Article:
Beyersdorff, O (2008) Tuples of disjoint NP-sets. Theory of Computing Systems, 43 (2). 118 - 135 . ISSN 1432-4350

https://doi.org/10.1007/s00224-007-9023-8

Tuples of Disjoint NP-Sets*

Olaf Beyersdorff**

Institut für Informatik, Humboldt-Universität zu 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 possess 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 [8, 15] and propositional proof complexity [17, 12]. In this paper we investigate a natural generalization of disjoint NP-pairs: instead of pairs we consider tuples of pairwise disjoint NP-sets. This generalization is in accordance with many applications where not only two but a greater number of different, mutually exclusive conditions is of interest. In particular, such tuples naturally emerge from public-key cryptosystems and one-way functions.

One of the major open problems in the field of disjoint NP-pairs is the question, posed by Razborov [18], whether there exist disjoint NP-pairs that are complete for the class of all pairs under suitable reductions. Glaßer et al. [5] 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.

* An extended abstract of this paper appeared in the proceedings of the conference CSR 2006 [2]

** Supported by DFG grant KO 1053/5-1

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 [18]. However, Glaßer et al. [6] 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 k-tuples implies the existence of complete 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 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 $\mathsf{DNPP}_k(P)$ possess 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 a condition 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. 5 where we analyse arithmetic representations. The rest of the paper and in particular the main results in Sect. 6 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. Further, we define k-tuples from propositional proof systems which serve as hard languages for $\mathsf{DNPP}_k(P)$. In particular we generalize the interpolation pair from [17] and demonstrate that even these generalized variants still capture the feasible interpolation property of the proof system.

In Sect. 5 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 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. 4 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. 6.

2 Preliminaries

Propositional Proof Systems. Propositional proof systems were defined in a very general way by Cook and Reckhow in [4] as polynomial-time functions P which have as its range the set of all tautologies, which we consider in the language containing the connectives $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ and constants $\top$ and $\bot$. 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 [4] and [13]. 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 [13].

In [1] we investigated several natural properties of propositional proof systems. 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.

Propositional Proof Systems and Arithmetic Theories. In Sect. 5 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 [10]. 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_1^b-formula. These formulas describe NP-predicates. Likewise, Π_1^b-formulas only have bounded universal quantifiers and describe coNP-predicates. A Σ_1^b- or Π_1^b-formula $\varphi(x)$ is translated into a sequence $\|\varphi(x)\|^n$ of propositional formulas containing one formula per input length for the number x such that $\varphi(x)$ is true if and only if $\|\varphi(x)\|^n$ is a tautology where $n = |x|$. As usual we associate first-order formulas $\varphi(\bar{x})$ with free variables with their universally closed counterparts $(\forall \bar{x})\varphi(\bar{x})$. Therefore the translation $\|.\|$ is not only suitable for Π_1^b- but in fact for $\forall\Pi_1^b$-formulas. 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 $\forall\Pi_1^b$-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 [14] 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. 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 $\|\varphi(x)\|^n$.
2. $T \vdash \mathrm{RFN}(P)$ and if $T \vdash \mathrm{RFN}(Q)$ for some proof system Q, then $Q \leq_p P$.

We call a proof system P *regular* if there exists an arithmetic theory T such that properties 1 and 2 are fulfilled for (T, P). Probably the most important example of a regular proof system is the extended Frege system EF that corresponds to the theory S_2^1. The theory S_2^1 is one of the most prominent theories from a whole collection of arithmetic theories, known as bounded arithmetic, that are defined by adding a controlled amount of induction to a set of basic axioms. In the case of S_2^1 induction on the length of numbers is added for Σ_1^b-formulas, which allows the formalization of polynomial-time computations in S_2^1 (cf. [10]). The correspondence between S_2^1 and EF was established in [3] and [14].

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 $B \cap C = \emptyset$. Grollmann and Selman [8] 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. [9] 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 [18], who associated a canonical disjoint NP-pair with a proof system. This canonical pair is linked to the automatizablility and the reflection property of the proof system. Pudlák [17] introduced an *interpolation pair* for a proof system P which is p-separable if and only if the proof system P has the feasible interpolation property [11]. In [1] we analysed a variant of the interpolation pair. More information on the connection between disjoint NP-pairs and propositional proof systems can be found in [1, 7, 17].

3 Basic Definitions and Properties

Definition 1. *Let $k \geq 2$ be a number. A tuple $(A_1, \dots, A_k)$ 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.*

To require the nonemptiness of the components A_i is not essential, but it simplifies the statement of some results (like e.g. Theorem 5 below). We generalize the notion of a separator of a disjoint NP-pair as follows:

Definition 2. *A function $f : \{0,1\}^* \to \{1, \dots, k\}$ is a* separator *for a disjoint k-tuple $(A_1, \dots, A_k)$ if $a \in A_i$ implies $f(a) = i$ for $i = 1, \dots, k$ and all $a \in \{0,1\}^*$. 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 3. *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. The implications $1 \Rightarrow 2$ and $3 \Rightarrow 1$ are immediate. To prove $2 \Rightarrow 3$ let us assume that all disjoint NP-pairs are p-separable. To separate a k-tuple $(A_1, \dots, A_k)$ for some $k \geq 2$ we evaluate all separators $f_{i,j}$ for all disjoint NP-pairs (A_i, A_j) and output the number i such that we received 1 at all evaluations

$f_{i,j}$. If no such i exists, then we know that the input is outside $A_1 \cup \cdots \cup A_k$, and we can answer arbitrarily. $\square$

Let us pause to give an example of a disjoint k-tuple of NP-sets that is derived from the Clique-Coloring pair (cf. [17]). The tuple $(C_1, \ldots, C_k)$ has components C_i that contain all $i+1$-colorable graphs with a clique of size i. Clearly, the components C_i are NP-sets which are pairwise disjoint. This tuple is also p-separable, but to devise a separator for $(C_1, \ldots, C_k)$ is considerably simpler than to separate the Clique-Coloring pair: given a graph G we output the maximal number i between 1 and k such that G contains a clique of size i. For graphs with n vertices this number i can be computed in time $O(n^k)$.

Candidates for p-inseparable tuples arise from one-way functions. Let $\Sigma = \{a_1, \ldots, a_k\}$ be an alphabet of size $k \geq 2$. To an injective one-way function $f : \Sigma^* \to \Sigma^*$ we assign a disjoint k-tuple $(A_1(f), \ldots, A_k(f))$ of NP-sets with components

$$A_i(f) = \{(y, j) \mid (\exists x) f(x) = y \text{ and } x_j = a_i\}$$

where x_j is the j-th letter of x. This tuple is p-inseparable if f has indeed the one-way property.

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.

Definition 4. *A k-tuple $(A_1, \ldots, A_k)$ is* polynomially reducible *to a k-tuple $(B_1, \ldots, B_k)$, denoted by $(A_1, \ldots, A_k) \leq_p (B_1, \ldots, B_k)$, if there exists a polynomial-time computable function f such that $f(A_i) \subseteq B_i$ for $i = 1, \ldots, k$. If additionally $f(\overline{A_1 \cup \cdots \cup A_k}) \subseteq \overline{B_1 \cup \cdots \cup B_k}$ holds, then we call the reduction performed by f* strong. *Strong reductions are denoted by $\leq_s$.*

From $\leq_p$ and $\leq_s$ we define 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.

In the next theorem we separate the reductions $\leq_p$ and $\leq_s$ on the domain of all p-separable disjoint k-tuples of NP-sets:

Theorem 5. *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.*

Proof. Part 1 is easy. For part 2 we use the result of Ladner [16] that 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.

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

4 Disjoint k-Tuples from Propositional Proof Systems

In [1] we defined propositional representations for NP-sets as follows:

Definition 6. *Let A be a NP-set over the alphabet $\{0,1\}$. A* propositional representation *for A is a sequence of propositional formulas $\varphi_n(\bar{x},\bar{y})$ such that:*

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 7. *Let P be a propositional proof system. A 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 $1 \le i < j \le k$ 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*

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

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 [1] 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. The next proposition shows that these classes are closed under the reductions $\le_p$ and $\le_s$.

Proposition 8. *Let P be a proof system that is closed under conjunctions and disjunctions and that simulates resolution. Then for all numbers $k \ge 2$ the class $\mathsf{DNPP}_k(P)$ is closed under $\le_p$.*

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 $\le_p$-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 $(B_1,\dots,B_k) \in \mathsf{DNPP}_k(P)$.

Closure of P under conjunctions implies that for all $1 \le i < j \le k$ each of the disjoint NP-pairs (B_i,B_j) is contained in $\mathsf{DNPP}(P)$. In [1] we proved that $\mathsf{DNPP}(P)$ is closed under $\le_p$, if P simulates resolution and is closed under disjunctions. As f is a $\le_p$-reduction between the pairs (A_i,A_j) and (B_i,B_j) we infer that all pairs (A_i,A_j) are in $\mathsf{DNPP}(P)$. In fact, 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 $\bigwedge_{1\leq i<j\leq k} A'_i \cap A'_j = \emptyset$. This shows $(A_1, \ldots, A_k) \in \mathsf{DNPP}_k(P)$. $\square$

Now 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 [17] can be expanded to a k-tuple $(I_1(P), \ldots, I_k(P))$ by

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

for $i = 1, \ldots, k$, where $\mathrm{Var}(\varphi)$ denotes the set of propositional variables occurring in φ. This tuple still captures the feasible interpolation property of the proof system P as the next theorem shows.

Theorem 9. *Let P be a propositional proof system that is efficiently closed under substitutions by constants and conjunctions. Then $(I_1(P), \ldots, I_k(P))$ is p-separable if and only if P has the feasible interpolation property.*

Proof. Pudlák [17] showed that proof systems with efficient closure under substitutions by constants have the feasible interpolation property if and only if the interpolation pair $(I_1(P), I_2(P))$ is p-separable. It is therefore sufficient to show for every $k \geq 2$ that the pair $(I_1(P), I_2(P))$ is p-separable if and only if $(I_1(P), \ldots, I_k(P))$ is p-separable.

For the first direction assume that $(I_1(P), I_2(P))$ is separated by the polynomial-time computable function f, i.e.

$$\begin{aligned} (\varphi, \psi, \pi) \in I_1(P) \quad &\Longrightarrow \quad f(\varphi, \psi, \pi) = 1 \\ (\varphi, \psi, \pi) \in I_2(P) \quad &\Longrightarrow \quad f(\varphi, \psi, \pi) = 0 \ . \end{aligned}$$

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 π is indeed a P-proof of

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

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 $j \in \{1, \ldots, k\} \setminus \{i\}$ we have $f(\varphi_i, \varphi_j, \pi_{i,j}) = 1$. If such i exists, then we output this number 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 $\varphi_1, \ldots, \varphi_{i-1}, \varphi_{i+1}, \ldots, \varphi_k$ are tautologies. Therefore $f(\varphi_i, \varphi_j, \pi_{i,j})$ always outputs 1. As this can happen for at most one i we give the correct answer.

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

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

for $i = 1, \ldots, k$. Let (φ, ψ, π) be given. We first check whether $P(\pi) = \varphi \vee \psi$. If this is fulfilled we expand (φ, ψ) to the k-tuple

$$(\varphi_1, \ldots, \varphi_k) = (\varphi, \psi, \top, \ldots, \top) \ .$$

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

Searching for canonical candidates for hard tuples for the classes $\mathsf{DNPP}_k(P)$ we modify the interpolation tuple to the following tuple $(U_1(P), \ldots, U_k(P))$ with

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

for $i = 1, \ldots, k$. The next theorem shows that for all reasonable proof systems P these tuples are hard for the classes $\mathsf{DNPP}_k(P)$.

Theorem 10. *Let P be a proof system that is closed under substitutions by constants. Then $(U_1(P), \ldots, U_k(P))$ is $\le_s$-hard for $\mathsf{DNPP}_k(P)$ for all $k \ge 2$.*

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

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

Then the $\le_s$-reduction from $(A_1, \ldots, A_k)$ to $(U_1(P), \ldots, U_k(P))$ is performed by

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

for some suitable polynomial p. $\square$

For technical reasons we now introduce a modification $(V_1(P), \ldots, V_k(P))$ 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 $(V_1(P), \ldots, V_k(P))$ as:

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

for $r = 1, \ldots, k$. 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 $((\varphi_{i,j} \mid 1 \leq i, j \leq k, i \neq j), 1^m)$ is contained both in $V_r(P)$ and $V_s(P)$ for $r, s \in \{1, \ldots, k\}$, $r < s$. 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 also showing the hardness result for the V-tuple.

5 Arithmetic Representations

In [18] and [1] 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 11. *A Σ_1^b-formula φ is an* arithmetic representation *of an NP-set A if for all natural numbers a we have $\mathbb{N} \models \varphi(a)$ if and only if $a \in A$.*

A disjoint k-tuple $(A_1, \ldots, A_k)$ of NP-sets is representable *in an arithmetic theory T if there are Σ_1^b-formulas $\varphi_1(x), \ldots, \varphi_k(x)$ representing $A_1, \ldots, A_k$ such that $T \vdash (\forall x) \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \vee \neg\varphi_j(x)$. The class $\mathsf{DNPP}_k(T)$ contains all disjoint k-tuples of NP-sets that are representable in T.*

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

Theorem 12. *Let $P \geq EF$ be a regular proof system which is closed under substitutions by constants and conjunctions and let $T \supseteq S_2^1$ be a theory corresponding to T. Then we have $\mathsf{DNPP}_k(P) = \mathsf{DNPP}_k(T)$ for all $k \geq 2$.*

Proof. We reduce the proof of the theorem to the case $k = 2$ which we proved in [1].

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

$$P \vdash_* \bigwedge_{1 \leq i < j \leq k} \neg\varphi_n^i \vee \neg\varphi_n^j \quad . \tag{1}$$

Because P is closed under conjunctions this in particular means $P \vdash_* \neg\varphi_n^i \vee \neg\varphi_n^j$ for all $1 \leq i < j \leq k$, i.e., all disjoint NP-pairs (A_i, A_j) are contained in

$\mathsf{DNPP}(P)$. By the mentioned result from [1] 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 (1). Hence we get

$$T \vdash (\forall x) \bigwedge_{1 \leq i < j \leq k} \neg\psi_i(x) \vee \neg\psi_j(x) \tag{2}$$

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

For the other inclusion let $\psi_1(x), \ldots, \psi_k(x)$ be arithmetic representations of $A_1, \ldots, A_k$ such that (2) holds. Then the translations $\|\psi_i(x)\|^n$ of the arithmetic representations ψ_i provide propositional representations of A_i for $i = 1, \ldots, k$. In these translations we choose the auxiliary variables disjoint. Because $\bigwedge_{1 \leq i < j \leq k} \neg\psi_i(x) \vee \neg\psi_j(x)$ is a Π_1^b-formula we get from (2)

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

Using elementary properties of the translation $\|.\|$ this yields $(A_1, \ldots, A_k) \in \mathsf{DNPP}_k(P)$. □

Theorem 12 states the somewhat unusual fact that the non-uniform and uniform concepts equal when representing disjoint k-tuples of NP-sets in regular proof systems. We now observe that the k-tuples that we associated with a proof system P are representable in P if the system is regular.

Lemma 13. *Let P be a regular proof system. Then for all numbers $k \geq 2$ the tuples $(I_1(P), \ldots, I_k(P))$, $(U_1(P), \ldots, U_k(P))$ and $(V_1(P), \ldots, V_k(P))$ are representable in P.*

Proof. We choose straightforward arithmetic representations for the components $I_i(P)$, $U_i(P)$ and $V_i(P)$. Using the reflection principle of P we can prove the disjointness of the components of the respective tuples in the theory T associated with P, from which the lemma follows by Theorem 12. □

With this lemma we can improve the hardness result of Theorem 10 to a completeness result for regular proof systems. Additionally, we can show the $\leq_s$-completeness of the interpolation tuple for $\mathsf{DNPP}_k(P)$:

Theorem 14. *Let $P \geq EF$ be a regular proof system that is efficiently closed under substitutions by constants. Then for all $k \geq 2$ the tuples $(U_1(P), \ldots, U_k(P))$ and $(I_1(P), \ldots, I_k(P))$ are $\leq_s$-complete for $\mathsf{DNPP}_k(P)$. In particular we have $(U_1(P), \ldots, U_k(P)) \equiv_s (I_1(P), \ldots, I_k(P))$.*

Proof. Completeness of the U-tuple follows from Theorem 10 together with the previous lemma. As by Lemma 13 also $(I_1(P), \ldots, I_k(P))$ is representable in P it remains to show that $(I_1(P), \ldots, I_k(P))$ is $\leq_s$-hard for $\mathsf{DNPP}_k(P)$. For this let $(A_1, \ldots, A_k)$ be a disjoint k-tuple of NP-sets that is representable in P.

By Theorem 12 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

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

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

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

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

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

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

Then the $\le_s$-reduction from $(A_1,\dots,A_k)$ to $(I_1(P),\dots,I_k(P))$ is given by

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

where the auxiliary variables of $\|\neg\varphi_i(x)\|^{|a|}$ are all chosen disjoint. $\square$

This corollary is true for EF as well as for all extensions $EF+\|\Phi\|$ of the extended Frege system 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 14 might come unexpected as the first idea for a reduction from the U-tuple to the I-tuple probably is to generate proofs for $\bigwedge_{1\le j<l\le k}\varphi_j \vee \varphi_l$ 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 $P\ge EF$ under cryptographic assumptions [15, 17].

6 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 $\le_p$ and $\le_s$. 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 15. *The following conditions are equivalent:*

1. *For all numbers $k\ge 2$ there exists a $\le_s$-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. The proof is structured as follows: $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 6 \Rightarrow 1$ and $3 \Leftrightarrow 4$, $5 \Leftrightarrow 6$, $6 \Leftrightarrow 7$. Apparently, items 1 to 4 and items 5 to 7 are conditions of decreasing strength. For the implication $3 \Rightarrow 6$ assume that (A, B) is a $\leq_p$-complete pair. We choose some representations φ_n and ψ_n for A and B, respectively. Consider the proof system $P = EF + \{\neg\varphi_n \vee \neg\psi_n \,|\, n \geq 0\}$, which simulates resolution and is closed under disjunctions. Because (A, B) is representable in P and $\mathsf{DNPP}(P)$ is closed under $\leq_p$ by Proposition 8, 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 $(V_1(Q), \ldots, V_k(Q))$ is $\leq_s$-complete for the class of all disjoint k-tuples of NP-sets. To verify the claim let $(A_1, \ldots, A_k)$ 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 $(A_1, \ldots, A_k)$ to $(U_1(Q), \ldots, U_k(Q))$. But we can reduce $(A_1, \ldots, A_k)$ to $(V_1(Q), \ldots, V_k(Q))$ 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

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

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

$$Q \vdash_* \bigwedge_{i=1}^{k} \bigwedge_{j=i+1}^{k} \neg\varphi_n^{i,j}(\bar{x}, \bar{y}^{i,j}) \vee \neg\varphi_n^{j,i}(\bar{x}, \bar{y}^{j,i}) \ . \tag{3}$$

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

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

for some appropriate polynomial p which comes from (3) 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 (3) 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 $((\neg\varphi_n^{i,j}(\bar{a}, \bar{y}^{i,j}) \mid 1 \le i, j \le k, i \ne j), 1^{p(m)}) \in V_r(Q)$.

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 $V_1(Q) \cup \dots \cup V_k(Q)$.

We proceed with the proof of the implication $4 \Rightarrow 3$. Assume that the tuple $(A_1, \dots, A_k)$ is $\le_p$-complete for all disjoint k-tuples of NP-sets. We claim that (A_1, A_2) is a $\le_p$-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 $\le_p$-equivalent pair with this property. Since $(A_1, \dots, A_k)$ is $\le_p$-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 $6 \Rightarrow 5$. 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 $6 \Rightarrow 1$ we see that condition 6 implies that for all $k \ge 2$ the k-tuple $(V_1(Q), \dots, V_k(Q))$ is $\le_s$-complete for the class of all disjoint k-tuples of NP-sets. By Lemma 13 $(V_1(Q), \dots, V_k(Q))$ is representable in Q and by Proposition 8 the class $\mathsf{DNPP}_k(Q)$ is closed under $\le_s$. Hence for all $k \ge 2$ all disjoint k-tuples of NP-sets are representable in Q.

The last part of the proof is the implication $7 \Rightarrow 6$. 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 $Q \ge P$ 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 $4 \Rightarrow 3$ 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. $\square$

Using Theorem 12 we can also characterize the existence of complete disjoint k-tuples of NP-sets by a condition on arithmetic theories, thereby extending the list of characterizations from Theorem 15 by the following items:

Theorem 16. *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 $1 \Rightarrow 2$. By Theorem 15 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 $S^1_2 + \mathrm{RFN}(P)$. Therefore all disjoint k-tuples of NP-sets are representable in $S^1_2 + \mathrm{RFN}(P)$ by Theorem 12. As the theory S^1_2 is finitely axiomatizable (cf. [10]) we have proven condition 2.

As condition 3 obviously is a weakening of condition 2 it remains to prove $3 \Rightarrow 1$. 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 [13] 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

$$T \ \vdash \ (\forall x) \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \vee \neg\varphi_j(x) \ . \tag{4}$$

For Π^b_1-formulas ψ we have $S^1_2 \vdash (\forall x)\psi(x) \rightarrow (\forall y)\mathrm{Taut}(\|\psi\|^{|y|})$, thereby getting from (4)

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

By the construction of P this implies

$$P \ \vdash_* \ \| \bigwedge_{1 \leq i < j \leq k} \neg\varphi_i(x) \vee \neg\varphi_j(x)\|^n \ . \tag{5}$$

The translations $\|\varphi_i\|^n$ are propositional representations for A_i for $i = 1, \dots, k$. By the definition of the translation $\|.\|$ we conclude from (5) the representability of $(A_1, \dots, A_k)$ in P. Therefore all disjoint k-tuples of NP-sets are representable in P, which by Theorem 15 implies condition 1. □

In Theorem 15 we stated that the existence of complete disjoint NP-pairs is equivalent to the existence of a proof system P in which every 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.

Theorem 17. *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.*

Proof. For the implication $1 \Rightarrow 2$ let P be an optimal proof system. For all choices of representations of k-tuples the sequence of tautologies expressing the disjointness of the tuple can be generated in polynomial time. Therefore these sequences have polynomial-size P-proofs.

Item 3 is a weakening of 2. For $3 \Rightarrow 1$ we use the following fact (cf. [10]): if optimal proof systems do not exist, then every proof system P admits hard sequences of tautologies, i.e., the sequence can be generated in polynomial time but does not have polynomial-size P-proofs.

Let us assume now that optimal proof system do not exist and let P be an arbitrary proof system. We choose some proof system $Q \geq P$ with sufficient closure properties, for instance $Q = EF + \|\mathrm{RFN}(P)\|$. By the mentioned result from [10] there exists a sequence $\tau_n(\bar{u})$ of hard tautologies for Q. Given an NP-pair (A, B) and arbitrary propositional representations $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ of A and B, respectively, we code these hard tautologies into the representations φ_n and ψ_n, obtaining representations

$$\begin{aligned} \varphi_n'(\bar{x}, \bar{y}, \bar{u}) &= \varphi_n(\bar{x}, \bar{y}) \vee \neg\tau_n(\bar{u}) \\ \psi_n'(\bar{x}, \bar{z}, \bar{v}) &= \psi_n(\bar{x}, \bar{z}) \vee \neg\tau_n(\bar{v}) \end{aligned}$$

for which Q does not prove the disjointness of (A, B). Assume on the contrary that $Q \vdash_* \neg\varphi_n' \vee \neg\psi_n'$. By definition this means

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

Using basic manipulations of formulas, which can be efficiently performed in Q, we get polynomial-size Q-proofs of $\tau_n(\bar{u})$, contradicting the choice of τ_n as hard tautologies for Q. □

As an immediate corollary to Theorems 15 and 17 we get a strengthening of a theorem of Köbler, Messner and Torán [9], stating that the existence of optimal proof systems implies the existence of $\leq_s$-complete disjoint NP-pairs:

Corollary 18. *If there exist optimal propositional proof systems, then there exist $\leq_s$-complete disjoint k-tuples of NP-sets for all numbers $k \geq 2$.*

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

References

1. O. Beyersdorff. Classes of representable disjoint NP-pairs. *Theoretical Computer Science*. To appear.
2. O. Beyersdorff. Tuples of disjoint NP-sets. In *Proc. 1st International Computer Science Symposium in Russia*, volume 3967 of *Lecture Notes in Computer Science*, pages 80–91. Springer-Verlag, Berlin Heidelberg, 2006.
3. S. R. Buss. *Bounded Arithmetic*. Bibliopolis, Napoli, 1986.
4. S. A. Cook and R. A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44:36–50, 1979.
5. C. Glaßer, A. L. Selman, and S. Sengupta. Reductions between disjoint NP-pairs. *Information and Computation*, 200(2):247–267, 2005.
6. C. Glaßer, A. L. Selman, S. Sengupta, and L. Zhang. Disjoint NP-pairs. *SIAM Journal on Computing*, 33(6):1369–1416, 2004.
7. C. Glaßer, A. L. Selman, and L. Zhang. Survey of disjoint NP-pairs and relations to propositional proof systems. In O. Reingold, A. L. Rosenberg, and A. L. Selman, editors, *Essays in Theoretical Computer Science in Memory of Shimon Even*, pages 241–253. Springer-Verlag, Berlin Heidelberg, 2006.
8. J. Grollmann and A. L. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing*, 17(2):309–335, 1988.
9. J. Köbler, J. Messner, and J. Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation*, 184:71–92, 2003.
10. J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory*, volume 60 of *Encyclopedia of Mathematics and Its Applications*. Cambridge University Press, Cambridge, 1995.
11. J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *The Journal of Symbolic Logic*, 62(2):457–486, 1997.
12. J. Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *The Journal of Symbolic Logic*, 69(1):265–286, 2004.
13. J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *The Journal of Symbolic Logic*, 54:1963–1079, 1989.
14. J. Krajíček and P. Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschrift für mathematische Logik und Grundlagen der Mathematik*, 36:29–46, 1990.
15. J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S^1_2 and EF. *Information and Computation*, 140(1):82–94, 1998.

16. R. E. Ladner. On the structure of polynomial-time reducibility. *Journal of the ACM*, 22:155–171, 1975.
17. P. Pudlák. On reducibility and symmetry of disjoint NP-pairs. *Theoretical Computer Science*, 295:323–339, 2003.
18. A. A. Razborov. On provably disjoint NP-pairs. Technical Report TR94-006, Electronic Colloquium on Computational Complexity, 1994.