Tuples of Disjoint NP-Sets

Olaf Beyersdorff

Institute of Computer Science
Humboldt-University Berlin
Germany

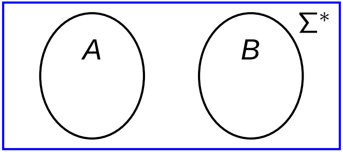
International Computer Science Symposium in Russia
2006

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Disjoint NP-Pairs

Definition (Grollmann, Selman 88)

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



Example

Clique-Colouring pair (CC_0, CC_1)

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

$CC_1 = \{(G, k) \mid G \text{ can be coloured with } k - 1 \text{ colours }\}$

Basic Definitions

Pairs and Tuples

P-Seperable Tuples

Reductions Between Tuples

Tuples and Proof Systems

Propositional Proof Systems

Representable Pairs

Tuples from Proof Systems

The Complexity Classes $\mathrm{DNPP}_k(P)$

Complete Tuples and Optimal Proof Systems

Summary

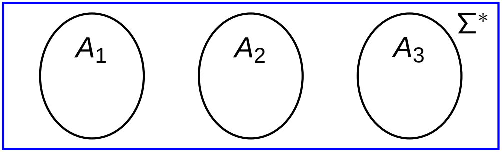
Applications and Relations to Other Areas

- 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]

Tuples instead of Pairs

Definition

$(A_1, \ldots, A_k)$ is a disjoint k-tuple of NP-sets if all components $A_1, \ldots, A_k$ are nonempty languages in NP which are pairwise disjoint.



Example

$(C_1, \ldots, C_k)$ where C_i contains all $i + 1$-colourable graphs with a clique of size i.

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $DNPP_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

P-Separable Pairs

Definition

A tuple $(A_1, \ldots, A_k)$ is p-separable if there exists a polynomial time computable function $f : \Sigma^* \to \{1, \ldots, k\}$ such that

$$a \in A_i \quad \Longrightarrow \quad f(a) = i$$

for $i = 1, \ldots, k$ and $a \in \Sigma^*$.

Example

$(C_1, \ldots, C_k)$ is p-separable (where C_i contains all $i + 1$-colourable graphs with a clique of size i.)

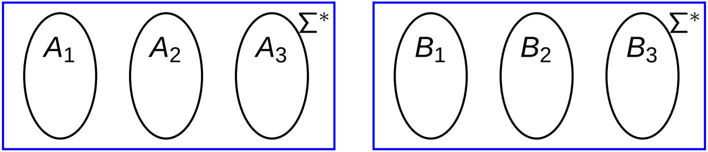
input:	graph G
output:	$max\{i \leq k \mid G \text{ contains a clique of size } i\}$

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $DNPP_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Reductions Between Tuples

Definition

$(A_1, \ldots, A_k) \leq_p (B_1, \ldots, B_k) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f(A_i) \subseteq B_i$ for $i = 1, \ldots, k$.

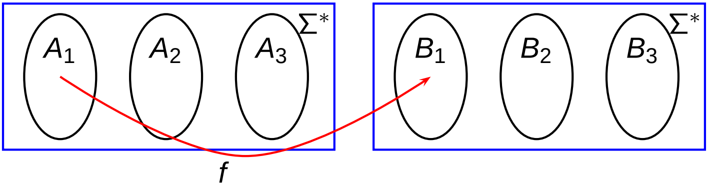


Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Reductions Between Tuples

Definition

$(A_1, \ldots, A_k) \leq_p (B_1, \ldots, B_k) \stackrel{df}{\Longleftrightarrow}$ there exists a polynomial time computable function f such that $f(A_i) \subseteq B_i$ for $i = 1, \ldots, k$.



Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Reductions Between Tuples

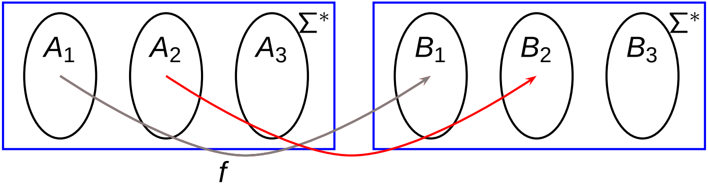
Tuples of Disjoint NP-Sets

Olaf Beyersdorff

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Definition

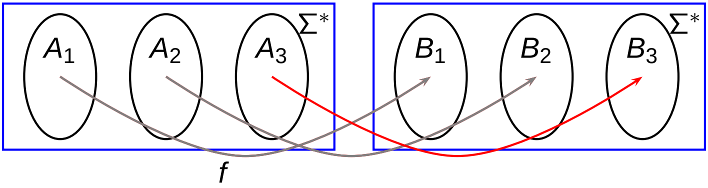
$(A_1, \dots, A_k) \leq_p (B_1, \dots, B_k) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f(A_i) \subseteq B_i$ for $i = 1, \dots, k$.



Reductions Between Tuples

Definition

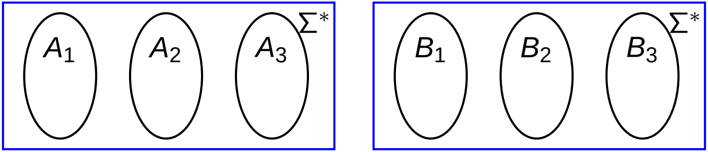
$(A_1, \ldots, A_k) \leq_p (B_1, \ldots, B_k) \overset{df}{\iff}$ there exists a polynomial time computable function f such that $f(A_i) \subseteq B_i$ for $i = 1, \ldots, k$.



A Stronger Reduction

Definition

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

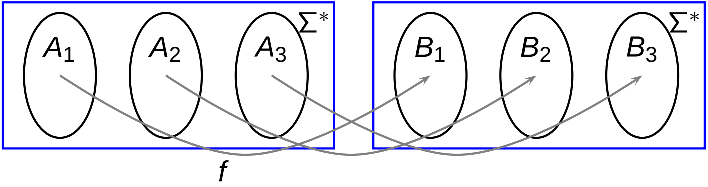


Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\text{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

A Stronger Reduction

Definition

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

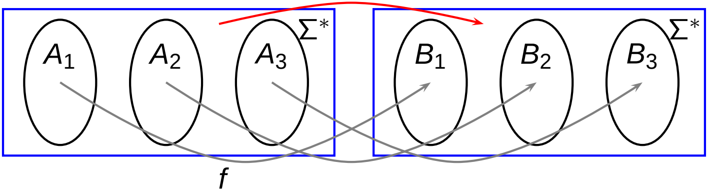


Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

A Stronger Reduction

Definition

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



The Two Reductions are Different.

Theorem

For all $k \geq 2$ the following holds:

- *All p-separable k-tuples are $\leq_p$-equivalent. They form the minimal $\leq_p$-degree of disjoint k-tuples of NP-sets.*
- *If $P \neq NP$, then there exist infinitely many $\leq_s$-degrees of p-separable disjoint k-tuples of NP-sets.*

The Two Reductions are Different.

Theorem

For all $k \geq 2$ the following holds:

- *All p-separable k-tuples are $\leq_p$-equivalent. They form the minimal $\leq_p$-degree of disjoint k-tuples of NP-sets.*
- *If $P \neq NP$, then there exist infinitely many $\leq_s$-degrees of p-separable disjoint k-tuples of NP-sets.*

Problem

Do there exist k-tuples which are complete for the class of all disjoint k-tuples of NP-sets?

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $DNPP_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

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

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $DNPP_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

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.

Definition

A proof system is optimal, if it simulates all other proof systems.

Problem (Krajíček, Pudlák 89)

Do there exist optimal proof systems?

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

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 disjoint k-tuple $(A_1, \ldots, A_k)$ of NP-sets is representable in a proof system P if there exist representations

$$\varphi_n^i(\bar{x}, \bar{y}^i) \quad \text{of } A_i \quad \text{for } i = 1, \ldots, k$$

such that

$$P \vdash_* \bigwedge_{1 \le i < j \le k} \neg\varphi_n^i(\bar{x}, \bar{y}^i) \vee \neg\varphi_n^j(\bar{x}, \bar{y}^j) \ .$$

$\mathrm{DNPP}_k(P)$ contains all disjoint k-tuples of NP-sets which are representable in P.

Proposition

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

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Tuples from Proof Systems

Definition

To a proof system P we associate a k-tuple $(U_1(P), \ldots, U_k(P))$, where $U_i(P)$ contains tuples $(\varphi_1, \ldots, \varphi_k, 1^m)$ such that

- φ_j and φ_l do not share variables for all $1 \leq j < l \leq k$,
- φ_i is satisfiable, and
- $P \vdash_{\leq m} \bigwedge_{1 \leq j < l \leq k} \neg\varphi_j \vee \neg\varphi_l$.

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

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)

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Theorem

For every normal proof system P and every number $k \geq 2$ we have:

- $\mathrm{DNPP}_k(P)$ *is closed under* $\leq_p$ *for* $P \geq$ *Resolution.*
- $(U_1(P), \ldots, U_k(P))$ *is* $\leq_s$*-hard for* $\mathrm{DNPP}_k(P)$.
- *If* P *has reflection, then* $(U_1(P), \ldots, U_k(P))$ *is* $\leq_s$*-complete for* $\mathrm{DNPP}(P)$.

Complete Tuples

Theorem

The following conditions are equivalent:

1. *For all $k \geq 2$ there exist $\leq_s$-complete disjoint k-tuples of* NP*-sets.*
2. *For all $k \geq 2$ there exist $\leq_p$-complete disjoint k-tuples of* NP*-sets.*
3. *There exist $\leq_p$-complete disjoint* NP*-pairs.*
4. *There exists $k \geq 2$ such that there exist $\leq_p$-complete disjoint k-tuples of* NP*-sets.*
5. *There exists a proof system P such that for all $k \geq 2$ all disjoint k-tuples of* NP*-sets are representable in P.*
6. *There exists a proof system P such that all disjoint* NP*-pairs are representable in P.*

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Optimal Proof Systems and Complete Tuples

Theorem

The following conditions are equivalent:

1. *There exists an optimal propositional proof system.*
2. *There exists a proof system that proves the disjointness of all disjoint k-tuples of* NP*-sets with respect to all representations.*
3. *There exists a proof system that proves the disjointness of all disjoint* NP*-pairs with respect to all representations.*

Corollary

If optimal proof systems exist, then there exist $\leq_s$-complete disjoint k-tuples of NP*-sets for all $k \geq 2$.*

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\text{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary

Summary

- For every propositional proof system P we define complexity classes $\mathrm{DNPP}_k(P)$ of disjoint k-tuples of NP-sets.
- Canonical tuples associated with the proof system P serve as hard or complete pairs for $\mathrm{DNPP}_k(P)$.
- If complete k-tuples exist for some $k \geq 2$, then complete k-tuples exist for all $k \geq 2$.
- Optimal proof systems imply complete k-tuples for all $k \geq 2$.

Basic Definitions
Pairs and Tuples
P-Seperable Tuples
Reductions Between Tuples
Tuples and Proof Systems
Propositional Proof Systems
Representable Pairs
Tuples from Proof Systems
The Complexity Classes $\mathrm{DNPP}_k(P)$
Complete Tuples and Optimal Proof Systems
Summary