Optimal proof systems and disjoint NP pairs.

Dmitry Antipov

Department of Mathematics
Saint Petersburg State University

Joint Advanced Student School 2009
Saint Petersburg
Course 1: “Propositional Proof Complexity”

17 мая 2009 г.
Optimal p.p.s and canonical NP pair
  optimal and p-optimal
  \textbf{NP} pairs
  canonical \textbf{NP} pairs

Connections with other notions
  automatizability
  representability
Definition

Let \( f \) and \( f' \) be two proof systems. \( f \) simulates \( f' \) if \( \exists \) function \( h : \Sigma^* \to \Sigma^* \), \( \forall w \in \Sigma^*, f(h(w)) = f'(w) \) and \( \exists p : |h(w)| \leq p(|w|) \). If \( h \in \text{FP} \), \( f \) p-simulates \( f' \).

Definition

A proof system is **optimal** if it simulates every other proof system (for the same language!).

Definition

A proof system is **p-optimal** if it p-simulates every other proof system.

In this talk, all proof systems are **propositional** proof systems, that is proof systems for \( \text{TAUT} \).
**Definition**

**Disjoint NP-pair** is just a pair of two disjoint NP sets.

**Definition**

A set $S$ is a **separator** of disjoint NP pair $(A, B)$ if $A \in S$ and $B \in \overline{S}$. Disjoint NP-pair is called **p-separable** if it has a separator from P.

**Definition**

A set $A$ is **many-one reducible** in polynomial time to $B$ ($A \leq^p_m B$) if there exists a polynomial time computable function $f$ such that $x \in A \iff f(x) \in B$.

A set $A$ is **Turing reducible** in polynomial time to $B$ ($A \leq^p_T B$) if there exists a polynomial-time oracle DTM $M : A = L(M, B)$. 
Definition

Let \((A, B)\) and \((C, D)\) be disjoint pairs.

\((A, B) \leq_{m}^{PP} (C, D)\) if \(\exists\) a function \(f \in FP\) such that \(f(A) \subseteq C\) and \(f(B) \subseteq D\)

\((A, B) \leq_{T}^{PP} (C, D)\) if \(\exists\) a polynomial-time oracle DTM \(M\) such that for \(\forall\) separator \(T\) of \((C, D)\) \(\exists\) a separator \(S\) of \((A, B)\), such that \(S = L(M, T)\)

Lemma

If \((A, B) \leq_{m}^{PP} (C, D)\) and \((C, D)\) is p-separable then \((A, B)\) is p-separable
Optimal p.p.s and canonical NP pair  canonical NP pairs

Canonical pair (Razborov)

Definition

The canonical pair of a proof system $f$ is the disjoint NP-pair $(SA^*, \text{REF}_f)$ where

$$SA^* = \{(x, 0^n) | x \in SAT \text{ and } n \in N\}$$

$$\text{REF}_f = \{(x, 0^n) | \neg x \in TAUT \text{ and } \exists y : (|y| \leq n \text{ and } f(y) = \neg x)\}.$$  

Why is it disjoint NP-pair?

$REF = \{(x | \neg x \in TAUT)\}; \text{REF} \in \text{co-NP}.$

If $x \in SAT$, then $\neg x \notin TAUT$. $SA^*$ is evidently in $NP$ and witness for $REF_f$ is $y$. 

6 / 16
Theorem

Let $f$ and $g$ be propositional proof systems. If $g$ simulates $f$ then $(\text{SAT}^*, \text{REF}_f) \leq_{PP}^{m} (\text{SAT}^*, \text{REF}_g)$.

Proof

$\exists h : \Sigma^* \rightarrow \Sigma^*$ and $p : \forall y (g(h(y) = f(y) \text{ and } |h(y)| \leq p(|y|))$.

$r(x, 0^n) := (x, 0^{p(n)})$. Evidently $(x, 0^{p(n)}) \in \text{SAT}^*$. 

$(x, 0^n) \in \text{REF}_f \Rightarrow \exists y : |y| \leq n \text{ and } f(y) = \neg x \Rightarrow$

$\Rightarrow \text{ for } y' := h(y), (|y'| \leq p(n); g(y') = \neg x) \Rightarrow$

$\Rightarrow (x, 0^{p(n)}) \in \text{REF}_g$. 
**Definition**

A set $A$ is paddable if there is a polynomial-time computable length-increasing function $g$ such that for all strings $x$ and $y$, $x$ is in $A$ if and only if $g(x, y)$ is in $A$.

**Lemma**

SAT is paddable.
**Theorem**

For every disjoint NP-pair \((A, B)\) \(\exists\) a proof system \(f\) : 
\((SAT^*, \text{REF}_f) \equiv_{pp}^m (A, B)\).

**Proof**

Let \(g\) be polynomially invertible function such that \(A \leq_P^{m} SAT\) via \(g\). Such \(g\) exists because \(SAT\) is paddable. Let \(M \in NDTM, L(M) = B, \text{time}(M)\) is bounded by \(p\). Let \(<.,.> \in FP\) and polynomially invertible function, 
\(|<x, w>| = 2 \ast (|x| + |w|)\).

\[ f(z) = \begin{cases} 
\neg g(x) & \text{if } z = <x, w>, |w| = p(|x|), M(x) \text{ accepts along path } w \\
2^{x} & \text{if } z = <x, w>, |w| \neq p(|x|), |z| \geq 2^{|x|}, x \in TAUT \\
1 & \text{otherwise;}
\end{cases} \]
Lemma

\((SAT^*, \text{REF}_f) \leq_{pp}^m (A, B)\).

Let \(a \in A\) and \(b \in B\).
We need a reduction function \(h\):

1. input\((x, 0^n)\);
2. if \((n \geq 2^{|x|})\) {
   1. if \((x \in SAT)\) return \(a\) else return \(b\);
3. if \((g^{-1}(x)\) exists) return \(g^{-1}(x)\) else return \(a\);
Lemma

\((SAT^*, \text{REF}_f) \geq_{PP}^{m} (A, B)\).

The reduction function \(h'(x) := (g(x), 0^{2^*(|x| + p(|x|)))\).

So, \((SAT^*, \text{REF}_f) \equiv_{PP}^{m} (A, B)\).

Theorem

\exist\text{ optimal } p.p.s \ f \Rightarrow \text{ its canonical disjoint } \text{NP}-\text{pair is } \leq_{PP}^{m} \text{ complete.}
**Definition**

A proof system $f$ is automatizable if $\exists \text{DTM } M$:
$\forall x \in TAUT : \exists w : f(w) = x; f(M(x)) = x$ and $M$ works in time polynomial of $|w|$

**Lemma**

If a proof system is automatizable then its canonical NP-pair is p-separable.

**But not vice versa!**:

**Lemma**

$\exists$ a proof system $f : (SAT^*, REF_f)$ is p-separable and $f$ is not automatizable unless $P = NP$
Connections with other notions

Proof

\[ f(z) = \begin{cases} 
  x & \text{if } z = \langle x, 1^m \rangle \text{ and } m \geq 2^{|x|} \\
  (x \lor T) & \text{if } z = \langle x, \alpha \rangle, \alpha \text{ is a satisfiable assignment for } x \\
  T & \text{otherwise}; 
\end{cases} \]

Definition

A proof system $f$ is \textbf{weakly automatizable} if $\exists g : g$ is automatizable and $g$ $p$-simulates $f$. 
Theorem

A proof system is weakly automatizable ⇐ its canonic NP-pair is p-separable.

Proof

⇐: Let’s take $h \in FP$: $h(SAT^*) = 1$ and $h(REF_f) = 0$.

$$g(z) := \begin{cases} x : & \text{if } z = \langle x, 1^m \rangle \text{ and } h \langle x, 1^m \rangle = 0 \\ True : & \text{otherwise} \end{cases}$$

⇒: $g$ p-simulates $f$ ⇒ $g$ simulates $f$

⇒ $(SAT^*, REF_f) \leq_{PP}^m (SAT^*, REF_g)$ ⇒ $(SAT^*, REF_f)$ is p-separable.
Theorem

\[ \exists \text{ complete disjoint NP-pair} \iff \exists \text{ a proof system for TAUT in which disj-NP is emph\text{(p-)representable}} \text{ i.e. every language } A \in \text{ disj-NP has short P-proofs of fact, that } A \in \text{ disj-NP and this proofs can be constructed in polynomial time.} \]
Glasser, Selman, Zhang: Survey on Disjoint $\text{NP}$-pairs and relations to propositional proof systems.

Beyesdorff, Sadovski: Characterizing the existence of optimal proof systems and complete set for promise class.

Beyersdorff: Disjoint $\text{NP}$ pairs from propositional proof system

Razborov: On provably disjoint $\text{NP}$ pairs.