Proof System Representations of Degrees of Disjoint NP-Pairs

Liyu Zhang*

December 30, 2010

Abstract

Let $\mathcal{D}$ be a set of many-one degrees of disjoint NP-pairs. We define a *proof system representation* of $\mathcal{D}$ to be a set of propositional proof systems $\mathcal{P}$ such that each degree in $\mathcal{D}$ contains the canonical NP-pair of a corresponding proof system in $\mathcal{P}$ and the degree structure of $\mathcal{D}$ is reflected by the simulation order among the corresponding proof systems in $\mathcal{P}$. We also define a *nesting representation* of $\mathcal{D}$ to be a set of NP-pairs $\mathcal{S}$ such that each degree in $\mathcal{D}$ contains a representative NP-pair in $\mathcal{S}$ and the degree structure of $\mathcal{D}$ is reflected by the inclusion relations among their representative NP-pairs in $\mathcal{S}$. We show that proof system and nesting representations both exist for $\mathcal{D}$ if the lower span of each degree in $\mathcal{D}$ overlaps with $\mathcal{D}$ on a finite set only. In particular, a linear chain of many-one degrees of NP-pairs has both a proof system representation and a nesting representation. This extends a result by Glaßer et al., 2009. We also show that in general $\mathcal{D}$ has a proof system representation if it has a nesting representation where all representative NP-pairs share the same set as their first components.

1 Introduction

The *canonical disjoint* NP*-pairs* (*canonical pairs*, for short) has played an important role in the study of disjoint NP-pairs and their relations to propositional proof systems (proof system, for short) [8]. Razborov [15] first defined the canonical pair, denoted by $can(f)$, for every proof system f. He showed that if there exists an optimal proof system f, then its canonical pair is a complete pair for the class of disjoint NP-pairs. Pudlák [14] related canonical pairs of proof systems to the reflection principle and *automatizabilities* of proof systems. In particular, he showed that the canonical pair of a proof system is P*-separable* if and only if the proof system is simulated by an automatizable proof system. Glaßer et al. [9] showed that every disjoint NP-pair is polynomial-time many-one equivalent to the canonical pair of some proof system. This implies that the degree structures of the class of disjoint NP-pairs and of all canonical pairs are identical. Beyersdorff [2] studied proof systems and their canonical pairs from a proof theoretic point of view. He defined the subclasses DNPP(P) of disjoint NP-pairs that are representable in some proof system P and showed that the canonical pairs of P are complete for DNPP(P). This interesting result tells us that for certain meaningful subclasses of disjoint NP-pairs, complete pairs do exist.

*Department of Computer and Information Sciences, University of Texas at Brownsville, Brownsville, TX, 78520, USA. Email: liyu.zhang@utb.edu

More recently Glaßer et al. [10] further studied the connections between proof systems and their canonical pairs and showed that proof systems whose simulation order do not reflect the degree structures between their corresponding canonical pairs exist almost everywhere. This generalizes previous results by Pudlák [14] and Beyersdorff [2]. Glaßer et al. also asked the question for which propositional proof systems f and g the implication $can(f) \leq_m^p can(g) \Rightarrow f \leq g$ holds, where $\leq_m^p$ and $\leq$ denote the many-one reducibility between NP-pairs and simulation order between proof systems, respectively. In answering this question, they showed that for any two degrees d_1 and d_2 of NP-pairs, where $d_1 \leq d_2$, there exist proof systems f_1 and f_2 such that $can(f_1) \in d_1$, $can(f_2) \in d_2$, and $can(f_1) \leq_m^p can(f_2)$.

Let $\mathcal{D}$ be a set of many-one degrees of disjoint NP-pairs. We define a *proof system representation* of $\mathcal{D}$ to be a set of propositional proof systems $\mathcal{P}$ such that each degree in $\mathcal{D}$ contains the canonical NP-pair of a corresponding proof system in $\mathcal{P}$ and the degree structure of $\mathcal{D}$ is reflected by the simulation order among the corresponding proof systems in $\mathcal{P}$. The result of Glaßer at al. can be restated as that any $\mathcal{D}$ consisting of two comparable degrees of NP-pairs has a proof system representation. In this paper we show that any $\mathcal{D}$ where the lower span of each degree consists only of a finite set of degrees in $\mathcal{D}$ has a proof system representation, and hence extend the previous result. Interestingly, essentially the same proof shows also that any $\mathcal{D}$ satisfying the same property has a *nesting* representation. Here we define a *nesting representation* of $\mathcal{D}$ to be a set of NP-pairs such that each degree contains a representative NP-pair and the degree structure of $\mathcal{D}$ is reflected by the inclusion relations among the representative NP-pairs. A corollary following immediately is that a linear chain of many-one degrees of NP-pairs has both a proof system representation and a nesting representation. Regarding the general relations between proof system representations and nesting representations, we show that a set of many-one degrees of NP-pairs has a proof-system representation if it has a nesting representation where the first components of all representative NP-pairs are the same set.

We will give basic definitions in Section 2 and present our results in detail in Section 3. We refer the reader to the survey by Glaßer et al. [8] and recent literature [13, 5, 4, 3, 16] for more developments on the study of (canonical) disjoint NP-pairs.

2 Preliminaries

We assume familiarity with basic notions in complexity theory [12, 1].

A *disjoint* NP*-pair* (NP*-pairs*, for short) is a pair (A, B) of nonempty sets A and B such that $A, B \in$ NP and $A \cap B = \emptyset$. An NP-pair (A, B) is *many-one reducible in polynomial time* to (C, D) [1], $(A, B) \leq_m^p (C, D)$, if there exists a polynomial-time computable function $f : \Sigma^* \to \Sigma^*$ such that $f(A) \subseteq C$ and $f(B) \subseteq D$. (A, B) is *many-one equivalent in polynomial-time* to (C, D), $(A, B) \equiv_m^p (C, D)$, if $(A, B) \leq_m^p (C, D)$ and $(C, D) \leq_m^p (A, B)$.

[1] Here we only give the uniform version of many-one reducibilities between NP-pairs, which is equivalent to the original nonuniform version [11, 7].

Definition 2.1 *For any disjoint* NP*-pair* (A, B)*, the* polynomial-time many-one degree *(*many-one degree*, for short) of* (A, B) *is defined as*

$$\mathbf{d}(A, B) = \{(C, D) \mid (C, D) \textit{ is a disjoint } \text{NP}\textit{-pair and } (A, B) \equiv_m^p (C, D)\}.$$

The relation $\leq$ between many-one degrees of NP-pairs is defined as

$$d_1 \leq d_2 \stackrel{df}{=} \text{for some } (A, B) \in d_1 \text{ and } (C, D) \in d_2, (A, B) \leq_m^p (C, D)$$

Note that in light of Definition 2.1

$$d_1 \leq d_2 \Leftrightarrow \text{for every } (A, B) \in d_1 \text{ and } (C, D) \in d_2, (A, B) \leq_m^p (C, D).$$

The *lower span* of a many-one degree d of NP-pairs is the set of many-one degrees d' of NP-pairs such that $d' \leq d$.

Let SAT denote the set of satisfiable propositional formulas and let UNSAT denote the set of unsatisfiable propositional formulas. Moreover, let TAUT denote the set of tautologies over the basis $\{\wedge, \vee, \neg, \text{TRUE}, \text{FALSE}\}$ [6].

Cook and Reckhow [6] defined a *propositional proof system* (proof system, for short) to be a function $f : \Sigma^* \to \text{TAUT}$ such that f is onto and f is polynomial-time computable. For every tautology α, if $f(w) = \alpha$, then we say w is an f*-proof* of α. Let f and f' be two propositional proof systems. We say that f *simulates* f' ($f' \leq f$) if there is a polynomial p and a function $h : \Sigma^* \to \Sigma^*$ such that for every $w \in \Sigma^*$, $f(h(w)) = f'(w)$ and $|h(w)| \leq p(|w|)$. A proof system is *optimal* if it simulates every other proof system.

We use $f < g$ to denote that $f \leq g$ and $g \not\leq f$. We use $(A, B) <_m^p (C, D)$ to denote that $(A, B) \leq_m^p (C, D)$ and $(C, D) \not\leq_m^p (A, B)$. Throughout this paper, we assume an alphabet that contains 0 and 1. We also fix a polynomial-time computable and polynomial-time invertible pairing function $\langle \cdot, \cdot \rangle$ such that $|\langle v, w \rangle| = 2|vw|$.

The *canonical* NP*-pair* (*canonical pair*, for short) of f [15, 14] is the disjoint NP-pair $(\text{SAT}^*, \text{REF}(f))$, denoted by $can(f)$, where

$$\begin{aligned} \text{SAT}^* &= \{(x, 0^n) \,\big|\, x \in \text{SAT and } n \geq 0 \text{ is an integer}\} \quad \text{and} \\ \text{REF}(f) &= \{(x, 0^n) \,\big|\, \neg x \in \text{TAUT and } \exists y[|y| \leq n \text{ and } f(y) = \neg x]\}. \end{aligned}$$

Conversely, for every disjoint NP-pair (A, B), we can define a proof system $f_{A,B}$ [9] as follows. Choose a g that is polynomial-time computable and polynomial-time invertible such that $A \leq_m^p \text{SAT}$ via g and $range(g)$ consists only of propositional formulas. Let N be an NP-machine that accepts B in time p. Define

$$f_{A,B}(z) \stackrel{df}{=} \begin{cases} \neg g(x) & : \text{ if } z = 0\langle x, w \rangle, |w| = p(|x|), \text{ and } N(x) \text{ accepts along path } w \\ x & : \text{ if } z = 1\langle x, w \rangle, |z| \geq 2^{|x|}, \text{ and } x \in \text{TAUT} \\ \text{TRUE} & : \text{ otherwise} \end{cases}$$

Theorem 2.1 ([9]) *For every disjoint* NP*-pair* (A, B)*,* $f_{A,B}$ *is a propositional proof system and* $(A, B) \equiv_m^p can(f_{A,B})$*.*

Definition 2.2 *Let* $\mathcal{D} = \{d_i\}_{i\geq 0}$ *be a set of many-one degrees of disjoint NP-pairs and* $\mathcal{P} = \{f_i\}_{i\geq 0}$ *be a set of proof systems. We say that* $\mathcal{P}$ *is a* proof-system representation *of* $\mathcal{D}$ *if the following hold:*

i. $\forall i \geq 0,\ can(f_i) \in d_i$*,*

ii. $\forall i, j \geq 0,\ d_i \leq d_j \Rightarrow f_i \leq f_j$*.*

Note that Item (ii) in the above definition can be really stated as $\forall i, j \geq 0,\ d_i \leq d_j \Leftrightarrow f_i \leq f_j$ since for any proof systems f and g, $f \leq g \Rightarrow\ can(f) \leq_m^p can(g)$ [9].

Definition 2.3 *Let* $\mathcal{D} = \{d_i\}_{i\geq 0}$ *be a set of many-one degrees of disjoint* NP*-pairs and* $\mathcal{S} = \{(A_i, B_i)\}_{i\geq 0}$ *be a set of* NP*-pairs. We say that* $\mathcal{S}$ *is a nesting representation of* $\mathcal{D}$ *if the following hold:*

i. $\forall i \geq 0,\ (A_i, B_i) \in d_i$*,*

ii. $\forall i, j \geq 0,\ d_i \leq d_j \Rightarrow\ A_i \subseteq A_j\ \wedge\ B_i \subseteq B_j$*.*

In the above definition, each (A_i, B_i) is called the *representative* NP-pair of d_i.

3 Results

Glaßer et al. [10] showed that any set of two comparable many-one degrees d_1 and d_2 of NP-pairs has a proof system representation. We generalize this result to any set of many-one degrees of NP-pairs that overlaps with the lower span of each degree on a finite set only.

Theorem 3.1 *Let* $\mathcal{D} = \{d_i\}_{i\geq 0}$ *be a set of many-one degrees of* NP*-pairs such that the intersection of the lower span of each* d_i *with* $\mathcal{D}$ *is a finite set. Then* $\mathcal{D}$ *has a proof-system representation.*

Proof. Fix a set of disjoint NP-pairs $\{(A_i, B_i)\}_{i\geq 0}$ such that for every $i \geq 0$, $(A_i, B_i) \in d_i$. Furthermore, for each i let N_i be the NP-machine that accepts B_i in time bounded by a polynomial p_i and let g_i be a one-to-one and polynomial-time invertible reduction such that $A_i \leq_m^p$ SAT via g_i and $range(g_i)$ is a subet of propositional formulas. (Such a g_i exists since SAT is a paddable complete set [1].) Furthermore, we assume that for every $i \neq j \geq 0$, $range(g_i) \cap range(g_j) = \emptyset$. This can be done by replacing g_i with $g_i'(x) = \underbrace{\text{TRUE} \wedge \text{TRUE} \wedge \cdots \wedge \text{TRUE}}_{i} \wedge (\neg\text{FALSE}) \wedge g_i(x)$.

For any $i \geq 0$, since the intersection of the lower span of d_i with $\mathcal{D}$ is a finite set, let $d_{i_1}, d_{i_2}, \cdots, d_{i_k}$, where $k \geq 0$, be the only degrees in $\mathcal{D}$ such that $d_j < d_i$ for every $j \in \{i_1, i_2, \cdots, i_k\}$.

Now we define f_i as follows:

$$f_i(z) \stackrel{df}{=} \begin{cases} \neg g_j(x) & : \text{ if } z = 0^{j+1}1\langle x, w\rangle,\ |w| = p_j(|x|), \text{ and } N_j(x) \text{ accepts along path } w, \\ & \quad \text{where } j \in \{i_1, i_2, \cdots, i_k, i\}. \\ x & : \text{ if } z = 1\langle x, w\rangle,\ |z| \geq 2^{|x|}, \text{ and } x \in \text{TAUT} \\ \text{TRUE} & : \text{ otherwise} \end{cases}$$

Line 3 of the definition of f_i can be computed in polynomial time by brute-force search. Hence, f_i is a polynomial-time computable function. Note that for any x accepted by N_j, $x \in B_j \subseteq \overline{A_j}$ and hence $g_j(x) \in$ UNSAT since g_j is a many-one reduction from A_j to SAT and $range(g_j)$ contains only propositional formulas. This shows $range(f_i) \subseteq$ TAUT. Also, for every tautology y,

$$f(1\langle y, 0^{2^{|y|}}\rangle) = y,$$

and so f_i is a mapping onto TAUT. Therefore, f_i is a proof system.

We claim that $\{f_i\}$ defined above is a proof system representation of $\mathcal{D}$. First we note that for each tautology $x \neq$ TRUE and $j \in \{i_1, i_2, \cdots, i_k\}$, every f_j-proof of x is also an f_i-proof of x. It follows that $f_j \leq f_i$ for every $j \in \{i_1, i_2, \cdots, i_k\}$. This proves that for every $i, j \geq 0$, $d_j \leq d_i \Rightarrow f_j \leq f_i$.

It remains to show that $can(f_i) \equiv_m^p (A_i, B_i)$ for every $i \geq 0$. We first show that $(A_i, B_i) \leq_m^p can(f_i)$. The reduction is given by

$$h_i' : \ x \mapsto (g_i(x), 0^{2(|x|+p_i(|x|))+i+2}).$$

Clearly h_i' is polynomial-time computable. Assume $x \in A_i$. Then $g_i(x) \in$ SAT since g_i many-one reduces A_i to SAT, and hence $h_i'(x) \in \text{SAT}^*$. Now assume $x \in B_i$. Then $g_i(x) \in$ UNSAT and hence $\neg g_i(x)$ is a tautology. Let w be an accepting path of N_i on x with $|w| = p_i(|x|)$. Then $f_i(0^{i+1}1\langle x, w\rangle) = \neg g_i(x)$ and hence $h_i'(x) \in \text{REF}(f_i)$, since $|0^{i+1}1\langle x, w\rangle| = 2(|x| + p_i(|x|)) + i + 2$.

Now we show that $can(f_i) \leq_m^p (A_i, B_i)$. For each $j \in \{i_1, i_2, \cdots, i_k\}$, let r_{ji} be a polynomial-time many-one reduction from (A_j, B_j) to (A_i, B_i). Let r_{ii} be the identity function. Choose elements $a_i \in A_i$ and $b_i \in B_i$. Define a reduction function h_i as follows.

```
1       input (y, 0^n)
2       if n ≥ 2^(|y|+1) then
3          if y ∈ SAT then output a_i else output b_i
4       for each j ∈ {i_1, i_2, ··· , i_k, i} do
5          if g_j^(-1)(y) exists
6             let x = g_j^(-1)(y)
7             if n ≥ 2(|x| + p_j(|x|)) + j + 2 then output r_ji(x)
8       output a_i
```

The exhaustive search in line 3 is possible in quadratic time in n, so h_i is polynomial-time computable.

Assume $(y, 0^n) \in \mathrm{SAT}^*$. Then $y \in \mathrm{SAT}$. If the output is made in line 3, then we output $a_i \in A_i$. Otherwise we reach line 4. If the output is made in line 7 for some $j \in \{i_1, i_2, \cdots, i_k, i\}$, then $x = g_j^{-1}(y) \in A_j$ and we output $r_{ji}(x) \in A_i$ since r_{ji} is a many-one reduction from (A_j, B_j) to (A_i, B_i). Otherwise we reach line 8 and we output $a_i \in A_i$. Therefore, in all cases we output an element in A_i.

Assume $(y, 0^n) \in \mathrm{REF}(f_i)$ (in particular $y \in \mathrm{UNSAT}$). So there exists z such that $|z| \leq n$ and $f_i(z) = \neg y$. If the output is made in line 3, then we output $b_i \in B_i$. Otherwise we reach line 4. So far we have $\neg y \neq \mathrm{TRUE}$ (syntactically) and $|z| \leq n < 2^{|y|+1}$. Therefore, $f_i(z) = \neg y$ must be due to line 1 in the definition of f_i. Since $range(g_i), range(g_{i_1}), range(g_{i_2}), \cdots, range(g_{i_k})$ are all pair-wise disjoint, this implies that there is a unique $j \in \{i_1, i_2, \cdots, i_k, i\}$ such that $x = g_j^{-1}(y)$ exists and $n \geq 2(|x| + p_j(|x|)) + j + 2$. Then the output of h_i must be made in line 7, which outputs $r_{ji}(x)$. Since $x = g_j^{-1}(y) \in B_j$ (again by line 1 of f_i's definition) and r_{ji} is a many-one reduction (or the identity function in case $j = i$) from (A_j, B_j) to (A_i, B_i), it follows that the output $r_{ji}(x) \in B_i$. This shows that $can(f_i) \leq_m^p (A_i, B_i)$ via h_i and finishes the proof of Theorem 3.1. □

The proof of Theorem 3.1 essentially shows also that a set of many-one degrees of disjoint NP-pairs has a nesting representation if it satisfies the same property as in Theorem 3.1:

Corollary 3.2 *Let $\mathcal{D} = \{d_i\}_{i \geq 0}$ be a set of many-one degrees of disjoint* NP*-pairs where the lower span of each d_i consists only of a finite set of degrees in $\mathcal{D}$. Then $\mathcal{D}$ has a nesting representation.*

Proof. Let $\mathcal{D}$ be a set of many-one degrees of disjoint NP-pairs as in the premise. Consider the proof systems $\{f_i\}_{i \geq 0}$ constructed in the proof of Theorem 3.1. Note that for every $i \geq 0$, $(\mathrm{TRUE}, 0^0) \in \mathrm{REF}(f_i)$ since $f_i(\lambda) = \mathrm{TRUE}$. For every tautology $x \neq \mathrm{TRUE}$, an f_j-proof of x is also an f_i-proof if $f_j \leq f_i$. Therefore, for every $i, j \geq 0$, $f_j \leq f_i$ implies that $\mathrm{REF}(f_j) \subseteq \mathrm{REF}(f_i)$. Now let $(A_i, B_i) = can(f_i)$ for every $i \geq 0$ and it is clear that $\{(A_i, B_i)\}$ is a nesting representation of $\mathcal{D}$. □

We define a *linear chain* of many-one degrees of NP-pairs to be a set of many-one degrees of NP-pairs $\mathcal{D} = \{d_i\}_{i \geq 0}$ such that $d_0 \leq d_1 \leq d_2 \leq \cdots$.

Corollary 3.3 *Any linear chain of many-one degrees of* NP*-pairs has both a proof system representation and a nesting representation.*

Now let $\mathcal{D}$ be a set of many-one degrees of disjoint NP-pairs. We have shown that $\mathcal{D}$ has both a proof system representation and a nesting representation if the intersection of $\mathcal{D}$ with the lower span of each degree in $\mathcal{D}$ is a finite set. A more general question is under exactly what condition $\mathcal{D}$ possesses these representations. We don't see a straightforward adaption of the proof that generalizes Theorem 3.1 or Corollary 3.2 significantly. Another related question is whether proof system and nesting representations yield each other for $\mathcal{D}$. In probing into this question, we were only able to show that $\mathcal{D}$ has a proof system representation if it has a nesting representation where all representative NP-pairs share the same set as their first components.

Theorem 3.4 *Suppose that $\mathcal{D} = \{d_i\}_{i\geq 0}$ is a set of many-one degrees of NP-pairs with a nesting representation $\{(A, B_i)\}_{i\geq 0}$. Then $\mathcal{D}$ has a proof-system representation.*

Proof. Fix $\mathcal{D}$ and $\{(A, B_i\}_{i\geq 0}$ as in the premise. Then the following hold:

- $\forall i \geq 0,\ (A, B_i) \in d_i$,
- $\forall i, j \geq 0,\ d_i \leq d_j \Rightarrow\ B_i \subseteq B_j$.

For each $i \geq 0$ let N_i be the NP-machine that accepts B_i in time bounded by a polynomial p_i and let g be a polynomial-time invertible reduction such that $A \leq_m^p$ SAT via g. Let $f_i = f_{A,B_i}$ using N_i and g. By Theorem 2.1, $can(f_i) \equiv_m^p (A, B_i)$.

Now let $d_i, d_j \in \mathcal{D}$ such that $d_i \leq d_j$. Then we have $B_i = L(N_i) \subseteq B_j = L(N_j)$. Now consider any tautology $y \neq$ TRUE. If y has an f_i-proof of the form $z = 0\langle x, w\rangle$, then by line 1 of the definition of f_i we have $y = \neg g(x)$, where $x \in B_i \subseteq B_j$. Now let w' be an accepting path of N_j on x with length $p_j(|x|)$. Then $z' = 0\langle x, w'\rangle$ is an f_j-proof of y. Note that $|x|$ is bounded by a polynomial in $|y|$ since g is polynomial-time invertible. Hence, $|z'| = 2(|x| + p_j(|x|)) + 1$ is bounded by a polynomial in $|y|$. Now assume that y has an f_i-proof of the form $z = 1\langle x, w\rangle$, where $|z| \geq 2^{|x|}$, then clearly z is also an f_j-proof of y by the definition of f_j. This shows that $f_i \leq f_j$ and hence $\{f_i\}$ is a proof system representation of $\mathcal{D}$.

□

4 Acknowledgment

We thank Ken Regan for asking the question of whether a linear chain of many-one degrees of disjoint NP-pairs has a nesting representation, which motivated the work in this paper.

References

[1] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity I & II.* Springer, 1989 and 1990.

[2] O. Beyersdorff. Disjoint NP-pairs from propositional proof systems. In *Proceedings 3rd Conference on Theory and Applications of Models of Computation*, volume 3959 of *Lecture Notes in Computer Science*, pages 236–247, 2006.

[3] O. Beyersdorff. Classes of representable disjoint NP-pairs. *Theoretical Computer Science*, 377(1-3):93–109, 2007.

[4] O. Beyersdorff. On the existence of complete disjoint NP-pairs. In *11th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 282–289. IEEE, 2009.

[5] O. Beyersdorff and Z. Sadowski. Characterizing the existence of optimal proof systems and complete sets for promise classes. In *Proceedings Fourth International Computer Science Symposium in Russia*, pages 47–58, Novosibirsk, Russia, August 2009.

[6] S. A. Cook and R. A. Reckhow. The relative efficiency of propositional proof systems. *The Journal of Symbolic Logic*, 44(1):36–50, 1979.

[7] C. Glaßer, A. Selman, S. Sengupta, and L. Zhang. Disjoint NP-pairs. *SIAM Journal on Computing*, 33(6):1369–1416, 2004.

[8] C. Glaßer, A. Selman, and L. Zhang. Survey of disjoint NP-pairs and relations to propositional proof systems. In O. Goldreich, A. L. Rosenberg, and A. L. Selman, editors, *Theoretical Computer Science - Essays in Memory of Shimon Even*, volume 3895 of *Lecture Notes in Computer Science*. Springer, 2006.

[9] C. Glaßer, A. L. Selman, and L. Zhang. Canonical disjoint NP-pairs of propositional proof systems. *Theoretical Computer Science*, 370:60–73, 2007.

[10] C. Glaßer, A. L. Selman, and L. Zhang. The informational content of canonical disjoint NP-pairs. *International Journal of Foundations of Computer Science*, 20(3):501–522, 2009.

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

[12] S. Homer and A. Selman. *Computability and Complexity Theory*. Texts in Computer Science. Springer, New York, 2001.

[13] J. Lutz L. Fortnow and E. Mayordomo. Inseparability and strong hypotheses for disjoint NP pairs. In *Proceedings of the Twenty-Seventhth International Symposium on Theoretical Aspects of Computer Science*, pages 395–404, March) 2010.

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

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

[16] Z. Sadowski. Optimal proof systems, optimal acceptors and recursive presentability. *Fundamenta Informaticae*, 79(1-2):169–185, 2007.