Electronic Colloquium on Computational Complexity, Report No. 83 (2005)

Disjoint NP-Pairs from Propositional Proof Systems

Olaf Beyersdorff

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

Abstract. For a proof system P we introduce the complexity class $\mathsf{DNPP}(P)$ of all disjoint NP-pairs for which the disjointness of the pair is efficiently provable in the proof system P. We exhibit structural properties of proof systems which make the previously defined canonical NP-pairs of these proof systems hard or complete for $\mathsf{DNPP}(P)$. Moreover we demonstrate that non-equivalent proof systems can have equivalent canonical pairs and that depending on the properties of the proof systems different scenarios for $\mathsf{DNPP}(P)$ and the reductions between the canonical pairs exist.

1 Introduction

Disjoint NP-pairs (DNPP) naturally occur in cryptography (cf. [GS88]). The investigation of disjoint NP-pairs in connection with propositional proof systems was initiated by Razborov [Raz94] and further developed by Pudlák [Pud03] and Köbler et al. [KMT03]. These applications attracted more complexity theoretic research on the structure of the class of disjoint NP-pairs (cf. [GSS04,GSSZ04,GSZ05,Bey04a]).

Various disjoint NP-pairs have been defined from propositional proof systems which model properties of these proof systems. Razborov [Raz94] was the first to associate a canonical pair with a proof system. This pair corresponds to the reflection property of the proof system. Pudlák [Pud03] showed that also the automatizability of the proof system which is of great importance for automated theorem proving is tightly connected to the separability of the canonical pair. Pudlák also introduced an interpolation pair of a proof system which captures the notion of feasible interpolation of the proof system. In [Bey04a] we defined another canonical pair which plays a similar role as Razborov's canonical pair for a stronger reduction introduced in [KMT03].

In this paper we analyse the reductions between these pairs. We also explain different techniques to construct non-equivalent proof systems which have equivalent canonical pairs. We define the notions of propositional representations for NP-sets and pairs. The complexity class $\mathsf{DNPP}(P)$ contains all disjoint NP-pairs for which there exist short P-proofs of its disjointness with respect to some representation of the pair. In [Raz94] and [Bey04a] these complexity classes were considered for strong systems corresponding to arithmetic theories with the main goal to obtain information on the open problem of the existence of complete pairs for the class of all DNPP. However, the results of [Raz94] and [Bey04a] do not apply for weaker systems like resolution or cutting planes which are nevertheless of great interest.

The aim of this paper is to demonstrate that also weak proof systems P satisfying certain regularity conditions define reasonable complexity classes $\mathsf{DNPP}(P)$ for which the canonical pairs are complete or hard under the respective reductions. The mentioned regularity conditions are of logical nature: it should be feasible to carry out basic operations like modus ponens or substitutions by constants in the proof system. We also show that proof systems P not satisfying these conditions do not define natural complexity classes $\mathsf{DNPP}(P)$. A recent result of Glaßer et al. [GSZ05]

ISSN 1433-8092

states that every DNPP is equivalent to the canonical pair of some proof system. However, the proof systems constructed for this purpose do not satisfy our regularity conditions. The observations of this paper indicate that the Cook-Reckhow framework for propositional proof systems might be too broad for the study of naturally defined classes of disjoint NP-pairs (and in fact for other topics in proof complexity as well). It therefore seems to be natural to make additional assumptions on the properties of proof systems. Consequently, in our opinion, the canonical pairs of these natural proof systems deserve special attention.

The paper is organized as follows. In Sects. 2 and 3 we recall relevant material about propositional proof systems and disjoint NP-pairs. We also define and investigate natural properties of proof systems which we use throughout the paper. In Sect. 3 we introduce propositional representations for NP-pairs and the complexity class $\mathsf{DNPP}(P)$.

In Sect. 4 we analyse a weak notion of simulation for proof systems introduced in [KP89] but not much studied elsewhere. This simulation is provably weaker than the ordinary reduction between proof systems but is equivalent with respect to the existence of optimal proof systems.

In Sect. 5 we provide different ways to construct non-equivalent proof systems with equivalent canonical pairs. A first example for this situation is due to Pudlák [Pud03]. Here we prove that all proof systems that are equivalent with respect to the weak simulation from Sect. 4 posses equivalent canonical pairs. Some results of Sects. 4 and 5 are included in the technical report [Bey04b] but not in [Bey04a].

Section 6 is devoted to the complexity class $\mathsf{DNPP}(P)$. We demonstrate that proof systems P with different properties give rise to different scenarios for $\mathsf{DNPP}(P)$ and the reductions between the NP-pairs associated with P.

2 Proof Systems with Natural Properties

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 $P \vdash_* \Phi$.

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. A proof system P is called polynomially bounded if there is a polynomial p such that $P \vdash_{\leq p(|\varphi|)} \varphi$ for all tautologies φ. By a theorem of Cook and Reckhow in [CR79] polynomially bounded proof systems exist iff $\mathsf{NP} = \mathsf{coNP}$.

We call a proof system *line based* if proofs in the system consist of sequences of formulas and formulas such a sequence are derived from earlier formulas in the sequence by the rules available in the proof system. Most of the studied proof systems like resolution, cutting planes and Frege systems are line based in this sense. The most interesting proof system for us will be the *extended Frege proof system EF* that is a usual textbook proof system based on axioms and rules and augmented by the possibility to abbreviate complex formulas by propositional variables to reduce the proof size (see e.g. [Kra95]).

In the following we will often enhance line based proof systems by additional axioms. We will do this in two different ways. Let Φ be a set of tautologies which can

be decided in polynomial time. By $P + \Phi$ we denote the proof system P augmented by the possibility to use all formulas from Φ as axiom schemes. This means that formulas from Φ as well as substitution instances of these formulas can be freely introduced as new lines in $P + \Phi$ -proofs. In contrast to this we use the notation $P \cup \Phi$ for the proof system that extends P by formulas from Φ as new axioms. The difference to $P + \Phi$ is that in $P \cup \Phi$ we are only allowed to use formulas from Φ but not their substitution instances in proofs.

We say that a line based proof system P allows *efficient deduction* if there exists a polynomial p such that for all finite sets of tautologies Φ

$$P \cup \Phi \vdash_{\leq m} \psi \quad \text{implies} \quad P \vdash_{\leq p(m+m')} (\bigwedge_{\varphi \in \Phi} \varphi) \to \psi$$

where $m' = |\bigwedge_{\varphi \in \Phi} \varphi|$. Along the lines of the proof of the deduction theorem for Frege systems (see e.g. [Kra95]) we can prove:

Theorem 1 (Deduction theorem for EF). *EF allows efficient deduction.*

Proof. For every F-rule

$$R_i = \frac{A_1, \ldots, A_r}{A}$$

we fix a F-proof π_i of the tautology

$$((q \to A_1) \wedge \ldots \wedge (q \to A_r)) \to (q \to A) \ .$$

Note that for $r = 0$ this also includes the case that R_i is an axiom scheme.

Let $\varphi_1, \ldots, \varphi_n$ be tautologies and let $(\theta_1, \ldots, \theta_k)$ be a proof of φ of size m in the system $EF \cup \{\varphi_1, \ldots, \varphi_n\}$. Let $m' = \sum_{i=1}^{n} |\varphi_i|$. By induction on j we construct proofs of the implications

$$(\bigwedge_{i=1}^{n} \varphi_i) \to \theta_j \ .$$

We distinguish three cases on how the formula θ_j was derived.

If θ_j was inferred from $\theta_{j_1}, \ldots, \theta_{j_r}$ by the F-rule R_i then we can get from π_i a F-proof of size $O(m' + |\theta_j| + \sum_{l=1}^{r} |\theta_{j_l}|)$ of the tautology

$$(((\bigwedge_{i=1}^{n} \varphi_i) \to \theta_{j_1}) \wedge \ldots \wedge ((\bigwedge_{i=1}^{n} \varphi_i) \to \theta_{j_r})) \to ((\bigwedge_{i=1}^{n} \varphi_i) \to \theta_j) \ .$$

Using modus ponens and the earlier proved implications

$$(\bigwedge_{i=1}^{n} \varphi_i) \to \theta_{j_l}, \ l = 1, \ldots, r$$

we get the desired implication

$$(\bigwedge_{i=1}^{n} \varphi_i) \to \theta_j$$

in a proof of size $O(m + m')$.

If θ_j is one of the formulas from $\{\varphi_1, \ldots, \varphi_n\}$ then we get $(\bigwedge_{i=1}^{n} \varphi_i) \to \theta_j$ in a proof of size $O(m')$.

Let now θ_j be derived by the extension rule, i.e.

$$\theta_j = (q \leftrightarrow \theta)$$

with a new variable q. In this case we also use the extension rule to get $(q \leftrightarrow \theta)$ and then derive

$$(\bigvee_{i=1}^{n} \neg\varphi_i) \vee (q \leftrightarrow \theta) = (\bigwedge_{i=1}^{n} \varphi_i) \rightarrow (q \leftrightarrow \theta) \ .$$

in a proof of size $O(m' + |\theta|)$. □

In the following we will often consider proof systems satisfying some additional properties. We say that a proof system P is *closed under modus ponens* if there exists a polynomial p such that for all formulas φ and ψ

$$P \vdash_{\leq m} \varphi \quad \text{and} \quad P \vdash_{\leq n} \varphi \rightarrow \psi \quad \text{imply} \quad P \vdash_{\leq p(m+n)} \psi \ .$$

This definition is a weak form of saying that modus ponens is available as a rule in the proof system. If P is closed under modus ponens then we can apply modus ponens constantly many times with only polynomial increase in the proof length. In Frege systems, however, modus ponens can be used arbitrarily often whereas with our definition this might produce exponentially long proofs. Therefore a stronger form of closure under modus ponens would be to infer from $P \vdash_{\leq m} \varphi$ and $P \vdash_{\leq n} \varphi \rightarrow \psi$ that $P \vdash_{\leq m+n} \psi$. In this paper, however, we only need the first weaker variant.

P is *closed under substitutions* if there exists a polynomial q such that $P \vdash_{\leq n} \varphi$ implies $P \vdash_{\leq q(n+|\sigma(\varphi)|)} \sigma(\varphi)$ for all formulas φ and all substitutions σ. Likewise we say that 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 $\bar{a} \in \{0,1\}^{|\bar{x}|}$.

Occasionally we will also consider other properties. We say that a proof system *evaluates formulas without variables* if these formulas have polynomially long proofs. As this is true even for truth table evaluations all proof systems simulating the truth table system evaluate formulas without variables. 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 $P \vdash_{\leq q(m)} \varphi$ as well as $P \vdash_{\leq q(m)} \psi$. Another natural assumption is that P can *perform basic operations with formulas*. By this we mean for example that a proof of $\varphi \rightarrow \psi$ can be modified to a proof of $\neg\varphi \vee \psi$ with only polynomial increase in proof length.

A class of particularly well behaved proof systems is formed by *regular proof systems* which correspond to arithmetic theories. To explain this correspondence we have to translate first order arithmetic formulas into propositional formulas. Π_1^b-formulas have only bounded universal quantifiers and describe coNP-predicates. A 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. We use $\|\varphi(x)\|$ to denote the set $\{\|\varphi(x)\|^n \mid n \geq 0\}$.

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

$$P \vdash_* \|\mathrm{RFN}(P)\|^n \ .$$

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 $T \vdash \mathrm{RFN}(S)$ for a proof system S then $S \leq_p P$.

The most prominent example for this correspondence is the pair (S_2^1, EF) (cf. [Bus86]). Furthermore, a combination of our extra assumptions on proof systems guarantees the regularity of the system, namely:

Theorem 2. *Let P be a proof system such that $EF \leq P$ and P has reflection and is closed under modus ponens and substitutions. Then $EF + \|\mathrm{RFN}(P)\| \equiv P$. Hence P is regular and corresponds to the theory $S_2^1 + \mathrm{RFN}(P)$.*

The proof of Theorem 2 requires a series of propositions which will also be useful in later sections.

Lemma 3. *Let P be a proof system such that $EF \leq P$ and P is closed under modus ponens and substitutions. Let Φ be some polynomial time set of tautologies such that $P \vdash_* \Phi$. Then $EF + \Phi \leq P$.*

Proof. Let $EF + \Phi \vdash_{\leq m} \varphi$. This means that there are substitution instances $\psi_1, \ldots, \psi_k$ of formulas from Φ such that

$$EF \cup \{\psi_1, \ldots, \psi_k\} \vdash_{\leq m} \varphi \ .$$

Using the deduction theorem for EF we get

$$EF \vdash_{\leq p(m)} (\bigwedge_{i=1}^{k} \psi_i) \to \varphi$$

where p is the polynomial from the deduction theorem. The hypothesis $P \geq EF$ gives us

$$P \vdash_{\leq r(m)} (\bigwedge_{i=1}^{k} \psi_i) \to \varphi$$

for some polynomial r. Since $P \vdash_* \Phi$ and P is closed under substitutions we get polynomial size P-proofs of $\bigwedge_{i=1}^{k} \psi_i$. Finally using the closure of P under modus ponens we obtain polynomial size P-proofs of φ. □

We will mostly use Lemma 3 in the following form:

Corollary 4. *Let P be a proof system with the reflection property such that $EF \leq P$ and P is closed under modus ponens and substitutions. Then*

$$EF + \|\mathrm{RFN}(P)\| \leq P \ .$$

Further comparing the proof systems $EF + \|\mathrm{RFN}(P)\|$ and P we now come to the reverse reduction shown in [Kra95]. This reduction is even a $\leq_p$-reduction and no assumptions on P are necessary.

Proposition 5 (Krajíček [Kra95]). *Let P be a proof system. Then*

$$P \leq_p EF + \|\mathrm{RFN}(P)\| \ .$$

Proof. Let π be a P-proof of φ. Because $\mathrm{RFN}(P)$ is available as an axiom we get by substitution a polynomial size $EF + \|\mathrm{RFN}(P)\|$-proof of

$$\|\mathrm{Prf}_P(x, y)\|(x/\pi, y/\varphi) \to \|\mathrm{Taut}(y)\|(y/\varphi) \ ,$$

where the suffix (x/π) indicates that the propositional variables for x are substituted by the bits of π, and similarly for (y/φ). $\|\mathrm{Prf}_P(x, y)\|(x/\pi, y/\varphi)$ can be evaluated in EF to $\top$, giving a polynomial size proof of $\|\mathrm{Taut}(y)\|(y/\varphi)$ in the proof system $EF + \|\mathrm{RFN}(P)\|$. From this we get again by a polynomial size EF-proof the tautology φ. As these proofs can be constructed in polynomial time we get the $\leq_p$-reduction. □

The previous proposition can be seen as a propositional version of property 2 of the correspondence to arithmetic theories and documents the importance of the proof systems $EF + \|\mathrm{RFN}(P)\|$. For later use we now prove a lemma which is very similar to Proposition 5.

Lemma 6. *Let P be a proof system and Φ be some polynomial time set of tautologies. Then*

$$EF + \Phi \vdash_* \|\mathrm{RFN}(P)\|^n \quad \textit{implies} \quad P \leq EF + \Phi \ .$$

Proof. Let π be a P-proof of φ. Because $EF + \Phi \vdash_* \|\mathrm{RFN}(P)\|^n$ and $EF + \Phi$ is closed under substitutions we get a polynomial size $EF + \Phi$-proof of

$$\|\mathrm{Prf}_P(x, y)\|(x/\pi, y/\varphi) \to \|\mathrm{Taut}(y)\|(y/\varphi) \ .$$

$\|\mathrm{Prf}_P(x, y)\|(x/\pi, y/\varphi)$ can be evaluated in EF to $\top$, giving a polynomial size $EF + \Phi$-proof of $\|\mathrm{Taut}(y)\|(y/\varphi)$. From this we get again by a polynomial size EF-proof the tautology φ. Combining these proofs by modus ponens we get the $EF + \Phi$-proof of ϕ. □

Note that the reduction in the last lemma is only $\leq$ as the $EF + \Phi$-proofs of $\|\mathrm{RFN}(P)\|^n$ are not assumed to be constructible in polynomial time.

Now we come to the proof of Theorem 2.

Proof of Theorem 2. Let P be a proof system such that $EF \leq P$ and P has reflection and is closed under modus ponens and substitutions. By Corollary 4 we have $EF + \|\mathrm{RFN}(P)\| \leq P$ and Proposition 5 gives $P \leq_p EF + \|\mathrm{RFN}(P)\|$. Hence $EF + \|\mathrm{RFN}(P)\|$ and P are $\leq$-equivalent.

Next we have to check the axioms of the correspondence for $S^1_2 + \mathrm{RFN}(P)$ and P. Suppose φ is a $\forall \Pi^b_1$-formula such that

$$S^1_2 + \mathrm{RFN}(P) \vdash \varphi \ .$$

The proof of the correspondence of S^1_2 and EF in [Bus86] generalizes to the case that S^1_2 and EF are enhanced by additional axioms. Hence we get

$$EF + \|\mathrm{RFN}(P)\| \vdash_* \|\varphi\|^n \ .$$

By Corollary 4 we have

$$EF + \|\mathrm{RFN}(P)\| \leq P \ .$$

and therefore $P \vdash_* \|\varphi\|^n$. This proves part 1 of the correspondence.

It remains to check the second part. Clearly

$$S^1_2 + \mathrm{RFN}(P) \vdash \mathrm{RFN}(P) \ .$$

Finally suppose

$$S^1_2 + \mathrm{RFN}(P) \vdash \mathrm{RFN}(Q)$$

for some proof system Q. Again the results from [Bus86] and Corollary 4 give us

$$Q \leq EF + \|\mathrm{RFN}(P)\| \leq P \ .$$

□

In [Kra95] a sequence of tautologies φ_n is called *hard for a proof system P* if φ_n is constructible in polynomial time and $P \nvdash_* \varphi_n$. The next theorem from [Kra95] collects some of the most important information on optimal proof systems.

Theorem 7 (Krajíček [Kra95]). *For all proof systems $P \geq EF$ that are closed under modus ponens and substitutions the following conditions are equivalent:*

1. *There exists a sequence of tautologies hard for P.*
2. *The proof system P is not optimal.*
3. *There is a proof system Q such that $P \nvdash_* \|\mathrm{RFN}(Q)\|^n$.*

Since we are interested in the degree of a proof system and not in the particular representative of that degree we should only study properties of proof systems which are *robust* in the sense that the property is preserved when we change to a $\leq$-equivalent system. Closure under modus ponens and closure under substitutions are robust properties in this sense. Moreover they are also independent as the next proposition shows.

Proposition 8. *1. Let $P \equiv Q$ be proof systems. If P is closed under modus ponens then also Q is closed under modus ponens. The same applies for closure under substitutions and substitutions by constants.*
2. There exist proof systems which are closed under substitutions but not under modus ponens. There are also proof systems that are closed under modus ponens but not under substitutions by constants.

Proof. To prove the first part of the proposition assume that P is closed under modus ponens and let p be the polynomial from the definition of closure under modus ponens. Let q_1 and q_2 be the polynomials from $P \leq Q$ and $Q \leq P$, respectively. If $Q \vdash_{\leq m} \varphi$ and $Q \vdash_{\leq n} \varphi \to \psi$ then $P \vdash_{\leq q_2(m)} \varphi$ and $P \vdash_{\leq q_2(n)} \varphi \to \psi$. By closure of P under modus ponens we have $P \vdash_{\leq p(q_2(m)+q_2(n))} \psi$ and by $P \leq Q$ we get $Q \vdash_{\leq q_1(p(q_2(m)+q_2(n)))} \psi$.

Robustness of closure under substitutions and substitutions by constants follow in an analogous manner.

To prove part 2 of the proposition let P be a non-optimal proof system that is closed under substitutions. Because P is not optimal we know by Theorem 7 below that there exists a polynomial time constructible sequence of tautologies ψ_n such that $P \nvdash_* \psi_n$. We may assume that the formulas ψ_n do not contain implications.

Let φ_n be an arbitrary polynomial time constructible sequence of tautologies with polynomially long P-proofs. We define the system Q as:

$$Q(\pi) = \begin{cases} P(\pi') & \text{if } \pi = 0\pi' \\ \sigma(\varphi_n \to \psi_n) & \text{if } \pi = 10^n 1\sigma \text{ for some substitution } \sigma \\ \top & \text{otherwise.} \end{cases}$$

Because P is closed under substitutions this is also true for Q according to the second line of its definition. From $P \vdash_* \varphi_n$ and $P \leq_p Q$ we get $Q \vdash_* \varphi_n$. We also have $Q \vdash_* \varphi_n \to \psi_n$ according to the definition of Q. By hypothesis we have $P \nvdash_* \psi_n$. Substitution instances of $\varphi_n \to \psi_n$ are different from the formulas ψ_n because the former are implications whereas the latter do not contain the connective $\to$. Therefore also $Q \nvdash_* \psi_n$ and hence Q is not closed under modus ponens.

To construct a proof system that is closed under modus ponens but not under substitutions by constants let P be a non-optimal line based proof system that has modus ponens available among its rules. Hence P is closed under modus ponens. Let φ_n be a sequence of polynomial time constructible tautologies with $P \nvdash_* \varphi_n$. Then the proof system $P \cup \{\varphi_n \,|\, n \geq 0\}$ is closed under modus ponens but not under substitutions by constants. □

Unfortunately, unlike the other properties, reflection is not robust as the next proposition shows.

Proposition 9. *For every regular non-optimal proof system P there exists a proof system $Q \equiv_p P$ that does not have the reflection property.*

Proof. Let P be a regular and non-optimal proof system. Because P is not optimal there exists a proof system R such that $R \not\leq P$. We define the system Q as:

$$Q(\pi) = \begin{cases} P(\pi') & \text{if } \pi = 0\pi' \\ R(\pi') & \text{if } \pi = 1\pi' \text{ and } R(\pi') \in \{\top, \bot\} \\ \top & \text{otherwise.} \end{cases}$$

Then P and Q are $\leq_p$-equivalent because $P \leq_p$-reduces to Q via $\pi \mapsto 0\pi$ and the opposite reduction $Q \leq_p P$ is given by:

$$\pi \mapsto \begin{cases} \pi' & \text{if } \pi = 0\pi' \\ \pi_0 & \text{if } \pi = 1\pi' \end{cases}$$

where π_0 is a P-proof of $\top$. We have to show that Q does not have the reflection property. Assume on the contrary that $Q \vdash_* \|\mathrm{RFN}(Q)\|$. $P \equiv_p Q$ implies that also $P \vdash_* \|\mathrm{RFN}(Q)\|$. Because of line 2 of the definition of Q this means that we can efficiently prove in P that there is no R-proof of $\bot$, i.e. P proves the consistency statement of R. For strong systems short proofs of the propositional consistency statements of a proof system imply short proofs of the reflection principle. Therefore $P \vdash_* \|\mathrm{RFN}(R)\|$. Because P is regular we infer with Lemma 6 $R \leq P$ in contradiction to the choice of the system R. Hence Q does not have reflection. □

3 NP-pairs Defined from Proof Systems

A pair (A, B) is called a disjoint NP-pair (DNPP), if $A, B \in \mathsf{NP}$ and $A \cap B = \emptyset$. A DNPP (A, B) is polynomially reducible to a DNPP (C, D) ($(A, B) \leq_p (C, D)$), if there exists a polynomial time computable function f such that $f(A) \subseteq C$ and $f(B) \subseteq D$. Note that because also elements from $\overline{A \cup B}$ can be mapped to $C \cup D$ a reduction $(A, B) \leq_p (C, D)$ does not in general imply that A and B are reducible to C and D, respectively. This is, however, the case for the following stronger reduction defined in [KMT03]: $(A, B) \leq_s (C, D)$ if there exists a function $f \in FP$ such that $f^{-1}(C) = A$ and $f^{-1}(D) = B$.

In order to speak about disjoint NP-pairs in proof systems we need to define a propositional encoding of NP-sets.

Definition 10. *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 a propositional description of NP-sets we can also represent disjoint NP-sets in propositional proof systems. This notion is captured by the next definition.

Definition 11. *Let P be a proof system. A disjoint* NP*-pair (A, B) is* representable in P *if there are representations $\varphi_n(\bar{x}, \bar{y})$ of A and $\psi_n(\bar{x}, \bar{z})$ of B such that $\bar{x}$ are the common variables of $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ and*

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

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

We remark that the provability of the disjointness of a pair (A, B) in some proof system depends crucially on the choice of the representations for A and B.

Proposition 12. *Let P be a non-optimal proof system that fulfills the following assumptions:*

1. *P is closed under conjunctions and can perform basic operations with formulas.*
2. *There exists a polynomial p such that for all formulas τ $P \vdash_{\leq m} \tau(\bar{u}) \vee \tau(\bar{v})$ implies $P \vdash_{\leq p(m)} \tau(\bar{u})$ where $\bar{u}$ and $\bar{v}$ are disjoint tuples of variables.*

Let $(A, B) \in \mathsf{DNPP}(P)$. Then there exist representations φ_n of A and ψ_n of B such that $P \nvdash_* \neg\varphi_n \vee \neg\psi_n$.

Proof. Let (A, B) be representable in P via the representations φ'_n and ψ'_n, i.e. $P \vdash_* \varphi'_n \vee \psi'_n$. Because P is not optimal there exists by Theorem 7 a sequence τ_n of hard tautologies for P. We define

$$\varphi_n(\bar{x}, \bar{y}, \bar{u}) = \varphi'_n(\bar{x}, \bar{y}) \vee \neg\tau_n(\bar{u})$$
$$\psi_n(\bar{x}, \bar{z}, \bar{v}) = \psi'_n(\bar{x}, \bar{z}) \vee \neg\tau_n(\bar{v})$$

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 $\varphi'_n(\bar{x}, \bar{y}) \vee \neg\tau_n(\bar{u})$ represents A. Similarly, ψ_n is a propositional representation for B. But P does not prove the disjointness of A and B with respect to the representations φ_n and ψ_n. Assume on the contrary that

$$P \vdash_* \neg\varphi_n \vee \neg\psi_n \ .$$

By definition this means

$$P \vdash_* \neg(\varphi'_n(\bar{x}, \bar{y}) \vee \neg\tau_n(\bar{u})) \vee \neg(\psi'_n(\bar{x}, \bar{z}) \vee \neg\tau_n(\bar{v})) \ .$$

P can perform basic operations with formulas. Hence we get polynomial size P-proofs of

$$(\neg\varphi'_n(\bar{x}, \bar{y}) \vee \neg\psi'_n(\bar{x}, \bar{z})) \wedge (\neg\varphi'_n(\bar{x}, \bar{y}) \vee \tau_n(\bar{v})) \wedge (\neg\psi'_n(\bar{x}, \bar{z}) \vee \tau_n(\bar{u})) \wedge (\tau_n(\bar{u}) \vee \tau_n(\bar{v})) \ .$$

Because P is closed under conjunctions we obtain

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

Using our extra assumption on P we derive $P \vdash_* \tau_n(\bar{u})$. This contradicts the choice of τ_n as hard tautologies for P. □

Razborov [Raz94] associates a disjoint NP-pair $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ with a proof system P with

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

$(\mathrm{Ref}(P), \mathrm{SAT}^*)$ is called the *canonical pair* of P. The canonical pair corresponds to the reflection principle of the proof system. Using the above terminology we can express this more precisely as: if P has reflection then $(\mathrm{Ref}(P), \mathrm{SAT}^*) \in \mathsf{DNPP}(P)$. Canonical pairs of strong systems provide candidates for complete NP-pairs. Namely, Razborov showed that if P is an optimal proof system then the canonical pair of P is $\leq_p$-complete for the class of all DNPP.

The canonical pair is also linked to the automatizability of the proof system, a concept that is of great relevance for automated theorem proving. In [BPR00] a proof system P is called *automatizable* if there exists a deterministic procedure

that takes as input a formula φ and outputs a P-proof of φ in time polynomial in the length of the shortest P-proof of φ provided that φ is a tautology. This is equivalent to the existence of a deterministic polynomial time algorithm that takes as input $(\varphi, 1^m)$ and produces a P-proof of φ if $(\varphi, 1^m) \in \mathrm{Ref}(P)$. From this reformulation of automatizability it is clear that automatizable proof systems have p-separable canonical pairs. The converse is probably not true as the following proposition shows.

Proposition 13. *There exists a proof system P that has a p-separable canonical pair. But P is not automatizable unless* $\mathsf{P} = \mathsf{NP}$.

Proof. We define the proof system P as follows:

$$P(\pi) = \begin{cases} \varphi & \text{if } \pi = (\varphi, 1^m) \text{ and } m \geq 2^{|\varphi|} \\ \varphi \vee \top & \text{if } \pi = (\varphi, \alpha) \text{ and } \alpha \text{ is a satisfying assignment for } \varphi \\ \top & \text{otherwise .} \end{cases}$$

The following algorithm separates the canonical pair of P:

```
1  Input: (φ, 1^m)
2  IF φ = ψ ∨ ⊤ or φ = ⊤ THEN output 1
3  IF m ≥ 2^|φ| THEN
4    IF φ ∈ TAUT THEN output 1
5  output 0 .
```

The test $\varphi \in \mathrm{TAUT}$ in line 4 can be performed in polynomial time by checking all assignments because the parameter m is big enough according to line 3. Hence the algorithm is efficient.

Since formulas $\varphi = \psi \vee \top$ are always tautological the algorithm only outputs 1 if the formula φ is a tautology. Therefore $(\varphi, 1^m) \in \mathrm{SAT}^*$ always leads to the answer 0 whereas inputs $(\varphi, 1^m) \in \mathrm{Ref}(P)$ are always answered by 1 according to lines 2 and 4.

The proof system P is not automatizable because this would mean that on input $\varphi \vee \top$ we would have to produce in polynomial time a satisfying assignment of φ provided $\varphi \in \mathrm{SAT}$. This implies in particular the existence of a deterministic polynomial time algorithm to decide SAT and hence $\mathsf{P} = \mathsf{NP}$. □

This example is not entirely satisfactory as the proof system constructed in the last proof is not very natural. But it might be hard to prove Proposition 13 for natural proof systems as it is conjectured that the canonical pairs of all studied proof systems are not p-separable (cf. [Pud03]). At least for proof systems stronger than bounded depth Frege systems we have good reason to believe that their canonical pairs are not p-separable because cryptographic pairs reduce to the canonical pairs of these systems [KP98,BPR00].

As we have seen the p-separability of the canonical pair might not imply the automatizability of the system but at least it implies that there exists a stronger automatizable system as the next theorem by Pudlák shows.

Theorem 14 (Pudlák [Pud03]). *Let P be a proof system. Then* $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ *is p-separable if and only if there exists an automatizable proof system Q which p-simulates P.*

This theorem indicates that instead of concentrating on automatizability it might be more important to investigate the p-separability of the canonical pairs. Therefore proof systems which have automatizable extensions $Q \geq_p P$ are called *weakly automatizable* (cf. [AB02]). Alekhnovich and Razborov establish in [AR01] the non-automatizability of resolution under an assumption from parameterized complexity

($W[P]$ is not tractable). The question whether resolution is weakly automatizable is still open. Atserias and Bonet [AB02] show that this question is equivalent to whether an extension of resolution $Res(2)$ has the efficient interpolation property.

Pudlák [Pud03] introduced a second NP-pair for a proof system:

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

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 efficient interpolation property. Efficient interpolation has been successfully used to show lower bounds to the proof size of a number of proof systems like resolution and cutting planes.

In [Bey04a] we have defined another kind of canonical pair which is quite similar to the previous pair and which corresponds to the stronger reduction $\leq_s$:

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

Using the correspondence to bounded arithmetic we proved in [Bey04a] the following:

Theorem 15. *Let P be a regular proof system. Then $(U_1(P), U_2)$ and $(I_1(P), I_2(P))$ are $\leq_s$-complete for $\mathsf{DNPP}(P)$. In particular $(U_1(P), U_2) \equiv_s (I_1(P), I_2(P))$.*

In Sect. 6 we will analyse this situation for non-regular proof systems.

4 A Weak Reduction Between Proof Systems

Besides $\leq$ and $\leq_p$ we can also study weaker reductions for propositional proof systems. In [KP89] a weak reduction $\leq'$ is defined between proof systems P and Q as follows: $P \leq' Q$ holds if for all polynomials p there exists a polynomial q such that

$$P \vdash_{\leq p(|\varphi|)} \varphi \quad \text{implies} \quad Q \vdash_{\leq q(|\varphi|)} \varphi$$

for all tautologies φ. Using the notation $\vdash_*$ which hides the actual polynomials we can also express the reduction $\leq'$ more compactly as: $P \leq' Q$ iff for all sets Φ of tautologies

$$P \vdash_* \Phi \quad \text{implies} \quad Q \vdash_* \Phi\ .$$

Let us try to motivate the above definition. If we express combinatorial principles in propositional logic or if we translate true arithmetic formulas into propositional logic as explained earlier we arrive at collections Φ of tautologies that typically contain one tautology per input length. We say that a proof system P proves a combinatorial principle or an arithmetic formula if there exist polynomially long P-proofs of the corresponding collection of tautologies. If $P \leq Q$ then every principle that is provable in P is also provable in Q. The Q-proofs are allowed to be longer than the P-proofs but only up to fixed polynomial amount independent of the principle proven. The reduction $\leq'$ is more flexible as it allows a different polynomial increase for each principle.

To prove $P \not\leq Q$ one typically shows super-polynomial lower bounds on the length of Q-proofs of some principle like e.g. the pigeon hole principle whereas the principle is provable in P. As basically all separations between proof systems are achieved in this manner all these results also separate the corresponding proof systems with respect to the weaker $\leq'$-reduction.

To further motivate the definition we remark that we can characterize an ordinary $\leq$-simulation of P by Q by

$$(\exists q \in \mathrm{Poly})(\forall p \in \mathrm{Poly})(\forall \varphi)\ P \vdash_{\leq p(|\varphi|)} \varphi \implies Q \vdash_{\leq q(p(|\varphi|))} \varphi$$

where Poly denotes the set of all polynomials. On the other hand it is easily seen that $P \leq' Q$ holds iff

$$(\forall p \in \mathrm{Poly})(\exists q \in \mathrm{Poly})(\forall \varphi)\ P \vdash_{\leq p(|\varphi|)} \varphi \implies Q \vdash_{\leq q(p(|\varphi|))} \varphi\ .$$

Hence we get the definition of $\leq'$ by changing the order of the quantifiers from $\exists q \forall p$ to $\forall p \exists q$ in the above characterization of $\leq$.

It is clear from the above explanation that $\leq$ is a refinement of $\leq'$. We first observe that it is indeed a proper refinement, i.e. we can separate $\leq$ and $\leq'$. It is, however, not possible to achieve this separation with regular proof systems.

Proposition 16. *1. Let P be a proof system that is not polynomially bounded. Then there exists a proof system Q such that $P \leq' Q$ but $P \not\leq Q$.*
2. Let P and Q be regular proof systems. Then $P \leq' Q$ implies $P \leq Q$.

Proof. To prove part 1 let P be a proof system that is not polynomially bounded. We define the system Q. Q-proofs consist of multiple copies of P-proofs where the number of copies depends on the length of the P-proof, more precisely $Q(\pi) = \varphi$ iff there exists a P-proof π' of φ such that $\pi = (\pi')^l$ where the number l of the copies of π' is determined as follows. Let k be a number such that $|\varphi|^{k-1} \leq |\pi'| < |\varphi|^k$. Then l is chosen as $l = |\varphi|^{(k-1)k}$. Hence we have

$$|\varphi|^{k-1}|\varphi|^{(k-1)k} = |\varphi|^{k^2-1} \leq |\pi| < |\varphi|^k|\varphi|^{(k-1)k} = |\varphi|^{k^2}\ .$$

P is $\leq'$-simulated by Q because for each polynomial p majorized by n^k we can choose q as n^{k^2}, i.e.

$$P \vdash_{\leq |\varphi|^k} \varphi \implies Q \vdash_{\leq |\varphi|^{k^2}} \varphi\ .$$

But if P is not polynomially bounded then there is apparently no polynomial q such that

$$P \vdash_{\leq m} \varphi \implies Q \vdash_{\leq q(m)} \varphi\ ,$$

i.e. $P \not\leq Q$.

Now we prove part 2. Let P and Q be regular proof systems such that $P \leq' Q$. The regularity of P implies $P \vdash_* \|\mathrm{RFN}(P)\|^n$. Because $P \leq' Q$ we also have $Q \vdash_* \|\mathrm{RFN}(P)\|^n$. Since also Q is regular we can use Lemma 6 to infer $P \leq Q$ as claimed. □

We call a proof system $\leq'$-optimal if it $\leq'$-simulates all proof systems. Krajíček and Pudlák [KP89] proved that the existence of a $\leq'$-optimal proof system already implies the existence of an optimal proof system. Comparing $\leq$ and $\leq_p$ it is interesting to mention that it is neither known how to separate these reductions nor how to infer from the existence of an optimal proof system the existence of a p-optimal proof system. For the sake of completeness we give a proof.

Theorem 17 ([KP89]). *There exists an optimal proof system if and only if there exists a $\leq'$-optimal proof system.*

Proof. The forward direction is immediate as $\leq$ is a refinement of $\leq'$.

For the reverse implication let P be a $\leq'$-optimal proof system. We claim that the proof system

$$P' = EF + \|\mathrm{RFN}(P)\|$$

is optimal. To see this let Q be a proof system. Consider the proof system $Q' = EF + \|\mathrm{RFN}(Q)\|$. Obviously $Q' \vdash_* \|\mathrm{RFN}(Q)\|^n$. Because P is $\leq'$-optimal we have $Q' \leq' P$ and hence $P \vdash_* \|\mathrm{RFN}(Q)\|^n$. From the definition of P' and Proposition 5 we get $P \leq_p P'$ and therefore also $P' \vdash_* \|\mathrm{RFN}(Q)\|^n$. Since P' is regular we infer with Lemma 6 $Q \leq P'$ as desired. □

As Razborov in [Raz94] already noted that optimal proof systems imply complete DNPP we can formulate the following corollary:

Corollary 18. *If there exists a $\leq'$-optimal proof system then there exist disjoint NP-pairs which are $\leq_p$- and $\leq_s$-complete for the class of all DNPP.*

5 Proof Systems with Equivalent Canonical Pairs

The simulation order of proof systems is reflected in reductions between canonical pairs as the following well known proposition shows (see e.g. [Pud03]):

Proposition 19. *If P and Q are proof systems with $P \leq Q$ then the canonical pair of P is $\leq_p$-reducible to the canonical pair of Q.*

Proof. The reduction is given by $(\varphi, 1^m) \mapsto (\varphi, 1^{p(m)})$ where p is the polynomial from $P \leq Q$. □

If $P \not\leq Q$ then we can not hope to reduce $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ to $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ by a reduction of the form $(\varphi, 1^m) \mapsto (\varphi, 1^n)$ that changes only the proof length but leaves the formula unchanged. However, unlike in the case of simulations between proof systems the reductions between canonical pairs have the flexibility to change the formula.

The aim of this section is to provide different techniques for the construction of non-equivalent proof systems with equivalent pairs. One such example is given by Pudlák in [Pud03] where he shows that two versions of the cutting planes proof system CP which do not $\leq$-simulate each other have $\leq_p$-equivalent canonical pairs. Here we search for general conditions on proof systems which imply the equivalence of the canonical pairs. The first condition will be the $\leq'$-equivalence of the proof systems. For this we show an analogue of Proposition 19 for $\leq'$.

Proposition 20. *Let P be a proof system that is closed under disjunctions and let Q be a proof system such that $P \leq' Q$. Then $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$.*

Proof. We claim that for some suitable polynomial q the mapping

$$(\varphi, 1^m) \mapsto (\varphi \vee \bot^m, 1^{q(m)})$$

performs the desired $\leq_p$-reduction where $\bot^m$ stands for $\bot \vee \ldots \vee \bot$ (m disjuncts). To see this let first $(\varphi, 1^m) \in \mathrm{Ref}(P)$. Because P is closed under disjunctions there exists a polynomial p such that $P \vdash_{\leq m} \varphi$ implies $P \vdash_{\leq p(m)} \varphi \vee \bot^m$. Because of $P \leq' Q$ there is a polynomial q such that $Q \vdash_{\leq q(m)} \varphi \vee \bot^m$, i.e $(\varphi \vee \bot^m, 1^{q(m)}) \in \mathrm{Ref}(Q)$.

If $(\varphi, 1^m) \in \mathrm{SAT}^*$ then the satisfiability of $\neg\varphi$ is transferred to $\neg(\varphi \vee \bot^m) = \neg\varphi \wedge \top \wedge \ldots \wedge \top$. □

Combining Propositions 16 and 20 we get the afore mentioned counterexamples to the converse of Proposition 19.

Corollary 21. *Let P be a proof system that is closed under disjunctions and is not polynomially bounded. Then there exists a proof system Q such that*

$$P \not\equiv Q \quad \textit{and} \quad (\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(Q), \mathrm{SAT}^*) \ .$$

Proof. The proof system Q constructed from P in Proposition 16 fulfills $P \leq' Q \leq P$ and $P \not\leq Q$. Hence $P \not\equiv Q$.

By Proposition 19 we have $(\mathrm{Ref}(Q), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ and applying Proposition 20 we conclude $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$. □

The proof systems P and Q from the last corollary have equivalent canonical pairs and are also $\leq'$-equivalent. Moreover it follows from Proposition 20 that the canonical pair of a disjunctively closed proof system is already determined by the $\leq'$-degree of the system. More precisely:

Proposition 22. *Let P and Q be $\leq'$-equivalent proof systems that are closed under disjunctions. Then $(\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$.*

Nevertheless we can also construct proof systems that have equivalent canonical pairs but are not $\leq'$-equivalent. We show this in the next proposition.

Proposition 23. *Let P be a proof system that is not optimal. Then there exists a proof system Q such that*

$$Q \not\equiv' P \quad \text{and} \quad (\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(Q), \mathrm{SAT}^*) \ .$$

Proof. Because P is not optimal there exists by Theorem 7 a sequence of polynomial time constructible tautologies φ_n such that $P \nvdash_* \varphi_n$. We define Q as

$$Q(\pi) = \begin{cases} P(\pi') & \text{if } \pi = 0\pi' \\ \varphi_n & \text{if } \pi = 1\varphi_n \text{ for some } n \\ \top & \text{otherwise.} \end{cases}$$

Clearly $P \leq Q$ and therefore $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$. The converse reduction from $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ to $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ is given by

$$(\varphi, 1^m) \mapsto \begin{cases} (\psi, 1^k) & \text{if } \varphi = \varphi_n \text{ for some } n \text{ or } \varphi = \top \\ (\varphi, 1^{m-1}) & \text{otherwise} \end{cases}$$

where ψ is some fixed tautology with a P-proof of length k.

Finally, since $P \nvdash_* \varphi_n$ and $Q \vdash_* \varphi_n$ we have $Q \not\leq' P$. □

The proof systems Q constructed in Proposition 23 have the drawback that they do not satisfy the normality conditions from Sect. 2. In the next proposition we will construct proof systems with somewhat better properties.

Proposition 24. *Let P be a line based proof system that allows efficient deduction and let Φ be a sparse set of tautologies which can be generated in polynomial time. Then*

$$(\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*) \ .$$

Proof. As P is simulated by $P \cup \Phi$ we get

$$(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*) \ .$$

Now we describe the converse reduction. Let p be the polynomial from the efficient deduction property of P. Because Φ is a sparse set there exists a polynomial q such that for each number m Φ contains at most $q(m)$ tautologies of length $\leq m$. Let $\Phi_m = \Phi \cap \Sigma^{\leq m}$ be the set of these tautologies.

Then $(\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*)$ reduces to $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ via the function

$$(\psi, 1^m) \ \mapsto \ (\ (\bigwedge_{\varphi \in \Phi_m} \varphi) \to \psi, 1^{p(mq(m)+m)}) \ .$$

To verify the claim assume that $(\psi, 1^m) \in \mathrm{Ref}(P \cup \Phi)$. Let π be a $P \cup \Phi$-proof of ψ of length $\leq m$. This proof π can use only formulas of length $\leq m$ from Φ of which there are only $\leq q(m)$ many. Hence the tautologies used in the proof π are contained in $\bigwedge_{\varphi \in \Phi_m} \varphi$. Therefore we know that π is also a proof for ψ in the proof system $P \cup \Phi_m$. Using the efficient deduction property of P we get a P-proof of size $\leq p(mq(m) + m)$ of $(\bigwedge_{\varphi \in \Phi_m} \varphi) \to \psi$.

Now assume $(\psi, 1^m) \in \mathrm{SAT}^*$. Then $\neg\psi$ is satisfiable and therefore

$$\neg((\bigwedge_{\varphi \in \Phi_m} \varphi) \to \psi) \;=\; (\bigwedge_{\varphi \in \Phi_m} \varphi) \wedge \neg\psi$$

is also satisfiable because $(\bigwedge_{\varphi \in \Phi_m} \varphi)$ is a tautology. □

By Theorem 7 we know that for any non-optimal proof system we can find a sequence of hard tautologies. Hence we get:

Corollary 25. *For any non-optimal line based proof system P that admits efficient deduction there exists a sparse set Φ of tautologies which can be generated in polynomial time such that*

$$P \cup \Phi \not\leq' P \quad \textit{and} \quad (\mathrm{Ref}(P), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(P \cup \Phi), \mathrm{SAT}^*) \ .$$

Because EF admits efficient deduction (Theorem 1) we can formulate the following corollary:

Corollary 26. *Let Φ be a sparse set of tautologies which can be generated in polynomial time. Then we have*

$$(\mathrm{Ref}(EF), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(EF \cup \Phi), \mathrm{SAT}^*) \ .$$

As explained in Sect. 2 every proof system P is simulated by $EF + \|\mathrm{RFN}(P)\|$. Clearly $\|\mathrm{RFN}(P)\|$ is a sparse polynomial time set of tautologies. From this information together with Corollary 26 it might be tempting to deduce that the canonical pair of EF is $\leq_p$-complete for the class of all disjoint NP-pairs. The problem, however, is that Corollary 26 only holds for the system $EF \cup \|\mathrm{RFN}(P)\|$ whereas to show the $\leq_p$-completeness of $(\mathrm{Ref}(EF), \mathrm{SAT}^*)$ we would need it for $EF + \|\mathrm{RFN}(P)\|$. We can formulate this observation somewhat differently as:

Proposition 27. *At least one of the following is true:*

1. *The canonical pair of EF is complete for the class of all disjoint NP-pairs.*
2. *There exists a proof system P such that*

$$EF \;\leq_p\; EF \cup \|\mathrm{RFN}(P)\| \;\leq_p\; EF + \|\mathrm{RFN}(P)\|$$

is a chain of pairwise non-equivalent proof systems.

Proof. Assume that 2 fails. We will show that $(\mathrm{Ref}(EF), \mathrm{SAT}^*)$ is complete for the class of all DNPP. To prove this let (A, B) be a disjoint NP-pair. Choose some proof system P such that (A, B) is representable in P and P is closed under substitutions by constants and modus ponens and can evaluate formulas without variables. Because (A, B) is representable in P we can use Proposition 29 below to infer that

$$(A, B) \;\leq_p\; (\mathrm{Ref}(P), \mathrm{SAT}^*) \ .$$

Since condition 2 fails for P we have $EF \equiv EF \cup \|\mathrm{RFN}(P)\|$ or $EF \cup \|\mathrm{RFN}(P)\| \equiv EF + \|\mathrm{RFN}(P)\|$. If $EF \equiv EF \cup \|\mathrm{RFN}(P)\|$ then $EF \vdash_* \|\mathrm{RFN}(P)\|$. By Lemma 6 this implies $P \leq EF$ and hence Proposition 19 yields

$$(A, B) \leq_p (\mathrm{Ref}(EF), \mathrm{SAT}^*) \ .$$

Now assume that $EF \cup \|\mathrm{RFN}(P)\| \equiv EF + \|\mathrm{RFN}(P)\|$ is satisfied for P. By Proposition 5

$$P \ \leq_p \ EF + \|\mathrm{RFN}(P)\|$$

and hence

$$(\mathrm{Ref}(P), \mathrm{SAT}^*) \ \leq_p \ (\mathrm{Ref}(EF + \|\mathrm{RFN}(P)\|), \mathrm{SAT}^*) \ .$$

By assumption we have

$$EF + \|\mathrm{RFN}(P)\| \ \leq \ EF \cup \|\mathrm{RFN}(P)\| \ .$$

Hence Proposition 19 and Corollary 26 give us

$$(\mathrm{Ref}(EF+\|\mathrm{RFN}(P)\|), \mathrm{SAT}^*) \ \leq_p \ (\mathrm{Ref}(EF\cup\|\mathrm{RFN}(P)\|), \mathrm{SAT}^*) \ \leq_p \ (\mathrm{Ref}(EF), \mathrm{SAT}^*) \ .$$

Combining all these reductions we arrive at

$$(A, B) \ \leq_p \ (\mathrm{Ref}(EF), \mathrm{SAT}^*) \ ,$$

as desired. □

6 The Complexity Class DNPP(P)

In this section we investigate $\mathsf{DNPP}(P)$ for non-regular proof systems. Translating the reductions to the propositional level we have to work with uniform circuit families computing the reduction functions. We start by giving sufficient conditions for the closure of $\mathsf{DNPP}(P)$ under $\leq_p$. Since it is possible in resolution to prove the uniqueness of circuit computations we can show the following:

Proposition 28. *Let P be a proof system which simulates resolution and is closed under disjunctions. Then $\mathsf{DNPP}(P)$ is closed under $\leq_p$.*

Proof. Let (A, B) and (C, D) be disjoint NP-pairs. Let (C, D) be representable in P, i.e. there exist representations $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ of C and D, respectively, such that

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

Assume further that (A, B) is $\leq_p$-reducible to (C, D) via the polynomial time computable function f. We have to show that also (A, B) is representable in P. For this we fix arbitrary representations $\chi_n(\bar{x}, \bar{r})$ and $\theta_n(\bar{x}, \bar{s})$ for A and B, respectively. Without loss of generality we may assume that the reduction function f generates on inputs of length n outputs of length exactly $p(n)$ for some fixed polynomial p. This can be achieved for example by adding leading zeros to outputs of length $\leq p(n)$. Let

$$C_n : \{0,1\}^n \to \{0,1\}^{p(n)}$$

be a uniform circuit family which computes the function f. The computation of the circuits C_n can be described by propositional formulas $C_n(\bar{x}, \bar{p}, \bar{u})$ which state that on input corresponding to the propositional variables $\bar{x}$ the circuit produces the output corresponding to $\bar{p}$. The variables $\bar{u}$ are auxiliary variables for the gates of the circuit.

Consider the sequence of propositional formulas

$$\chi_n(\bar{x}, \bar{r}) \wedge C_n(\bar{x}, \bar{p}, \bar{u}) \wedge \varphi_{p(n)}(\bar{p}, \bar{y}) \ . \tag{1}$$

These formulas provide a propositional representation of the set A because they propositionally express that $\bar{x} \in A$ and there exists a computation of C_n on input $\bar{x}$ that outputs an element from the set C. Similarly the sequence

$$\theta_n(\bar{x}, \bar{s}) \wedge C_n(\bar{x}, \bar{q}, \bar{v}) \wedge \psi_{p(n)}(\bar{q}, \bar{z}) \tag{2}$$

represents B. We have to check that P proves the disjointness of A and B with respect to these representations. The P-proof proceeds along the following lines. By hypothesis we have polynomial size P-proofs for the formulas

$$\neg\varphi_{p(n)}(\bar{p},\bar{y}) \vee \neg\psi_{p(n)}(\bar{p},\bar{z}) \ . \tag{3}$$

By induction on the number of gates of a circuit we can show that resolution proves the uniqueness of computations of Boolean circuits in polynomial size resolution proofs. Because P simulates resolution this means that we have polynomial size P-proofs of the formulas

$$C_n(\bar{x},\bar{p},\bar{u}) \wedge C_n(\bar{x},\bar{q},\bar{v}) \ \rightarrow \ (\bar{p} \leftrightarrow \bar{q}) \ . \tag{4}$$

From (3) and (4) we obtain polynomial size P-proofs of

$$C_n(\bar{x},\bar{p},\bar{u}) \wedge C_n(\bar{x},\bar{q},\bar{v}) \ \rightarrow \ \neg\varphi_{p(n)}(\bar{p},\bar{y}) \vee \neg\psi_{p(n)}(\bar{q},\bar{z}) \ . \tag{5}$$

Because P is closed under disjunctions we get from (5) polynomial size P-proofs of

$$\neg\chi_n(\bar{x},\bar{r}) \vee \neg\theta_n(\bar{x},\bar{s}) \vee \neg C_n(\bar{x},\bar{p},\bar{u}) \vee \neg C_n(\bar{x},\bar{q},\bar{v}) \vee \neg\varphi_{p(n)}(\bar{p},\bar{y}) \vee \neg\psi_{p(n)}(\bar{q},\bar{z}) \ .$$

But this exactly means that P proves the disjointness of A and B with respect to the propositional representations (1) and (2). Hence $(A,B) \in \mathsf{DNPP}(P)$. □

Next we show the hardness of the canonical pair for $\mathsf{DNPP}(P)$ for non-regular proof systems P.

Proposition 29. *Let P be a proof system that is closed under substitutions by constants and modus ponens and can evaluate formulas without variables. Then $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ is $\leq_p$-hard for $\mathsf{DNPP}(P)$.*

Proof. Let (A,B) be a DNPP and let $\varphi_n(\bar{x},\bar{y})$ and $\psi_n(\bar{x},\bar{z})$ be propositional representations of A and B, respectively, such that

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

We have to show that

$$(A,B) \ \leq_p \ (\mathrm{Ref}(P), \mathrm{SAT}^*) \ .$$

We claim that the reduction is given by

$$a \ \mapsto \ (\neg\psi_{|a|}(\bar{a},\bar{z}), 1^{p(|a|)})$$

for some suitable polynomial p. To see the correctness of the reduction let first be $a \in A$. Then there exists a witness b such that $\models \varphi_{|a|}(\bar{a},\bar{b})$. From the P-proof of $\neg\varphi_{|a|}(\bar{x},\bar{y}) \vee \neg\psi_{|a|}(\bar{x},\bar{z})$ we get by substituting $\bar{a}$ for $\bar{x}$ and $\bar{b}$ for $\bar{y}$ a polynomially longer P-proof of $\neg\varphi_{|a|}(\bar{a},\bar{b}) \vee \neg\psi_{|a|}(\bar{a},\bar{z})$. $\neg\varphi_{|a|}(\bar{a},\bar{b})$ is a false propositional formula without free variables and hence can be refuted with polynomial size P-proofs. An application of modus ponens gives a P-proof of $\neg\psi_{|a|}(\bar{a},\bar{z})$ as desired.

Assume now $a \in B$. Then $\neg\neg\psi_{|a|}(\bar{a},\bar{z}) = \psi_{|a|}(\bar{a},\bar{z})$ is satisfiable and hence $(\neg\psi_{|a|}(\bar{a},\bar{z}), 1^{p(|a|)}) \in \mathrm{SAT}^*$. □

The next proposition shows that the hypothesis that P is closed under substitutions by constants seems indeed to be necessary.

Proposition 30. *For all disjoint NP-pairs (A,B) which are not $\leq_p$-reducible to $(\mathrm{Ref}(EF), \mathrm{SAT}^*)$ there exists a proof system P with the following properties:*

1. *P evaluates formulas without variables and is closed under modus ponens.*

2. (A, B) *is representable in* P.
3. $(A, B) \not\leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$.

Proof. Let $(A, B) \not\leq_p (\mathrm{Ref}(EF), \mathrm{SAT}^*)$. Choose some representations φ_n and ψ_n of A and B, respectively. We define the system P as

$$P = EF \cup \{\neg\varphi_n \vee \neg\psi_n \mid n \geq 0\} \ .$$

Clearly P can evaluate formulas without variables and is closed under modus ponens. By definition we have $P \vdash_* \neg\varphi_n \vee \neg\psi_n$, hence (A, B) is representable in P. By Corollary 26 we have $(\mathrm{Ref}(EF), \mathrm{SAT}^*) \equiv_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$. Hence $(A, B) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ would imply $(A, B) \leq_p (\mathrm{Ref}(EF), \mathrm{SAT}^*)$ in contradiction to our assumption. □

Disjoint NP-pairs $(A, B) \not\leq_p (\mathrm{Ref}(EF), \mathrm{SAT}^*)$ exist if $(\mathrm{Ref}(EF), \mathrm{SAT}^*)$ is not $\leq_p$-complete for the class of all DNPP. By using Proposition 24 we can also establish a version of Proposition 30 for other line based proof systems which admit efficient deduction.

We can interpret Propositions 29 and 30 in such a way that the canonical pairs of sufficiently well defined proof systems like regular proof systems are meaningful as complete pairs for some class of DNPP but that this property is lost for canonical pairs defined from arbitrary proof systems. Therefore the canonical pairs of regular proof systems seem to deserve special attention.

Analogously to Proposition 29 we can also prove a propositional variant of Theorem 15.

Proposition 31. *Let P be a proof system that is closed under substitutions by constants. Then $(U_1(P), U_2)$ is $\leq_s$-hard for* DNPP(P).

Proof. Let (A, B) be a DNPP and let $\varphi_n(\bar{x}, \bar{y})$ and $\psi_n(\bar{x}, \bar{z})$ be propositional representations of A and B, respectively, such that

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

We claim that there exists a polynomial p such that

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

realizes a $\leq_s$-reduction from (A, B) to $(U_1(P), U_2)$.

Let first a be an element from A of length n. Because $\varphi_n(\bar{x}, \bar{y})$ represents A the formula $\varphi_n(\bar{a}, \bar{y})$ is satisfiable. As P is closed under substitutions by constants we have

$$P \ \vdash_{\leq p(n)} \ \neg\varphi_n(\bar{a}, \bar{y}) \vee \neg\psi_n(\bar{a}, \bar{z})$$

for the appropriate polynomial p. This confirms that $(\neg\varphi_n(\bar{a}, \bar{y}), \neg\psi_n(\bar{a}, \bar{z}), 1^{p(n)}) \in U_1(P)$.

If $a \in B$ then $\psi_{|a|}(\bar{a}, \bar{z})$ is satisfiable and hence $(\neg\varphi_{|a|}(\bar{a}, \bar{y}), \neg\psi_{|a|}(\bar{a}, \bar{z}), 1^{p(|a|)}) \in U_2$.

If $a \notin A \cup B$ then neither $\varphi_{|a|}(\bar{a}, \bar{y})$ nor $\psi_{|a|}(\bar{a}, \bar{z})$ is satisfiable and hence $(\neg\varphi_{|a|}(\bar{a}, \bar{z}), \neg\psi_{|a|}(\bar{a}, \bar{z}), 1^{p(|a|)}) \notin U_1(P) \cup U_2$. □

The next proposition contains the well known observation (see e.g. [Pud03]) that the reflection property of a proof system corresponds to the representability of the canonical pair in the proof system.

Proposition 32. *Let P be a proof system. Then P has the reflection property if and only if the canonical pair of P is representable in P with respect to the standard representations of* $\mathrm{Ref}(P)$ *and* SAT^*.

Proof. By the standard representation of $\mathrm{Ref}(P)$ and SAT^* we mean the $\|.\|$-translations of the first order formulas

$$(\exists \pi)\ |\pi| \leq m \wedge \mathrm{Prf}_P(\pi, \varphi)$$

for $\mathrm{Ref}(P)$ and

$$(\exists \alpha)\ |\alpha| \leq |\varphi| \wedge \alpha \models \neg\varphi$$

for SAT^*. The representability of $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ with respect to these representations means

$$P \vdash_* \|(\varphi, 1^m) \notin \mathrm{Ref}(P) \vee (\varphi, 1^m) \notin \mathrm{SAT}^*\|^{n,m} \ ,$$

i.e.

$$P \vdash_* \|\neg \mathrm{Prf}_P(\pi, \varphi) \vee \alpha \not\models \neg\varphi\|^{n,m} \ .$$

$(\forall \alpha)\ |\alpha| \leq |\varphi| \wedge \alpha \not\models \neg\varphi$ is equivalent to $\mathrm{Taut}(\varphi)$, hence

$$P \vdash_* \|\neg \mathrm{Prf}_P(\pi, \varphi) \vee \mathrm{Taut}(\varphi)\|^{n,m} \ ,$$

i.e.

$$P \vdash_* \|\mathrm{Prf}_P(\pi, \varphi) \rightarrow \mathrm{Taut}(\varphi)\|^{n,m} \ ,$$

which is by definition $P \vdash_* \|\mathrm{RFN}(P)\|$. □

Hence the Propositions 29 and 31 immediately imply:

Proposition 33. *Let P be a proof system that has the reflection property. Assume further that P is closed under substitutions by constants, modus ponens and disjunctions and can evaluate formulas without variables. Then the following holds.*

1. $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ *is $\leq_p$-complete for* $\mathsf{DNPP}(P)$.
2. $(U_1(P), U_2)$ *is $\leq_s$-complete for* $\mathsf{DNPP}(P)$.

Proof. The first part follows directly from Propositions 29 and 32.

For the second part we can use a reduction from $(U_1(P), U_2)$ to $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ as given by Proposition 35 below to infer with Propositions 28 and 32 that $(U_1(P), U_2)$ is representable in P. Together with Proposition 31 this yields the $\leq_s$-completeness of $(U_1(P), U_2)$ for $\mathsf{DNPP}(P)$. □

What is actually needed for Proposition 33 is not the reflection property of P but the representability of $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ in the proof system P. As we pointed out in Proposition 32 reflection for P implies $(\mathrm{Ref}(P), \mathrm{SAT}^*) \in \mathsf{DNPP}(P)$. The converse, however, is not true as we show in the next proposition.

Proposition 34. *Let P be a regular proof system. Let further Q be proof system such that*

$$Q \not\leq P \quad \textit{but} \quad (\mathrm{Ref}(Q), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*) \ .$$

Then $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ is representable in P but the disjointness of $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ is not provable in P with respect to the standard representation of $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$.

Proof. Suppose the function f performs the $\leq_p$-reduction from $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ to $(\mathrm{Ref}(P), \mathrm{SAT}^*)$. From this we conclude with Propositions 28 and 32 the representability of $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ in P. Going back to the proof of Proposition 28 we see that P proves the disjointness of $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ with respect to the following representations:

$$\mathrm{Ref}(Q) = \{(\varphi, 1^m) \mid (\varphi, 1^m) \in \mathrm{Ref}(Q) \text{ and } f(\varphi, 1^m) \in \mathrm{Ref}(P)\}$$

and

$$\mathrm{SAT}^* = \{(\varphi, 1^m) \mid (\varphi, 1^m) \in \mathrm{SAT}^* \text{ and } f(\varphi, 1^m) \in \mathrm{SAT}^*\} \ .$$

But if P proves the disjointness of $(\mathrm{Ref}(Q), \mathrm{SAT}^*)$ with respect to the standard representations

$$\mathrm{Ref}(Q) = \{(\varphi, 1^m) \mid (\exists \pi)\ |\pi| \leq m \wedge \mathrm{Prf}_P(\pi, \varphi)\}$$

and

$$\mathrm{SAT}^* = \{(\varphi, 1^m) \mid (\exists \alpha)\ |\alpha| \leq |\varphi| \wedge \alpha \models \neg\varphi\}$$

this means $P \vdash_* \|\mathrm{RFN}(Q)\|$ and by Lemma 6 we get $Q \leq P$ in contradiction to the hypothesis $Q \not\leq P$. □

We summarize the results obtained so far in this section in the following table:

proof system P	$(\mathrm{Ref}(P), \mathrm{SAT}^*)$	$(U_1(P), U_2)$	$(I_1(P), I_2(P))$	closed under
resolution, CP	$\leq_p$-hard*	$\leq_s$-hard*	p-separable	subst. + MP
$EF + \Phi$	$\leq_p$-complete*	$\leq_s$-compl.*	$\leq_s$-compl.*	subst. + MP
$EF \cup \Phi$	not $\leq_p$-hard for $\mathsf{DNPP}(P)$**			MP

* for $\mathsf{DNPP}(P)$ ** unless $(\mathrm{Ref}(EF), \mathrm{SAT}^*)$ is a $\leq_p$-complete pair

In the second row the statements apply to all proof systems $EF + \Phi$ for polynomial time sets $\Phi \subseteq \mathrm{TAUT}$ according to Theorem 15. The last row requires a suitable choice of the polynomial time set $\Phi \subseteq \mathrm{TAUT}$ as in the proof of Proposition 30. Additionally, to prove that a particular pair is not $\leq_p$-hard for some class of DNPP we need a suitable hypothesis, in this case that $(\mathrm{Ref}(EF), \mathrm{SAT}^*)$ is not $\leq_p$-complete for the class of all DNPP. It would be interesting to weaken or modify this hypothesis but some assumption is certainly necessary as $\mathsf{P} = \mathsf{NP}$ for example implies that all pairs with nonempty components are $\leq_p$-complete for the class of all DNPP.

For regular proof systems we have shown the $\leq_s$-equivalence of $(U_1(P), U_2)$ and $(I_1(P), I_2(P))$ as well as the $\leq_p$-equivalence of $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ and $(U_1(P), U_2)$. Now we investigate these reductions for other proof systems for which we can not use the strong tools of arithmetic theories. The canonical pairs of such proof systems as resolution or CP are nevertheless of great interest. We start with the relationship between $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ and $(U_1(P), U_2)$.

Proposition 35. *1. Let P be a proof system that is closed under disjunctions. Then $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (U_1(P), U_2)$.*

2. Let P be a proof system that is closed under substitutions by constants and modus ponens and evaluates formulas without variables. Then $(U_1(P), U_2) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$.

Proof. The first reduction is given by

$$(\varphi, 1^m) \mapsto (\bot, \varphi, 1^{p(m)})\ .$$

for a suitable polynomial p. To verify the correctness of the reduction let first $(\varphi, 1^m) \in \mathrm{Ref}(P)$. This means that $P \vdash_{\leq m} \varphi$ and because P is closed under disjunctions we infer $P \vdash_{\leq p(m)} \varphi \vee \bot$ for the respective polynomial p. We assume that the variables of φ and $\bot$ are chosen disjoint and since $\neg\bot = \top$ is satisfiable we get $(\bot, \varphi, 1^{p(m)}) \in U_1(P)$.

If $(\varphi, 1^m) \in \mathrm{SAT}^*$ then $\neg\varphi$ is satisfiable, hence $(\bot, \varphi, 1^{p(m)}) \in U_2$.

The reduction in part 2 of this proposition is performed by

$$(\varphi, \psi, 1^m) \mapsto (\psi, 1^{p(m)})$$

for some suitable polynomial p depending on the proof system P.

To verify the reduction let first $(\varphi(\bar{x}), \psi(\bar{y}), 1^m) \in U_1(P)$. Then $P \vdash_{\leq m} \varphi(\bar{x}) \vee \psi(\bar{y})$ and $\neg\varphi(\bar{x}) \in \mathrm{SAT}$. Choose a satisfying assignment $\bar{a}$ for $\neg\varphi(\bar{x})$. Because P

is closed under substitutions by constants we get polynomially long P-proofs of $\varphi(\bar{a}) \vee \psi(\bar{y})$. $\varphi(\bar{a})$ is a false propositional formula without variables which can be evaluated in P to $\bot$ in polynomially long proofs. Using modus ponens we obtain a P-proof of $\psi(\bar{y})$.

If $(\varphi, \psi, 1^m) \in U_2$ then $\neg\psi \in \mathrm{SAT}$ and hence $(\psi, 1^m) \in \mathrm{SAT}^*$. □

Now we come to the question how the interpolation pair $(I_1(P), I_2(P))$ compares to $(U_1(P), U_2)$. For regular proof systems this question is settled by Theorem 15. Clearly, for all proof systems $(\varphi, \psi, \pi) \mapsto (\varphi, \psi, 1^{|\pi|})$ computes a $\leq_p$-reduction from $(I_1(P), I_2(P))$ to $(U_1(P), U_2)$. For weak systems like resolution or cutting planes the opposite reduction is not possible unless the system is weakly automatizable. This is the contents of the next proposition.

Proposition 36. *Let P be a proof system that has the feasible interpolation property and is closed under disjunctions. Then $(U_1(P), U_2) \leq_p (I_1(P), I_2(P))$ implies that P is weakly automatizable.*

Proof. Feasible interpolation for P means that $(I_1(P), I_2(P))$ is p-separable. Therefore $(U_1(P), U_2) \leq_p (I_1(P), I_2(P))$ implies that also $(U_1(P), U_2)$ is p-separable. Closure of P under disjunctions together with Proposition 35 guarantees

$$(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (U_1(P), U_2) \ ,$$

hence also $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ is p-separable and therefore P is weakly automatizable. □

Of course we can use part 2 of Proposition 35 together with an analogous argument as above to infer that weak automatizability of P is also a sufficient condition to reduce $(U_1(P), U_2)$ to $(I_1(P), I_2(P))$. Instead we just state the reduction for automatizable proof systems.

Proposition 37. *Let P be an automatizable proof system. Then*

$$(U_1(P), U_2) \leq_p (I_1(P), I_2(P)) \ .$$

Proof. Let P be automatizable. Hence there exists a polynomial time computable function f that on input $(\varphi, 1^m)$ produces a P-proof of φ provided $(\varphi, 1^m) \in \mathrm{Ref}(P)$. If $(\varphi, 1^m) \notin \mathrm{Ref}(P)$ the behaviour of f is unspecified. The desired reduction is given by

$$(\varphi, \psi, 1^m) \mapsto \begin{cases} (\varphi, \psi, f(\varphi \vee \psi, 1^m)) & \text{if } P(f(\varphi \vee \psi, 1^m)) = \varphi \vee \psi \\ (\varphi_0, \psi_0, \pi_0) & \text{otherwise} \end{cases}$$

where $(\varphi_0, \psi_0, \pi_0)$ is a fixed triple from $I_2(P)$. □

It is also interesting to compare $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ and $(U_1(P), U_2)$ with respect to the strong reduction $\leq_s$. At least for regular systems we know that $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_s (U_1(P), U_2)$. Since $U_1(P)$ is NP-complete the NP-completeness of $\mathrm{Ref}(P)$ is a necessary condition for the opposite reduction to exist. To determine the complexity of $\mathrm{Ref}(P)$ for natural proof systems seems to be an interesting open problem. Approaching this question we note the following:

Proposition 38. *1. For every proof system P that is closed under disjunctions there is a proof system P' with $P' \equiv_p P$ such that $\mathrm{Ref}(P')$ is NP-complete.*

2. On the other hand there are proof systems P and P' such that $P \equiv_p P'$ and $\mathrm{Ref}(P)$ is decidable in polynomial time while $\mathrm{Ref}(P')$ is NP-complete.

Proof. To show part 1 of the proposition let P be a proof system that is closed under disjunctions. Closure under disjunctions implies in particular the existence of polynomial size proofs of all formulas of the form $\varphi \vee \top$ for arbitrary formulas φ. We define P' as

$$P'(\pi) = \begin{cases} P(\pi') & \text{if } \pi = 0^{q(|P(\pi')|)}1\pi' \\ \varphi \vee \top & \text{if } \pi = (\varphi, \alpha) \text{ and } \alpha \text{ is a satisfying assignment for } \varphi \\ \top & \text{otherwise} \end{cases}$$

with some polynomial q such that

$$q(n) \geq \max\{|(\varphi, \alpha)| \mid |\varphi \vee \top| = n\} \ .$$

Obviously P' is a correct proof system with $P \equiv_p P'$. Furthermore $\mathrm{Ref}(P')$ is NP-complete because SAT reduces to $\mathrm{Ref}(P')$ via

$$\varphi \mapsto (\varphi \vee \top, 1^{q(|\varphi \vee \top|)}) \ .$$

For part 2 we define the proof system P as follows: (π, φ) is a P-proof of φ, if either π is a correct truth table evaluation of φ with all entries 1, or φ is of the form $\psi \vee \top$ for some formula ψ and $\pi = 1^{\|\mathrm{Var}(\psi)\|}$.

The proof system P satisfies the condition $P \vdash_* \psi \vee \top$ for all formulas ψ. Hence by the proof of part 1 of this proposition there is a proof system P' with $P \equiv_p P'$ and NP-complete $\mathrm{Ref}(P')$. On the other hand the set

$$\begin{aligned} \mathrm{Ref}(P) = \{&(\varphi, 1^m) \mid \varphi \in \mathrm{TAUT},\ m \geq 2^{\|\mathrm{Var}(\varphi)\|} + |\varphi|\} \cup \\ \{&(\psi \vee \top, 1^m) \mid \psi \text{ is a formula}, m \geq \|\mathrm{Var}(\psi)\| + |\psi|\} \end{aligned}$$

is decidable in polynomial time. □

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

References

[AB02] Albert Atserias and Maria Luisa Bonet. On the automatizability of resolution and related propositional proof systems. In *Computer Science Logic, 16th International Workshop*, 569–583, 2002.

[AR01] Michael Alekhnovich and Alexander A. Razborov. Resolution is not automatizable unless W[P] is tractable. In *Proc. 42nd IEEE Foundations of Computer Science*, 210–219, 2001.

[Bey04a] Olaf Beyersdorff. Representable disjoint NP-pairs. In *Proc. 24th Conference on Foundations of Software Technology and Theoretical Computer Science*, 122–134, 2004.

[Bey04b] Olaf Beyersdorff. Representable disjoint NP-pairs. Technical Report TR04-082, Electronic Colloquium on Computational Complexity, 2004. Extended version.

[BPR00] Maria Luisa Bonet, Toniann Pitassi, and Ran Raz. On interpolation and automatization for Frege systems. *SIAM Journal on Computing*, **29**(6):1939–1967, 2000.

[Bus86] Samuel R. Buss. *Bounded Arithmetic*. Bibliopolis, 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. Canonical disjoint NP-pairs of propositional proof systems. In *Proc. 30th International Symposium on the Mathematical Foundations of Computer Science*, 399–409, 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, 1995.

[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.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'