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
- **NP** pairs
- canonical **NP** pairs

Connections with other notions

- automatizability
- representability

- **Definition**

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

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 ($A \leq_m^P B$) if there exists a polynomial time computable function f such that
$x \in A \Leftrightarrow f(x) \in B$.

A set A is Turing reducible in polynomial time to B ($A \leq_T^P B$) 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

Canonical pair(Razborov)

Definition

The canonical pair of a proof system f is the disjoint **NP**-pair (SAT^*, REF_f) where

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

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

- Why is it disjoint **NP**-pair?
- $REF = \{(x | \neg x \in TAUT)\}$; $REF \in$ **co-NP**.
- If $x \in SAT$, then $\neg x \notin TAUT$. SAT^* is evidently in **NP** and witness for REF_f is y.

Theorem

Let f and g be propositional proof systems. If g simulates f then $(SAT^*, REF_f) \leq_m^{PP} (SAT^*, REF_g)$.

Proof

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

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

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

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

$$\Rightarrow (x, 0^{p(n)}) \in REF_g.$$

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 :
$(SAT^*, REF_f) \equiv_m^{PP} (A, B)$.

Proof

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

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

Lemma

$(SAT^*, REF_f) \leq_m^{PP} (A, B)$.

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

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

Lemma

$(SAT^*, REF_f) \geq_m^{PP} (A, B)$.
The reduction function $h'(x) := (g(x), 0^{2*(|x|+p(|x|))})$.

So, $(SAT^*, REF_f) \equiv_m^{PP} (A, B)$.

Theorem

$\exists$ optimal p.p.s f $\Rightarrow$ its canonical disjoint **NP***-pair is $\leq_m^{PP}$ complete.*

Definition

A proof system f is automatizable if $\exists DTM\ M$:
$\forall x \in TAUT : \exists w : f(w) = x$; $f(M(x)) = x$ 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 $\mathbf{P} = \mathbf{NP}$

Proof

$$f(z) = \begin{cases} x \text{ if } z =< x, 1^m > \text{ and } m \geq 2^{|x|} \\ (x \vee T) : \text{ if } z =< x, \alpha >, \alpha \text{ is a satisfiable assignment for } x \\ T : \text{ otherwise;} \end{cases}$$

Definition

A proof system f is weakly automatizable if $\exists\ g$: g is automatizable and g p-simulates f

Theorem

A proof system is weakly automatizable $\Leftrightarrow$ *its canonic* **NP***-pair is p-separable.*

Proof

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

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

$\Rightarrow$:g p-simulates f $\Rightarrow$ g simulates f
$\Rightarrow (SAT^*, REF_f) \leq_m^{PP} (SAT^*, REF_g) \Rightarrow (SAT^*, REF_f)$is p-separable.

Theorem

$\exists$ complete disjoint **NP**-*pair* $\Leftrightarrow$ $\exists$ *a proof system for TAUT in which* **disj -NP** *is emph(p-)representable .i.e.every language* $A \in$ **disj -NP** *has short P-proofs of fact, that* $A \in$ **disj -NP** *and this proofs can be constructed in polynomial time.*

Bibliography

Glasser, Selman, Zhang: Survey on Disjoint **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 **NP** pairs from propositional proof system

Razborov: On provably disjoint **NP** pairs.