Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 82 (2004)

Representable Disjoint NP-Pairs[*]

Olaf Beyersdorff

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

Abstract. We investigate the class of disjoint NP-pairs under different reductions. The structure of this class is intimately linked to the simulation order of propositional proof systems, and we make use of the relationship between propositional proof systems and theories of bounded arithmetic as the main tool of our analysis. Specifically we exhibit a pair which is complete under strong reductions for all disjoint NP-pairs representable in a theory. We use these pairs to explain the simulation order of NP-pairs under these reductions. As corollaries we also get simplified proofs of results obtained earlier in [5] and [7].

1 Introduction

Disjoint NP-pairs (DNPP) naturally occur in cryptography (cf. [6]). The investigation of disjoint NP-pairs in connection with propositional proof systems was initiated by Razborov [17] and further developed by Pudlák [16] and Köbler et al. [7]. These applications attracted more complexity theoretic research on the structure of the class of disjoint NP-pairs (cf. [4, 5, 7]). Various reductions between NP-pairs were introduced by Grollmann and Selman [6]. For the most usual form of a many-one-reduction between DNPP a polynomial time computable function is required to map the components of the two pairs to each other. We denote this reduction here by $\leq_p$. Later Köbler et al. defined in [7] a strong reduction (denoted by $\leq_s$), where additionally to $\leq_p$ the reduction function has to map the complements of the pairs to each other.

One of the most prominent questions regarding disjoint NP-pairs is whether there exist complete pairs for the class of all DNPP under these reductions. These problems remain open and various oracle results from [4] indicate that these are indeed difficult questions. Under the assumption that there is an optimal proof system, however, Razborov showed the existence of a $\leq_p$-complete pair. This was improved by Köbler et al. in [7] to the existence of a complete pair for $\leq_s$.

Razborov associates to a proof system a canonical disjoint NP-pair and uses the relationship between theories of bounded arithmetic and propositional proof systems for his investigation. In this paper we define another canonical pair for a proof system which plays the same role for the stronger $\leq_s$-reduction as Razborov's pair for $\leq_p$. We show that these canonical pairs are quite typical for the class of all DNPP in the sense that every DNPP is $\leq_s$-reducible to such

[*] A shorter version of this paper will appear in the Proceedings of the 24th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), Chennai, India, 2004.

ISSN 1433-8092

a canonical pair, and if there exists a $\leq_s$-complete pair then it is equivalent to a canonical pair. As one consequence we obtain that, while $\leq_p$ and $\leq_s$ are generally different, the existence of a $\leq_p$-complete pair already implies the existence of a $\leq_s$-complete pair. This was also observed by Glaßer et al. in [5] using direct arguments where no reference to proof systems is made.

In this paper, however, we aim to explain some facts about the structure of disjoint NP-pairs by using the close relationship between NP-pairs, proof systems and bounded arithmetic. This also considerably simplifies proofs of earlier results in [5] and [7] which were originally shown by more involved simulation techniques.

Pursuing the afore mentioned goal we start in Sect. 2 by reviewing relevant facts about the connection between propositional proof systems and bounded arithmetic. We only give a very brief presentation tailored to our applications in later sections and refer the reader to [8] or [15] for a detailed account of this rich relationship.

In Sect. 3 we define and separate the afore mentioned reductions between NP-pairs.

In Sect. 4 we start to explain the relationship between disjoint NP-pairs and propositional proof systems by restricting the class of all DNPP to the DNPP representable in some theory T of bounded arithmetic, where a DNPP is called representable in T if the disjointness of the pair is provable in the theory T. We present a $\leq_s$-complete pair for all DNPP representable in sufficiently strong theories. To make the paper self contained we also reprove some known results.

In Sect. 5 we show that if $\leq_s$-complete pairs exist then these are equivalent to a canonical pair from Sect. 4 and derive some consequences on the relationship between the simulation order of proof systems and the class of DNPP.

In Sect. 6 we discuss separators and Turing reductions. We show that our pairs from Sect. 4 are candidates for NP-pairs which can not be separated by sets from P, and that the class of all DNPP representable in some theory T is closed under smart Turing-reductions implying that even the existence of smart Turing-complete pairs suffices for the existence of $\leq_s$-complete DNPP which is also shown in [5].

Finally in Sect. 7 we conclude with an application to the construction of hard tautologies from pseudorandom generators (see [1], [9] and [10]).

2 Preliminaries

Propositional proof systems were defined in a very general way by Cook and Reckhow in [3] 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_n is a sequence of propositional formulas we write $P \vdash_* \varphi_n$ if there is a polynomial p such that $P \vdash_{\leq p(|\varphi_n|)} \varphi_n$.

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 [3] polynomially bounded proof systems exist iff NP=coNP.

In this paper we are only concerned with sufficiently strong proof systems simulating the extended Frege proof system EF, where EF 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. [8]). For simplicity we call proof systems simulating EF strong. A method how to actually construct strong proof systems was recently described in [11].

We now review the relationship between theories of arithmetic and proof systems. Let L be the language of arithmetic (cf. [8]). Bounded L-formulas are formulas in the language of L where only quantifiers of the form $(\forall x \leq t(y))$ and $(\exists x \leq s(y))$ occur with L-terms t and s. In the following we are particularly interested in Π_1^b and Σ_1^b-formulas where only bounded universal and bounded existential quantifiers are allowed, respectively.

To explain the connection to propositional proof systems we have to translate L-formulas into propositional formulas. Let $\varphi(x)$ be a Π_1^b-formula. We can assume that φ is of the form $(\forall y)\, |y| \leq |x|^k \to \psi(x,y)$ with some polynomial time computable predicate ψ. Hence we can compute $\psi(x,y)$ by polynomial size boolean circuits C_n for numbers x of length n. From C_n we build a propositional formula $||\varphi||^n$ with atoms $p_1,\dots,p_n$ for the bits of x, atoms $q_1,\dots,q_{n^k}$ for the bits of y and auxiliary atoms $r_1,\dots,r_{n^{O(1)}}$ for the inner nodes of C_n. The formula $||\varphi||^n$ describes that if the values for $\bar{r}$ are correctly computed from $\bar{p}$ and $\bar{q}$ then the output of the computation of C_n is 1. Thus we get a sequence of propositional formulas $||\varphi||^n$ of polynomial size in n and $||\varphi||^n$ is a tautology iff $\varphi(x)$ holds for all natural numbers of length $\leq n$.

Encoding propositional formulas as numbers in some straightforward way we can in a theory T speak of propositional formulas, assignments and proofs. Let $\mathrm{Prf}_P(\pi,\varphi)$ be a L-formula describing that π is the encoding of a correct P-proof of the propositional formula encoded by φ. Similarly, let $\mathrm{Taut}(\varphi)$ be a L-formula asserting that all assignments satisfy the formula φ. Because P is a polynomial time computable function Prf_P is definable by a Σ_1^b-formula whereas Taut is in Π_1^b.

The reflection principle for a propositional proof system P is the L-formula

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

and states a strong form of the consistency of the proof system P. From the last remark it follows that $\mathrm{RFN}(P)$ is a $\forall\Pi_1^b$-formula.

In [13] a general correspondence between L-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 polynomially long P-proofs of the tautologies $||\varphi(x)||^n$.

2. T proves the correctness of P, i.e. $T \vdash \mathrm{RFN}(P)$. Furthermore P is the strongest proof system for which T proves the correctness, i.e. $T \vdash \mathrm{RFN}(S)$ for a proof system S implies $S \leq_p P$.

The most prominent example for this correspondence is the pair (S^1_2, EF) where S^1_2 is a L-theory with induction for Σ^b_1-formulas. This in particular allows the formalization of polynomial time computations and the provability of its basic properties (see e.g. [8] Chapter 6).

To every L-theory $T \supseteq S^1_2$ with a polynomial time set of axioms we can associate a proof system P which is unique up to $\leq_p$-equivalence by property 2 above. Conversely every strong proof system has a corresponding theory, but here according to property 1 only the $\forall\Pi^b_1$-consequences of T are determined by P.

As the correspondence only works for sufficiently strong proof systems we will restrict ourselves to proof systems P simulating the extended Frege-system EF and theories $T \supseteq S^1_2$.

By $\mathcal{N}$ we denote the standard model of arithmetic which is in particular a submodel of all models of theories T considered here.

3 Reductions between NP-Pairs

A pair (A, B) is called a disjoint NP-pair (DNPP), if $A, B \in NP$ and $A \cap B = \emptyset$. To exclude trivial cases we additionally require $A \neq \emptyset$ and $B \neq \emptyset$. We consider the following reductions between disjoint NP-pairs.

Definition 1. *Let (A, B) and (C, D) be DNPP.*

1. *(A, B) is polynomially reducible to (C, D) ($(A, B) \leq_p (C, D)$), if there exists a function $f \in FP$ such that $f(A) \subseteq C$ and $f(B) \subseteq D$.*
2. *(A, B) is strongly reducible to (C, D) ($(A, B) \leq_s (C, D)$), if there exists a function $f \in FP$ such that $f^{-1}(C) = A$ and $f^{-1}(D) = B$.*
3. *As usual we write $(A, B) \equiv_p (C, D)$ for $(A, B) \leq_p (C, D)$ and $(C, D) \leq_p (A, B)$. $\equiv_s$ is defined in the same way.*

$(A, B) \leq_p (C, D)$ does not in general imply that A and B are reducible to C and D, respectively, but if f realizes a $\leq_s$-reduction from (A, B) to (C, D), then f is simultaneously a many-one-reduction between A and C as well as between B and D. Equivalently we can also view $\leq_s$ as a reduction between triples. In addition to the two conditions $f(A) \subseteq C$ and $f(B) \subseteq D$ for $\leq_p$ we also require $f(\overline{A \cup B}) \subseteq \overline{C \cup D}$.

Obviously $\leq_s$ is a refinement of $\leq_p$. Under the assumption P $\neq$ NP this is indeed a proper refinement. The reason for this lies in the following proposition:

Proposition 2. *For every DNPP (A, B) there exists a DNPP (A', B') such that $(A, B) \equiv_p (A', B')$ and A', B' are NP-complete.*

Proof. Choose $A' = A \times \mathrm{SAT}$ and $B' = B \times \mathrm{SAT}$. Then we have $(A, B) \leq_p (A', B')$ via $x \mapsto (x, \varphi_0)$ with a fixed formula $\varphi_0 \in \mathrm{SAT}$, and $(A', B') \leq_p (A, B)$ via the projection $(x, \varphi) \mapsto x$. □

With this proposition we can easily separate the reductions $\leq_p$ and $\leq_s$ under the assumption P $\neq$ NP. Namely, let A and B be nonempty sets in P such that $\overline{A \cup B}$ is also nonempty. Choose A' and B' as in the last proposition. Then $(A, B) \equiv_p (A', B')$ but $(A, B) \not\equiv_s (A', B')$ because $(A', B') \leq_s (A, B)$ would imply in particular $A' \leq_m^p A$ and hence P=NP. On the other hand if P=NP then all DNPP (A, B) where all three components $A, B, \overline{A \cup B}$ are nonempty would be $\leq_s$-equivalent. This equivalence of P $\neq$ NP and the separation of $\leq_p$ from $\leq_s$ for DNPP with all three components nonempty (or equivalently for DNPP with all three components infinite) is also observed in [5].

4 Representable NP-Pairs

In the following we investigate the relationship between disjoint NP-pairs and propositional proof systems. For this we will use the correspondence between proof systems and theories of bounded arithmetic as explained in the Sect. 2. For this section let P be a strong proof system and T be a corresponding theory.

Following Razborov we call a Σ_1^b-formula φ a representation of an NP-set A, if for all natural numbers a

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

A DNPP (A, B) is representable in T, if there are Σ_1^b-formulas φ and ψ representing A and B, respectively, such that

$$T \vdash (\forall x)(\neg\varphi(x) \vee \neg\psi(x)) \ .$$

For the last line we also use the abbreviation $T \vdash A \cap B = \emptyset$. Since $A \cap B = \emptyset$ is a $\forall\Pi_1^b$-formula we can also express the disjointness of A and B propositionally by the sequence of tautologies $\|\neg\varphi(x) \vee \neg\psi(x)\|^n$, which we again shortly denote by $\|A \cap B = \emptyset\|^n$.

The DNPP representable in T can also be characterized via the corresponding proof system P in the following way:

Proposition 3. *A DNPP (A, B) is representable in T if and only if*

$$P \vdash_* \|A \cap B = \emptyset\|^n$$

for suitable representations of A and B.

Proof. Let φ and ψ be representations for A and B, respectively, such that

$$T \vdash (\forall x)(\neg\varphi(x) \vee \neg\psi(x)) \ .$$

Because this is a $\forall\Pi_1^b$-formula, we have

$$P \vdash_* \|\neg\varphi(x) \vee \neg\psi(x)\|^n,$$

which we write by definition as $P \vdash_* \|A \cap B = \emptyset\|^n$.

For the other direction let φ and ψ be representations of A and B, such that for some natural number k we have

$$P \vdash_{\leq n^k} \|\neg\varphi(x) \vee \neg\psi(x)\|^n \ .$$

Consider the formula

$$\psi'(x) = \psi(x) \wedge (\exists \pi)|\pi| \leq |x|^k \wedge \operatorname{Prf}_P(\pi, \|\neg\varphi(y) \vee \neg\psi(y)\|^{|x|}) \ .$$

We have $\psi' \in \Sigma_1^b$ and furthermore $\mathcal{N} \models (\forall x)\psi'(x) \leftrightarrow \psi(x)$, i.e. ψ' is also a representation of B. From $T \vdash \mathrm{RFN}(P)$ it follows that $T \vdash (\forall x)(\neg\varphi(x) \vee \neg\psi'(x))$, hence (A, B) is representable in T. □

We remark that in the last proof we only have to change the representation of one of the NP-sets (in the proof of that of B) when switching between the representation of the DNPP (A, B) in the proof system P and in the corresponding theory T.

Lemma 4 (Razborov [17]). *The set of all DNPP representable in T is closed under $\leq_p$-reductions.*

Proof. Let (A, B) and (C, D) be DNPP such that $f : (A, B) \leq_p (C, D)$ and $T \vdash C \cap D = \emptyset$. Consider the NP-sets

$$\begin{aligned} A' &= \{x \mid x \in A \text{ and } f(x) \in C\} \\ B' &= \{x \mid x \in B \text{ and } f(x) \in D\} \ . \end{aligned}$$

Obviously $A = A'$ and $B = B'$. From $T \supseteq S_2^1$ and $f \in FP$ we get $T \vdash (\forall x)(\exists! y) f(x) = y$. Hence

$$T \vdash (\forall x)(x \in A' \cap B' \rightarrow f(x) \in C \cap D)$$

and with $T \vdash C \cap D = \emptyset$ we conclude $T \vdash A' \cap B' = \emptyset$. □

Following Razborov [17] we associate a disjoint NP-pair $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ with a proof system P with

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

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

Lemma 5 (Razborov [17]). *The canonical pair of P is representable in the theory T.*

Proof. We argue in T. Let $(\varphi, 1^m) \in \mathrm{Ref}(P)$. Then there is a P-proof π of φ. Since $\mathrm{RFN}(P)$ is available in T we conclude from $\operatorname{Prf}_P(\pi, \varphi)$ the formula $\mathrm{Taut}(\varphi)$, hence $\neg\varphi \notin \mathrm{SAT}$ and therefore $(\varphi, 1^m) \notin \mathrm{SAT}^*$. □

Now we associate a second disjoint NP-pair with a proof system P. For a propositional formula φ let $\mathrm{Var}(\varphi)$ be the set of propositional variables occurring in φ. Let

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

Let us first argue that $(U_1(P), U_2)$ is indeed a disjoint NP-pair. Clearly both components are in NP. Let $(\varphi, \psi, 1^m) \in U_1(P)$. Since we have a P-proof of $\varphi \vee \psi$ the formula is a tautology. Because φ and ψ do not share variables one of φ or ψ is itself a tautology. Because $\neg\varphi$ is satisfiable ψ is a tautology. Therefore $\neg\psi \notin \mathrm{SAT}$ and hence $(\varphi, \psi, 1^m) \notin U_2$.

We could have defined the pair in a more symmetric way by requiring $P \vdash_{\leq m} \varphi \vee \psi$ also for the second component but for the following this is not important. As for the canonical pair we get:

Lemma 6. *The pair $(U_1(P), U_2)$ is representable in T.*

Proof. Let $(\varphi, \psi, 1^m) \in U_1(P)$ and π be a P-proof of $\varphi \vee \psi$ of length $\leq m$. Because $\neg\varphi \in \mathrm{SAT}$ we have an assignment α with $\varphi(\alpha) = 0$. If we substitute the variables of φ by 0 or 1 according to α, we get from the proof π a proof π' of ψ. Hence we have

$$T \vdash (\exists \pi')\mathrm{Prf}_P(\pi', \psi)\ .$$

Because T proves the correctness of P, we get $T \vdash \mathrm{Taut}(\psi)$ and thus $T \vdash (\varphi, \psi, 1^m) \notin U_2$. □

Now we come to the main theorem of this section which states the completeness of $(U_1(P), U_2)$ for all DNPP representable in T under $\leq_s$-reductions.

Theorem 7. *A DNPP (A, B) is representable in T if and only if $(A, B) \leq_s (U_1(P), U_2)$.*

Proof. Let (A, B) be a DNPP such that $T \vdash A \cap B = \emptyset$. Let the NP-sets A and B be of the form

$$\begin{aligned} A &= \{x \mid (\exists y)|y| \leq |x|^{O(1)} \wedge (x, y) \in C\} \\ B &= \{x \mid (\exists z)|z| \leq |x|^{O(1)} \wedge (x, z) \in D\} \end{aligned}$$

with polynomial time predicates C and D. Because of the correspondence between T and P there is a polynomial p for the $\forall\Pi_1^b$-formula $A \cap B = \emptyset$ such that

$$P \vdash_{\leq p(n)} \|A \cap B = \emptyset\|^n\ .$$

Here the formula $\|A \cap B = \emptyset\|^n$ is more explicitly $\|(x, y) \notin C \vee (x, z) \notin D\|^n$ and has propositional variables for x, y and z and auxiliary variables for the computation of boolean circuits for C and D. We can plug into this formula natural numbers a of length n for x by substituting the propositional variables corresponding to x by the bits of a. We indicate this by the suffix (x/a).

Now we claim that the function

$$f(a) = (\|(x,y) \notin C\|^{|a|}(x/a), \|(x,z) \notin D\|^{|a|}(x/a), 1^{p(|a|)})$$

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

If we choose different auxiliary variables for the computation of C and D and also disjoint variables for y and z, then the formulas $\|(x,y) \notin C\|^{|a|}(x/a)$ and $\|(x,z) \notin D\|^{|a|}(x/a)$ have no common variables. Furthermore for every natural number a the formulas

$$\begin{array}{rl} \|(x,y) \notin C\|^{|a|}(x/a) \vee \|(x,z) \notin D\|^{|a|}(x/a) & = \\ \|(x,y) \notin C \vee (x,z) \notin D\|^{|a|}(x/a) & = \\ \|A \cap B = \emptyset\|^{|a|}(x/a) & \end{array}$$

have P-proofs of length $\leq p(|a|)$, which we get from the P-proofs of $\|A \cap B = \emptyset\|^{|a|}$ by substituting the variables for x by the bits of a.

The last thing to check is that the formula

$$\neg\|(x,y) \notin C\|^{|a|} = \|(x,y) \in C\|^{|a|},$$

expressing, that there is a correct accepting computation of C with input (x,y), is satisfiable if and only if the variables of x are substituted by the bits of a number $a \in A$.

Similarly, $\neg\|(x,z) \notin D\|^{|a|}(x/a)$ is satisfiable if and only if $a \in B$.

The backward implication follows from Lemma 6 and the fact, that the DNPP representable in T are closed under $\leq_p$ and hence also under $\leq_s$ according to Lemma 4. □

The pair $(U_1(P), U_2)$ strongly resembles the interpolation pair defined by Pudlák in [16]:

$$\begin{array}{l} I_P^0 = \{(\varphi, \psi, \pi) \mid P(\pi) = \varphi \vee \psi,\ \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset \text{ and } \neg\varphi \in \mathrm{SAT}\} \\ I_P^1 = \{(\varphi, \psi, \pi) \mid P(\pi) = \varphi \vee \psi,\ \mathrm{Var}(\varphi) \cap \mathrm{Var}(\psi) = \emptyset \text{ and } \neg\psi \in \mathrm{SAT}\}\ . \end{array}$$

This pair is p-separable, if and only if the proof system P has the efficient interpolation property. For $\|.\|$-translations of $\forall\Pi_1^b$-formulas provable in T we can efficiently construct polynomially long P-proofs (i.e. with functions from FP). Hence the proof of the last theorem also shows the $\leq_s$-completeness of (I_P^0, I_P^1) for all DNPP representable in T.

In [16] Pudlák defined a DNPP (A,B) to be symmetric if $(B,A) \leq (A,B)$. With Lemma 6 also the pair $(U_2, U_1(P))$ is representable in T, hence by the last theorem $(U_1(P), U_2)$ is symmetric even with respect to the stronger $\leq_s$-reduction.

As a corollary of Theorem 7 we obtain the $\leq_p$-completeness of the canonical pair for all DNPP representable in T, which was shown by Razborov:

Theorem 8 (Razborov [17]). *A DNPP (A,B) is representable in T if and only if $(A,B) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$.*

Proof. For the forward implication we reduce $(U_1(P), U_2)$ to $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ via the projection

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

with a suitable polynomial p.

Let $(\varphi, \psi, 1^m) \in U_1(P)$. Then there is a P-proof π of length $\leq m$ of $\varphi(\bar{x}) \vee \psi(\bar{y})$. The formula $\neg\varphi(\bar{x})$ is satisfiable, so by substituting a satisfying assignment $\bar{a}$ into the proof π we get a proof π' with $|\pi'| \leq m$ for $\varphi(\bar{a}) \vee \psi(\bar{y})$. Since $\varphi(\bar{a})$ is a false formula without free variables we can evaluate it in polynomially long P-proofs to $\perp$. Let p be a corresponding polynomial. Thus we get a P-proof of length $\leq m + p(|\varphi|)$ for ψ.

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

This $\leq_p$-reduction from $(U_1(P), U_2)$ to $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ yields together with the last theorem the $\leq_p$-completeness of $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ for all DNPP representable in T.

The backward implication follows from Lemma 4 and Lemma 5. □

Thus the pairs $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ and $(U_1(P), U_2)$ are complete for all DNPP representable in T under $\leq_p$- and $\leq_s$-reductions, respectively.

5 NP-Pairs and the Simulation Order of Proof Systems

Now we use the results of the last section to make some observations about the connection between the simulation order of proof systems and disjoint NP-pairs.

In Sect. 3 it was shown that the reductions $\leq_p$ and $\leq_s$ are different under the assumption P $\neq$ NP. Still we have:

Proposition 9. *For all strong proof systems P and DNPP (A, B) it holds*

$$(A, B) \leq_p (U_1(P), U_2) \iff (A, B) \leq_s (U_1(P), U_2) \ .$$

Proof. Let $(A, B) \leq_p (U_1(P), U_2)$. $(U_1(P), U_2)$ is representable in T. Hence with Lemma 4 also (A, B) is representable in T, from which we conclude with Theorem 7

$$(A, B) \leq_s (U_1(P), U_2) \ .$$

The opposite implication follows by definition. □

Corollary 10. *Let P and S be strong proof systems. Then we have:*

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

Proof. For the first direction we get from

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

together with the last proposition

$$(U_1(P), U_2) \leq_s (U_1(S), U_2) \ .$$

The other implication follows from

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

□

The following proposition is well known (see e.g. [16]):

Proposition 11. *If P and S are proof systems with $P \leq S$, then we have*

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

Proof. By assumption there is a polynomial p, such that for all formulas φ and P-proofs π of φ there is a S-proof π' of length $\leq p(|\pi|)$. Therefore the mapping

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

is a $\leq_p$-reduction from $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ to $(\mathrm{Ref}(S), \mathrm{SAT}^*)$. □

Proposition 11 and Corollary 10 yield:

Corollary 12. *If P and S are strong proof systems with $P \leq S$, then we have*

$$(U_1(P), U_2) \leq_s (U_1(S), U_2) \ .$$

Köbler, Messner and Torán proved in [7] that the existence of an optimal proof system implies the existence of $\leq_s$-complete NP-pairs. This result also follows from the last corollary. Additionally we can exhibit a complete DNPP in this case:

Corollary 13. *If P is an optimal proof system, then $(U_1(P), U_2)$ is $\leq_s$-complete for the class of all DNPP.*

Proof. Let P be an optimal proof system and (A, B) a DNPP. The sequence of tautologies $\|A \cap B = \emptyset\|^n$ can be constructed in polynomial time. Hence there is a proof system S with polynomially long proofs of these tautologies (for example just add these tautologies as axioms to the extended Frege system). Using Proposition 3 and Theorem 7 we get $(A, B) \leq_s (U_1(S), U_2)$. By assumption we have $S \leq P$. Together with the previous corollary this yields $(U_1(S), U_2) \leq_s (U_1(P), U_2)$, and hence $(A, B) \leq_s (U_1(P), U_2)$.

Therefore the pair $(U_1(P), U_2)$ is $\leq_s$-complete for all DNPP. □

Proposition 14. *Let (A, B) be $\leq_p$-complete for the class of all DNPP. Then we have $(A, B) \equiv_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ for some proof system P.*

Proof. As in the last proof let P be a proof system with $P \vdash_* \|A \cap B = \emptyset\|^n$. Then $(A, B) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ and by assumption $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (A, B)$. □

In the same way we get:

Proposition 15. *Let (A, B) be $\leq_s$-complete for the class of all DNPP. Then we have $(A, B) \equiv_s (U_1(P), U_2)$ for some proof system P.*

The following proposition is also observed in [5]:

Proposition 16. *The class of all DNPP contains a $\leq_p$-complete DNPP if and only if it contains a $\leq_s$-complete DNPP.*

Proof. For the first direction we can assume with Proposition 14 that the $\leq_p$-complete DNPP has the form $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ for some proof system P. Then by Theorem 7 and Theorem 8 all DNPP are $\leq_s$-reducible to $(U_1(P), U_2)$.

The other direction holds by definition. □

Besides $\leq$ and $\leq_p$ we can also study weaker reductions for propositional proof systems. In [12] a weak reduction $\leq'$ is defined between proof systems P and Q as follows: $P \leq' Q$ holds iff for all polynomials p there exists a polynomial q such that for all tautologies φ

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

We first observe that it is easy to separate $\leq$ and $\leq'$:

Proposition 17. *Let P be a proof system that is not polynomially bounded. Then there exists a proof system Q such that $P \leq' Q$ but $P \not\leq Q$.*

Proof. Let P be given. 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 want to use this observation to illustrate with some examples that the converse of Proposition 11 does not hold. We first show an analogue of Proposition 11 for $\leq'$ for proof systems fulfilling the moderate condition of the next proposition.

Proposition 18. *Let P be a proof system with the following property. There is a polynomial p such that for all tautologies φ $P \vdash_{\leq m} \varphi$ implies $P \vdash_{\leq p(m)} \varphi \vee \bot^m$ where $\bot^m$ stands for $\bot \vee \ldots \vee \bot$ (m disjuncts).*

Let further 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. To see this let first $(\varphi, 1^m)$ be in $\mathrm{Ref}(P)$. From $P \vdash_{\leq m} \varphi$ we get by assumption $P \vdash_{\leq p(m)} \varphi \vee \bot^m$. Because of $P \leq' Q$ there is a polynomial q such that $Q \vdash_{\leq q(m)} \varphi \vee \bot^m$, i.e $(\varphi \vee \bot^m, 1^{q(m)})$ is 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 the last two propositions we get the afore mentioned counterexamples to the converse of Proposition 11. One such example is given by Pudlák in [16], 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 construct to every proof system P which fulfills the weak condition from the last proposition a nonequivalent proof system Q with the same canonical pair.

Corollary 19. *Let P be a proof system which fulfills the condition from Proposition 18 and is not polynomially bounded. Then there exists a proof system Q such that*

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

Proof. The proof system Q constructed from P in Proposition 17 fulfills $P \leq' Q \leq P$ and $P \not\leq Q$. Hence $P \not\equiv Q$.

By Proposition 11 we have $(\mathrm{Ref}(Q), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(P), \mathrm{SAT}^*)$ and applying Proposition 18 we conclude $(\mathrm{Ref}(P), \mathrm{SAT}^*) \leq_p (\mathrm{Ref}(Q), \mathrm{SAT}^*)$. □

We call a proof system $\leq'$-optimal if it $\leq'$-simulates all proof systems. The hypothesis of Proposition 18 is fulfilled by all proof systems which are closed under the weakening rule, i.e. which can infer from a formula φ the disjunction $\varphi \vee \psi$ for an arbitrary formula ψ. Therefore we have for any proof system P a stronger system fulfilling the hypothesis of Proposition 18 which can be obtained for example by augmenting P by the weakening rule.

Hence from Proposition 18 we get in the same manner as in Corollary 13 the existence of complete NP-pairs under a possibly weaker assumption:

Corollary 20. *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.*

6 Separators and Turing Reductions

For disjoint NP-pairs we can also study Turing reductions as defined by Grollmann and Selman in [6]. For this we need the notion of a separator.

Definition 21. *A set S is a separator for the DNPP (A, B) if $A \subseteq S$ and $B \subseteq \overline{S}$.*

Of central interest is the case where a given DNPP has a separator belonging to P. Such a pair (A, B) is called p-separable. The set of all p-separable DNPP form the lowest degree with respect to the $\leq_p$-reduction, namely:

Proposition 22. *Let (A, B) be a p-separable DNPP. Then (A, B) is $\leq_p$-reducible to any other disjoint NP-pair. If on the other hand a pair (C, D) is $\leq_p$-reducible to (A, B) then also (C, D) is p-separable.*

For the stronger $\leq_s$-reduction this minimal degree shrinks to the set of all p-separable pairs with empty complement, i.e. sets of the form $(A, \bar{A})$ with $A \in$ P:

Proposition 23. *Let A be a set in* P*. Then $(A, \bar{A})$ is $\leq_s$-reducible to any other disjoint NP-pair. If on the other hand a pair (C, D) is $\leq_s$-reducible to $(A, \bar{A})$ then $D = \bar{C}$ and $C \in$* P*.*

But also the set of all p-separable pairs with nonempty complement splits into different $\equiv_s$-degrees. Firstly, no such pair is $\leq_s$-reducible to any pair from the minimal $\equiv_s$-degree. Secondly, if (A, B) is a p-separable DNPP then the pair $(A \times \mathrm{SAT}, B \times \mathrm{SAT})$ is also p-separable and both of its components are NP-complete, hence we have:

Proposition 24. *$P \neq NP$ iff there exist p-separable pairs (A, B) and (C, D), such that $\overline{A \cup B}$ and $\overline{C \cup D}$ are nonempty and $(A, B) \not\equiv_s (C, D)$.*

The question whether p-inseparable pairs exist is open. Candidates for p-inseparable pairs come from cryptography (see [6]) and proof systems. Namely, Krajíček and Pudlák demonstrate in [14] that a pair (A_0, A_1) associated with the RSA-cryptosystem is representable in the theory S^1_2 corresponding to EF. By the results from Sect. 4 this means that $(A_0, A_1) \leq_p (\mathrm{Ref}(EF), \mathrm{SAT}^*)$ and $(A_0, A_1) \leq_s (U_1(EF), U_2)$. Assuming the security of RSA the pair (A_0, A_1) is not p-separable, hence under this assumption neither $(\mathrm{Ref}(P), \mathrm{SAT}^*)$ nor $(U_1(P), U_2)$ is p-separable for any $P \geq EF$.

If we look at the property of symmetry of pairs under $\leq_s$ it is clear that a DNPP (A, B) can not be symmetric if we choose A from P and B NP-complete. In other words:

Proposition 25. *$P \neq NP$ iff there exist non-symmetric pairs with respect to $\leq_s$.*

A similar result for $\leq_p$ is not known as $\leq_p$-non-symmetric pairs are p-inseparable and it is not clear how to derive the existence of p-inseparable pairs from the assumption P $\neq$ NP.

We now come to the definition of Turing-reductions between DNPP from [6]:

Definition 26. *Let (A, B) and (C, D) be DNPP. We say that (A, B) is Turing reducible to (C, D) ($(A, B) \leq_T (C, D)$), if there exists a polynomial time oracle Turing machine M such that for every separator T of (C, D) $L(M^T)$ separates (A, B).*

If for inputs from $A \cup B$ the machine M makes only queries to $C \cup D$ we call the reduction performed by M a smart Turing reduction.

In [5] Glaßer et al. prove that the existence of a complete DNPP under smart Turing reductions already implies the existence of a $\leq_p$-complete DNPP (and hence by Proposition 16 also of a $\leq_s$-complete pair). We can easily reprove their result in our framework by noticing:

Lemma 27. *The set of all DNPP representable in a theory T is closed under smart Turing reductions.*

Proof. Let the pair (A, B) be smartly Turing reducible to (C, D) via the deterministic oracle Turing machine M, and let (C, D) be representable in T. Consider the NP-sets

$$
\begin{aligned}
A' &= \{x \mid x \in A \text{ and } M(x) \text{ accepts}\} \\
B' &= \{x \mid x \in B \text{ and } M(x) \text{ rejects}\} \ .
\end{aligned}
$$

By "$M(x)$ accepts" we mean that M accepts the input x by a computation where all oracle queries that are positively answered are verified by a computation of a nondeterministic machine for C and all negative answers are verified by D. Since the reduction is smart we have $A = A'$ and $B = B'$. For $T \vdash A' \cap B' = \emptyset$ it suffices to show in T the uniqueness of the computation of M at inputs x from $A \cup B$. T can prove the uniqueness of computations of the deterministic machine M, and the possibility to answer an oracle query both positively and negatively is excluded by $T \vdash C \cap D = \emptyset$. □

From this we conclude:

Proposition 28. *Suppose (A, B) is a smart $\leq_T$-complete pair. Then for any theory T such that $T \vdash A \cap B = \emptyset$ the pair $(U_1(P), U_2)$ is $\leq_s$-complete for all DNPP where P is the proof system corresponding to T.*

Proof. Choose a theory T with $T \vdash A \cap B = \emptyset$. Then by the last lemma all DNPP are representable in T and hence by Theorem 7 the pair $(U_1(P), U_2)$ is $\leq_s$-complete. □

It is not clear whether the class of pairs representable in some theory T is also closed under $\leq_T$-reductions. This corresponds to the open problem from [5] whether the existence of a $\leq_T$-complete pair implies the existence of a $\leq_p$-complete DNPP.

7 An Application

We conclude by mentioning a potential application of the results of Sect. 4 for the construction of hard tautologies from pseudorandom generators (called τ-formulas) as described in [1], [9] and [10]. These τ-formulas are candidates for tautologies without polynomially long proofs in the strong proof systems considered here. Proving super polynomial lower bounds for strong proof systems constitutes a major open problem in propositional proof complexity. The aim of this section is to illustrate that the hardness of τ-formulas can be expressed by properties of disjoint NP-sets.

We recall some terminology from [10]. Let $C = (C_n)_{n \in \mathcal{N}}$ be a family of polynomial size boolean circuits such that C_n is a circuit with n input and $m(n) > n$ output bits with some polynomial m. Functions f computed by such families C are called polynomially stretching (p-stretching).

For $b \in \{0,1\}^{m(n)}$ we consider propositional formulas $\tau(C)_b$. The formula $\tau(C)_b$ has propositional variables $p_1, \dots, p_n$ for the bits of the input of C_n, $q_1, \dots, q_{m(n)}$ for the bits of the output of C_n and $r_1, \dots, r_{n^{O(1)}}$ for the inner nodes of C_n. The formula $\tau(C)_b$ expresses, that, if $\bar{r}$ are correctly computed according to C_n from the input variables $\bar{p}$, then the values of the output variables $\bar{q}$ are different from the bits of b. The formula $\tau(C)_b$ is a tautology, if and only if $b \notin \mathrm{rng}(f)$. But apparently $\tau(C)_b$ does not only depend on $\mathrm{rng}(f)$, but also on the particular circuits C_n used for the computation of f.

The formulas $\tau(C)$ from a circuit family C_n are called hard for a proof system P, if there does not exist a sequence of pairwise different numbers $b_n \in \{0,1\}^{m(n)}$, $n \in \mathcal{N}$, such that

$$P \vdash_* \tau(C)_{b_n} \ .$$

The intuition is that for functions having pseudorandom properties it should be hard to prove that a given element lies outside the range of the function. In fact the hardness of the function f should not depend on the particular circuits used for the computation of f. Focusing on the case where the circuit families are uniformly given we therefore say that a polynomial time computable p-stretching function f yields representationally independent hard τ-formulas for P, if for every uniformly given circuit family C computing f the resulting formulas $\tau(C)$ are hard for P.

The connection between the hardness of τ-formulas and disjoint NP-pairs is established by the following theorem:

Theorem 29 (Krajíček [10]). *Let $f \in FP$ be a p-stretching function and C a polynomial size uniform circuit family computing f. Then the following are equivalent:*

1. *The formulas $\tau(C)$ are hard for P.*
2. *Every set $A \in NP$ with $P \vdash_* \|A \cap \mathrm{rng}(C) = \emptyset\|^n$ is finite.*

With Proposition 3 we can replace condition 2 of the theorem by the following condition 2':

2'. Every set $A \in NP$ with $T \vdash A \cap \mathrm{rng}(C) = \emptyset$ is finite.

We point out that in condition 2' the disjointness of A and $\mathrm{rng}(f)$ has to be proven with respect to the circuit family used for the computation of f, while the representation of A can be chosen arbitrarily.

Using Theorem 7 we can restate Theorem 29 in the following form:

Corollary 30. *For every p-stretching function $f \in FP$ the following are equivalent:*

1. *f yields representationally independent hard τ-formulas for P.*
2. *Every set $A \in NP$ with $A \cap \mathrm{rng}(f) = \emptyset$ and $(A, \mathrm{rng}(f)) \leq_s (U_1(P), U_2)$ is finite.*

Dropping the condition $(A, \mathrm{rng}(f)) \leq_s (U_1(P), U_2)$ from 2 we arrive at an NP-set $B = \mathrm{rng}(f)$ containing no infinite NP-set in its complement $\bar{B}$. Such sets B are called NP-simple (see [2] or [18]). By Corollary 30 NP-simple sets would yield representationally independent hard τ-formulas for all proof systems, but their existence is open.

On the other hand it is easy to see that a set $B = \text{rng}(f)$ satisfying condition 2 of Corollary 30 cannot contain an infinite P-set in its complement, i.e. $\bar{B}$ has to be P-immune. Therefore condition 2 of Corollary 30 asks for the existence of NP-sets which are NP-simple "relative to the DNPP $(U_1(P), U_2)$", a notion which lies in strength between P-immunity of the complement and NP-simplicity.

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

References

1. M. Alekhnovich, E. Ben-Sasson, A. A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof complexity. In *Proceedings 41st Annual Symposium on Foundations of Computer Science*, pages 43-53, 2000.
2. J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural complexity, volumes I and II.* Springer, Berlin, 1988.
3. S. Cook and R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic* **44**:36-50, 1979.
4. C. Glaßer, A. Selman, S. Sengupta, and L. Zhang. Disjoint NP-pairs. In *Proceedings 18th Annual IEEE Conference on Computational Complexity*, pages 313-332, 2003.
5. C. Glaßer, A. Selman, and S. Sengupta. Reductions between disjoint NP-pairs. In *Proceedings 19th Annual IEEE Conference on Computational Complexity*, 2004.
6. J. Grollmann and A. Selman. Complexity measures for public-key cryptosystems. *SIAM Journal on Computing* **17(2)**:309-335, 1988.
7. J. Köbler, J. Messner, and J. Torán. Optimal proof systems imply complete sets for promise classes. *Information and Computation* **184**:71-92, 2003.
8. J. Krajíček. *Bounded Arithmetic, Propositional Logic, and Complexity Theory.* Encyclopedia of Mathematics and Its Applications, volume **60**, Cambridge University Press, Cambridge, 1995.
9. J. Krajíček. Tautologies from pseudo-random generators. *Bulletin of Symbolic Logic* **7(2)**:197-212, 2001.
10. J. Krajíček. Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds. *Journal of Symbolic Logic* **69(1)**:265-286, 2004.
11. J. Krajíček. Implicit proofs. *Journal of Symbolic Logic* **69(2)**:387-397, 2004.
12. J. Krajíček and P. Pudlák. Propositional proof systems, the consistency of first order theories and the complexity of computations. *Journal of Symbolic Logic* **34**:1063-1079, 1989.
13. J. Krajíček and P. Pudlák. Quantified propositional calculi and fragments of bounded arithmetic. *Zeitschr. f. math. Logik und Grundlagen d. Math.* **36**:29-46, 1990.
14. J. Krajíček and P. Pudlák. Some consequences of cryptographical conjectures for S^1_2 and *EF*. *Information and Computation* **140(1)**:82-94, 1998.
15. P. Pudlák. The lengths of proofs. In *Handbook of Proof Theory*, S. R. Buss ed., pages 547-637, Elsevier, Amsterdam, 1998.
16. P. Pudlák. On reducibility and symmetry of disjoint NP-pairs. In *Proceedings 26th International Symposium on Mathematical Foundations of Computer Science*, volume 2136 of *Lecture Notes in Computer Science*, pages 621-632. Springer-Verlag, Berlin, 2001.
17. A. A. Razborov. On provably disjoint NP-pairs. Technical Report TR94-006, Electronic Colloquium on Computational Complexity, 1994.
18. T. Suzuki and T. Yamakami. Resource bounded immunity and simplicity. In *Proceedings 3rd IFIP International Conference on Theoretical Computer Science*, pages 81-95, Kluwer Academic Publishers, 2004.