Canonical Disjoint NP-Pairs of Propositional Proof Systems[*]

Christian Glaßer [†] Alan L. Selman[‡] Liyu Zhang[§]

September 26, 2006

Abstract

We prove that every disjoint NP-pair is polynomial-time, many-one equivalent to the canonical disjoint NP-pair of some propositional proof system. Therefore, the degree structure of the class of disjoint NP-pairs and of all canonical pairs is identical. We show that this degree structure is not superficial: Assuming there exist P-inseparable disjoint NP-pairs, *every* countable distributive lattice can be embedded into every interval of polynomial NP-*degrees* of disjoint pairs by maps that preserve the least and greatest element, respectively. As one consequence of this embedding, under the same assumption, there exist intermediate disjoint NP-pairs. That is, if (A, B) is a P-separable disjoint NP-pair and (C, D) is a P-inseparable disjoint NP-pair, then there exist P-inseparable, incomparable NP-pairs (E, F) and (G, H) whose degrees lie strictly between (A, B) and (C, D). Furthermore, between any two disjoint NP-pairs that are comparable and inequivalent, such a diamond exists.

1 Introduction

One reason why it is important to study the class DisjNP of all disjoint NP-pairs is its relationship to the theory of proof systems for propositional calculus. Specifically, Razborov [Raz94] defined the canonical disjoint NP-pair, $(\mathrm{SAT}^*, \mathrm{REF}_f)$, for every propositional proof system f, and he showed that if there exists an optimal propositional proof system f, then its canonical pair is a complete pair for DisjNP. (We will explain this notation later.) In the same paper he asked for evidence of existence of a propositional proof system whose canonical disjoint NP-pair is not separable by a set belonging to the complexity class P, and, relatedly, he asked whether it is possible to reduce to canonical pairs $(\mathrm{SAT}^*, \mathrm{REF}_f)$, another disjoint NP-pair that we believe to be hard (i.e., not separable by a set in P). We answer these questions in the strongest possible way. We prove

[*] A preliminary version of this paper was presented at the 30th International Symposium on Mathematical Foundations of Computer Science, Gdansk, Poland, 2005.

[†] Lehrstuhl für Informatik IV, Universität Würzburg, Am Hubland, 97074 Würzburg, Germany. Email: glasser@informatik.uni-wuerzburg.de

[‡] Department of Computer Science and Engineering, University at Buffalo, Buffalo, NY 14260. Research partially supported by NSF grant CCR-0307077 and by the Alexander von Humboldt-Stiftung. Email: selman@cse.buffalo.edu

[§] Department of Computer Science and Engineering, University at Buffalo, Buffalo, NY 14260. Email: lzhang7@cse.buffalo.edu

that every disjoint NP-pair is polynomial-time, many-one equivalent to the canonical disjoint NP-pair of some propositional proof system. It follows immediately that every disjoint NP-pair we believe to be P-inseparable (cannot be separated by a set in P) is many-one equivalent to some pair $(\mathrm{SAT}^*, \mathrm{REF}_f)$ that is also P-inseparable.

This paper does not address the question of whether P-inseparable disjoint NP-pairs exist, but we mention that there is evidence for their existence, for example, if $\mathrm{P} \neq \mathrm{UP}$ or if $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$ [GS88]. On the other hand, the hypothesis that $\mathrm{P} \neq \mathrm{NP}$ does not seem to be sufficient to obtain P-inseparable disjoint NP-pairs. Homer and Selman [HS92] constructed an oracle relative to which $\mathrm{P} \neq \mathrm{NP}$ and all disjoint NP-pairs are P-separable.

It is easy to see that if proof system f simulates proof system g, then the pair $(\mathrm{SAT}^*, \mathrm{REF}_g)$ is many-one reducible to the pair $(\mathrm{SAT}^*, \mathrm{REF}_f)$. A proof system is *optimal* if it simulates every other propositional proof system. Although it is an open question whether optimal proof systems exist, as we stated above, Razborov showed that if there exists an optimal propositional proof system f, then its canonical pair is a complete pair for DisjNP. We obtain this result of Razborov as a corollary of our result above.

Glaßer et al. [GSSZ04] constructed an oracle relative to which the converse of Razborov's result does not hold; i.e., relative to this oracle, using our current result, there is a propositional proof system f whose canonical pair is complete, but f is not optimal. Hence, there is a propositional proof system g such that the canonical pair of g many-one reduces to the canonical pair of f, but f does not simulate g. Our Theorem 3.1 presents a tight connection between disjoint NP-pairs and propositional proof systems. Nevertheless, relative to this oracle, the relationship is not as tight as we might hope for.

In light of our result above, by examining the degree structure of the class DisjNP, we can understand the degree structure of canonical pairs $(\mathrm{SAT}^*, \mathrm{REF}_f)$. Thus, as Pudlák [Pud03] has expressed, we should try to understand the degree structure of DisjNP. Assuming P-inseparable disjoint NP-pairs exist, we prove that every countable distributive lattice can be embedded into every interval of polynomial NP-*degrees* of disjoint NP-pairs by maps that preserve the least and greatest element, respectively. Our proof is an adaptation of the techniques of Ambos-Spies [AS84] for the analogous results about the degrees of NP-sets. As a consequence, between any two comparable and inequivalent disjoint NP-pairs (A, B) and (C, D) there exist P-inseparable, incomparable disjoint NP-pairs (E, F) and (G, H) whose degrees lie strictly between (A, B) and (C, D). This corollary is an analogue of Ladner's result for NP [Lad75]. Thus, assuming that P-inseparable disjoint NP-pairs exist, the class DisjNP has a rich, dense, degree structure—and each of these degrees contains a canonical pair.

2 Preliminaries

A disjoint NP-pair (NP-pair for short) is a pair (A, B) of nonempty sets A and B such that $A, B \in \mathrm{NP}$ and $A \cap B = \emptyset$. Let DisjNP denote the class of all disjoint NP-pairs.

Given a disjoint NP-pair (A, B), a *separator* is a set S such that $A \subseteq S$ and $B \subseteq \overline{S}$; we say that S *separates* (A, B). Let $Sep(A, B)$ denote the class of all separators of (A, B). For disjoint NP-pairs

(A, B), the fundamental question is whether $Sep(A, B)$ contains a set belonging to P. In that case the pair is P-*separable*; otherwise, the pair is P-*inseparable*. The following proposition summarizes known results about P-separability.

Proposition 2.1

1. $\mathrm{P} \neq \mathrm{NP} \cap co\text{-}\mathrm{NP}$ *implies* DisjNP *contains* P-*inseparable pairs.*
2. $\mathrm{P} \neq \mathrm{UP}$ *implies* DisjNP *contains* P-*inseparable pairs [GS88].*
3. *If* DisjNP *contains* P-*inseparable pairs, then there exists a* P-*inseparable* $(A, B) \in$ DisjNP *such that* A *and* B *are* NP-*complete [GS88].*

While it is probably the case that DisjNP contains P-inseparable pairs, there is an oracle relative to which $\mathrm{P} \neq \mathrm{NP}$ and P-inseparable pairs in DisjNP do not exist [HS92]. So $\mathrm{P} \neq \mathrm{NP}$ probably is not a sufficiently strong hypothesis to show existence of P-inseparable pairs in DisjNP.

We review the natural notions of reducibilities between disjoint pairs. The original notions are nonuniform [GS88]. Here we state only the known equivalent uniform versions [GS88, GSSZ04].

Definition 2.2 *Let* (A, B) *and* (C, D) *be disjoint pairs.*

1. (A, B) *is* many-one reducible in polynomial-time *to* (C, D), $(A, B) \leq_m^{pp} (C, D)$, *if there exists a polynomial-time computable function* f *such that* $f(A) \subseteq C$ *and* $f(B) \subseteq D$.
2. (A, B) *is* Turing reducible in polynomial-time *to* (C, D), $(A, B) \leq_T^{pp} (C, D)$, *if there exists a polynomial-time oracle Turing machine* M *such that for every separator* S *of* (C, D), $L(M, S)$ *is a separator of* (A, B).
3. (A, B) *is* polynomial-time many-one equivalent *to* (C, D), $(A, B) \equiv_m^{pp} (C, D)$, *if* $(A, B) \leq_m^{pp} (C, D)$ *and* $(C, D) \leq_m^{pp} (A, B)$.
4. (A, B) *is* polynomial-time Turing equivalent *to* (C, D), $(A, B) \equiv_T^{pp} (C, D)$, *if* $(A, B) \leq_T^{pp} (C, D)$ *and* $(C, D) \leq_T^{pp} (A, B)$.
5. (A, B) *is a* polynomial-time many-one-complete disjoint NP-pair *(complete disjoint* NP-*pair for short), if* $(A, B) \in$ DisjNP *and for all* $(C, D) \in$ DisjNP, $(C, D) \leq_m^{pp} (A, B)$.

Definition 2.3 *For every disjoint pair* (A, B), *the* polynomial-time NP-Turing-degree *(*NP-*Turing-degree for short) of* (A, B) *is defined as*

$$\mathbf{d}(A, B)|\mathrm{NP} = \{(C, D) \in \mathrm{DisjNP} \mid (A, B) \equiv_T^{pp} (C, D)\}.$$

We use $\mathcal{R}^{pp}_{T,\mathrm{NP}}|\mathrm{NP}$ to denote the collection of NP-Turing-degrees of disjoint NP-pairs, i.e.,

$$\mathcal{R}^{pp}_{T,\mathrm{NP}}|\mathrm{NP} = \{\mathbf{d}(A,B) \mid (A,B) \in \mathrm{DisjNP}\}.$$

Note that NP-Turing-degrees are actually confinements of Turing-degrees of disjoint-pairs on DisjNP, which could be denoted by $\mathbf{d}(A,B)$ in the standard way. However, since we are only interested in NP-Turing-degrees of disjoint NP-pairs and want to keep notations simple, we will use $\mathbf{d}(A,B)$ for $\mathbf{d}(A,B)|\mathrm{NP}$ and $\mathcal{R}^{pp}_{T,\mathrm{NP}}$ for $\mathcal{R}^{pp}_{T,\mathrm{NP}}|\mathrm{NP}$ throughout the rest of the paper.

We will denote elements in $\mathcal{R}^{pp}_{T,\mathrm{NP}}$ by $\mathbf{a}$, $\mathbf{b}$, ...

Let TAUT denote the set of tautologies. Cook and Reckhow [CR79] defined a *propositional proof system* (proof system for short) to be a function $f : \Sigma^* \to \mathrm{TAUT}$ such that f is onto and computable in polynomial time. The canonical pair of f [Raz94, Pud01] is the disjoint NP-pair $(\mathrm{SAT}^*, \mathrm{REF}_f)$ where

$$\begin{aligned}
\mathrm{SAT}^* &= \{(x, 0^n) \,|\, x \in \mathrm{SAT}\} \quad \text{and}\\
\mathrm{REF}_f &= \{(x, 0^n) \,|\, \neg x \in \mathrm{TAUT} \text{ and } \exists y[|y| \le n \text{ and } f(y) = \neg x]\}.
\end{aligned}$$

Let f and f' be two propositional proof systems. We say that f *simulates* 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 $|h(w)| \le p(|w|)$. A proof system is *optimal* if it simulates every other proof system.

3 Canonical Pairs of Proof Systems

Now we state the main result of this paper. We show that for every disjoint NP-pair (A,B) there exists a proof system f such that $(\mathrm{SAT}^*, \mathrm{REF}_f) \equiv^{pp}_m (A,B)$. This shows that disjoint NP-pairs and canonical pairs of proof systems have identical degree structures.

Theorem 3.1 *For every disjoint* NP*-pair* (A,B) *there exists a proof system* f *such that* $(\mathrm{SAT}^*, \mathrm{REF}_f) \equiv^{pp}_m (A,B)$.

Proof. Let $\langle \cdot, \cdot \rangle$ be a polynomial-time computable, polynomial-time invertible pairing function such that $|\langle v, w \rangle| = 2|vw|$. Choose g that is polynomial-time computable and polynomial-time invertible such that $A \le^p_m \mathrm{SAT}$ via g (such a g exists, since SAT is a paddable NP-complete set). Let M be an NP-machine that accepts B in time p. Define the following function f.

$$f(z) \overset{df}{=} \begin{cases} \neg g(x) & : \text{ if } z = \langle x, w \rangle,\ |w| = p(|x|),\ M(x) \text{ accepts along path } w \\ x & : \text{ if } z = \langle x, w \rangle,\ |w| \ne p(|x|),\ |z| \ge 2^{|x|},\ x \in \mathrm{TAUT} \\ \text{true} & : \text{ otherwise} \end{cases}$$

The function is polynomial-time computable, since in the second case, $|z|$ is large enough so that $x \in \mathrm{TAUT}$ can be decided by the brute force algorithm in deterministic time $O(|z|^2)$. (Note that in the second case, the condition $|z| \geq 2^{|x|}$ is equivalent to the condition $\log |z| \geq |x|$.) In the first case of f's definition, $x \in B$ and so $g(x) \notin \mathrm{SAT}$. It follows that $f : \Sigma^* \rightarrow \mathrm{TAUT}$. The mapping is onto, since for every tautology y,

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

Therefore, f is a propositional proof system.

Claim 3.2 $(\mathrm{SAT}^*, \mathrm{REF}_f) \leq_m^{pp} (A, B)$.

Choose elements $a \in A$ and $b \in B$. The reduction function h is as follows.

```
1   input $(y, 0^n)$
2   if $n \geq 2^{|y|}$ then
3       if $y \in SAT$ then output a else output b
4   endif
5   if $g^{-1}(y)$ exists then output $g^{-1}(y)$
6   output a
```

The condition in line 2 is equivalent to $\log n \geq |y|$. The exhaustive search in line 3 is possible in quadratic time in n. So h is computable in polynomial time.

Assume $(y, 0^n) \in \mathrm{SAT}^*$. If we reach line 3, then we output $a \in A$. Otherwise we reach line 5. If $g^{-1}(y)$ exists, then it belongs to A. Therefore, in either case (output in line 5 or in line 6) we output an element from A.

Assume $(y, 0^n) \in \mathrm{REF}_f$ (in particular $\neg y \in \mathrm{TAUT}$). So there exists z such that $|z| \leq n$ and $f(z) = \neg y$. If we reach line 3, then we output b. Otherwise we reach line 5 and so it holds that $|z| \leq n < 2^{|y|}$ and $\neg y$ syntactically differs from the expression true. Therefore, $f(z) = \neg y$ must be due to line 1 in the definition of f. It follows that $g^{-1}(y)$ exists. So we output $g^{-1}(y)$ which belongs to B (again by line 1 of f's definition). This shows Claim 3.2.

Claim 3.3 $(A, B) \leq_m^{pp} (\mathrm{SAT}^*, \mathrm{REF}_f)$.

The reduction function is $h'(x) \stackrel{df}{=} (g(x), 0^{2(|x|+p(|x|))})$. If $x \in A$, then $g(x) \in \mathrm{SAT}$ and therefore, $h'(x) \in \mathrm{SAT}^*$. Otherwise, let $x \in B$. Let w be an accepting path of $M(x)$ and define $z \stackrel{df}{=} \langle x, w \rangle$. So $|w| = p(|x|)$ and $|z| = 2(|x| + p(|x|))$. By line 1 in f's definition, $f(z) = \neg g(x)$. Therefore, $h'(x) \in \mathrm{REF}_f$. This proves Claim 3.3 and finishes the proof of Theorem 3.1. □

Corollary 3.4 *Disjoint* NP*-pairs and canonical pairs for proof systems have identical degree structures.*

The following easy to prove proposition also states a strong connection between proof systems and disjoint NP-pairs:

Proposition 3.5 *Let f and g be proof systems. If g simulates f, then*

$$(\mathrm{SAT}^*, \mathrm{REF}_f) \leq_m^{pp} (\mathrm{SAT}^*, \mathrm{REF}_g).$$

Proof. By assumption there exists a total function $h : \Sigma^* \to \Sigma^*$ and a polynomial p such that for all x, $g(h(x)) = f(x)$ and $|h(x)| \leq p(|x|)$. We claim that $(\mathrm{SAT}^*, \mathrm{REF}_f) \leq_m^{pp} (\mathrm{SAT}^*, \mathrm{REF}_g)$ via reduction r where $r(x, 0^n) \overset{df}{=} (x, 0^{p(n)})$. Clearly, if $(x, 0^n) \in \mathrm{SAT}^*$, then $(x, 0^{p(n)}) \in \mathrm{SAT}^*$ as well. Let $(x, 0^n) \in \mathrm{REF}_f$, i.e., $\neg x$ is a tautology and there exists y such that $|y| \leq n$ and $f(y) = \neg x$. So for $y' \overset{df}{=} h(x)$ it holds that $|y'| \leq p(n)$ and $g(y') = \neg x$ which shows $(x, 0^{p(n)}) \in \mathrm{REF}_g$. □

The following result of Razborov [Raz94] is an immediate consequence of Theorem 3.1 and Proposition 3.5.

Corollary 3.6 (Razborov) *If there exists an optimal propositional proof system f, then $(\mathrm{SAT}^*, \mathrm{REF}_f)$ is a complete disjoint* NP*-pair.*

We remind the reader that it is known neither whether there exists an optimal propositional proof systems nor whether there exist complete NP-pairs. Now it is appropriate to repeat a comment we stated in the introduction. Glaßer et al. [GSSZ04] constructed an oracle relative to which the converse of Corollary 3.6 does not hold; i.e., relative to this oracle, by Theorem 3.1, there is a propositional proof system f whose canonical pair is complete, but f is not optimal. Hence, there is a propositional proof system g such that the canonical pair of g many-one reduces to the canonical pair of f, but f does not simulate g. The results of this section present tight connections between disjoint NP-pairs and propositional proof systems. Nevertheless, relative to this oracle, the relationship is not as tight as one might hope for.

4 Degree Structure of Disjoint NP-Pairs

We are interested in the structure of NP-Turing-degrees of disjoint NP-pairs. We will show that any countable distributive lattice can be embedded into the interval between two comparable NP-Turing-degrees of disjoint NP-pairs while preserving either the least or greatest element. Similar results on NP-sets were shown by Ambos-Spies [AS84] and extended by Merkle [Mer02]. However, the previous results were only shown for degree of sets and there has been no proof that such embedding results would also hold on disjoint NP-pairs. The proof techniques are similar to those used in the previous results.

We follow the approach of Ambos-Spies [AS84], combined with notations and results of Schöning [Sch82].

4.1 Distributive Lattices and Elementary Results

A *partially ordered (p.o.)* set $\mathcal{L} = \langle L; \leq \rangle$ is a set L with a partial ordering[1] $\leq$ defined on L. For any $a, b \in L$, define

$$\sup\{a,b\} = c, \text{ where } c \in L \text{ and } (\forall d \in L)\ [(a \leq d) \wedge (b \leq d) \Rightarrow (c \leq d)],$$

and

$$\inf\{a,b\} = c, \text{ where } c \in L \text{ and } (\forall d \in L)\ [(d \leq a) \wedge (d \leq b) \Rightarrow (d \leq c)].$$

If $\mathcal{L} = \langle L; \leq \rangle$ is a p.o. set and $\sup\{a,b\}$ ($\inf\{a,b\}$) exists for $a, b \in L$, then we call $\sup\{a,b\}$ ($\inf\{a,b\}$) the *join* (*meet*) of a and b and denote it by $a \vee b$ ($a \wedge b$). A p.o. set $\mathcal{L} = \langle L; \leq \rangle$ is an *upper semilattice* if $a \vee b$ exists for every $a, b \in L$; if in addition $a \wedge b$ exists for every $a, b \in L$, then $\mathcal{L}$ is called a *lattice.*

An *order embedding* of a p.o. set $\mathcal{L}_1 = \langle L_1; \leq_1 \rangle$ into a p.o. set $\mathcal{L}_2 = \langle L_2; \leq_2 \rangle$ is a one-to-one map $f : L_1 \rightarrow L_2$ such that $\forall a, b \in L_1$ $(a \leq_1 b \Rightarrow f(a) \leq_2 f(b))$. An order embedding of a lattice $\mathcal{L}_1$ into an upper semilattice $\mathcal{L}_2$ is a *lattice embedding* if

$$\forall a, b \in L_1\ [(f(a \vee b) = f(a) \vee f(b)) \text{ and } (f(a) \wedge f(b) \text{ exists}) \text{ and } (f(a \wedge b) = f(a) \wedge f(b))].$$

The least (greatest) element of a p.o. set $\mathcal{L}$ is denoted by $0_{\mathcal{L}}$ ($1_{\mathcal{L}}$) or simply by 0 (1) if there is no confusion from the context. We say an embedding f of $\mathcal{L}_1$ into $\mathcal{L}_2$ *preserves* the least element or 0 (greatest element or 1) if either $f(0_{\mathcal{L}_1}) = 0_{\mathcal{L}_2}$ ($f(1_{\mathcal{L}_1}) = 1_{\mathcal{L}_2}$) or $0_{\mathcal{L}_1}$ ($1_{\mathcal{L}_1}$) does not exist. A lattice $\mathcal{L} = \langle L; \leq \rangle$ is *distributive* if

$$\forall a, b, c \in L\ ((a \vee b) \wedge (a \vee c) = a \vee (b \wedge c)).$$

A lattice $\mathcal{L}$ is *complemented* if $\forall a \in L\ \exists \overline{a} \in L\ (a \vee \overline{a} = 1 \text{ and } a \wedge \overline{a} = 0)$. A distributive and complemented lattice $\mathcal{L} = \langle L; \leq \rangle$ is *Boolean* if $\mathcal{L}$ possesses 0 and 1, and $0 \neq 1$. An element a of a lattice $\mathcal{L}$ with least element 0 is an *atom* of $\mathcal{L}$ if $0 < a$ and

$$\forall b \in L\ (0 \leq b \leq a \Rightarrow b = 0 \text{ or } b = a).$$

A lattice $\mathcal{L}$ with 0 is atomless if it has no atoms. A proper subset $I \neq \emptyset$ of L is an *ideal* of the upper semilattice $\mathcal{L} = \langle L; \leq \rangle$ if I is closed under joins and $\forall a \in L \forall b \in I\ (a \leq b \Rightarrow a \in I)$. The quotient upper semilattice $\mathcal{L}/I = \langle L^*; \leq^* \rangle$ of $\mathcal{L}$ over the ideal I is defined by $L^* = \{[a] \mid a \in L\}$, where $[a] = \{a \vee b \mid b \in I\}$ and $[a] \leq^* [b]$ if and only if $a \leq b \vee c$ for some $c \in I$. Note that for a Boolean lattice $\mathcal{L}$, $\mathcal{L}/I$ is a Boolean lattice too.

Since it is known [Grä78, Page 64, Theorem 19] that any countable distributive lattice (with at least two elements) can be embedded into the (up to isomorphism unique) countably infinite atomless Boolean lattice by a map that preserves both 0 and 1, it suffices to embed an arbitrary countable atomless Boolean lattice for our purpose. We will use the one stated in the following theorem.

Let $\mathbb{N}$ denote the set of natural numbers. Define

$$\mathrm{P}_{\mathbb{N}} = \{S \mid S \subseteq \mathbb{N} \wedge \mathrm{TALLY}(S) \in \mathrm{P}\},$$

[1] A partial ordering is a binary relation that is reflexive, antisymmetric and transitive.

where $\mathrm{TALLY}(S) = \{0^n \mid n \in S\}$. Let $\langle \mathrm{P}^*_{\mathbb{N}}; \subseteq^* \rangle$ be the quotient lattice of $\langle \mathrm{P}_{\mathbb{N}}; \subseteq \rangle$ over ideal of finite sets. Namely, $\mathrm{P}^*_{\mathbb{N}} = \{[\alpha] | \alpha \in \mathrm{P}_{\mathbb{N}}\}$, where $[\alpha] = \{\beta \mid \alpha \overset{*}{=} \beta\}$ and $\alpha \overset{*}{=} \beta$ if and only if α is a finite variation of β, and $[\alpha] \subseteq^* [\beta]$ if and only if a finite variation of α is a subset of β.

Theorem 4.1 (Ambos-Spies) *1. $\langle \mathrm{P}_{\mathbb{N}}; \subseteq \rangle$ is a Boolean lattice.*

2. $\langle \mathrm{P}^*_{\mathbb{N}}; \subseteq^* \rangle$ is a countable atomless Boolean lattice.

We refer the readers to Ambos-Spies [AS84] for the proof of Theorem 4.1 and to Grätzer [Grä78] for a detailed treatment of the above notions from lattice theory.

The partial ordering on the NP-Turing-degrees of NP-pairs induced by the Turing reduction ($\leq^{pp}_T$) between NP-pairs is denoted by $\leq$. So for $\mathbf{a}, \mathbf{b} \in \mathcal{R}^{pp}_{T,\mathrm{NP}}$,

$$\begin{aligned} \mathbf{a} \leq \mathbf{b} &\Leftrightarrow \exists (A,B) \in \mathbf{a}\ \exists (C,D) \in \mathbf{b}\ (A,B) \leq^{pp}_T (C,D) \\ &\Leftrightarrow \forall (A,B) \in \mathbf{a}\ \forall (C,D) \in \mathbf{b}\ (A,B) \leq^{pp}_T (C,D). \end{aligned}$$

As usual, we write $\mathbf{a} < \mathbf{b}$ if $\mathbf{a} \leq \mathbf{b}$ but not $\mathbf{a} = \mathbf{b}$. We use $\mathbf{a} \vee \mathbf{b}$ and $\mathbf{a} \wedge \mathbf{b}$ to denote the least upper bound and greatest lower bound of $\mathbf{a}$ and $\mathbf{b}$, respectively. Note that given two NP-Turing-degrees $\mathbf{a}$ and $\mathbf{b}$, $\mathbf{a} \wedge \mathbf{b}$ might not exist. We also use the interval $[\mathbf{a}, \mathbf{b}]$ to denote $\{\mathbf{d} \in \mathcal{R}^{pp}_{T,\mathrm{NP}} | \mathbf{a} \leq \mathbf{d} \leq \mathbf{b}\}$.

For sets A and B, let $A \oplus B \overset{df}{=} 0A \cup 1B$ be the disjoint union of A and B. We observe that $\langle \mathcal{R}^{pp}_{T,\mathrm{NP}}; \leq \rangle$ is an upper semilattice because of the following proposition:

Proposition 4.2 *For every (A,B), $(C,D) \in \mathrm{DisjNP}$,*

$$\mathbf{d}(A,B) \vee \mathbf{d}(C,D) = \mathbf{d}(A \oplus C, B \oplus D).$$

Proof. First of all, it is trivial that $(A \oplus C, B \oplus D)$ is an NP-pair, given that (A,B) and (C,D) are NP-pairs. Also, it is easy to see $(A,B) \leq^{pp}_m (A \oplus C, B \oplus D)$ via the function $f(x) = 0x$ and $(C,D) \leq^{pp}_m (A \oplus C, B \oplus D)$ via the function $f(x) = 1x$. So $\mathbf{d}(A,B) \leq \mathbf{d}(A \oplus C, B \oplus D)$ and $\mathbf{d}(C,D) \leq \mathbf{d}(A \oplus C, B \oplus D)$. Now given $\mathbf{d} \in \mathcal{R}^{pp}_{T,\mathrm{NP}}$ such that $\mathbf{d}(A,B) \leq \mathbf{d}$ and $\mathbf{d}(C,D) \leq \mathbf{d}$, we need to show $\mathbf{d}(A \oplus C, B \oplus D) \leq \mathbf{d}$. Let $\mathbf{d} = \mathbf{d}(E,F)$ for some $(E,F) \in \mathrm{DisjNP}$. Then $(A,B) \leq^{pp}_T (E,F)$ and $(C,D) \leq^{pp}_T (E,F)$. Now let S be a separator of (E,F). Then there exists a separator S_1 of (A,B) such that $S_1 \leq^p_T S$ and there exists a separator S_2 of (C,D) such that $S_2 \leq^p_T S$. Define $S' = S_1 \oplus S_2$. Then S' is a separator of $(A \oplus C, B \oplus D)$ and $S' \leq^p_T S$. Hence, $(A \oplus C, B \oplus D) \leq^{pp}_T (E,F)$ and so $\mathbf{d}(A \oplus C, B \oplus D) \leq \mathbf{d}$. □

We also have the following easy to prove proposition that will be used quite often later.

Proposition 4.3 *For any set $G \in \mathrm{P}$ and $(A,B) \in \mathrm{DisjNP}$,*

$$\mathbf{d}(A,B) = \mathbf{d}(A \cap G, B \cap G) \vee \mathbf{d}(A \cap \overline{G}, B \cap \overline{G}).$$

Proof. Clearly, both $(A \cap G, B \cap G)$ and $(A \cap \overline{G}, B \cap \overline{G})$ are NP-pairs too and are many-one (hence, Turing) reducible to (A, B) via the identity function $f(x) = x$. We only have to show for any NP-pair (E, F) that $(A \cap G, B \cap G) \leq_T^{pp} (E, F)$ and $(A \cap \overline{G}, B \cap \overline{G}) \leq_T^{pp} (E, F)$ implies $(A, B) \leq_T^{pp} (E, F)$. Let S be a separator of (E, F). Then there exist a separator S_1 of $(A \cap G, B \cap G)$ and a separator S_2 of $(A \cap \overline{G}, B \cap \overline{G})$ such that $S_1 \leq_T^p S$ and $S_2 \leq_T^p S$. So $S' = (S_1 \cap G) \cup (S_2 \cap \overline{G})$ is a separator of (A, B) and $S' \leq_T^p S$, since $G \in \mathrm{P}$. □

4.2 Effectively Presentable Classes of Disjoint NP-Pairs

In this section, we show that various classes of disjoint NP-pairs are effectively presentable.

Let $\{M_i\}_i$ be a standard effective enumeration of all deterministic Turing machines and let $\{N_i\}_i$ be a standard effective enumeration of all polynomial-time nondeterministic Turing machines.

Definition 4.4 *Define a class $\mathcal{C}$ of disjoint pairs to be* effectively presentable *if there exists a total computable function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ such that*

1. *for all $(i, j) \in \mathrm{range}(f)$, M_i and M_j halt on all inputs, and*
2. *$\mathcal{C} = \{(L(M_i), L(M_j)) \mid (i, j) \in \mathrm{range}(f)\}$.*

Theorem 4.5 *For every disjoint* NP*-pair (A, B), $\mathbf{d}(A, B)$ is effectively presentable.*

Proof. Let $T_1, T_2, \ldots$ be an effective enumeration of deterministic polynomial-time-bounded oracle Turing machines such that T_l's running time on inputs of length n is $n^l + l$. Without loss of generality, we assume A and B are infinite sets. (Otherwise we can always pick $(A', B') = (A \times \Sigma^*, B \times \Sigma^*) \in \mathbf{d}(A, B)$ and A', B' are both infinite.) Define the predicate $\mathrm{Test}(i, j, k, l, m, x)$ to be true if and only if all of the following holds:

1. $L(N_i) \cap L(N_j) \cap \Sigma^{\leq |x|} = \emptyset$
2. for all y such that $|y|^k + k \leq |x|$ and for all $S \subseteq \Sigma^{\leq |x|}$ such that S separates $(L(N_i) \cap \Sigma^{\leq |x|}, L(N_j) \cap \Sigma^{\leq |x|})$ it holds that $(y \in A \Rightarrow T_k^S(y)$ accepts) and $(y \in B \Rightarrow T_k^S(y)$ rejects)
3. for all y such that $|y|^l + l \leq |x|$ and for all $S \subseteq \Sigma^{\leq |x|}$ such that S separates $(A \cap \Sigma^{\leq |x|}, B \cap \Sigma^{\leq |x|})$ it holds that $(y \in L(N_i) \Rightarrow T_l^S(y)$ accepts) and $(y \in L(N_j) \Rightarrow T_l^S(y)$ rejects)
4. $L(N_i) \cap \Sigma^{\leq m} \neq \emptyset$ and $L(N_j) \cap \Sigma^{\leq m} \neq \emptyset$

The predicate Test is certainly decidable. Define

$$f(\langle i, j, k, l, m \rangle) \stackrel{df}{=} (c, d)$$

where c and d are the indices of the machines described below.

- M_c on input x: If $\mathrm{Test}(i,j,k,l,m,x)$, then accept if and only if $x \in L(N_i) - L(N_j)$. Otherwise, accept if and only if $x \in A$.
- M_d on input x: If $\mathrm{Test}(i,j,k,l,m,x)$, then accept if and only if $x \in L(N_j) - L(N_i)$. Otherwise, accept if and only if $x \in B$.

We show that $\mathcal{C}$ is effectively presented by f.

Clearly, f is total and computable. Also, M_c and M_d halt on all inputs, which shows Statement 1 in Definition 4.4. Statement 2 is shown by the following claims.

Claim 4.6 *For every* $(c,d) \in \mathrm{range}(f)$, $(L(M_c), L(M_d)) \in \mathrm{DisjNP}$ *and*

$$(A,B) \equiv_T^{pp} (L(M_c), L(M_d)).$$

Proof. Choose i,j,k,l,m such that $(c,d) = f(\langle i,j,k,l,m \rangle)$. By definitions of M_c and M_d it holds that $L(M_c) \cap L(M_d) = \emptyset$.

Case 1: Assume $\mathrm{Test}(i,j,k,l,m,x)$ holds for all x. Then $L(N_i) \cap L(N_j) = \emptyset$, $L(N_i) \neq \emptyset$ and $L(N_j) \neq \emptyset$. So $L(M_c) = L(N_i) \neq \emptyset$ and $L(M_d) = L(N_j) \neq \emptyset$, and hence, $(L(M_c), L(M_d)) \in \mathrm{DisjNP}$.

We show $(A,B) \leq_T^{pp} (L(M_c), L(M_d))$ via machine T_k and $(L(M_c), L(M_d)) \leq_T^{pp} (A,B)$ via T_l. Let S' be an arbitrary separator of $(L(M_c), L(M_d))$. Assume there exists $y \in A$ such that $T_k^{S'}(y)$ rejects. So $T_k^S(y)$ rejects where $S \overset{df}{=} S' \cap \Sigma^{\leq |y|^k + k}$. Hence Statement 2 in the definition of Test does not hold for $x = 0^{|y|^k + k}$. This contradicts our assumption in Case 1. It follows that if $y \in A$, then $T_k^{S'}(y)$ accepts. Analogously, if $y \in B$, then $T_k^{S'}(y)$ rejects. This shows that $L(T_k^{S'})$ is a separator of (A,B) and hence, $(A,B) \leq_T^{pp} (L(M_c), L(M_d))$. Similar arguments show $(L(M_c), L(M_d)) \leq_T^{pp} (A,B)$.

Case 2: Assume there exists x such that $\mathrm{Test}(i,j,k,l,m,x)$ does not hold. Then $\mathrm{Test}(i,j,k,l,m,y)$ does not hold for all y such that $|y| \geq |x|$. So by the definitions of M_c and M_d, $L(M_c)$ is a finite variation of A, and $L(M_d)$ is a finite variation of B. Hence, trivially $(A,B) \equiv_T^{pp} (L(M_c), L(M_d))$. Note that both A and B are infinite sets. So $L(M_c) \neq \emptyset$ and $L(M_d) \neq \emptyset$ and hence, $(L(M_c), L(M_d)) \in \mathrm{DisjNP}$. This finishes the proof of Claim 4.6.

□

Claim 4.7 *For all* $(X,Y) \in \mathrm{DisjNP}$ *such that* $(A,B) \equiv_T^{pp} (X,Y)$, *there exists* n *such that* $f(n) = (c,d)$, $L(M_c) = X$, *and* $L(M_d) = Y$.

Proof. Let X and Y be as above and choose indices i,j such that $X = L(N_i)$ and $Y = L(N_j)$. Moreover, choose k,l such that $(A,B) \leq_T^{pp} (L(N_i), L(N_j))$ via T_k and $(L(N_i), L(N_j)) \leq_T^{pp} (A,B)$ via T_l. Choose m large enough such that $X \cap \Sigma^{\leq m} \neq \emptyset$ and $Y \cap \Sigma^{\leq m} \neq \emptyset$. Let $n = \langle i,j,k,l,m \rangle$ and $(c,d) = f(n)$.

We claim that $\mathrm{Test}(i,j,k,l,m,x)$ holds for all x. Clearly, Statement 1 in the definition of Test holds for all x. So does Statement 4 by the choice of m. Assume Statement 2 does not hold. So there exist x and y such that $|y|^k + k \leq |x|$ and there exists $S \subseteq \Sigma^{\leq |x|}$ separating $(L(N_i) \cap \Sigma^{\leq |x|}, L(N_j) \cap \Sigma^{\leq |x|})$ such that ($y \in A$ and $T_k^S(y)$ rejects) or ($y \in B$ and $T_k^S(y)$ accepts). Extend S to a separator S' of $(L(N_i), L(N_j))$ such that $S = S' \cap \Sigma^{\leq |x|}$. The computation $T_k^S(y)$ cannot ask strings longer than $|y|^k + k \leq |x|$. Therefore, either ($y \in A$ and $T_k^{S'}(y)$ rejects) or ($y \in B$ and $T_k^{S'}(y)$ accepts). So $T_k^{S'}(y)$ is not a separator of (A, B) showing that (A, B) does not Turing reduce to $(L(N_i), L(N_j)) = (X, Y)$ via machine T_k. This contradicts our assumption and therefore Statement 2 in the definition of Test holds for all x. Similar arguments show Statement 3 holds for all x. So we know that Test(i, j, k, l, x) holds for all x. It follows that $L(M_c) = L(N_i) = X$ and $L(M_d) = L(N_j) = Y$. This proves Claim 4.7. □

This finishes the proof of Theorem 4.5. □

If we remove the argument l and Statement 3 in the definition of the predicate Test and change f accordingly, the same proof shows the following:

Theorem 4.8 *For every disjoint* NP*-pair* (A, B)*, the class of disjoint* NP*-pairs*

$$\{(C, D) \in \text{DisjNP} \mid (C, D) \leq_T^{pp} (A, B)\}$$

is effectively presentable.

We will also need the following property of effectively presentable classes of disjoint pairs:

Theorem 4.9 *If $\mathcal{C}_1$ and $\mathcal{C}_2$ are both effectively presentable classes of disjoint pairs, then $\mathcal{C}_1 \cup \mathcal{C}_2$ is an effectively presentable class of disjoint pairs.*

Proof. Since $\mathcal{C}_1$ and $\mathcal{C}_2$ are effectively presentable, there exist total computable functions f_1 and f_2 such that

- for all $(i, j) \in \text{range}(f_1) \cup \text{range}(f_2)$, M_i and M_j halt on all inputs,
- $\mathcal{C}_1 = \{(L(M_i), L(M_j)) \mid (i, j) \in \text{range}(f_1)\}$, and
- $\mathcal{C}_2 = \{(L(M_i), L(M_j)) \mid (i, j) \in \text{range}(f_2)\}$.

Define a function f as follows: $f(n) = f_1(\frac{n}{2})$ if n is even and $f(n) = f_2(\frac{n-1}{2})$ if n is odd. Clearly, f is total computable too. For every $(i, j) \in \text{range}(f)$, either $(i, j) = f_1(\frac{n}{2})$ for some even number n or $(i, j) = f_2(\frac{n-1}{2})$ for some odd number n. So $(i, j) \in \text{range}(f_1) \cup \text{range}(f_2)$ and hence, M_i and M_j halt on all inputs. Now let $(X, Y) \in \mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2$. Then $(X, Y) \in \mathcal{C}_1$ or $(X, Y) \in \mathcal{C}_2$. So $(X, Y) = (L(M_i), L(M_j))$, where $(i, j) = f_1(n_1)$ for some $n_1 \in \mathbb{N}$ or $(i, j) = f_2(n_2)$ for some $n_2 \in \mathbb{N}$. Therefore, $(X, Y) = (L(M_i), L(M_j))$, where $(i, j) = f(2n_1)$ for some $n_1 \in \mathbb{N}$ or $(i, j) = f(2n_2 + 1)$ for some $n_2 \in \mathbb{N}$. This shows $\mathcal{C} \subseteq \{(L(M_i), L(M_j)) \mid (i, j) \in \text{range}(f)\}$. For the other direction, Let $(i, j) \in \text{range}(f)$. As shown above, $(i, j) \in \text{range}(f_1) \cup \text{range}(f_2)$. So $\{(L(M_i), L(M_j)) \mid (i, j) \in \text{range}(f)\} \in \mathcal{C}_1 \cup \mathcal{C}_2 = \mathcal{C}$. □

4.3 The Embedding Theorem

For a function f, let $f^0(x) = x$ and $f^{n+1}(x) = f(f^n(x))$. For any strictly increasing function $f : \mathbb{N} \to \mathbb{N}$, define the *$n$-th f-interval* I^f_n as follows:

$$I^f_n = \{x \in \Sigma^* \mid f^n(0) \leq |x| < f^{n+1}(0)\}.$$

For $\alpha \subseteq \mathbb{N}$, define

$$I^f_\alpha = \bigcup_{n\in\alpha} I^f_n.$$

Definition 4.10 ([Sch82]) *A function $f : \mathbb{N} \to \mathbb{N}$ is called* fast *if*

1. *for all $n \in \mathbb{N}$, $f(n) > n$, and*
2. *there is a Turing machine M that computes f in unary notation such that M writes a symbol on its output tape every move of its computation.*

Proposition 4.11 ([AS84]) *For every fast function f and $\alpha \in \mathrm{P}_\mathbb{N}$, it holds that $I^f_\alpha \in \mathrm{P}$.*

Definition 4.12 *Let f and g be functions that map $\mathbb{N}$ to $\mathbb{N}$. We say f* dominates *g if for every $n \in \mathbb{N}$, it holds that $f(n) > g(n)$.*

Proposition 4.13 ([Sch82]) *For every total computable function $f : \mathbb{N} \to \mathbb{N}$, there is a fast function $f' : \mathbb{N} \to \mathbb{N}$ that dominates f.*

Given natural numbers k and i, let $k\alpha + i = \{kn + i \mid n \in \alpha\}$. For two disjoint pairs (A, B) and (C, D), we use $(A, B)\triangle(C, D)$ to denote $(A\triangle C) \cup (B\triangle D)$ [2]. Note that $(A, B) = (C, D)$ if and only if $(A, B)\triangle(C, D) = \emptyset$.

Definition 4.14 *A disjoint pair (A', B') is called a* finite variation *of the pair (A, B) if $\|(A \triangle A') \cup (B \triangle B')\|$ is finite. A class $\mathcal{C}$ of disjoint* NP*-pairs is* closed under finite variations *if for all disjoint* NP*-pairs (A, B) and (A', B') it holds that if $(A, B) \in \mathcal{C}$, A' and B' are nonempty, and (A', B') is a finite variation of (A, B), then $(A', B') \in \mathcal{C}$.*

Theorem 4.15 *(Join Theorem) Let (A, B) and (C, D) be disjoint* NP*-pairs such that A, B, C and D are all infinite sets. Let $\mathcal{C}_0$ and $\mathcal{C}_1$ be effectively presentable classes of disjoint* NP*-pairs that are closed under finite variations such that $(C\oplus A, D\oplus B) \notin \mathcal{C}_0$ and $(\emptyset\oplus A, \emptyset\oplus B) \notin \mathcal{C}_1$. Then there exists a total computable function $g_0 : \mathbb{N} \to \mathbb{N}$ such that the following holds: if g is a fast function that dominates g_0 and $\alpha \in \mathrm{P}_\mathbb{N}$, $\|\alpha\| = \infty$, $\|\overline{\alpha}\| = \infty$, then $((C\cap I^g_\alpha)\oplus A, (D\cap I^g_\alpha)\oplus B) \in \mathrm{DisjNP} - (\mathcal{C}_0\cup\mathcal{C}_1)$.*

[2] For any two sets X and Y, $X\triangle Y$ denotes the symmetric difference of X and Y. Namely, $X\triangle Y = (X - Y) \cup (Y - X)$.

Proof. Since $\mathcal{C}_0$ and $\mathcal{C}_1$ are effectively presentable, there exist total computable functions f_1 and f_2 such that

- for all $(i, j) \in \text{range}(f_1) \cup \text{range}(f_2)$, M_i and M_j halt on all inputs,
- $\mathcal{C}_0 = \{(L(M_i), L(M_j)) \mid (i, j) \in \text{range}(f_0)\}$, and
- $\mathcal{C}_1 = \{(L(M_i), L(M_j)) \mid (i, j) \in \text{range}(f_1)\}$.

Define the following functions:

$$g_{00}(n) = \min\{m > n \mid (\forall k \leq n)\exists z\, (n < |z| \leq m) \wedge z \in (C \oplus A, D \oplus B) \triangle (L(M_i), L(M_j)) \wedge f_0(k) = (i, j)\}.$$

$$g_{01}(n) = \min\{m > n \mid (\forall k \leq n)\exists z\, (n < |z| \leq m) \wedge z \in (\emptyset \oplus A, \emptyset \oplus B) \triangle (L(M_i), L(M_j)) \wedge f_1(k) = (i, j)\}.$$

We prove that g_{00}, g_{01} are total computable functions. Since $(C \oplus A, D \oplus B) \notin \mathcal{C}_0$, for all $(i, j) \in \text{range}(f_1)$, $(C \oplus A, D \oplus B) \neq (L(M_i), L(M_j))$. As $\mathcal{C}_0$ is closed under finite variations, $(C \oplus A, D \oplus B) \triangle (L(M_i), L(M_j))$ is an infinite set. Thus, for all k, and for all $n \geq k$, there is a string z such that $|z| > n$ and $z \in (C \oplus A, D \oplus B) \triangle (L(M_i), L(M_j))$, where $(i, j) = f_0(k)$. Observe that the relation defined by "$z \in (C \oplus A, D \oplus B) \triangle (L(M_i), L(M_j)) \wedge f_1(k) = (i, j)$" is decidable, because A, B, C and D are all decidable, both M_i and M_j halt on all inputs and f_0 is total computable. Min is a computable operator, so g_{00} is computable. Similar arguments show that g_{01} are total and computable.

Define $g_0(n) = \max(g_{00}(n), g_{01}(n))$. Clearly, g_0 is total computable too. Now fix a fast function g that dominates g_0 and fix $\alpha \in \mathrm{P}_{\mathbb{N}}$ such that $\|\alpha\| = \infty$ and $\|\overline{\alpha}\| = \infty$. We have to show

$$\begin{aligned}
((C \cap I_\alpha^g) \oplus A, (D \cap I_\alpha^g) \oplus B) &\in \text{DisjNP} && (1)\\
((C \cap I_\alpha^g) \oplus A, (D \cap I_\alpha^g) \oplus B) &\notin \mathcal{C}_0 && (2)\\
((C \cap I_\alpha^g) \oplus A, (D \cap I_\alpha^g) \oplus B) &\notin \mathcal{C}_1 && (3)
\end{aligned}$$

Statement (1) clearly holds since $I_\alpha^g \in \mathrm{P}$ and A, B are infinite sets. For (2), we need to show for every $k \in \mathbb{N}$ that $((C \cap I_\alpha^g) \oplus A, (D \cap I_\alpha^g) \oplus B) \neq (L(M_i), L(M_j))$, where $(i, j) = f_0(k)$. Now fix k and choose $n \geq k$ and $n \in \alpha$. Substituting n with $g^n(0)$ in the definition of g_0 gives

$$\exists z\, (g^n(0) < |z| \leq g_0(g^n(0)) \leq g^{n+1}(0)) \wedge z \in (C \oplus A, D \oplus B) \triangle (L(M_i), L(M_j)). \qquad (4)$$

Take a string z given by (4). If $z = 0x$ for some x, then $g^n(0) \leq |x| \leq g^{n+1}(0) - 1 < g^{n+1}(0)$. So $x \in I_\alpha^g$. Hence, $z \in C \oplus A \Leftrightarrow z \in (C \cap I_\alpha^g) \oplus A \Leftrightarrow x \in C$ and $z \in D \oplus B \Leftrightarrow z \in (D \cap I_\alpha^g) \oplus B \Leftrightarrow x \in D$. Therefore, (4) implies $z \in ((C \cap I_\alpha^g) \oplus A, (D \cap I_\alpha^g) \oplus B) \triangle (L(M_i), L(M_j))$.

Otherwise, $z = 1x$ for some x. Then $z \in C \oplus A \Leftrightarrow z \in (C \cap I_\alpha^g) \oplus A \Leftrightarrow x \in A$ and $z \in D \oplus B \Leftrightarrow z \in (D \cap I_\alpha^g) \oplus B \Leftrightarrow x \in B$. So (4) implies $z \in ((C \cap I_\alpha^g) \oplus A, (D \cap I_\alpha^g) \oplus B) \triangle (L(M_i), L(M_j))$. This completes the proof of (2). The proof of (3) is similar (we choose $n \in \overline{\alpha}$ instead). □

Theorem 4.16 *(First Meet Theorem) For every disjoint* NP*-pair* (C, D) *there exists a total computable function* g_1 *such that the following holds. Let* g *be a fast function that dominates* g_1*. Let* (A, B) *be a disjoint* NP*-pair. Let* $\alpha, \beta \in \mathrm{P}_{\mathbb{N}}$ *such that*

$$(\forall n \in \mathbb{N})(\forall i \in \{0,1\})\ [(n+i \in \alpha \wedge n+1-i \in \beta) \Rightarrow (n \in \alpha \cap \beta \vee n+1 \in \alpha \cap \beta)]. \tag{5}$$

Then

$$\begin{aligned} & \mathbf{d}((C \cap I^g_{\alpha\cap\beta}) \oplus A, (D \cap I^g_{\alpha\cap\beta}) \oplus B) \\ = \ & \mathbf{d}((C \cap I^g_\alpha) \oplus A, (D \cap I^g_\alpha) \oplus B) \wedge \mathbf{d}((C \cap I^g_\beta) \oplus A, (D \cap I^g_\beta) \oplus B). \end{aligned}$$

Proof. Let M_C and M_D be Turing machines deciding C and D, with their running time bounded by total computable functions t_C and t_D, respectively. Let $g_1(n) = \max(t_C(n), t_D(n))$. So g_1 is total computable. Fix g, α, β and (A, B) as in the premise of the theorem. Then I_α, I_β and $I_{\alpha\cap\beta}$ all belong to P and $I_\alpha \cap I_\beta = I_{\alpha\cap\beta}$. Hence, by choosing the identity function as reduction function,

$$((C \cap I^g_{\alpha\cap\beta}) \oplus A, (D \cap I^g_{\alpha\cap\beta}) \oplus B) \leq^{pp}_m ((C \cap I^g_\alpha) \oplus A, (D \cap I^g_\alpha) \oplus B)$$

since $I^g_{\alpha\cap\beta} \subseteq I^g_\alpha$, and

$$((C \cap I^g_{\alpha\cap\beta}) \oplus A, (D \cap I^g_{\alpha\cap\beta}) \oplus B) \leq^{pp}_m ((C \cap I^g_\beta) \oplus A, (D \cap I^g_\beta) \oplus B)$$

since $I^g_{\alpha\cap\beta} \subseteq I^g_\beta$.

What remains to show is for every $(E, F) \in \mathrm{DisjNP}$ that $(E, F) \leq^{pp}_T ((C \cap I^g_\alpha) \oplus A, (D \cap I^g_\alpha) \oplus B)$ and $(E, F) \leq^{pp}_T ((C \cap I^g_\beta) \oplus A, (D \cap I^g_\beta) \oplus B)$ implies $(E, F) \leq^{pp}_T ((C \cap I^g_{\alpha\cap\beta}) \oplus A, (D \cap I^g_{\alpha\cap\beta}) \oplus B)$.

We can assume without loss of generality that

(a) $\alpha \cap \beta = \emptyset$,

(b) $(\forall n \in \mathbb{N})\ [(n \in \alpha \Rightarrow n+1, n-1 \notin \beta) \wedge (n \in \beta \Rightarrow n+1, n-1 \notin \alpha)]$.

Suppose not. Let $\alpha' = \alpha - \beta$, $\beta' = \beta - \alpha$ and $(A', B') = ((C \cap I^g_{\alpha\cap\beta}) \oplus A, (D \cap I^g_{\alpha\cap\beta}) \oplus B)$. Then $\alpha' \cap \beta' = \emptyset$. Also, if $n \in \alpha'$, then $n \in \alpha$ and $n \notin \beta$. Suppose $n+1 \in \beta'$. Then $n+1 \in \beta$ and $n+1 \notin \alpha$. Now we have $n \in \alpha$, $n+1 \in \beta$ but neither n nor $n+1$ can be in $\alpha \cap \beta$. This is a contradiction to (5). So $n+1 \notin \beta'$. Similar arguments show $n-1 \notin \beta'$. So $n \in \alpha'$ implies $n+1 \notin \beta'$ and $n-1 \notin \beta'$. By symmetry, we can also show $n \in \beta'$ implies $n+1 \notin \alpha'$ and $n-1 \notin \alpha'$. Therefore, α' and β' satisfies both (a) and (b), in place of α and β. Furthermore, we notice that

$$((C \cap I^g_\alpha) \oplus A, (D \cap I^g_\alpha) \oplus B) \equiv^{pp}_T ((C \cap I^g_{\alpha'}) \oplus A', (D \cap I^g_{\alpha'}) \oplus B'),$$

$$((C \cap I^g_\beta) \oplus A, (D \cap I^g_\beta) \oplus B) \equiv^{pp}_T ((C \cap I^g_{\beta'}) \oplus A', (D \cap I^g_{\beta'}) \oplus B'),$$

and

$$((C \cap I^g_{\alpha\cap\beta}) \oplus A, (D \cap I^g_{\alpha\cap\beta}) \oplus B) = (A', B') \equiv^{pp}_T ((C \cap I^g_{\alpha'\cap\beta'}) \oplus A', (D \cap I^g_{\alpha'\cap\beta'}) \oplus B')$$

since $\alpha' \cap \beta' = \emptyset$. So we can just work with (A', B'), in place of (A, B). This justifies our assumptions (a) and (b).

Now given $(E, F) \in \mathrm{DisjNP}$, suppose $(E, F) \leq_T^{pp} ((C \cap I_\alpha^g) \oplus A, (D \cap I_\alpha^g) \oplus B)$ via a polynomial time oracle Turing machine M_1 and $(E, F) \leq_T^{pp} ((C \cap I_\beta^g) \oplus A, (D \cap I_\beta^g) \oplus B)$ via a polynomial time oracle Turing machine M_2. Let p be a polynomial that bounds the running time of M_1 and M_2. We have to show $(E, F) \leq_T^{pp} ((C \cap I_{\alpha\cap\beta}^g) \oplus A, (D \cap I_{\alpha\cap\beta}^g) \oplus B)$. Note that $((C \cap I_{\alpha\cap\beta}^g) \oplus A, (D \cap I_{\alpha\cap\beta}^g) \oplus B) \equiv_T^{pp} (A, B)$ by Assumption (a).

We use the following algorithm to separate (E, F) relative to a separator S of (A, B):

```
//Algorithm for separating $(E,F)$ relative to a separator $S$ of $(A,B)$.
0   On input $x$
1   Compute $n$ such that $0^{p(|x|)} \in I_n^g$;
2   If $n \in \alpha$ or $n-1 \in \alpha$ then
3      Simulate $M_2(x)$ as follows:
4      If a query is $0y$ and $y \notin I_\beta^g$ then answer NO;
5      If a query is $0y$ and $y \in I_\beta^g$ then answer YES iff $M_C(y)$ accepts;
6      If a query is $1y$ then answer YES iff $y \in S$;
7   Else
8      Simulate $M_1(x)$ as follows:
9      If a query is $0y$ and $y \notin I_\alpha^g$ then answer NO;
10     If a query is $0y$ and $y \in I_\alpha^g$ then answer YES iff $M_D(y)$ rejects;
11     If a query is $1y$ then answer YES iff $y \in S$;
```

The algorithm is self-explanatory and clearly correct. It remains to show the algorithm runs in polynomial time. Since g is fast, an argument similar to the one in Proposition 4.11 shows line 1 can be executed in polynomial time. It suffices to show that line 5 and line 10 can be executed in polynomial time in $|x|$. At line 5, if the query is $0y$ and $y \in I_\beta^g$, then $y \in I_m^g$ for some $m \in \beta$. Since $|y| < |0y| \leq p(|x|)$, we have $m \leq n$. If $n \in \alpha$, then $n \notin \beta$ by our assumption (a) and $n+1$, $n-1 \notin \beta$ by our assumption (b). So $m \leq n-2$. Similarly we can show $n-1 \in \alpha$ implies $m \leq n-2$ too. Thus, since $y \in I_m^g$, we have $|y| < g^{n-1}(0)$. So the running time of M_C on y is no more than $g_1(|y|) \leq g(|y|) < g^n(0) \leq p(|x|)$. For line 10, we just need to observe that if the query is $0y$ and $y \in I_\alpha^g$ at line 10, then $y \in I_m^g$ for some $m \leq n-2$. The rest of the proof is the same as that for line 5. This finishes the proof of Theorem 4.16. □

For a set $\alpha \subseteq \mathbb{N}$ and $i \in \mathbb{N}$, let $2\alpha + i \overset{\mathrm{df}}{=} \{2n + i \mid n \in \alpha\}$.

Corollary 4.17 *(Second Meet Theorem) For every disjoint* NP*-pair* (C, D) *there exists a total computable function* g_1 *such that the following holds. Let* g *be a fast function that dominates* g_1*. Let* (A, B) *be a disjoint* NP*-pair. Let* α*,* $\beta \in \mathrm{P}_\mathbb{N}$*. Then for* $i \in \{0, 1\}$*,*

$$\begin{aligned} & \mathbf{d}((C \cap I_{2\alpha+i\cap 2\beta+i}^g) \oplus A, (D \cap I_{2\alpha+i\cap 2\beta+i}^g) \oplus B) \\ = \;& \mathbf{d}((C \cap I_{2\alpha+i}^g) \oplus A, (D \cap I_{2\alpha+i}^g) \oplus B) \wedge \mathbf{d}((C \cap I_{2\beta+i}^g) \oplus A, (D \cap I_{2\beta+i}^g) \oplus B). \end{aligned}$$

Proof. Take $\alpha' = 2\alpha + i$ and $\beta' = 2\beta + i$. Then (5) holds trivially for α' and β'. So the First Meet Theorem applies. □

Theorem 4.18 *(Embedding Theorem) Let (A, B) and (C, D) be disjoint* NP*-pairs such that $(A, B) \leq_T^{pp} (C, D)$ but $(C, D) \not\leq_T^{pp} (A, B)$, where A, B, C and D are all infinite sets.*[3] *Let $\mathcal{C}$ and $\mathcal{D}$ be effectively presentable classes of disjoint* NP*-pairs that are closed under finite variations such that $(C \oplus A, D \oplus B) \notin \mathcal{C}$ and $(\emptyset \oplus A, \emptyset \oplus B) \notin \mathcal{D}$. Then there exists a fast function g such that the following holds. The functions $f_i : \mathrm{P}_{\mathbb{N}} \to \mathrm{DisjNP}$ and $f_i^* : \mathrm{P}_{\mathbb{N}}^* \to \mathcal{R}_{T,NP}^{pp}$, where $i = 0, 1$, defined by*

$$\begin{aligned} f_0(\alpha) &= ((C \cap I_{2\alpha+1}^g) \oplus A, (D \cap I_{2\alpha+1}^g) \oplus B), & (6)\\ f_1(\alpha) &= ((C \cap I_{2\alpha\cup 2\mathbb{N}+1}^g) \oplus A, (D \cap I_{2\alpha\cup 2\mathbb{N}+1}^g) \oplus B), & (7)\\ f_i^*([\alpha]) &= \mathbf{d}(f_i(\alpha)), & (8) \end{aligned}$$

have the following properties:

(i) If $\alpha \in \mathrm{P}_{\mathbb{N}}$, $\|\alpha\| = \infty$, $\beta \in \mathrm{P}_{\mathbb{N}}$ and $\|\overline{\beta}\| = \infty$, then $f_0(\alpha)$, $f_1(\beta) \notin \mathcal{C} \cup \mathcal{D} \cup \mathbf{d}(A, B) \cup \mathbf{d}(C, D)$;

(ii) The function f_0^* (f_1^*, respectively) gives an embedding of the atomless Boolean lattice $\langle \mathrm{P}_{\mathbb{N}}^*; \subseteq^* \rangle$ into the interval $[\mathbf{d}(A, B), \mathbf{d}(C, D)]$ that preserves 0(1, respectively).

Proof. Let $\mathcal{C}_0 = \mathcal{C} \cup \{(E, F) \in \mathrm{DisjNP} \mid (E, F) \leq_T^{pp} (A, B)\}$ and $\mathcal{C}_1 = \mathcal{D} \cup \mathbf{d}(C, D)$. Then by Theorem 4.5, 4.8 and 4.9, both $\mathcal{C}_0$ and $\mathcal{C}_1$ are effectively presentable. Also, note that $(C \oplus A, D \oplus B) \notin \mathcal{C}_0$ and $(\emptyset \oplus A, \emptyset \oplus B) \notin \mathcal{C}_1$, since $(C, D) \not\leq_T^{pp} (A, B)$. So we can apply the Join Theorem and the Second Meet Theorem. Let g_0 and g_1 be functions as given by these Theorems. Let g be a fast function that dominates both g_0 and g_1. Then (i) is immediate by the Join Theorem. To show (ii), we first observe that $range(f_i) \subseteq \mathrm{DisjNP}$ since $I_\alpha^g \in \mathrm{P}$ for $\alpha \in \mathrm{P}_{\mathbb{N}}$. Now we observe the following: for every α, $\beta \in \mathbb{N}$,

$$\begin{aligned} \alpha \subseteq \beta &\Leftrightarrow I_\alpha^g \subseteq I_\beta^g, & (9)\\ \|\alpha\| \text{ is finite } &\Leftrightarrow \|I_\alpha^g\| \text{ is finite}, & (10)\\ \text{and } \alpha \in \mathrm{P}_{\mathbb{N}} &\Rightarrow I_\alpha^g \in \mathrm{P}. & (11) \end{aligned}$$

Also, for every NP-pair (E, F) and sets G_0, $G_1 \in \mathrm{P}$, we have

$$\mathbf{d}(E \cap (G_0 \cup G_1), F \cap (G_0 \cap G_1)) = \mathbf{d}(E \cap G_0, F \cap G_0) \vee \mathbf{d}(E \cap G_1, F \cap G_1), \quad (12)$$

and,

$$G_0 \subseteq G_1 \Rightarrow (E \cap G_0, F \cap G_0) \leq_m^{pp} (E \cap G_1, F \cap G_1). \quad (13)$$

By the definitions of f_i's and by Proposition 4.2 and (12), for every α, $\beta \in \mathrm{P}_{\mathbb{N}}$ and $i = 0, 1$, it holds that

$$\mathbf{d}(f_i(\alpha)) \vee \mathbf{d}(f_i(\beta)) = \mathbf{d}(f_i(\alpha \cup \beta)), \quad (14)$$

[3] Note that this premise is implied by the existence of a P-inseparable disjoint NP-pair (C, D).

and by (9), (13) and Proposition 4.2,

$$\alpha \subseteq \beta \Rightarrow (A,B) \leq_m^{pp} f_i(\alpha) \leq_m^{pp} f_i(\beta) \leq_m^{pp} (C \oplus A, D \oplus B). \tag{15}$$

Moreover, by (10) and the closure of NP-Turing-degrees of NP-pairs under finite variations,

$$\alpha \overset{*}{=} \beta \Rightarrow f_i(\alpha) \overset{*}{=} f_i(\beta) \Rightarrow f_i(\alpha) \equiv_T^{pp} f_i(\beta). \tag{16}$$

This shows that f_i^*, where $i = 0, 1$, is well-defined. By (15), range$(f_i^*) \subseteq [\mathbf{d}(A,B), \mathbf{d}(C,D)]$ since $(C \oplus A, D \oplus B) \equiv_T^{pp} (C,D)$.

Furthermore, since $f_0(\emptyset) = (\emptyset \oplus A, \emptyset \oplus B) \equiv_T^{pp} (A,B)$ and $f_1(\mathbb{N}) = (C \oplus A, D \oplus B) \equiv_T^{pp} (C,D)$, f_0^* and f_1^* preserve 0 and 1, respectively. It remains to show for $i = 0, 1$ that f_i^* embeds $\langle \mathrm{P}_{\mathbb{N}}^*; \subseteq^* \rangle$ into $\langle \mathcal{R}_T^{pp}; \leq_T^{pp} \rangle$. For this, we need to show for $i = 0, 1$ and for every $\alpha, \beta \in \mathrm{P}_{\mathbb{N}}$ that

- $[\alpha] \subseteq^* [\beta] \Leftrightarrow f_i^*([\alpha]) \leq f_i^*([\beta])$,
- $f_i^*([\alpha \cup \beta]) = f_i^*([\alpha]) \vee f_i^*([\beta])$, and
- $f_i^*([\alpha \cap \beta]) = f_i^*([\alpha]) \wedge f_i^*([\beta])$.

By definitions of f_i^* and by (16), we may replace these by

$$\alpha \subseteq^* \beta \Leftrightarrow f_i(\alpha) \leq_T^{pp} f_i(\beta), \tag{17}$$
$$\mathbf{d}(f_i(\alpha \cup \beta)) = \mathbf{d}(f_i(\alpha)) \vee \mathbf{d}(f_i(\beta)), \tag{18}$$
$$\mathbf{d}(f_i(\alpha \cap \beta)) = \mathbf{d}(f_i(\alpha)) \wedge \mathbf{d}(f_i(\beta)). \tag{19}$$

Equation (18) is the same as (14). The implication from left to right in (17) is immediate by (15) and (16). Equation (19) holds by the Second Meet Theorem and by the definitions of f_i's.

It remains to show "$\Leftarrow$" in (17). Fix $\alpha, \beta \in \mathrm{P}_{\mathbb{N}}$ such that $f_i(\alpha) \leq_T^{pp} f_i(\beta)$. For the purpose of contradiction, suppose $\|\alpha - \beta\| = \infty$. Let $\gamma = \alpha - \beta$. Note that $\gamma \in \mathrm{P}_{\mathbb{N}}$ and $\gamma \subseteq \alpha$. So by (15), $f_i(\gamma) \leq_T^{pp} f_i(\alpha)$. Therefore, $f_i(\gamma) \leq_T^{pp} f_i(\beta)$. Since trivially $f_i(\gamma) \leq_T^{pp} f_i(\gamma)$, by (19) we have $f_i(\gamma) \leq_T^{pp} f_i(\gamma \cap \beta) = f_i(\emptyset)$. So by (15) again,

$$f_i(\gamma) \equiv_T^{pp} f_i(\emptyset). \tag{20}$$

Now for $i = 0$, $f_0(\gamma) \equiv_T^{pp} f_0(\emptyset) \in \mathbf{d}(A,B)$, which contradicts (i). For $i = 1$,

$$\begin{array}{rcl} \mathbf{d}(f_1(\mathbb{N})) & = & \mathbf{d}(f_1(\gamma \cup \overline{\gamma})), \\ & = & \mathbf{d}(f_1(\gamma)) \vee \mathbf{d}(f_1(\overline{\gamma})), \text{ (by (18))} \\ & = & \mathbf{d}(f_1(\emptyset)) \vee \mathbf{d}(f_1(\overline{\gamma}), \text{ (by (20))} \\ & = & \mathbf{d}(f_1(\overline{\gamma})). \text{ (by (18) again)} \end{array}$$

Now we take $\beta' = \overline{\gamma}$. Then $\|\overline{\beta'}\| = \infty$ and $\mathbf{d}(f_1(\beta')) = \mathbf{d}(f_1(\mathbb{N})) = \mathbf{d}(C,D)$, which is a contradiction to (i).

□

Corollary 4.19 *Let $\mathbf{d_1}, \mathbf{d_2} \in \mathcal{R}^{pp}_{T,NP}$ be given such that $\mathbf{d_1} < \mathbf{d_2}$. Let $\mathcal{L}$ be a countable distributive lattice. Then there exists an embedding of $\mathcal{L}$ into the interval $[\mathbf{d_1}, \mathbf{d_2}]$ that preserves the least element and there exists an embedding of $\mathcal{L}$ into the interval $[\mathbf{d_1}, \mathbf{d_2}]$ that preserves the greatest element.*

Proof. Fix $(A, B) \in \mathbf{d_1}$ and $(C, D) \in \mathbf{d_2}$ such that A, B, C and D are all infinite sets and let $\mathcal{C} = \mathcal{D} = \emptyset$. The Embedding Theorem yields embeddings f^*_i of the countable atomless Boolean lattice $\langle \mathrm{P}^*_{\mathbb{N}}; \subseteq^* \rangle$ into the interval $[\mathbf{d_1}, \mathbf{d_2}]$ that preserves i, where $i = 0, 1$. It is known [Grä78, Page 64, Theorem 19] that every countable distributive lattice can be embedded into $\langle \mathrm{P}^*_{\mathbb{N}}; \subseteq^* \rangle$, so we have embeddings from every countable distributive lattice into the interval $[\mathbf{d_1}, \mathbf{d_2}]$. □

Corollary 4.20 *Suppose there exist disjoint* NP*-pairs (A, B) and (C, D) such that A, B, C, and D are infinite, $(A, B) \leq^{pp}_T (C, D)$, and $(C, D) \not\leq^{pp}_T (A, B)$. Then there exist incomparable, strictly intermediate disjoint* NP*-pairs (E, F) and (G, H) between (A, B) and (C, D) such that E, F, G, and H are infinite. Precisely, the following properties hold:*

- *$(A, B) \leq^{pp}_m (E, F) \leq^{pp}_T (C, D)$ and $(C, D) \not\leq^{pp}_T (E, F) \not\leq^{pp}_T (A, B)$;*
- *$(A, B) \leq^{pp}_m (G, H) \leq^{pp}_T (C, D)$ and $(C, D) \not\leq^{pp}_T (G, H) \not\leq^{pp}_T (A, B)$;*
- *$(E, F) \not\leq^{pp}_T (G, H)$ and $(G, H) \not\leq^{pp}_T (E, F)$.*

Proof. By the Embedding Theorem, we can embed the boolean lattice with two atoms into the interval $[\mathbf{d}(A, B), \mathbf{d}(C, D)]$ and obtain NP-pairs (E, F) and (G, H) that satisfy all the required properties except that $(A, B) \leq^{pp}_m (E, F)$ and $(A, B) \leq^{pp}_m (G, H)$. However, by the definitions of the functions f_i in the Embedding Theorem, it follows that (E, F) and (G, H) can be chosen such that $(A, B) \leq^{pp}_m (E, F)$ and $(A, B) \leq^{pp}_m (G, H)$. □

Corollary 4.21 *Suppose there exists a* P*-inseparable disjoint* NP*-pair (C, D). Let (A, B) be a* P*-separable disjoint* NP*-pair such that A and B are infinite. Then there exist incomparable,* P*-inseparable, strictly intermediate disjoint* NP*-pairs (E, F) and (G, H) between (A, B) and (C, D) that satisfy all of the consequences of Corollary 4.20, and in addition, satisfy the following conditions:*

- *$(A, B) \leq^{pp}_m (E, F) \leq^{pp}_m (C, D)$, and*
- *$(A, B) \leq^{pp}_m (G, H) \leq^{pp}_m (C, D)$.*

Proof. We just need to observe that now $(A, B) \leq^{pp}_m (C, D)$. Therefore, the disjoint NP-pairs (E, F) and (G, H) defined in the proof of Corollary 4.20 (which is obtained by applying the Embedding Theorem) satisfies that

- $(A,B) \leq_m^{pp} (E,F) \leq_m^{pp} (C,D)$, and
- $(A,B) \leq_m^{pp} (G,H) \leq_m^{pp} (C,D)$.

□

Corollary 4.22 *Assuming there exist* P*-inseparable disjoint* NP*-pairs, there exist propositional proof systems f and g so that f does not simulate g and g does not simulate f.*

Proof. Follows from Corollary 4.21, Theorem 3.1, and Proposition 3.5. □

However, Messner [Mes00, Mes02] unconditionally proved the existence of propositional proof systems f and g such that f does not simulate g and g does not simulate f. Messner further shows that the simulation order of propositional proof systems is dense. However, as the following argument shows, these results do not replace our study of the degree structure of disjoint NP-pairs. Messner [Mes] observed that there exist infinite, strictly increasing chains of propositional proof systems (using simulation as the order relation $\leq$) such that all canonical pairs of these proofs systems belong to the same many-one degree of disjoint NP-pairs.

For the sake of simplicity, here we only argue that the previous statement holds in some relativized world (although the statement indeed holds in the real world). First, observe that for every non-optimal propositional proof system f there is a proof system g such that g simulates f, but f does not simulate g (i.e., $f < g$). (For example, for some h that is not simulated by f, let $g(x) = f(x/2)$ if x is even and $g(x) = h((x-1)/2)$ otherwise.) Glaßer et al. [GSSZ04] constructed an oracle O_2 relative to which many-one complete disjoint NP-pairs exist, but optimal propositional proof systems do not exist. So relative to this oracle, there is a proof system f_0 whose canonical pair is complete, but optimal proof systems do not exist. By our observation, there exists an infinite, strictly increasing chain of proof systems $f_0 < f_1 < \cdots$. However, by Proposition 3.5, the canonical pair of each f_i is many-one complete.

Acknowledgments.
The authors thank Jochen Messner and Kenneth W. Regan for informing them of the methods in their papers [Mes00, Mes02, Reg83, Reg88]. We thank an anonymous referee for finding an error in a previous version.

References

[AS84] K. Ambos-Spies. On the structure of the polynomial time degrees of recursive sets. Habilitationsschrift, Zur Erlangung der Venia Legendi Für das Fach Informatik an der Abteilung Informatik der Universität Dortmund, September 1984.

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

[Grä78] G. Grätzer. *General Lattice Theorey.* Birkhäuser Verlag, 1978.

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

[GSSZ04] C. Glaßer, A. Selman, S. Sengupta, and L. Zhang. Disjoint NP-pairs. *SIAM Journal on Computing*, 33(6):1369–1416, 2004.

[HS92] S. Homer and A. Selman. Oracles for structural properties: The isomorphism problem and public-key cryptography. *Journal of Computer and System Sciences*, 44(2):287–301, 1992.

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

[Mer02] W. Merkle. Lattice embeddings for abstract bounded reducibilities. *SIAM J. Comput.*, 31(4):1119–1155, 2002.

[Mes] J. Messner. Personal correspondence.

[Mes00] J. Messner. *On the Simulation Order of Proof Systems.* PhD thesis, Universität Ulm, 2000.

[Mes02] J. Messner. On the structure of the simulation order of proof systems. In *Proceedings of the 27rd Mathematical Foundations of Computer Science*, Lecture Notes in Computer Science 1450, pages 581–592. Springer-Verlag, 2002.

[Pud01] 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.

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

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

[Reg83] K. Regan. On diagonalization methods and the structure of language classes. In *Proceedings of the Fundamentals of Computation Theory Conference*, volume 158 of *Lecture Notes in Computer Science*, pages 368–380. Springer Verlag, 1983.

[Reg88] K. Regan. The topology of provability in complexity theory. *Journal of Computer and System Sciences*, 36:384–432, 1988.

[Sch82] U. Schöning. A uniform approach to obtain diagonal sets in complexity classes. *Theoretical Computer Science*, 18:95–103, 1982.