$, and

b. $\forall x, y ((x \in L \lor y \in L) \Rightarrow (\text{set-f}(x, y) \subseteq L \land \text{set-f}(x, y) \neq \emptyset))$. 
Theorem 3.21

If all NPMV functions have NPSV refinements, then $\text{PH} = \text{NP}^{\text{NP}}$. 
We will use the following two lemmas:

1) \( \text{NPSV-sel} \cap \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly} \). (Lemma 3.25)

2) \( \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly} \Rightarrow \text{PH} = \text{NP}^\text{NP} \). (Lemma 3.26)
Proof of Lemma 3.25: \( \text{NPSV-sel} \cap \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly} \)

Let \( L \) be a language in \( \text{NPSV-sel} \cap \text{NP} \). Let \( N_L \) be a NPTM accepting \( L \), and \( f \) an NPSV selector.

WLOG, for any \( x,y \) we have \( \text{set-}\text{f}(x,y) = \text{set-}\text{f}(y,x) \).

Now we construct an \( \text{NP} \cap \text{coNP} \) interpreter \( A \) and an advice function \( g \).

Let \( A \) be all strings of the form \(<x, <<a_1,a_2,\ldots,a_z>, <w_1,\ldots,w_z>>\) such that:

\[
\begin{align*}
    z &= z' \\
    \forall \ i \ (w_i \text{ is an accepting path of } N_L \text{ on } a_i) \\
    \exists \ i \ (x \in \text{set-}\text{f}(x,a_i))
\end{align*}
\]
Proof of Lemma 3.25:  \( \text{NPSV}\text{-sel} \cap \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly} \)

Clearly, \( A \) is in NP.

\( \overline{A} \) is also in NP, as follows:

Accept any syntactically ill-formed input, or if \( z \neq z' \) 
Deterministically check that each \( w_i \) is an accepting path of \( a_i \) 
Reject if, for some \( i \), \( x = a_i \) 
Since we now know each \( a_i \) is in \( L \), \( \text{set-f}(a_i,x) \) must have exactly one value 
For each \( i \), non-deterministically choose a path for \( f(a_i,x) \) 
  If it outputs nothing, reject 
  If it outputs \( x \), reject 
  If it outputs \( a_i \), continue 
Accept if each path gives \( f(a_i,x) = a_i \).
Proof of Lemma 3.25: $\text{NPSV-sel} \cap \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly}$

Create a tournament on $L^{=n}$. If $a, b \in L^{=n}$, then there is an edge from $a$ to $b$ if $\text{set-f}(a, b) = \{b\}$.

Now use Theorem 3.1 to get a set $H$ with at most $n+1$ strings. For every $x \in L^{=n}$, there is an $h \in H$, such that $x = h$ or $\text{set-f}(x, h) = \{x\}$.

Then our advice function is $g(n) = \langle \langle h_1, h_2, \ldots, h_n \rangle, \langle w_1, w_2, \ldots, w_n \rangle \rangle$, where each $w_i$ is an accepting path of $h_i$. This is polynomial length in $n$.

$x \in L$ iff $\langle x, g(|x|) \rangle \in A$

So $L \in (\text{NP} \cap \text{coNP})/\text{poly}$, and since $L$ was arbitrary in $\text{NPSV-sel} \cap \text{NP}$, we get the Lemma.
Proof of Lemma 3.26: $\text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly} \Rightarrow \text{PH} = \text{NP}^{\text{NP}}$

By theorem 1.16 (Karp-Lipton)

$$\text{NP} \subseteq \text{P/poly} \Rightarrow \text{PH} = \text{NP}^{\text{NP}}.$$ 

This result relativizes, i.e.

$$\forall A (\text{NP}^A \subseteq \text{P}^A/\text{poly} \Rightarrow \text{PH}^A = \text{NP}^{\text{NP}^A}).$$
Proof of Lemma 3.26: $\text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly} \Rightarrow \text{PH} = \text{NP}^{\text{NP}}$

Assume $\text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly}$. Then $\text{SAT} \in (\text{NP} \cap \text{coNP})/\text{poly}$ via some $B \in \text{NP} \cap \text{coNP}$, and some advice $g$ in poly.

From

$$\forall A (\text{NP}^A \subseteq P^A/\text{poly} \Rightarrow \text{PH}^A = \text{NP}^{\text{NP}^A})$$

we have

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

Having

\[
NP^B \subseteq P^B/\text{poly} \Rightarrow PH^B = NP^{NP^{NP^B}},
\]

we are going to prove that

\[
NP \subseteq (NP \cap \text{coNP})/\text{poly} \Rightarrow NP^B \subseteq P^B/\text{poly}
\]

and

\[
PH^B = NP^{NP^{NP^B}} \Rightarrow PH = NP^{NP}.
\]
Proof of Lemma 3.26: $\text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly} \Rightarrow \text{PH} = \text{NP}^{\text{NP}}$

It is easy to prove that

$$\text{NP} \subseteq \text{NP}^B \subseteq \text{NP}^{\text{NP}} \cap \text{coNP} = \text{NP}$$

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

For any $L \in \text{NP}$, let $h$ be a reduction from $L$ to SAT.

Let $\text{pad}_n(x)$ add dummy clauses to a SAT formula so that it is length $n$, and let $l(n)$ be the maximum length of $h(x)$ for $x$ in $\{0,1\}^n$.

$x \in L$ iff $h(x) \in \text{SAT}$ iff $\text{pad}_{l(n)}(h(x)) \in \text{SAT}$ iff $\{<\text{pad}_{l(n)}(h(x)),g(l(n))>\} \in B$

So $L$ can be decided with advice $g'(n) = <l(n),g(l(n))>$

By the advice interpreter:

$\{<x,<\text{len},w>> | <\text{pad}_{\text{len}}(h(x)), w> \in B\}$, which is $\text{P}^B$

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

By Karp-Lipton, \( \text{PH}^B = \text{NP}^{\text{NP}^B} \)

Finally, note that

\[ B \in NP \cap \text{coNP}, \text{PH}^B = \text{PH} \text{ and } \text{NP}^{\text{NP}^B} = \text{NP}^{\text{NP}}. \]

So

\[ NP \subseteq (NP \cap \text{coNP})/\text{poly} \Rightarrow \text{PH} = \text{NP}^{\text{NP}}. \]
Theorem 3.21

Now, using these two lemmas, we can prove Theorem 3.20, as follows.

Construct a NPMV-selector for SAT by set $f(x,y) = \{x,y\} \cap \text{SAT}$. This is NPMV by guessing an argument and assignment of variables, then outputting the argument if the assignment is valid.

By the hypothesis of the Theorem, $f$ has a NPSV refinement $g$.

Then $g$ is a NPSV selector for SAT.

Then $\text{SAT} \in \text{NPSV-sel}$. 
Theorem 3.21

SAT ∈ NPSV-sel. Will show that this gives NP ⊆ NPSV-sel.

For any NP language L, let h polynomial many-one reduce L to SAT.

Then define $g'(x,y) =$

\[
\begin{align*}
  \{x\} & \text{ if } g(h(x),h(y)) = h(x) \\
  \{y\} & \text{ if } g(h(x),h(y)) = h(y) \\
  \emptyset & \text{ otherwise}
\end{align*}
\]

Then $g'(x,y)$ is an NPSV-selector for L, so $L \in \text{NPSV-sel}$, and $\text{NP} \subseteq \text{NPSV-sel}$. 
Theorem 3.21

So we have that, if every NPMV function has an NPSV refinement, then $\text{NP} \subseteq \text{NPSV-sel}$.  

Lemma 3.25 says $\text{NPSV-sel} \cap \text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly}$.  

So $\text{NP} \subseteq (\text{NP} \cap \text{coNP})/\text{poly}$.  

This is the hypothesis of Lemma 3.26, so $\text{PH} = \text{NP}^{\text{NP}}$. 
Thank you!