Department of Mathematics
Saint Petersburg State University

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

Optimal proof systems and disjoint NP pairs.

Dmitry Antipov

May 17, 2009

Contents

1 Optimal propositional proof system and canonical NP pair **2**
1.1 Optimal and p-optimal proof systems 2
1.2 **NP** pairs 3

2 Canonical disjoint NP-Pairs **3**

3 Automatizability **5**

1 Optimal propositional proof system and canonical NP pair

1.1 Optimal and p-optimal proof systems

The notion of proof system was formalized in classic work by Cook and Reckhow [CR79].
Definition 1 *A* proof system *for a set $S \in \Sigma^*$ is a total function $f{:}\Sigma^* \to S$ such that $f \in \mathbf{FP}$ and f is onto. If $f(w) = \phi$, it is said that w is the proof for ϕ*

Definition 2 *Let f and f' be two proof systems.* f simulates f' *if there exists function $h : \Sigma^* \to \Sigma^*$, such that $\forall w \in \Sigma^*, f(h(w)) = f'(w)$ and $\exists p : |h(w)| \leq p(|w|)$. If $h \in \mathbf{FP}$, we say that f* p-simulates *f'.*

Definition 3 *A proof system is* optimal *if it simulates every other proof system (for the same language!).*

Definition 4 *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 $TAUT$.

1.2 NP pairs

Definition 5 Disjoint **NP**-pair *is just a pair of two disjoint* **NP** *sets.*

For example, sets of codes of 0 and 1 for most of cryptosystem which encodes 1 bit forms a disjoint **NP** pair.

Definition 6 *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.*

Conjecture of existence of p-unseparable disjoint **NP** pairs is stronger, than $\mathbf{P} \neq \mathbf{NP}$ conjecture, and from it's negation we can obtain $\mathbf{co\text{-}NP} \cap \mathbf{NP} \subset P$.

Definition 7 *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 : $A = L(M, B)$.*

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

Definition 8 *(A, B) is* many-one reducible *in polynomial time to (C, D),$(A, B) \leq_m^{PP} (C, D)$ if there exists a function $f \in FP$ such that $f(A) \subseteq C$ and $f(B) \subseteq D$*

Definition 9 *(A, B) is* Turing reducible *in polynomial time to (C, D), $(A, B) \leq_T^{PP} (C, D)$, if there exists a polynomial-time oracle DTM M such that for every separator T of (C, D) exists a separator S of (A, B), such that $S = L(M, T)$*

It's easy to see connection between reducibility and p-separability:
If $(A, B) \leq_m^{PP} (C, D)$ and (C, D) is *p-separable* then (A, B) is *p-separable*

2 Canonical disjoint NP-Pairs

The canonical pair of a propositional proof system, introduced by Razborov [Raz95], is the disjoint **NP**-pair (SAT^*, REF_f),where

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

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

This pair is disjoint, because in first set there are only padded satisfiable formulas, and in second- unsatisfiable. First set is evidently in **NP**. The second set is in **NP** because we take only such formulas, whose negations have short proofs, and this proof can be taken as advice.

Theorem 1 *Let f and g be propositional proof systems. If g simulates f then $(SAT^*, REF_f) \leq_m^{PP} (SAT^*, REF_g)$.*

By assumption, there exists a total function h and a polynomial p:
$g(h(y)) = f(y)$ and $|h(y)| \leq p(|y|)$. Let's define a reduction function $r(x, 0^n) := (x, 0^{p(n)})$. Evidently $(x, 0^{p(n)}) \in SAT^*$. If $(x, 0^n) \in REF_f$ then there is a proof y: $|y| \leq n$ and $f(y) = \neg x$. But $g(h(y) = f(y)$ and $|h(y)| \leq p(|y|)$, so $|h(y)| < p(n)$,so there is a proof of $\neg x$ in g, with length no more than $p(n)$, so $(x, 0^{p(n)}) \in REF_g$.

Theorem 2 ([SGSZ04]) *For every disjoint* **NP***-pair (A, B) $\exists$ a proof system f : $(SAT^*, REF_f) \equiv_m^{PP} (A, B)$.*

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, $| < x, w > | = 2(|x| + |w|)$.

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

It's easy to see, that f is a proof system for TAUT.

Lemma 1 $(SAT^*, REF_f) \leq_m^{PP} (A, B)$.

Let a and b be an arbitrary element of A and B resp. So,we use this reduction algorithm.

- 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;

The condition $x \in SAT$ can be checked in polynomial time due to exponential padding, so this algorithm is polynomial-time. If $(x, 0^n) \in SAT^*$, then we output either a or $g^{-1}(x)$, both from A. If $(x, 0^n) \in REF_f$, then if padding's length was more than $2^{|x|}$ we returned b else, due the first case in definition of f, $g^{-1}(x)$ exists and belongs to B.

Lemma 2 $(SAT^*, REF_f) \geq_m^{PP} (A, B)$.

The reduction function is $h'(x) := (g(x), 0^{2(|x|+p(|x|))})$.
If $x \in A$ then $g(x) \in SAT$ and $h'(x) \in SAT^*$. Else, if $x \in B$ let w be an accepting path of $M(x)$ and let $z =< x, w >$, so $|w| = p(|x|)$ and $|z| = 2(|x| + p(|x|))$. By the first case of definition of f, $f(z) = \neg g(x)$, so $h'(x) \in Ref_f$
So, we proved the theorem.

Corollary 1 *If there exists an optimal propositional proof system f, then (SAT^*, REF_f) is a many-one complete disjoint* **NP** *pair*

Assume,that f is optimal proof system. As we prooved, for every disjoint **NP** pair(A, B) there exists propositional proof system g, which canonical **NP** pair is equivalent to (A, B)but because f is optimal, $(SAT^*, REF_f) \geq_m^{PP} (SAT^*, REF_g)$, so $(SAT^*, REF_f) \geq_m^{PP} (A, B)$

3 Automatizability

Definition 10 *A proof system f is automatizable if exists deterministic Turing machine M: $\forall x \in TAUT : \exists w : f(w) = x$; $f(M(x)) = x$ and M works in time polynomial of $|w|$*

In other words, it means our possibility to construct a proof for a formula in reasonable time.
It's easy to see, that if a proof system is automatizable then it's canonical **NP**-pair is p-separable. But not vice versa!:

Lemma 3 ([Bey06]) *$\exists$ a proof system $f : (SAT^*, REF_f)$ is p-separable and f is not automatizable unless* $\mathbf{P} = \mathbf{NP}$

Let's take this function f:

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

In first case, exponential padding allows us to separate $SAT^*$and REF_f in polynomial time. And for second case formulas are always tautologies, and it can be determined in polynomial time too. But the length of the shortest proof is the length of satisfying assignment, so unless $\mathbf{P} = \mathbf{NP}$ this proof system is not automatizable.

Definition 11 *A proof system f is* weakly automatizable *if there exists a proof system g : g is automatizable and g p-simulates f*

Theorem 3 ([Pud03]) *A proof system is weakly automatizable $\Leftrightarrow$ its canonic* **NP***-pair is p-separable.*

If canonic pair of proof system f is separable, let's take function $h \in FP$ which separates canonical pair of f: $h(SAT^*) = 1$ and $h(REF_f) = 0$. Let's define proof system g:

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

g p-simulates f by the function $x \to (f(x), |x|)$ In the other way, if g p-simulates f then g simulates f, then, as we proved in section 2, $(SAT^*, REF_f) \leq_m^{PP} (SAT^*, REF_g)$ But canonical pair of g is p-separable, so the canonical pair of f is also p-separable.

References

[Bey06] Olaf Beyersdorff. Disjoint NP-pairs from propositional proof systems. In *In Proc. 3rd Conference on Theory and Applications of Models of Computation*, pages 236–247. Springer-Verlag, 2006.

[CR79] Stephen A. Cook and Robert A. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44:36–50, 1979.

[Pud03] Pavel Pudlak. On reducibility and symmetry of disjoint np-pairs, 2003.

[Raz95] Alexander A. Razborov. On provably disjoint np-pairs. Technical report, Electronic Colloquium on Computational Complexity, 1995.

[SGSZ04] Samik Sengupta, Christian Glasser, Alan L. Selman, and Liyu Zhang. Canonical disjoint np-pairs of propositional proof systems. In *In Proc. 30th International Symposium on the Mathematical Foundations of Computer Science*, pages 399–409, 2004.