Representable Disjoint NP-pairs

Olaf Beyersdorff

Institut für Informatik

Humboldt- Universität zu Berlin

Germany

Outline of the talk

- disjoint NP-pairs
- propositional proof systems and bounded arithmetic
- disjoint NP-pairs corresponding to proof systems

Disjoint NP-pairs

(A, B) is a disjoint NP-pair (DNPP), if $A, B \in$ **NP** and $A \cap B = \emptyset$.

Reductions between DNPP

Let (A, B) and (C, D) be DNPP.

1. $(A, B) \leq_p (C, D)$, if there exists $f \in$ **FP** such that $f(A) \subseteq C$ and $f(B) \subseteq D$.
2. $(A, B) \leq_s (C, D)$, if there exists $f \in$ **FP** such that $f^{-1}(C) = A$ and $f^{-1}(D) = B$.

Simple properties

(A,B) is called p-separable if there exists $C \in$**P** with $A \subseteq C$ and $B \cap C = \emptyset$.

Fact: If $(A, B) \leq_p (C, D)$ and (C, D) is p-separable then also (A, B) is p-separable.

Problem: Does there exist a polynomially inseparable DNPP?

Yes, if **P** $\neq$ **NP** $\cap$ **coNP**.

Problem: Do there exist pairs that are $\leq_p$- or $\leq_s$-complete for the class of all DNPP?

Simple properties

Fact: For every (A, B) there exists (A', B') such that $(A, B) \equiv_p (A', B')$ and A', B' are **NP**-complete.

Proof: $(A', B') = (A \times \mathrm{SAT}, B \times \mathrm{SAT})$

Problem: Are $\leq_p$ and $\leq_s$ different?

Proposition: **P** $\neq$ **NP** iff there are DNPP (A, B) and (C, D), such that A, B, C, D, $\overline{A \cup B}$ and $\overline{C \cup D}$ are infinite and $(A, B) \leq_p (C, D)$, but $(A, B) \not\leq_s (C, D)$.

Examples

1. a nontrivial p-separable pair

$CC_0 = \{(G, k) \mid G$ contains a clique of size $k\}$

$CC_1 = \{(G, k) \mid G$ can be colored by $k - 1$ colors $\}$

(CC_0, CC_1) is p-separable (Lovász [1979])

2. a pair from cryptography

$RSA_0 = \{(n, e, y, i) \mid \quad (n, e)$ is a valid RSA key, $\exists x\ x^e \equiv y \bmod n$
and the i-th bit of x is 0$\}$

$RSA_1 = \{(n, e, y, i) \mid \quad \ldots$ is 1 $\}$

If RSA is secure then (RSA_0, RSA_1) is not p-separable.

Propositional proof systems

A propositional proof system is a polynomial time computable function P with $\mathrm{rng}(P) =$TAUT.

A string π with $f(\pi) = \varphi$ is called a P-proof of φ.

Motivation: proofs can be easily checked

Examples: truth table method, Resolution, Frege-Systems

Propositional proof systems

A proof system P is simulated by a proof system S ($P \leq S$) if S-proofs are at most polynomially longer than P-proofs.

P is optimal if P simulates all proof systems.

Open problem: Do optimal proof systems exist?

Proof systems and bounded arithmetic

Let L be the language of arithmetic using the symbols

$$0,\ S,\ +,\ *,\ \leq\ \ldots$$

Σ_1^b-formulas are formulas in prenex normal form with only bounded $\exists$-quantifiers, i.e. $(\exists x \leq t(y))\psi(x,y)$.

Σ_1^b-formulas describe NP-sets.

Π_1^b-formulas: $(\forall x \leq t(y))\psi(x,y)$ $\Rightarrow$ coNP-sets

Representable disjoint NP-pairs

A Σ_1^b-formula φ is a representation of an NP-set A

if for all natural numbers a

$$\mathcal{N} \models \varphi(a) \iff a \in A.$$

A DNPP (A, B) is representable in T if there are Σ_1^b-formulas φ and ψ representing A and B such that

$$T \vdash (\forall x)(\neg\varphi(x) \lor \neg\psi(x)).$$

DNPP from proof systems

To a proof system P we associate a canonical DNPP $(Ref(P), SAT^*)$:

$$\begin{aligned} Ref(P) &= \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\} \\ SAT^* &= \{(\varphi, 1^m) \mid \neg\varphi \in SAT\} \end{aligned}$$

Proposition: If P and S are proof systems with $P \leq S$ then $(Ref(P), SAT^*) \leq_p (Ref(S), SAT^*)$.

Proof: $(\varphi, 1^m) \mapsto (\varphi, 1^{p(m)})$ where p is the polynomial from $P \leq S$.

Proposition: There are non-equivalent proof systems with the same canonical pair.

A second pair from a proof system

Let P be a proof system.

$$U_1(P) = \{(\varphi, \psi, 1^m) \mid \varphi, \psi \text{ are propositional formulas without common variables, } \neg\varphi \in SAT,\ P \vdash_{\leq m} \varphi \vee \psi\}$$

$$U_2 = \{(\varphi, \psi, 1^m) \mid \varphi, \psi \text{ are propositional formulas without common variables, } \neg\psi \in SAT\}.$$

Complete NP-pairs

Let (T, P) be a pair.

$DNPP(T) = \{(A, B) \mid (A, B)$ is representable in $T\}$

Theorem: 1. $DNPP(T)$ is closed under $\leq_p$-reductions. [Razborov 94]

2. $(Ref(P), SAT^*)$ is $\leq_p$-complete for $DNPP(T)$. [Razborov 94]

3. $(U_1(P), U_2)$ is $\leq_s$-complete for $DNPP(T)$.

Proof: 1: code polynomial time computations in T

2+3: representability: use $T \vdash Con(P)$

hardness: use the simulation of T by P

Implications

Proposition [Razborov 94]: If S is an optimal proof system then $(Ref(S), SAT^*)$ is $\leq_p$-complete for the class of all DNPP.

Proof: Let (A, B) be a DNPP.

Choose a theory T such that (A, B) is representable in T.

Let P be the proof system corresponding to T.

Then $(A, B) \leq_p (Ref(P), SAT^*)$.

S optimal $\Rightarrow P \leq S \Rightarrow (Ref(P), SAT^*) \leq_p (Ref(S), SAT^*)$

Implications

Proposition: If P is an optimal proof system then $(U_1(P), U_2)$ is $\leq_s$-complete for the class of all DNPP.

Proposition [Glaßer, Selman, Sengupta 04]: There exists a $\leq_p$-complete pair iff there exists a $\leq_s$-complete pair.

Open Problems

- Does $(U_1(P), U_2) \equiv_s (Ref(P), SAT^*)$ hold?
- Does the existence of $\leq_s$-complete pairs imply the existence of optimal proof systems?
- Find combinatorial characterizations of $(Ref(P), SAT^*)$ or $(U_1(P), U_2)$.