Disjoint NP-Pairs from Propositional Proof Systems

Olaf Beyersdorff

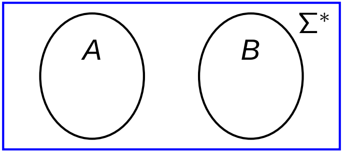
Institute of Computer Science
Humboldt-University Berlin
Germany

Theory and Applications of Models of Computation
2006

Disjoint NP-Pairs

Definition (Grollmann, Selman 88)

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



Example

Clique-Colouring pair (CC_0, CC_1)

$CC_0 = \{(G, k) \mid G \text{ contains a clique of size } k\}$
$CC_1 = \{(G, k) \mid G \text{ can be coloured with } k - 1 \text{ colours }\}$

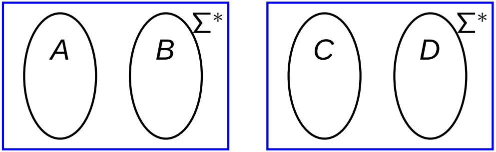
Applications and Relations to Other Areas

- security of public-key crypto systems
  [Grollmann, Selman 88], [Homer, Selman 92]
- characterization of properties of propositional proof systems
  [Bonet, Pitassi, Raz 00], [Pudlák 03]
- lower bounds to the length of propositional proofs
  [Razborov 96], [Pudlák 97], [Krajíček 04]
- complete problems for promise classes
  [Köbler et al. 03], [Glaßer et al. 04]

Reductions Between Pairs

Definition (Grollmann, Selman 88)

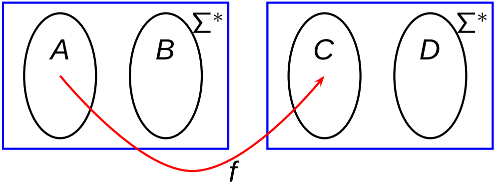
$(A, B) \leq_p (C, D) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.



Reductions Between Pairs

Definition (Grollmann, Selman 88)

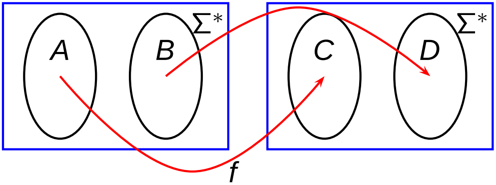
$(A, B) \leq_p (C, D) \stackrel{df}{\Longleftrightarrow}$ there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.



Reductions Between Pairs

Definition (Grollmann, Selman 88)

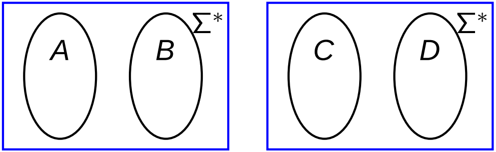
$(A, B) \leq_p (C, D) \overset{df}{\Longleftrightarrow}$ there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$.



A Strong Reduction Between Pairs

Definition (Köbler, Messner, Torán 03)

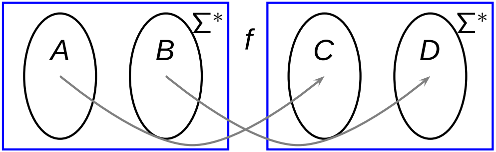
$(A, B) \leq_s (C, D) \stackrel{df}{\Longleftrightarrow}$ there exists a polynomial time computable function f such that $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



A Strong Reduction Between Pairs

Definition (Köbler, Messner, Torán 03)

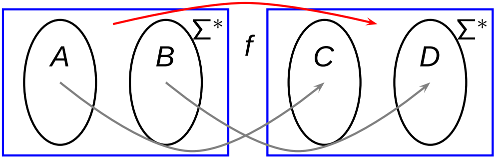
$(A, B) \leq_s (C, D) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



A Strong Reduction Between Pairs

Definition (Köbler, Messner, Torán 03)

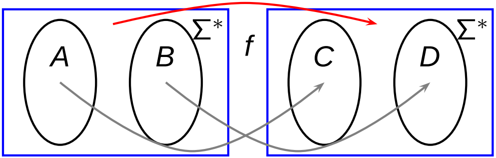
$(A, B) \leq_s (C, D) \overset{df}{\Longleftrightarrow}$ there exists a polynomial time computable function f such that $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



A Strong Reduction Between Pairs

Definition (Köbler, Messner, Torán 03)

$(A, B) \leq_s (C, D) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f : A \leq_m^p C$ und $f : B \leq_m^p D$.



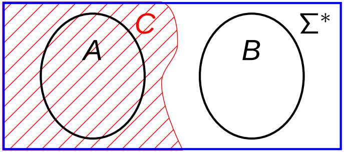
Theorem (Glaßer, Selman, Sengupta 04)

The reduction $\leq_s$ is a proper refinement of $\leq_p$ if and only if P $\neq$ NP.

P-Separable Pairs

Definition (Grollmann, Selman 88)

(A,B) is p-separable, if there exists a set $C \in$ P such that $A \subseteq C$ and $B \cap C = \emptyset$.



Theorem (Lovász 79)

(CC_0, CC_1) is p-separable.

Theorem (Grollmann, Selman 88)

The p-separable pairs form the minimal $\leq_p$-degree in the lattice of disjoint NP-pairs.

Problem

Do there exist p-inseparable DNPP?

Answer

Yes, if $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$.

Candidates

- cryptographic pairs [Grollmann, Selman 88]
- pairs from propositional proof systems [Krajíček, Pudlák 98]

Problem (Razborov 94)

Do there exist NP-Pairs which are complete for the class of all DNPP?

Propositional Proof Systems

Definition (Cook, Reckhow 79)

- A propositional proof system is a polynomial time computable function P with $rng(P) = TAUT$.
- A string π with $P(\pi) = \varphi$ is called a P-proof of φ.
- $P \vdash_{\leq m} \varphi \overset{df}{\iff} \varphi$ has a P-proof of size $\leq m$.

Motivation

Proofs can be easily checked.

Examples

truth-table method, resolution, Frege systems

The Extended Frege System *EF*

Extended Frege *EF*

- axiom schemes: $\varphi \to \varphi, \quad \varphi \to \varphi \lor \psi, \quad \ldots$
- rules: $\dfrac{\varphi \quad \varphi \to \psi}{\psi}$ (modus ponens)
- abbreviations for complex formulas: $p \leftrightarrow \varphi$

Extensions of *EF*

Let Φ be a polynomial time computable set of tautologies.

- $EF \cup \Phi$: Φ as new axioms
- $EF + \Phi$: Φ as axiom schemes

Simulations Between Proof Systems

Definition (Cook, Reckhow 79)

A proof system Q simulates a proof system P ($P \leq Q$), if Q-proofs are at most polynomially longer than P-proofs.

Theorem (Krajíček, Pudlák 89)

For all proof systems P we have: $P \leq EF + RFN(P)$.

Reflection principle:
$RFN(P) = (\forall\pi)(\forall\varphi)Prf_P(\pi,\varphi) \rightarrow Taut(\varphi)$

Canonical NP-Pairs

Definition (Razborov 94)

To a proof system P we associate a canonical pair:

$$\begin{aligned} Ref(P) &= \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\} \\ Sat^* &= \{(\varphi, 1^m) \mid \neg\varphi \text{ is satisfiable}\} \end{aligned}$$

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 $P \leq S$. □

Canonical NP-Pairs

Definition (Razborov 94)

To a proof system P we associate a canonical pair:

$$\begin{aligned} Ref(P) &= \{(\varphi, 1^m) \mid P \vdash_{\leq m} \varphi\} \\ Sat^* &= \{(\varphi, 1^m) \mid \neg\varphi \text{ is satisfiable}\} \end{aligned}$$

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 $P \leq S$. □

The converse does not hold.

Theorem

Let $\Phi \subset TAUT$ be a sparse polynomial time set. Then $(Ref(EF), Sat^*) \equiv_p (Ref(EF \cup \Phi), Sat^*)$.

Proof.

- EF has efficient deduction: for all finite $\Phi_0 \subset TAUT$

  $$EF \cup \Phi_0 \vdash_{\leq m} \psi \quad \text{implies} \quad EF \vdash_{m^{O(1)}} (\bigwedge_{\varphi \in \Phi_0} \varphi) \to \psi$$

  with a fixed polynomial p.
- reduce the canonical pair of $EF \cup \Phi$ to the canonical pair of EF by

  $$(\psi, 1^m) \mapsto ((\bigwedge_{\varphi \in \Phi \cap \Sigma^{\leq m}} \varphi) \to \psi, 1^{m^{O(1)}})$$

  for a suitable polynomial q.

Representations of NP-Sets

Definition

A representation of an NP-set A is a sequence of prop. formulas

$$\varphi_n(\bar{x}, \bar{y}) \quad |\bar{x}| = n$$

such that

- there exists a polynomial time algorithm which on input 1^n constructs $\varphi_n(\bar{x}, \bar{y})$
- for all $a \in \{0, 1\}^n$

$$a \in A \iff \varphi_n(\bar{a}, \bar{y}) \text{ is satisfiable.}$$

Representable Disjoint NP-Pairs

Definition

A DNPP (A, B) is **representable in P** if there are representations

$$\varphi_n(\bar{x}, \bar{y}) \quad \text{of } A \quad \text{and}$$
$$\psi_n(\bar{x}, \bar{z}) \quad \text{of } B$$

such that $P \vdash_* \neg\varphi_n(\bar{x}, \bar{y}) \vee \neg\psi_n(\bar{x}, \bar{z})$.

$\mathrm{DNPP}(P) = \{(A, B) \mid (A, B) \text{ is representable in } P\}$

Proposition

The representability of a pair depends on the choice of the representations for A and B.

Normal Proof Systems

Definition

We call a proof system P normal if

- P is closed under modus ponens, i.e.

  $$P \vdash_{\leq n} \varphi \text{ and } P \vdash_{\leq m} \varphi \to \psi \implies P \vdash_{\leq p(n+m)} \psi \ .$$

  for some polynomial p.
- P is closed under substitutions by constants, i.e.

  $$P \vdash_{\leq n} \varphi(\bar{x}, \bar{y}) \implies P \vdash_{\leq q(n)} \varphi(\bar{a}, \bar{y})$$

  for some polynomial q.

The Complexity Class DNPP(P)

Theorem

For every normal proof system P we have:

- DNPP(P) *is closed under* $\leq_p$ *for* $P \geq$ *Resolution.*
- $(Ref(P), Sat^*)$ *is* $\leq_p$*-hard for* DNPP(P)*.*
- *If P has reflection, then* $(Ref(P), Sat^*)$ *is* $\leq_p$*-complete for* DNPP(P)*.*

DNPP(P) Under the Strong $\leq_s$-Reduction

A second pair:

$$
\begin{aligned}
U_1(P) &= \{(\varphi, \psi, 1^m) \mid \varphi, \psi \text{ do not share variables,} \\
&\qquad P \vdash_{\leq m} \varphi \vee \psi \text{ and } \neg\varphi \in SAT\} \\
U_2(P) &= \{(\varphi, \psi, 1^m) \mid \ldots \neg\psi \in SAT\}.
\end{aligned}
$$

Theorem

For normal proof systems P we have:

- *$(U_1(P), U_2(P))$ is $\leq_s$-hard for* DNPP(P).
- *If P has reflection, then $(U_1(P), U_2(P))$ is $\leq_s$-complete for* DNPP(P).

Different Scenarios for DNPP(P)

proof system P	Res, CP	$EF + \Phi$	$EF \cup \Phi$
$(Ref(P), Sat^*)$	$\leq_p$-hard	$\leq_p$-complete	not $\leq_p$-hard*
$(U_1(P), U_2(P))$	$\leq_s$-hard	$\leq_s$-complete	
$(I_1(P), I_2(P))$	p-separable	$\leq_s$-complete	
closed under	modus ponens, substitutions		mod. pon.

* unless $(Ref(EF), Sat^*)$ is a $\leq_p$-complete pair

Summary

- For every propositional proof system P we define a complexity class DNPP(P) of disjoint NP-pairs.
- Canonical pairs associated with the proof system P serve as hard or complete pairs for DNPP(P).
- Properties of the class DNPP(P) depend on closure properties of the underlying proof system P.