Electronic Colloquium on Computational Complexity, Report No. 123 (2005)

Tuples of Disjoint NP-Sets

Olaf Beyersdorff

Institut für Informatik, Humboldt-Universität zu Berlin, 10099 Berlin, Germany
beyersdo@informatik.hu-berlin.de

Abstract. Disjoint NP-pairs are a well studied complexity theoretic concept with important applications in cryptography and propositional proof complexity. In this paper we introduce a natural generalization of the notion of disjoint NP-pairs to disjoint k-tuples of NP-sets for $k \geq 2$. We define subclasses of the class of all disjoint k-tuples of NP-sets. These subclasses are associated with a propositional proof system and posses complete tuples which are defined from the proof system.
In our main result we show that complete disjoint NP-pairs exist if and only if complete disjoint k-tuples of NP-sets exist for all $k \geq 2$. Further, this is equivalent to the existence of a propositional proof system in which the disjointness of all k-tuples is shortly provable. We also show that a strengthening of this conditions characterizes the existence of optimal proof systems.

1 Introduction

During the last years the theory of disjoint NP-pairs has been intensively studied. This interest stems mainly from the applications of disjoint NP-pairs in the field of cryptography [GS88,KP98] and propositional proof complexity [Pud03,Kra04]. In this paper we investigate a natural generalization of disjoint NP-pairs: instead of pairs we consider k-tuples of pairwise disjoint NP-sets. Concepts such as reductions and separators are smoothly generalized from pairs to k-tuples.

One of the major open problems in the field of disjoint NP-pairs is the question, posed by Razborov [Raz94], whether there exist disjoint NP-pairs that are complete for the class of all pairs under suitable reductions. Glaßer et al. [GSSZ04] gave a characterization in terms of uniform enumerations of disjoint NP-pairs and also proved that the answer to the problem does not depend on the reductions used, i.e. there are reductions for pairs which vary in strength but are equivalent with respect to the existence of complete pairs.

The close relation between propositional proof systems and disjoint NP-pairs provides a partial answer to the question of the existence of complete pairs. Namely, the existence of optimal propositional proof systems is a sufficient condition for the existence of complete disjoint NP-pairs. This result is already implicitly contained in [Raz94]. However, Glaßer et al. [GSS04] construct an oracle relative to which there exist complete pairs but optimal proof systems do not exist. Hence, the problems on the existence of optimal proof systems and of complete disjoint NP-pairs appear to be of different strength.

Our main contribution in this paper is the characterization of these two problems in terms of disjoint k-tuples of NP-sets. In particular we address the question whether there exist complete disjoint k-tuples under different reductions. Considering this problem it is easy to see that the existence of complete disjoint k-tuples implies the existence of complete disjoint l-tuples for $l \leq k$: the first l components of a complete k-tuple are complete for all l-tuples. Conversely, it is a priori not clear how to construct a complete k-tuple from a complete l-tuple for $l < k$. Therefore it might be tempting to conjecture that the existence of complete k-tuples forms

ISSN 1433-8092

a hierarchy of assumptions of increasing strength for greater k. However, we show that this does not happen: there exist complete disjoint NP-pairs if and only if there exist complete disjoint k-tuples of NP-sets for all $k \geq 2$, and this is even true under reductions of different strength. Further, we prove that this is equivalent to the existence of a propositional proof system in which the disjointness of all k-tuples with respect to suitable propositional representations of these tuples is provable with short proofs. We also characterize the existence of optimal proof systems with a similar but apparently stronger condition.

We achieve this by extending the connection between proof systems and NP-pairs to k-tuples. In particular we define representations for disjoint k-tuples of NP-sets. This can be done on a propositional level with sequences of tautologies but also with first-order formulas in arithmetic theories. To any propositional proof system P we associate a subclass $\mathsf{DNPP}_k(P)$ of the class of all disjoint k-tuples of NP-sets. This subclass contains those k-tuples for which the disjointness is provable with short P-proofs. We show that the classes $\mathsf{DNPP}_k(P)$ posses complete tuples which are defined from the proof system P. Somewhat surprisingly, under suitable conditions on P these non-uniform classes $\mathsf{DNPP}_k(P)$ equal their uniform versions which are defined via arithmetic representations. This enables us to further characterize the existence of complete disjoint k-tuples by conditions on arithmetic theories.

The paper is organized as follows. In Sect. 2 we recall some relevant definitions concerning propositional proof systems and disjoint NP-pairs. We also give a very brief description of the correspondence between propositional proof systems and arithmetic theories. This reference to bounded arithmetic, however, only plays a role in Sect. 6 where we analyse arithmetic representations. The rest of the paper and in particular the main results in Sect. 7 are fully presented on the propositional level.

In Sect. 3 we define the basic concepts such as reductions and separators that we need for the investigation of disjoint k-tuples of NP-sets.

In Sect. 4 we define propositional representations for k-tuples and introduce the complexity classes $\mathsf{DNPP}_k(P)$ of all disjoint k-tuples of NP-sets that are representable in the system P. We show that these classes are closed under our reductions for k-tuples.

In Sect. 5 we proceed the investigation of the classes $\mathsf{DNPP}(P)$ by defining k-tuples from propositional proof systems which serve as hard languages for $\mathsf{DNPP}_k(P)$. In particular we generalize the interpolation pair from [Pud03] and demonstrate that even these generalized variants still capture the feasible interpolation property of the proof system.

In Sect. 6 we define first-order variants of the propositional representations from Sect. 4. We utilize the correspondence between proof systems and bounded arithmetic to show that a disjoint k-tuple of NP-sets is representable in P if and only if it is representable in the arithmetic theory associated with P. This equivalence allows easy proofs for the representability of the canonical k-tuples associated with P, thereby improving the hardness results for $\mathsf{DNPP}_k(P)$ from Sect. 5 to completeness results for proof systems corresponding to arithmetic theories.

The main results on the connections between complete NP-pairs, complete k-tuples and optimal proof systems follow in Sect. 7.

2 Preliminaries

2.1 Propositional Proof Systems

Propositional proof systems were defined in a very general way by Cook and Reckhow in [CR79] as polynomial time functions P which have as its range the set of all tautologies. A string π with $P(\pi) = \varphi$ is called a P-proof of the tautology φ.

By $P \vdash_{\leq m} \varphi$ we indicate that there is a P-proof of φ of length $\leq m$. If Φ is a set of propositional formulas we write $P \vdash_* \Phi$ if there is a polynomial p such that $P \vdash_{\leq p(|\varphi|)} \varphi$ for all $\varphi \in \Phi$. If $\Phi = \{\varphi_n \mid n \geq 0\}$ is a sequence of formulas we also write $P \vdash_* \varphi_n$ instead of $P \vdash_* \Phi$.

Proof systems are compared according to their strength by simulations introduced in [CR79] and [KP89]. Given two proof systems P and S we say that S *simulates* P (denoted by $P \leq S$) if there exists a polynomial p such that for all tautologies φ and P-proofs π of φ there is a S-proof π' of φ with $|\pi'| \leq p(|\pi|)$. If such a proof π' can even be computed from π in polynomial time we say that S *p-simulates* P and denote this by $P \leq_p S$. A proof system is called *(p-)optimal* if it (p-)simulates all proof systems. Whether or not optimal proof systems exist is an open problem posed by Krajíček and Pudlák [KP89].

In [Bey05] we investigated several natural properties of propositional proof system. We will just define those which we need in this paper. We say that a propositional proof system P is *closed under substitutions by constants* if there exists a polynomial q such that $P \vdash_{\leq n} \varphi(\bar{x}, \bar{y})$ implies $P \vdash_{\leq q(n)} \varphi(\bar{a}, \bar{y})$ for all formulas $\varphi(\bar{x}, \bar{y})$ and constants $\bar{a} \in \{0,1\}^{|\bar{x}|}$. We call P *efficiently closed under substitutions by constants* if we can transform any P-proof of a formula $\varphi(\bar{x}, \bar{y})$ in polynomial time to a P-proof of $\varphi(\bar{a}, \bar{y})$. A system P is *closed under disjunctions* if there is a polynomial q such that $P \vdash_{\leq m} \varphi$ implies $P \vdash_{\leq q(m+|\psi|)} \varphi \vee \psi$ for arbitrary formulas ψ. Similarly, we say that a proof system P is *closed under conjunctions* if there is a polynomial q such that $P \vdash_{\leq m} \varphi \wedge \psi$ implies $P \vdash_{\leq q(m)} \varphi$ and $P \vdash_{\leq q(m)} \psi$, and likewise $P \vdash_{\leq m} \varphi$ and $P \vdash_{\leq n} \psi$ imply $P \vdash_{\leq q(m+n)} \varphi \wedge \psi$ for all formulas φ and ψ. As with closure under substitutions by constants we also consider efficient versions of closure under disjunctions and conjunctions.

Another important property of weak proof systems is the *feasible interpolation property* defined in [Kra97]. A proof system P has feasible interpolation if there exists a polynomial time procedure that takes as input a formula $\varphi(\bar{x}, \bar{y}) \vee \psi(\bar{x}, \bar{z})$ and a P-proof π of $\varphi(\bar{x}, \bar{y}) \vee \psi(\bar{x}, \bar{z})$ and outputs a Boolean circuit $C(\bar{x})$ such that for every propositional assignment $\bar{a}$ the following holds:

- If $C(\bar{a})$ outputs 0, then $\varphi(\bar{a}, \bar{y})$ is a tautology.
- If $C(\bar{a})$ outputs 1, then $\psi(\bar{a}, \bar{z})$ is a tautology.

2.2 Propositional Proof Systems and Arithmetic Theories

In Sect. 6 we will use the correspondence of propositional proof systems to theories of bounded arithmetic. Here we will just briefly introduce some notation and otherwise refer to the monograph [Kra95]. To explain the correspondence we have to translate first-order arithmetic formulas into propositional formulas. An arithmetic formula in prenex normal form with only bounded existential quantifiers is called a Σ^b_1-formula. These formulas describe NP-predicates. Likewise, Π^b_1-formulas only have bounded universal quantifiers and describe coNP-predicates. A formula φ is Δ^b_1 with respect to an arithmetic theory T if φ is in T equivalent both to a Σ^b_1- and a Π^b_1-formula. A Σ^b_1- or Π^b_1-formula $\varphi(x)$ is translated into a sequence $\|\varphi(x)\|^n$ of propositional formulas containing one formula per input length for the number x. We use $\|\varphi(x)\|$ to denote the set $\{\|\varphi(x)\|^n \mid n \geq 1\}$.

The *reflection principle* for a propositional proof system P states a strong form of the consistency of the proof system P. It is formalized by the $\forall\Pi^b_1$-formula

$$\mathrm{RFN}(P) = (\forall\pi)(\forall\varphi)\mathrm{Prf}_P(\pi, \varphi) \rightarrow \mathrm{Taut}(\varphi)$$

where Prf_P and Taut are suitable arithmetic formulas describing P-proofs and tautologies, respectively. A proof system P has the *reflection property* if $P \vdash_* \|\mathrm{RFN}(P)\|^n$ holds.

In [KP90] a general correspondence between arithmetic theories T and propositional proof systems P is introduced. Pairs (T, P) from this correspondence possess in particular the following two properties:

1. For all $\varphi(x) \in \Pi_1^b$ with $T \vdash (\forall x)\varphi(x)$ we have $P \vdash_* \|\varphi(x)\|^n$.
2. P is the strongest system for which T proves the correctness, i.e. $T \vdash \mathrm{RFN}(P)$ and if $T \vdash \mathrm{RFN}(Q)$ for a proof system Q, then $Q \leq P$.

We call a proof system P *regular* if there exists an arithmetic theory T such that the properties 1 and 2 are fulfilled for (T, P).

We can strengthen these axioms by giving them a constructive formulation. In this way we define strongly regular proof systems. A propositional proof system P is *strongly regular* if there exists an arithmetic theory T such that the following two properties are fulfilled for (T, P):

3. Let $\varphi(x)$ be a Π_1^b-formula such that $T \vdash (\forall x)\varphi(x)$. Then there exists a polynomial time computable function f that on input 1^n outputs a P-proof of $\|\varphi(x)\|^n$.
4. $T \vdash \mathrm{RFN}(P)$ and if $T \vdash \mathrm{RFN}(Q)$ for some proof system Q, then $Q \leq_p P$.

Probably the most important example of a strongly regular proof system is the extended Frege system EF that corresponds to the theory S_2^1. This correspondence was established in [Bus86] and [KP90]. We refer to the monograph [Kra95] for detailed background information.

2.3 Disjoint NP-Pairs

A pair (A, B) is called a *disjoint* NP*-pair* if $A, B \in \mathsf{NP}$ and $A \cap B = \emptyset$. The pair (A, B) is called *p-separable* if there exists a polynomial time computable set C such that $A \subseteq C$ and $B \cap C = \emptyset$. Formulated differently, a disjoint NP-pair (A, B) is p-separable if there exists a polynomial time computable function f that outputs 1 on inputs from A and 0 on inputs from B and answers arbitrarily otherwise.

Grollmann and Selman [GS88] defined the following reduction between disjoint NP-pairs (A, B) and (C, D): $((A, B) \leq_p (C, D))$ if there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$. This variant of a many-one reduction for pairs was strengthened by Köbler et al. [KMT03] to: $(A, B) \leq_s (C, D)$ if there exists a function $f \in \mathsf{FP}$ such that $f^{-1}(C) = A$ and $f^{-1}(D) = B$.

The link between disjoint NP-pairs and propositional proof systems was established by Razborov [Raz94], who associated a disjoint NP-pair $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ with a proof system P with

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

$(\mathrm{Ref}(P), \mathrm{SAT}^*)$ is called the *canonical pair* of P.

Pudlák [Pud03] introduced an *interpolation pair* $(I_1(P), I_2(P))$ for a proof system P:

$$\begin{aligned} I_1(P) &= \{(\varphi, \psi, \pi) \mid P(\pi) = \varphi \vee \psi,\ \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset \text{ and } \neg\varphi \in \mathrm{SAT}\} \\ I_2(P) &= \{(\varphi, \psi, \pi) \mid P(\pi) = \varphi \vee \psi,\ \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset \text{ and } \neg\psi \in \mathrm{SAT}\} \end{aligned}$$

where $\mathrm{Var}(\varphi)$ denotes the set of propositional variables occurring in φ. This pair is p-separable if and only if the proof system P has the feasible interpolation property [Pud03].

In [Bey04] we analysed a variant $(U_1(P), U_2)$ of the interpolation pair:

$$\begin{aligned} U_1(P) &= \{(\varphi, \psi, 1^m) \mid \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset,\ \neg\varphi \in \mathrm{SAT} \text{ and } P \vdash_{\leq m} \varphi \vee \psi\} \\ U_2 &= \{(\varphi, \psi, 1^m) \mid \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset \text{ and } \neg\psi \in \mathrm{SAT}\} \ . \end{aligned}$$

In the following we will refer to this pair as the U-pair.

More information on the connection between disjoint NP-pairs and propositional proof systems can be found in [Pud03,Bey04,Bey05,GSZ05].

3 Basic Definitions and Properties

Definition 1. *Let $k \geq 2$ be a number. A tupel $(A_1, \dots, A_k)$ is a disjoint k-tuple of NP-sets if all components $A_1, \dots, A_k$ are nonempty languages in NP which are pairwise disjoint.*

Next we define reductions for k-tuples. We will only consider variants of many-one reductions which are easily obtained from the reductions $\leq_p$ and $\leq_s$ for pairs. As there is no danger of confusion we will use the same symbols $\leq_p$ and $\leq_s$ for the generalized versions.

Definition 2. *Let $(A_1, \dots, A_k)$ and $(B_1, \dots, B_k)$ be disjoint k-tuples of NP-sets. We say that $(A_1, \dots, A_k)$ is* polynomially reducible *to $(B_1, \dots, B_k)$, denoted by*

$$(A_1, \dots, A_k) \leq_p (B_1, \dots, B_k) \ ,$$

if there exists a polynomial time computable function f such that $f(A_i) \subseteq B_i$ for all $i = 1, \dots, k$.

The tuple $(A_1, \dots, A_k)$ is strongly reducible *to $(B_1, \dots, B_k)$, denoted by*

$$(A_1, \dots, A_k) \leq_s (B_1, \dots, B_k) \ ,$$

if there exists a polynomial time computable function f such that f is a $\leq_p$-reduction from $(A_1, \dots, A_k)$ to $(B_1, \dots, B_k)$ and additionally $f(\overline{A_1 \cup \dots \cup A_k}) \subseteq \overline{B_1 \cup \dots \cup B_k}$.

We define from $\leq_p$ and $\leq_s$ equivalence relations $\equiv_p$ and $\equiv_s$ and call their equivalence classes degrees*.*

Following common terminology we call a disjoint k-tuple of NP-sets *$\leq_p$-complete* if every disjoint k-tuple of NP-sets $\leq_p$-reduces to it. Similarly, we speak of $\leq_s$-complete tuples.

We observe that the complexity of the components of a k-tuple inside a $\leq_p$-degree can change while this is not possible for $\leq_s$-degrees.

Proposition 3.

1. *For every disjoint k-tuple $(A_1, \dots, A_k)$ of NP-sets there exists a disjoint k-tuple $(B_1, \dots, B_k)$ of NP-sets such that*

$$(A_1, \dots, A_k) \equiv_p (B_1, \dots, B_k)$$

and $B_1, \dots, B_k$ are NP-complete.

2. *If f is a $\leq_s$-reduction between the disjoint k-tuples $(A_1, \dots, A_k)$ and $(B_1, \dots, B_k)$, then f is a many-one reduction from A_i to B_i for every $i = 1, \dots, k$.*

Proof. For part 1 choose $B_i = A_i \times \mathrm{SAT}$. Part 2 follows immediately from the definition of $\leq_s$. □

We generalize the notion of a separator of a disjoint NP-pair in the following way:

Definition 4. *A function $f : \{0,1\}^* \to \{1, \dots, k\}$ is a* separator *for a disjoint k-tuple $(A_1, \dots, A_k)$ of NP-sets if for all $a \in \{0,1\}^*$*

$$a \in A_i \quad \Longrightarrow \quad f(a) = i \quad \text{for } i = 1, \dots, k \ .$$

For inputs from the complement $\overline{A_1 \cup \dots \cup A_k}$ the function f may answer arbitrarily.

If $(A_1, \dots, A_k)$ is a disjoint k-tuple of NP-sets that has a polynomial time computable separator we call the tuple p-separable*, otherwise* p-inseparable*.*

Whether there exist p-inseparable disjoint k-tuples of NP-sets is certainly a hard problem that cannot be answered with our current techniques. At least we can show that this question is not harder than the previously studied question whether there exist p-inseparable disjoint NP-pairs.

Theorem 5. *The following are equivalent:*

1. *For all numbers $k \geq 2$ there exist p-inseparable disjoint k-tuples of NP-sets.*
2. *There exists a number $k \geq 2$ such that there exist p-inseparable disjoint k-tuples of NP-sets.*
3. *There exist p-inseparable disjoint NP-pairs.*

Proof. Trivially, 1 implies 2. We will show $2 \Rightarrow 3$ and $3 \Rightarrow 1$.

In order to prove $2 \Rightarrow 3$ let us assume that all disjoint NP-pairs are p-separable. Let $k \geq 2$ be some number and $(A_1, \dots, A_k)$ be a disjoint k-tuple of NP-sets. By assumption we have separators $f_{i,j}$ for all disjoint NP-pairs (A_i, A_j) with $i, j \in \{1, \dots, k\}$, $i \neq j$. We devise a separator for $(A_1, \dots, A_k)$ as follows: at input a we first evaluate all functions $f_{i,j}(a)$. If there exists a number i such that we received 1 at all evaluations $f_{i,j}(a)$ for $j \in \{1, \dots, k\} \setminus \{i\}$, then we output this number i. If no such i exists, then we know that a is outside $A_1 \cup \dots \cup A_k$, and we can answer arbitrarily. If on the other hand $a \in A_i$, then we always get $f_{i,j}(a) = 1$ for $j \in \{1, \dots, k\} \setminus \{i\}$. As only one such i can exist we produce the correct answer.

To show the remaining implication $3 \Rightarrow 1$ let us assume that the disjoint NP-pair (A, B) is p-inseparable. Without loss of generality we may assume that $\overline{A \cup B}$ is infinite because otherwise the pair (A, B) can be trivially modified to a p-inseparable pair that meets this condition. For a given number k let $a_3, \dots, a_k$ be distinct elements from $\overline{A \cup B}$. Then $(A, B, \{a_3\}, \dots, \{a_k\})$ is a p-inseparable disjoint k-tuple of NP-sets. □

The difference between $\leq_p$ and $\leq_s$ as expressed in Proposition 3 allows us to separate the reductions $\leq_p$ and $\leq_s$ on the domain of all p-separable disjoint k-tuples of NP-sets:

Theorem 6. *For all numbers $k \geq 2$ the following holds:*

1. *All p-separable disjoint k-tuples of NP-sets are $\leq_p$-equivalent. They form the minimal $\leq_p$-degree of disjoint k-tuples of NP-sets.*
2. *If $\mathsf{P} \neq \mathsf{NP}$, then there exist infinitely many $\leq_s$-degrees of p-separable disjoint k-tuples of NP-sets.*
3. *$\mathsf{P} \neq \mathsf{NP}$ if and only if there exist disjoint k-tuples of NP-sets $(A_1, \dots, A_k)$ and $(B_1, \dots, B_k)$ with nonempty complements $\overline{A_1 \cup \dots \cup A_k}$ and $\overline{B_1 \cup \dots \cup B_k}$ such that $(A_1, \dots, A_k) \leq_p (B_1, \dots, B_k)$, but $(A_1, \dots, A_k) \not\leq_s (B_1, \dots, B_k)$.*

Proof. For part 1 let $(A_1, \dots, A_k)$ be a p-separable disjoint k-tuple with separator f and let $(B_1, \dots, B_k)$ be an arbitrary disjoint k-tuple of NP-sets. Fix arbitrary elements $b_i \in B_i$ for $i = 1, \dots, k$. To compute a reduction from $(A_1, \dots, A_k)$ to $(B_1, \dots, B_k)$ we map a to $b_{f(a)}$.

If on the other hand the k-tuple $(B_1, \dots, B_k)$ is p-separable via the function f, and g computes a $\leq_p$-reduction from $(A_1, \dots, A_k)$ to $(B_1, \dots, B_k)$, then $f \circ g$ separates $(A_1, \dots, A_k)$.

We now turn to the proof of part 2. By a theorem of Ladner [Lad75] there exist infinitely many different $\leq_m^p$-degrees of NP-sets assuming $\mathsf{P} \neq \mathsf{NP}$. Therefore Ladner's theorem together with the following claim imply part 2 of the proposition.

Claim. Let $(A_1, \dots, A_k)$ and $(B_1, \dots, B_k)$ be p-separable disjoint k-tuple of NP-sets . Let further $\overline{B_1 \cup \dots \cup B_k} \neq \emptyset$. Then $(A_1, \dots, A_k) \leq_s (B_1, \dots, B_k)$ if and only if $A_i \leq_m^p B_i$ for all $i = 1, \dots, k$.

The first direction is clear from the definition of $\leq_s$. For the reverse implication let $f, g \in \mathsf{FP}$ be separators of $(A_1, \dots, A_k)$ and $(B_1, \dots, B_k)$, respectively. Let further $h_i : A_i \leq_m^p B_i$ compute the many-one reductions for $i = 1, \dots, k$ and let x_0 be a fixed element from $\overline{B_1 \cup \dots \cup B_k}$. Then the polynomial time computable function

$$x \mapsto \begin{cases} h_{f(x)}(x) & \text{if } g(h_{f(x)}(x)) = f(x) \\ x_0 & \text{otherwise} \end{cases}$$

is a $\leq_s$-reduction from $(A_1, \dots, A_k)$ to $(B_1, \dots, B_k)$.

Part 3 is a consequence of parts 1 and 2. □

4 Representable Disjoint k-Tuples of NP-Sets

In [Bey05] we defined the notion of propositional representations for NP-sets as follows:

Definition 7. *Let A be a* NP*-set over the alphabet $\{0, 1\}$. A* propositional representation *for A is a sequence of propositional formulas $\varphi_n(\bar{x}, \bar{y})$ with the following properties:*

1. *$\varphi_n(\bar{x}, \bar{y})$ has propositional variables $\bar{x}$ and $\bar{y}$ such that $\bar{x}$ is a vector of n propositional variables.*
2. *There exists a polynomial time algorithm that on input 1^n outputs $\varphi_n(\bar{x}, \bar{y})$.*
3. *Let $\bar{a} \in \{0, 1\}^n$. Then $\bar{a} \in A$ if and only if $\varphi_n(\bar{a}, \bar{y})$ is satisfiable.*

Once we have propositional descriptions of NP-sets we can now represent disjoint k-tuples of NP-sets in propositional proof systems.

Definition 8. *Let P be a propositional proof system. A disjoint k-tuple $(A_1, \dots, A_k)$ of* NP*-sets is* representable in P *if there exist propositional representations $\varphi_n^i(\bar{x}, \bar{y}^i)$ of A_i for $i = 1, \dots, k$ such that for each $1 \leq i < j \leq k$ the formulas $\varphi_n^i(\bar{x}, \bar{y}^i)$ and $\varphi_n^j(\bar{x}, \bar{y}^j)$ have only the variables $\bar{x}$ in common, and further*

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

By $\mathsf{DNPP}_k(P)$ we denote the class of all disjoint k-tuples of NP*-sets which are representable in P.*

For $\mathsf{DNPP}_2(P)$ we will also write $\mathsf{DNPP}(P)$. In [Bey05] we have analysed this class for some standard proof systems. As the classes $\mathsf{DNPP}_k(P)$ provide natural generalizations of $\mathsf{DNPP}(P)$ we have chosen the same notation for the classes of k-tuples.

We will now show that the class $\mathsf{DNPP}_k(P)$ is closed under reductions.

Proposition 9. *Let P be a proof system that is closed under conjunctions and disjunctions and that simulates resolution. Then for all numbers $k \geq 2$ the class $\mathsf{DNPP}_k(P)$ is closed under $\leq_p$.*

Proof. Let $(A_1, \dots, A_k)$ and $(B_1, \dots, B_k)$ be disjoint k-tuples of NP-sets such that f is a $\leq_p$-reduction from $(A_1, \dots, A_k)$ to $(B_1, \dots, B_k)$. Let further P be a propositional proof system satisfying the above conditions and let $(B_1, \dots, B_k) \in \mathsf{DNPP}_k(P)$.

In [Bey05] we proved that for proof systems P that simulate resolution and are closed under disjunctions the class $\mathsf{DNPP}(P)$ is closed under $\leq_p$. Closure of P under conjunctions implies that for all $1 \leq i < j \leq k$ each of the disjoint NP-pairs (B_i, B_j) is contained in $\mathsf{DNPP}(P)$. As f is also a $\leq_p$-reduction between the disjoint NP-pairs (A_i, A_j) and (B_i, B_j) we infer that all pairs (A_i, A_j) are in $\mathsf{DNPP}(P)$. Inspecting the proof of the relevant result from [Bey05] we see that P proves the disjointness of these pairs with respect to the representations

$$A'_i = \{x \mid x \in A_i \text{ and } f(x) \in B_i\} \ .$$

In particular, the representation of A_i is always the same when proving the disjointness of A_i and A_j for different j. Therefore we can combine these proofs of disjointness by conjunctions and obtain a P-proof of a suitable propositional description of

$$\bigwedge_{1 \le i < j \le k} A'_i \cap A'_j = \emptyset \ .$$

This shows $(A_1, \dots, A_k) \in \mathsf{DNPP}_k(P)$. □

5 Disjoint k-Tuples of NP-Sets from Propositional Proof Systems

In this section we want to associate tuples of NP-sets with proof systems. It is not clear how the canonical pair could be modified for k-tuples but the interpolation pair as well as the U-pair can be stretched to more than two components. We start with the generalization of the U-pair.

For a propositional proof system P we define a k-tuple $(U_1(P), \dots, U_k(P))$ with the components

$$\begin{aligned} U_i(P) = \{(\varphi_1, \dots, \varphi_k, 1^m) \mid\ & \mathrm{Var}(\varphi_j) \cap \mathrm{Var}(\varphi_l) = \emptyset \text{ for all } 1 \le j < l \le k, \\ & \neg\varphi_i \in \mathrm{SAT} \text{ and } P \vdash_{\le m} \bigwedge_{1 \le j < l \le k} \varphi_j \vee \varphi_l\} \end{aligned}$$

for $i = 1, \dots, k$. It is clear that all components $U_i(P)$ are in NP. To see their pairwise disjointness assume that $(\varphi_1, \dots, \varphi_k, 1^m) \in U_i(P)$ and let $j \in \{1, \dots, k\} \setminus \{i\}$. Because we have a P-proof of $\bigwedge_{1 \le j < l \le k} \varphi_j \vee \varphi_l$, this formula is a tautology. Therefore in particular $\varphi_i \vee \varphi_j$ is a tautology and because φ_i and φ_j have no common variables either of these formulas must be tautological. As in the definition of $U_i(P)$ this is excluded for φ_i the formula φ_j is a tautology. But this implies $(\varphi_1, \dots, \varphi_k, 1^m) \notin U_j(P)$.

Similarly, we can expand the interpolation pair to a k-tuple $(I_1(P), \dots, I_k(P))$ be setting

$$\begin{aligned} I_i(P) = \{(\varphi_1, \dots, \varphi_k, \pi) \mid\ & \mathrm{Var}(\varphi_j) \cap \mathrm{Var}(\varphi_l) = \emptyset \text{ for all } 1 \le j < l \le k, \\ & \neg\varphi_i \in \mathrm{SAT} \text{ and } P(\pi) = \bigwedge_{1 \le j < l \le k} \varphi_j \vee \varphi_l\} \end{aligned}$$

for $i = 1, \dots, k$. The same argument as above shows that $(I_1(P), \dots, I_k(P))$ is indeed a disjoint k-tuple of NP-sets. Further, this tuple still captures the feasible interpolation property of the proof system P as the next theorem shows.

Theorem 10. *Let P be a propositional proof system that is efficiently closed under substitutions by constants and conjunctions. Then $(I_1(P), \dots, I_k(P))$ is p-separable if and only if P has the feasible interpolation property.*

Proof. For the first direction assume that $(I_1(P), \dots, I_k(P))$ is separated by the polynomial time computable function f, i.e.

$$(\varphi_1, \dots, \varphi_k, \pi) \in I_i(P) \quad \Longrightarrow \quad f(\varphi, \dots, \varphi_k, \pi) = i$$

for $i = 1, \ldots, k$. To show feasible interpolation for P let $\varphi(\bar{x}, \bar{y}) \vee \psi(\bar{x}, \bar{z})$ be given together with a P-proof π of this disjunction. In order to generate the interpolation circuit C we first compute at input $\bar{a}$ a P-proof π' of $\varphi(\bar{a}, \bar{y}) \vee \psi(\bar{a}, \bar{z})$ from π which is hardwired into C. Then we form the k-tuple

$$(\varphi_1, \ldots, \varphi_k) = (\varphi(\bar{a}, \bar{y}), \psi(\bar{a}, \bar{z}), \top, \ldots, \top)$$

where $\top$ is some simple tautology. We use the assumption that P is efficiently closed under conjunctions to generate a P-proof π'' of $\bigwedge_{1 \leq i < j \leq k} \varphi_i \vee \varphi_j$ from π'. Finally, we evaluate $f(\varphi, \psi, \top, \ldots, \top, \pi'')$. We use this answer to decide the input $\bar{a}$, i.e. on output 1 we also answer with 1 and on output 2 we answer with 0.

For the converse direction assume that P has feasible interpolation. Let f be a polynomial time computable function that on input $(\varphi(\bar{x}, \bar{y}) \vee \psi(\bar{x}, \bar{z}), \pi)$ computes an interpolation circuit for $\varphi(\bar{x}, \bar{y}) \vee \psi(\bar{x}, \bar{z})$. We separate the tuple $(I_1(P), \ldots, I_k(P))$ by the following algorithm: at input $(\varphi_1, \ldots, \varphi_k, \pi)$ we test whether the formulas φ_i have no common variables and π is indeed a P-proof of

$$\bigwedge_{1 \leq i < j \leq k} \varphi_i \vee \varphi_j \quad .$$

If this is the case we can use the assumption that P is efficiently closed under conjunctions to compute P-proofs $\pi_{i,j}$ of $\varphi_i \vee \varphi_j$ for all $i, j \in \{1, \ldots, k\}$, $i \neq j$. We then test whether there exists an $i \in \{1, \ldots, k\}$ such that for all $j \in \{1, \ldots, k\} \setminus \{i\}$ the function f on input $(\varphi_i \vee \varphi_j, \pi_{i,j})$ outputs a circuit without free inputs that evaluates to 1. If such i exists, then we output this i.

It is clear that this algorithm runs in polynomial time. To see the correctness of the algorithm assume that $(\varphi_1, \ldots, \varphi_k, \pi) \in I_i(P)$. Then $\neg\varphi_i$ is satisfiable and hence φ_i is not tautological. Therefore the circuit $f(\varphi_i \vee \varphi_j, \pi_{i,j})$ always evaluates to 1. As this can happen for at most one i we give the correct answer. □

The next theorem shows that for all proof systems P we can find hard k-tuples for the classes $\mathsf{DNPP}_k(P)$.

Theorem 11. *Let P be a proof system that is closed under substitutions by constants. Then for every $k \geq 2$ the k-tuple $(U_1(P), \ldots, U_k(P))$ is $\leq_s$-hard for $\mathsf{DNPP}_k(P)$.*

Proof. Let $(A_1, \ldots, A_k)$ be a disjoint k-tuple of NP-sets and let $\varphi^i_n(\bar{x}, \bar{y}^i)$ be propositional representations of A_i for $i = 1, \ldots, k$ such that

$$P \ \vdash_* \bigwedge_{1 \leq i < j \leq k} \neg\varphi^i_n(\bar{x}, \bar{y}^i) \vee \neg\varphi^j_n(\bar{x}, \bar{y}^j) \quad .$$

We claim that there exists a polynomial p such that

$$a \ \mapsto \ (\neg\varphi^1_{|a|}(\bar{a}, \bar{y}^1), \ldots, \neg\varphi^k_{|a|}(\bar{a}, \bar{y}^k), 1^{p(|a|)})$$

realizes a $\leq_s$-reduction from $(A_1, \ldots, A_k)$ to $(U_1(P), \ldots, U_k(P))$.

To verify the claim let a be an element from A_i of length n. Because $\varphi^i_n(\bar{x}, \bar{y}^i)$ represents A_i the formula $\varphi^i_n(\bar{a}, \bar{y})$ is satisfiable. As P is closed under substitutions by constants we have

$$P \ \vdash_{\leq p(n)} \bigwedge_{1 \leq i < j \leq k} \neg\varphi^i_n(\bar{a}, \bar{y}^i) \vee \neg\varphi^j_n(\bar{a}, \bar{y}^j)$$

for the appropriate polynomial p. Therefore

$$(\neg\varphi^1_n(\bar{a}, \bar{y}^1), \ldots, \neg\varphi^k_n(\bar{a}, \bar{y}^k), 1^{p(|a|)}) \in U_i(P) \quad .$$

If the element a comes from the complement of $A_1 \cup \cdots \cup A_k$, then none of the formulas $\varphi_i(\bar{a}, \bar{y}^i)$, $i = 1, \ldots, k$ is satisfiable and hence a is mapped to a tuple from the complement of $U_1(P) \cup \cdots \cup U_k(P)$. □

For technical reasons we now introduce a modification $(V_1(P),\dots,V_k(P))$ of the U-tuple for which we will also show the hardness for $\mathsf{DNPP}_k(P)$. Instead of k-tuples the components $V_r(P)$ now consist of sequences of $(k-1)k$ formulas together with an unary coded parameter m. For a propositional proof system P we define the k-tuple $(V_1(P),\dots,V_k(P))$ as:

$$\begin{aligned} V_r(P) = \{((\varphi_{i,j} \mid 1 \le i,j \le k, i \ne j), 1^m) \mid \\ \mathrm{Var}(\varphi_{i,j}) \cap \mathrm{Var}(\varphi_{l,n}) = \emptyset \text{ for all } i,j,l,n \in \{1,\dots,k\}, i \ne l, \\ \neg\varphi_{r,i} \in \mathrm{SAT} \text{ for } i \in \{1,\dots,k\} \setminus \{r\} \text{ and } P \vdash_{\le m} \bigwedge_{i=1}^{k} \bigwedge_{j=i+1}^{k} \varphi_{i,j} \vee \varphi_{j,i}\} \end{aligned}$$

for $i = r,\dots,k$. Let us verify that we have defined a disjoint k-tuple of NP-sets. It is clear that all components $V_r(P)$ are in NP. To prove their disjointness assume that the tuple $((\varphi_{i,j} \mid 1 \le i,j \le k, i \ne j), 1^m)$ is contained both in $V_r(P)$ and $V_s(P)$ for $r,s \in \{1,\dots,k\}$, $r < s$. The definition of V_r guarantees that

$$\bigwedge_{i=1}^{k} \bigwedge_{j=i+1}^{k} \varphi_{i,j} \vee \varphi_{j,i}$$

is a tautology. Therefore in particular $\varphi_{r,s} \vee \varphi_{s,r}$ is a tautology and because $\varphi_{r,s}$ and $\varphi_{s,r}$ have no common variables either of these formulas must be tautological. In the definition of $V_r(P)$ this is excluded for $\varphi_{r,s}$ and in the definition of $V_s(P)$ this is excluded for $\varphi_{s,r}$ which gives a contradiction.

As this V-tuple is a generalization of the previously defined U-tuple we can reduce the U-tuple to the V-tuple, thereby showing the hardness result for the V-tuple:

Proposition 12. *Let P be a proof system that is closed under substitutions by constants. Then for every $k \ge 2$ the pair $(V_1(P),\dots,V_k(P))$ is $\le_s$-hard for $\mathsf{DNPP}_k(P)$.*

Proof. By Theorem 11 we know that $(U_1(P),\dots,U_k(P))$ is $\le_s$-hard for $\mathsf{DNPP}_k(P)$ for proof systems P that are closed under substitutions by constants. Therefore, to prove the result it is sufficient to $\le_s$-reduce $(U_1(P),\dots,U_k(P))$ to $(V_1(P),\dots,V_k(P))$. The reduction is given by

$$f : (\varphi_1,\dots,\varphi_k,1^m) \ \mapsto \ (\underbrace{\varphi_1,\dots,\varphi_1}_{k-1},\underbrace{\varphi_2,\dots,\varphi_2}_{k-1},\dots,\underbrace{\varphi_k,\dots,\varphi_k}_{k-1},1^m) \ .$$

To prove the correctness of the reduction it is enough to observe that for each $i = 1\dots,k$ we have $(\varphi_1,\dots,\varphi_k,1^m) \in U_i(P)$ if and only if $f(\varphi_1,\dots,\varphi_k,1^m) \in V_i(P)$. This is true because the conditions on the satisfiability and the disjointness of the variables of the formulas are trivially preserved, and the formulas

$$\bigwedge_{1 \le j < l \le k} \varphi_j \vee \varphi_l = \bigwedge_{j=1}^{k} \bigwedge_{l=j+1}^{k} \varphi_j \vee \varphi_l$$

which should be P-provable in size $\le m$ are equal. □

6 Arithmetic Representations

In [Raz94] and [Bey04] arithmetic representations of disjoint NP-pairs were investigated. These form a uniform first-order counterpart to the propositional representations introduced in the previous section. We now generalize the notion of arithmetic representations to disjoint k-tuples of NP-sets.

Definition 13. *A Σ^b_1-formula φ is an* arithmetic representation *of an* NP*-set A if for all natural numbers a*

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

A disjoint k-tuple $(A_1, \dots, A_k)$ of NP*-sets is* representable *in an arithmetic theory T if there are Σ^b_1-formulas $\varphi_1(x), \dots, \varphi_k(x)$ representing $A_1, \dots, A_k$ such that*

$$T \ \vdash \ (\forall x) \bigwedge_{1 \le i < j \le k} \neg\varphi_i(x) \vee \neg\varphi_j(x) \ .$$

By $\mathsf{DNPP}_k(T)$ *we denote the class of all disjoint k-tuples of* NP*-sets that are representable in T.*

We now show that the uniformly defined classes $\mathsf{DNPP}_k(T)$ coincide with the non-uniformly defined classes $\mathsf{DNPP}_k(P)$ for regular proof systems P corresponding to the theory T.

Theorem 14. *Let $P \ge EF$ be a regular proof system which is closed under substitutions by constants and conjunctions and let $T \supseteq S^1_2$ be a theory corresponding to T. Then we have* $\mathsf{DNPP}_k(P) = \mathsf{DNPP}_k(T)$ *for all $k \ge 2$.*

Proof. We start with the proof of the inclusion $\mathsf{DNPP}_k(P) \subseteq \mathsf{DNPP}_k(T)$. We will first show this inclusion for $k = 2$ and then infer from it the inclusion for higher k.

Let (A, B) be a disjoint NP-pair in $\mathsf{DNPP}(P)$ and let $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ be propositional representations for A and B, respectively, such that

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

Because P is closed under substitutions by constants there exists a polynomial p such that for all $\bar{a} \in \{0,1\}^n$

$$P \ \vdash_{\le p(n)} \ \neg\varphi_n(\bar{a}, \bar{y}) \vee \neg\psi_n(\bar{a}, \bar{z}) \ . \tag{1}$$

Assume further that the polynomial time computable functions f and g generate the formulas φ_n and ψ_n, i.e.

$$f(1^n) = \varphi_n(\bar{x}, \bar{y}) \quad \text{and} \quad g(1^n) = \psi_n(\bar{x}, \bar{z}) \ .$$

Consider the first-order formula

$$\theta(\alpha) = \mathit{Assign}(\alpha, \bar{x}) \wedge \neg\mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y})) \ .$$

As this notation is not completely precise let us explain how to understand the definition of θ. At input $1^{|\alpha|}$ the function f outputs the formula $\varphi_{|\alpha|}(\bar{x}, \bar{y})$. In θ the computation of f is expressed by a Σ^b_1-formula. Then we use again the free variable α of θ to obtain a propositional assignment to the propositional variables $\bar{x}$. The formula $\neg\mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y}))$ then is a Σ^b_1-formulation for the unsatisfiability of $\varphi_{|\alpha|}(\bar{x}, \bar{y})$, where the variables $\bar{x}$ are substituted by the constants specified in α and only the variables $\bar{y}$ remain free.

The above explanation shows that θ is a Σ^b_1-formula. Moreover, it is clear that θ represents A. We augment this representation by a first-order description of (1), arriving at

$$\varphi(\alpha) = \theta(\alpha) \wedge (\exists \pi)|\pi| \le p(|\alpha|) \wedge \mathrm{Prf}_P(\pi, \neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})) \ .$$

Let us argue that this is indeed an arithmetic representation of A. We already verified that $\theta \in \Sigma^b_1$. As Prf_P has a Δ^b_1-definition in S^1_2 and $T \supseteq S^1_2$ also the second part can be given a Σ^b_1-formulation, and hence $\varphi \in \Sigma^b_1$.

Let $\bar{a} \in \{0,1\}^{|\alpha|}$ be the tupel of constants specified by the assignment α. Then θ expresses $\bar{a} \in A$. Because

$$\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})$$

equals the formula

$$\neg \varphi_{|\alpha|}(\bar{a}, \bar{y}) \vee \neg \psi_{|\alpha|}(\bar{a}, \bar{z})$$

which by assumption has a P-proof of length $\leq p(|\alpha|)$ also the second part of φ is fulfilled for $\bar{a} \in A$. Therefore φ represents A.

Similarly, we define a representation for B as

$$\begin{aligned}\psi(\alpha) = {} & \mathit{Assign}(\alpha, \bar{x}) \wedge \neg \mathrm{Taut}(\neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})) \wedge \\ & (\exists \pi) |\pi| \leq p(|\alpha|) \wedge \mathrm{Prf}_P(\pi, \neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})) \ .\end{aligned}$$

It remains to verify that T can prove the disjointness of A and B with respect to the above representations. For this assume that M is a model of T and $\alpha \in M$ is an element such that $M \models \psi(\alpha)$. In particular this means that there exists an element $\pi \in M$ such that

$$M \models \mathrm{Prf}_P(\pi, \neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})) \ .$$

Because $T \vdash \mathrm{RFN}(P)$ this implies

$$M \models \mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y}) \vee \neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})) \ .$$

The theory $T \supseteq S^1_2$ is strong enough to prove Tarski's truth conditions for the propositional satisfaction relation $\models$ (cf. [Kra95] Lemma 9.3.9). In particular T proves

$$(\forall \varphi, \psi, \alpha) \mathit{Assign}(\alpha, \varphi \vee \psi) \wedge (\alpha \models \varphi \vee \psi) \rightarrow (\alpha \models \varphi) \vee (\alpha \models \psi) \ .$$

Therefore T proves that a tautological disjunction of formulas without common variables contains at least one tautological disjunct, and hence we get

$$M \models \mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y})) \vee \mathrm{Taut}(\neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z})) \ .$$

But because $M \models \psi(\alpha)$ we also have

$$M \models \neg \mathrm{Taut}(\neg g(1^{|\alpha|})(\alpha(\bar{x}), \bar{z}))$$

implying

$$M \models \mathrm{Taut}(\neg f(1^{|\alpha|})(\alpha(\bar{x}), \bar{y})) \ .$$

and therefore $M \not\models \varphi(\alpha)$. Hence we have shown $T \vdash (\forall x) \neg \varphi(x) \vee \neg \psi(x)$.

To show $\mathsf{DNPP}_k(P) \subseteq \mathsf{DNPP}_k(T)$ for $k > 2$ let $(A_1, \dots, A_k)$ be a disjoint k-tuple of NP-sets in $\mathsf{DNPP}_k(P)$ and let φ^i_n be propositional representations of the sets A_i for $i = 1, \dots, k$, such that

$$P \vdash_* \bigwedge_{1 \leq i < j \leq k} \neg \varphi^i_n \vee \neg \varphi^j_n \ . \tag{2}$$

Because P is closed under conjunctions this in particular means

$$P \vdash_* \neg \varphi^i_n \vee \neg \varphi^j_n$$

for all $1 \leq i < j \leq k$, i.e. all disjoint NP-pairs (A_i, A_j) are contained in $\mathsf{DNPP}(P)$. As we have already shown $\mathsf{DNPP}(P) \subseteq \mathsf{DNPP}(T)$ this implies that for all $1 \leq i < j \leq k$ we have $(A_i, A_j) \in \mathsf{DNPP}(T)$ where the disjointness of (A_i, A_j) is T-provable via arithmetic representations $\psi_i(x)$ for A_i depending only on the set A_i and the polynomial in (2). Hence we get

$$T \vdash (\forall x) \bigwedge_{1 \le i < j \le k} \neg\psi_i(x) \vee \neg\psi_j(x) \tag{3}$$

and therefore $(A_1, \dots, A_k) \in \mathsf{DNPP}_k(T)$

To prove the inclusion $\mathsf{DNPP}_k(T) \subseteq \mathsf{DNPP}_k(P)$ let $\psi_1(x), \dots, \psi_k(x)$ be arithmetic representations of $A_1, \dots, A_k$ such that (3) holds. Then the translations $\|\psi_i(x)\|^n$ of the arithmetic representations ψ_i provide propositional representations of A_i for $i = 1, \dots, k$. In these translations we choose the auxiliary variables disjoint. Because $\bigwedge_{1 \le i < j \le k} \neg\psi_i(x) \vee \neg\psi_j(x)$ is a Π_1^b-formula we get from (3)

$$P \vdash_* \| \bigwedge_{1 \le i < j \le k} \neg\psi_i(x) \vee \neg\psi_j(x) \|^n \ .$$

By definition of the translation $\|.\|$ this is equivalent to

$$P \vdash_* \bigwedge_{1 \le i < j \le k} \neg\|\psi_i(x)\|^n \vee \neg\|\psi_j(x)\|^n$$

and therefore $(A_1, \dots, A_k) \in \mathsf{DNPP}_k(P)$ □

At first sight Theorem 14 might come as a surprise as it states that the non-uniform and uniform concepts equal when representing disjoint k-tuples of NP-sets in regular proof systems. The uniform representations of k-tuples are translated via $\|.\|$ to non-uniform representations in a straightforward manner. For the transformation of propositional representations into first-order formulas it is, however, necessary to essentially change the representations of the components.

We now observe that all the k-tuples that we associated with a proof system P are representable in P if the system is regular.

Lemma 15. *Let P be a regular proof system. Then for all numbers $k \ge 2$ the k-tuples $(U_1(P), \dots, U_k(P))$, $(V_1(P), \dots, V_k(P))$ and $(I_1(P), \dots, I_k(P))$ are representable in P.*

Proof. Let P be regular and T be a theory associated with P. We show the representability of $(U_1(P), \dots, U_k(P))$, $(V_1(P), \dots, V_k(P))$ and $(I_1(P), \dots, I_k(P))$ in T.

As arithmetic representations for the components $U_i(P)$, $V_i(P)$ and $I_i(P)$ we choose straightforward first-order formalizations which use the formulas Taut and Prf_P. Using the reflection principle of P which is available in T we can devise T-proofs of the arithmetic formalizations of $U_i(P) \cap U_j(P) = \emptyset$, $V_i(P) \cap V_j(P) = \emptyset$ and $I_i(P) \cap I_j(P) = \emptyset$ for all $1 \le i < j \le k$. Combining these proofs we get the representability of $(U_1(P), \dots, U_k(P))$, $(V_1(P), \dots, V_k(P))$ and $(I_1(P), \dots, I_k(P))$ in T.

Because the inclusion $\mathsf{DNPP}_k(T) \subseteq \mathsf{DNPP}_k(P)$ in Theorem 14 follows alone from the regularity of P we infer that these tuples are also representable in the proof system P. □

Combining Theorem 11 and Lemma 15 we conclude:

Corollary 16. *Let P be a regular proof system that is closed under substitutions by constants. Then for every $k \ge 2$ the pair $(U_1(P), \dots, U_k(P))$ is $\le_s$-complete for $\mathsf{DNPP}_k(P)$.*

For strongly regular proof systems P we can additionally show the $\le_s$-completeness of the k-tuple $(I_1(P), \dots, I_k(P))$ for $\mathsf{DNPP}_k(P)$:

Theorem 17. *Let $P \geq EF$ be a strongly regular proof system that is efficiently closed under substitutions by constants. Then for all numbers $k \geq 2$ the tuples $(U_1(P), \dots, U_k(P))$ and $(I_1(P), \dots, I_k(P))$ are $\leq_s$-complete for $\mathsf{DNPP}_k(P)$. In particular we have $(U_1(P), \dots, U_k(P)) \equiv_s (I_1(P), \dots, I_k(P))$.*

Proof. The $\leq_s$-completeness of $(U_1(P), \dots, U_k(P))$ was already stated in Corollary 16.

As by Lemma 15 also $(I_1(P), \dots, I_k(P))$ is representable in P it remains to show that $(I_1(P), \dots, I_k(P))$ is $\leq_s$-hard for $\mathsf{DNPP}_k(P)$. For this let $(A_1, \dots, A_k)$ be a disjoint k-tuple of NP-sets that is representable in P. By Theorem 14 we know that $(A_1, \dots, A_k)$ is also representable in the theory T corresponding to P. Let $\varphi_i(x)$ be arithmetic representations of A_i for $i = 1, \dots, k$ such that

$$T \vdash (\forall x) \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \lor \neg\varphi_j(x) \enspace .$$

Because this is a $\forall \Pi_1^b$-formula and P is strongly regular there exists a polynomial time computable function f that on input 1^n produces a P-proof of

$$\| \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \lor \neg\varphi_j(x) \|^n \enspace .$$

Further, because by assumption P is efficiently closed under substitutions by constants we can use f to obtain a polynomial time computable function g that on input $\bar{a} \in \{0,1\}^n$ outputs a P-proof of

$$\| \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \lor \neg\varphi_j(x) \|^n (\bar{p}^x / \bar{a})$$

where the propositional variables $\bar{p}^x$ for x are substituted by the bits of a.

We claim that the $\leq_s$-reduction from $(A_1, \dots, A_k)$ to $(I_1(P), \dots, I_k(P))$ is given by

$$a \mapsto ((\|\neg\varphi_i(x)\|^{|a|}(\bar{p}^x/\bar{a}) \mid 1 \leq i \leq k), g(\bar{a}))$$

where the auxiliary variables of $\|\neg\varphi_i(x)\|^{|a|}$ are all chosen disjoint. Verifying the correctness of the reduction then proceeds as in the proof of Theorem 11. □

As a corollary we get from Proposition 9 and Theorem 17 for the extended Frege system EF:

Corollary 18. *For every number $k \geq 2$ and every disjoint k-tuple $(A_1, \dots, A_k)$ of NP-sets we have $(A_1, \dots, A_k) \in \mathsf{DNPP}_k(EF)$ if and only if $(A_1, \dots, A_k) \leq_s (U_1(EF), \dots, U_k(EF))$.*

Additionally, we have $(U_1(EF), \dots, U_k(EF)) \equiv_s (I_1(EF), \dots, I_k(EF))$.

The corollary is also true for all extensions $EF + \|\Phi\|$ of the extended Frege systems for polynomial time sets Φ of true Π_1^b-formulas.

The equivalence of the interpolation tuple and the U-tuple for strong systems as stated in Theorem 17 might come unexpected as the first idea for a reduction from the U-tuple to the I-tuple probably is to generate proofs for $\bigwedge_{1 \leq j < l \leq k} \varphi_j \lor \varphi_l$ at input $(\varphi_1, \dots, \varphi_k, 1^m)$. This, however, is not possible for extensions of EF, because a reduction from $(U_1(P), \dots, U_k(P))$ to $(I_1(P), \dots, I_k(P))$ of the form

$$(\varphi_1, \dots, \varphi_k, 1^m) \mapsto (\varphi_1, \dots, \varphi_k, \pi)$$

implies the automatizability of the system P. But it is known that automatizability fails for strong systems $P \geq EF$ under cryptographic assumptions [KP98,Pud03].

7 On Complete Disjoint k-Tuples of NP-Sets

In this section we will study the question whether there exist complete disjoint k-tuples of NP-sets under the reductions $\leq_p$ and $\leq_s$. We will not be able to answer this question but we will relate it to the previously studied questions whether there exist complete disjoint NP-pairs or optimal propositional proof systems. The following is the main theorem of this section:

Theorem 19. *The following conditions are equivalent:*

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

Proof. To show the equivalence of 1 to 7 we will prove the following implications: 1 $\Rightarrow$ 2 $\Rightarrow$ 3 $\Rightarrow$ 6 $\Rightarrow$ 1 and the equivalences 3 $\Leftrightarrow$ 4, 5 $\Leftrightarrow$ 6 and 6 $\Leftrightarrow$ 7.

As the implications 1 $\Rightarrow$ 2 $\Rightarrow$ 3 $\Rightarrow$ 4 and 5 $\Rightarrow$ 6 $\Rightarrow$ 7 are trivial it remains to prove 3 $\Rightarrow$ 6 $\Rightarrow$ 1, 4 $\Rightarrow$ 3, 6 $\Rightarrow$ 5 and 7 $\Rightarrow$ 6.

To prove the implication 3 $\Rightarrow$ 6 assume that (A, B) is a $\leq_p$-complete disjoint NP-pair. We choose some representations φ_n and ψ_n for A and B, respectively. Let P be a proof system such that (A, B) is representable in P, and P simulates resolution and is closed under conjunctions and disjunctions. For instance the proof system

$$EF + \{\neg\varphi_n \vee \neg\psi_n \mid n \geq 0\}$$

fulfills these conditions. Because (A, B) is representable in P and $\mathsf{DNPP}(P)$ is closed under $\leq_p$ by Proposition 9, it follows that all disjoint NP-pairs are representable in the system P.

Next we prove the implication 6 $\Rightarrow$ 1. Let P be a propositional proof system such that all disjoint NP-pairs are representable in P. We choose a proof system $Q \geq P$ that is closed under conjunctions and substitutions by constants. As Q simulates P also the class $\mathsf{DNPP}(Q)$ contains all disjoint NP-pairs. We claim that for all $k \geq 2$ the pair $(V_1(Q), \dots, V_k(Q))$ is $\leq_s$-complete for the class of all disjoint k-tuples of NP-sets. To verify the claim let $(A_1, \dots, A_k)$ be a disjoint k-tuple of NP-sets. In particular, for all $1 \leq i < j \leq k$ the pair (A_i, A_j) is a disjoint NP-pair. By assumption all these pairs are representable in Q. However, we might need different representations for the sets A_i to prove the disjointness of all these pairs. For example proving $A_1 \cap A_2 = \emptyset$ and $A_1 \cap A_3 = \emptyset$ might require two different propositional representations for A_1. For this reason we cannot simply reduce $(A_1, \dots, A_k)$ to $(U_1(P), \dots, U_k(P))$. But we can reduce $(A_1, \dots, A_k)$ to $(V_1(P), \dots, V_k(P))$ which was designed for this particular purpose.

For $1 \leq i < j \leq k$ let $\varphi_n^{i,j}(\bar{x}, \bar{y}^{i,j})$ and $\varphi_n^{j,i}(\bar{x}, \bar{y}^{j,i})$ be propositional representations of A_i and A_j, respectively, such that all tuples of variables $\bar{y}^{i,j}$ are chosen distinct and

$$Q \vdash_* \neg\varphi_n^{i,j}(\bar{x}, \bar{y}^{i,j}) \vee \neg\varphi_n^{j,i}(\bar{x}, \bar{y}^{j,i}) \enspace .$$

Because Q is closed under conjunctions we can combine all these proofs to obtain

$$Q \vdash_* \bigwedge_{i=1}^{k} \bigwedge_{j=i+1}^{k} \neg\varphi_n^{i,j}(\bar{x}, \bar{y}^{i,j}) \vee \neg\varphi_n^{j,i}(\bar{x}, \bar{y}^{j,i}) \enspace . \tag{4}$$

The reduction from $(A_1, \dots, A_k)$ to $(V_1(P), \dots, V_k(P))$ is given by

$$a \mapsto ((\neg\varphi_n^{i,j}(\bar{a}, \bar{y}^{i,j}) \mid 1 \leq i, j \leq k, i \neq j), 1^{p(m)})$$

for some appropriate polynomial p which comes from (4) and the closure of Q under substitutions by constants. To prove the correctness of the reduction let a be an element from A_r for some $r \in \{1, \dots, k\}$. As for all $j \in \{1, \dots, k\} \setminus \{r\}$ the sequences $\varphi_n^{r,j}$ are representations for A_r all formulas $\varphi_n^{r,j}(\bar{a}, \bar{y}^{r,j})$ are satisfiable. By substituting the bits $\bar{a}$ of a for the variables $\bar{x}$ we get from (4) polynomial size Q-proofs of

$$\bigwedge_{i=1}^{k} \bigwedge_{j=i+1}^{k} \neg\varphi_n^{i,j}(\bar{a}, \bar{y}^{i,j}) \vee \neg\varphi_n^{j,i}(\bar{a}, \bar{y}^{j,i}) \ .$$

This shows $((\neg\varphi_n^{i,j}(\bar{a}, \bar{y}^{i,j}) \mid 1 \leq i, j \leq k, i \neq j), 1^{p(m)}) \in V_r(Q)$.

If a is in the complement of $A_1 \cup \dots \cup A_k$, then none of the formulas $\varphi_n^{i,j}(\bar{a}, \bar{y}^{i,j})$ is satisfiable and hence a is mapped to a tuple from the complement of $V_1(P) \cup \dots \cup V_k(P)$.

We proceed with the proof of the implication 4 ⇒ 3. Assume that $(A_1, \dots, A_k)$ is a $\leq_p$-complete disjoint k-tuple of NP-sets. We claim that (A_1, A_2) is a $\leq_p$-complete disjoint NP-pair. To prove this let (B_1, B_2) be an arbitrary disjoint NP-pair. Without loss of generality we may assume that the complement of $B_1 \cup B_2$ contains at least $k - 2$ distinct elements $b_3, \dots, b_k$, because otherwise we can change from (B_1, B_2) to a $\leq_p$-equivalent pair with this property. Since $(A_1, \dots, A_k)$ is $\leq_p$-complete for all k-tuples there exists a reduction f from $(B_1, B_2, \{b_3\}, \dots, \{b_k\})$ to $(A_1, \dots, A_k)$. In particular f is then a reduction from (B_1, B_2) to (A_1, A_2).

Next we prove the implication 6 ⇒ 5. Let P be a proof system such that all disjoint NP-pairs are representable in P. We choose a regular proof system Q that simulates P and is closed under conjunctions, disjunctions and substitutions by constants, for example $Q = EF + \mathrm{RFN}(P)$ is such a system. Clearly, every disjoint NP-pair is also representable in Q. Going back to the proof of 6 ⇒ 1 we see that condition 6 implies that for all $k \geq 2$ the k-tuple $(V_1(Q), \dots, V_k(Q))$ is $\leq_s$-complete for the class of all disjoint k-tuples of NP-sets. By Lemma 15 $(V_1(Q), \dots, V_k(Q))$ is representable in Q and by Proposition 9 the class $\mathsf{DNPP}_k(Q)$ is closed under $\leq_s$. Therefore for all $k \geq 2$ all disjoint k-tuples of NP-sets are representable in Q.

The last part of the proof is the implication 7 ⇒ 6. For this let P be a proof system and k be a number such that all disjoint k-tuples of NP-sets are representable in P. We choose some proof system Q that simulates P and is closed under conjunctions. As $Q \geq P$ all disjoint k-tuples of NP-sets are representable in Q. To show that also all disjoint NP-pairs are representable in the system Q let (B_1, B_2) be a disjoint NP-pair. As in the proof of 4 ⇒ 3 we stretch (B_1, B_2) to a disjoint k-tuple $(B_1, B_2, \{b_3\}, \dots, \{b_k\})$ with some elements $b_3, \dots, b_k \in \overline{B_1 \cup B_2}$. By assumption $(B_1, B_2, \{b_3\}, \dots, \{b_k\})$ is representable in Q via some representations $\varphi_n^1, \dots, \varphi_n^k$. Because Q is closed under conjunctions this implies that Q proves the disjointness of B_1 and B_2 with respect to φ_n^1 and φ_n^2, hence (B_1, B_2) is representable in Q. □

We can also characterize the existence of complete disjoint k-tuples of NP-sets by conditions on arithmetic theories, thereby extending the list of characterizations from Theorem 19 by the items listed in the next theorem:

Theorem 20. *The following conditions are equivalent:*

1. *For all numbers $k \geq 2$ there exists a $\leq_s$-complete disjoint k-tuple of* NP*-sets.*
2. *There exists a finitely axiomatized arithmetic theory T such that for all numbers $k \geq 2$ all disjoint k-tuples of* NP*-sets are representable in T.*

3. *There exists an arithmetic theory T with a polynomial time set of axioms such that for some number $k \geq 2$ all disjoint k-tuples of* NP*-sets are representable in T.*

Proof. We start with the proof of the implication 1 ⇒ 2. By Theorem 19 we know already that condition 1 implies the existence of a proof system P in which all disjoint k-tuples of NP-sets are representable. Because P is simulated by the proof system $EF + \mathrm{RFN}(P)$ all k-tuples are also representable in $EF + \mathrm{RFN}(P)$. This system is regular and corresponds to the theory S^1_2+RFN(P) (cf. [Bey05]). Therefore all disjoint k-tuples of NP-sets are representable in $S^1_2 + \mathrm{RFN}(P)$ by Theorem 14. As the theory S^1_2 is finitely axiomatizable (cf. [Kra95]) we have proven condition 2.

As condition 3 obviously is a weakening of condition 2 it remains to prove 3 ⇒ 1. For this let $k \geq 2$ be a natural number and T be an arithmetic theory such that $\mathsf{DNPP}_k(T)$ contains all disjoint k-tuples of NP-sets. Consider the theory $T' = T \cup S^1_2$. As T' is an extension of T all k-tuples are also representable in T'. As in [KP89] we define from the theory T' a propositional proof system P as follows:

$$P(\pi) = \begin{cases} \varphi & \text{if } \pi \text{ is a } T'\text{-proof of } \mathrm{Taut}(\varphi) \\ \top & \text{otherwise} \end{cases}$$

Because T' has a polynomial time axiomatization this defines indeed a propositional proof system. We claim that all k-tuples are representable in P. To verify this claim let $(A_1, \dots, A_k)$ be a disjoint k-tuple of NP-sets. By hypothesis there exist arithmetic representations $\varphi_1, \dots, \varphi_k$ of $A_1, \dots, A_k$ such that

$$T \ \vdash \ (\forall x) \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \vee \neg\varphi_j(x) \ . \tag{5}$$

By induction on the logical complexity of a Π^b_1-formula $\psi(x)$ we can prove

$$S^1_2 \ \vdash \ (\forall x)\psi(x) \to (\forall y)\mathrm{Taut}(\|\psi\|^y) \ .$$

Therefore we get from (5)

$$T' \ \vdash \ (\forall y)\mathrm{Taut}(\| \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \vee \neg\varphi_j(x)\|^y) \ .$$

By the construction of P this implies

$$P \ \vdash_* \ (\| \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \vee \neg\varphi_j(x)\|^n) \ . \tag{6}$$

The translations $\|\varphi_i\|^n$ are propositional representations for A_i for $i = 1, \dots, k$. By the definition of the translations $\|.\|$ we get from (6)

$$P \ \vdash_* \ (\bigwedge_{1 \leq i < j \leq k} \neg\|\varphi_i(x)\|^n \vee \neg\|\varphi_j(x)\|^n) \ ,$$

hence $(A_1, \dots, A_k)$ is representable in P. Thus all disjoint k-tuples of NP-sets are representable in P which by Theorem 19 implies condition 1. □

In Theorem 19 we stated that the existence of complete disjoint NP-pairs is equivalent to the existence of a propositional proof system P in which every disjoint NP-pair is representable. By definition this condition means that for all disjoint NP-pairs there exists a representation for which the disjointness of the pair is provable with short P-proofs. If we strengthen this condition by requiring that this is possible for all disjoint NP-pairs and all representations we arrive at a condition which is strong enough to characterize the existence of optimal proof systems. This is the contents of the next theorem.

Theorem 21. *The following conditions are equivalent:*

1. *There exists an optimal propositional proof system.*
2. *There exists a propositional proof system P such that for all $k \geq 2$ the system P proves the disjointness of all disjoint k-tuples of NP-sets with respect to all representations, i.e. for all disjoint k-tuples $(A_1, \dots, A_k)$ of NP-sets and all representations $\varphi_n^1, \dots, \varphi_n^k$ of $A_1, \dots, A_k$ we have $P \vdash_* \bigwedge_{1 \leq i < j \leq k} \neg\varphi_n^i \vee \neg\varphi_n^j$.*
3. *There exists a propositional proof system P that proves the disjointness of all disjoint NP-pairs with respect to all representations, i.e. for all disjoint NP-pairs (A, B) and all representations φ_n of A and ψ_n of B we have $P \vdash_* \neg\varphi_n \vee \neg\psi_n$.*
4. *There exists a propositional proof system P and a number $k \geq 2$ such that P proves the disjointness of all disjoint k-tuples of NP-sets with respect to all representations.*

Proof. To prove the implication $1 \Rightarrow 2$ let P be an optimal proof system. Let further $(A_1, \dots, A_k)$ be a disjoint k-tuple of NP-sets and let φ_n^i be propositional representations of A_i for $i = 1, \dots, k$. As the sequence of tautologies

$$\bigwedge_{1 \leq i < j \leq k} \neg\varphi_n^i \vee \neg\varphi_n^j$$

can be generated in polynomial time we can define some proof system Q with $Q \vdash_* \bigwedge_{1 \leq i < j \leq k} \neg\varphi_n^i \vee \neg\varphi_n^j$. But because P is optimal we have $Q \leq P$ and therefore also $P \vdash_* \bigwedge_{1 \leq i < j \leq k} \neg\varphi_n^i \vee \neg\varphi_n^j$.

As $2 \Rightarrow 3$ and $3 \Rightarrow 4$ trivially hold it only remains to show $4 \Rightarrow 1$. For this assume that optimal proof systems do not exist. To prove that condition 4 fails let k be a natural number and let P be a proof system. We choose some proof system Q that fulfills the following conditions:

1. Q simulates the systems EF and P. Further, Q is closed under modus ponens, substitutions and conjunctions.
2. There exists a polynomial p such that for all formulas τ $Q \vdash_{\leq m} \tau(\bar{u}) \vee \tau(\bar{v})$ implies $Q \vdash_{\leq p(m)} \tau(\bar{u})$ where $\bar{u}$ and $\bar{v}$ are disjoint tuples of variables.

Finding a system that fulfills condition 1 is easy: for instance we can take $EF + \mathrm{RFN}(P)$. To get also condition 2 we can enhance the system $EF + \mathrm{RFN}(P)$ by accepting $(\pi, \tau(\bar{u}))$ as a proof of $\tau(\bar{u})$ if π is an $EF + \mathrm{RFN}(P)$-proof of $\tau(\bar{u}) \vee \tau(\bar{v})$. The system Q defined in this way fulfills conditions 1 and 2.

Let now $(A_1, \dots, A_k)$ be a disjoint k-tuple of NP-sets. We will prove that there exists a representation of $(A_1, \dots, A_k)$ such that the disjointness of $(A_1, \dots, A_k)$ is not provable in P with respect to this representation. For this we prove the following claim:

Claim. There exist representations φ_n^1 of A_1 and φ_n^2 of A_2 such that

$$Q \not\vdash_* \neg\varphi_n^1 \vee \neg\varphi_n^2 \ .$$

To prove the claim we choose arbitrary representations θ_n for A_1 and ψ_n for A_2. Because $Q \geq EF$ is not optimal and fulfills the conditions listed in 1 there exists a polynomial time constructible sequence τ_n of tautologies such that $Q \not\vdash_* \tau_n$ (cf. [Kra95] Theorem 14.2.2). We define

$$\varphi_n^1(\bar{x}, \bar{y}, \bar{u}) = \theta_n(\bar{x}, \bar{y}) \vee \neg\tau_n(\bar{u})$$
$$\varphi_n^2(\bar{x}, \bar{z}, \bar{v}) = \psi_n(\bar{x}, \bar{z}) \vee \neg\tau_n(\bar{v})$$

where all tuples of variables $\bar{x}$, $\bar{y}$, $\bar{z}$, $\bar{u}$ and $\bar{v}$ are pairwise disjoint. As $\neg\tau_n(\bar{u})$ is not satisfiable $\theta_n(\bar{x},\bar{y}) \vee \neg\tau_n(\bar{u})$ represents A_1. Similarly, φ_n^2 is a propositional representation for A_2. But Q does not prove the disjointness of A_1 and A_2 with respect to the representations φ_n^1 and φ_n^2. Assume on the contrary that

$$Q \vdash_* \neg\varphi_n^1 \vee \neg\varphi_n^2 \ .$$

By definition this means

$$Q \vdash_* \neg(\theta_n(\bar{x},\bar{y}) \vee \neg\tau_n(\bar{u})) \ \vee \ \neg(\psi_n(\bar{x},\bar{z}) \vee \neg\tau_n(\bar{v})) \ .$$

By the choice of Q we get from this polynomial size Q-proofs of

$$(\neg\theta_n(\bar{x},\bar{y}) \vee \neg\psi_n(\bar{x},\bar{z})) \wedge (\neg\theta_n(\bar{x},\bar{y}) \vee \tau_n(\bar{v})) \wedge (\neg\psi_n(\bar{x},\bar{z}) \vee \tau_n(\bar{u})) \wedge (\tau_n(\bar{u}) \vee \tau_n(\bar{v})) \ .$$

Because Q is closed under conjunctions we obtain

$$Q \vdash_* \tau_n(\bar{u}) \vee \tau_n(\bar{v}) \ .$$

Using condition 2 on Q we derive $Q \vdash_* \tau_n(\bar{u})$. This contradicts the choice of τ_n as hard tautologies for Q, and the claim is proved.

To finish the proof we choose arbitrary representations $\varphi_n^3, \dots, \varphi_n^k$ for $A_3, \dots, A_k$. As Q is closed under conjunctions Q does not prove the disjointness of $(A_1, \dots, A_k)$ with respect to $\varphi_n^1, \dots, \varphi_n^k$ and as $P \leq Q$ this is also true for the system P. Hence condition 4 fails. □

As an immediate corollary to Theorems 19 and 21 we get a strengthening of a theorem of Köbler, Messner and Torán [KMT03], stating that the existence of optimal proof systems implies the existence of $\leq_s$-complete disjoint NP-pairs:

Corollary 22. *If there exist optimal propositional proof systems, then there exist $\leq_s$-complete disjoint k-tuples of NP-sets for all numbers $k \geq 2$.*

Proof. The existence of optimal proof systems implies condition 2 of Theorem 21. This condition is a strengthening of condition 5 from Theorem 19 which is equivalent to the existence of $\leq_s$-complete disjoint k-tuples of NP-sets for all $k \geq 2$. □

Acknowledgements. For helpful conversations and suggestions on this work I am very grateful to Johannes Köbler, Jan Krajíček, Pavel Pudlák, and Zenon Sadowski.

References

[Bey04] Olaf Beyersdorff. Representable disjoint NP-pairs. In *Proc. 24th Conference on Foundations of Software Technology and Theoretical Computer Science*, 122–134, 2004.

[Bey05] Olaf Beyersdorff. Disjoint NP-pairs from propositional proof systems. Technical Report TR05-083, Electronic Colloquium on Computational Complexity, 2005.

[Bus86] Samuel R. Buss. *Bounded Arithmetic.* Bibliopolis, Napoli, 1986.

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

[GS88] Joachim Grollmann and Alan L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, **17**(2):309–335, 1988.

[GSS04] Christian Glasser, Alan L. Selman, and Samik Sengupta. Reductions between disjoint NP-pairs. In *Proc. 19th Annual IEEE Conference on Computational Complexity*, 42–53, 2004.

[GSSZ04] Christian Glasser, Alan L. Selman, Samik Sengupta, and Liyu Zhang. Disjoint NP-pairs. *SIAM Journal on Computing*, **33**(6):1369–1416, 2004.

[GSZ05] Christian Glasser, Alan L. Selman, and Liyu Zhang. Survey of disjoint NP-pairs and relations to propositional proof systems. Technical Report TR05-072, Electronic Colloquium on Computational Complexity, 2005.

[KMT03] Johannes Köbler, Jochen Messner, and Jacobo Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation*, **184**:71–92, 2003.

[KP89] Jan Krajíček and Pavel Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *Journal of Symbolic Logic*, **54**:1963–1079, 1989.

[KP90] Jan Krajíček and Pavel Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, **36**:29–46, 1990.

[KP98] Jan Krajíček and Pavel Pudlák. Some consequences of cryptographical conjectures for S_2^1 and EF. *Information and Computation*, **140**(1):82–94, 1998.

[Kra95] Jan Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, Encyclopedia of Mathematics and Its Applications #60. Cambridge University Press, Cambridge, 1995.

[Kra97] Jan Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *Journal of Symbolic Logic*, **62**(2):457–486, 1997.

[Kra04] Jan Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *Journal of Symbolic Logic*, **69**(1):265–286, 2004.

[Lad75] Richard E. Ladner. On the structure of polynomial-time reducibility. *Journal of the ACM*, **22**:155–171, 1975.

[Pud03] Pavel Pudlák. On reducibility and symmetry of disjoint NP-pairs. *Theoretical Computer Science*, **295**:323–339, 2003.

[Raz94] Alexander A. Razborov. On provably disjoint NP-pairs. Technical Report TR94-006, Electronic Colloquium on Computational Complexity, 1994.