Canonical Disjoint NP-Pairs of Propositional Proof Systems

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

November 19, 2004

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. Secondly, we show that this degree structure is not superficial: Assuming there exist P-inseparable disjoint pairs, 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 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 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.

[*] 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. Email: selman@cse.buffalo.edu

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

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 $\mathrm{P} \neq \mathrm{NP} \cap \mathrm{coNP}$. 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 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, we should try to understand the degree structure of DisjNP. We prove that between any two comparable and inequivalent disjoint NP-pairs (A, B) and (C, D) there exist P-inseparable, incomparable NP-pairs (E, F) and (G, H) whose degrees lie strictly between (A, B) and (C, D). Our result is an analogue of Ladner's result for NP [Lad75], and our proof is based on Schöning's formulation [Sch82]. 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 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. P $\neq$ NP $\cap$ *co*-NP *implies* NP *contains* P*-inseparable sets.*
2. P $\neq$ UP *implies* NP *contains* P*-inseparable sets [GS88].*
3. *If* NP *contains* P*-inseparable sets, then* NP *contains* NP*-complete* P*-inseparable sets [GS88].*

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

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).*

Since we are interested only in comparing disjoint NP-pairs, it is convenient for us to define the Turing-degree of a pair $(A, B) \in$ DisjNP as follows:

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

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

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

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 $|h(w)| \leq p(|w|)$. 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 $(\mathrm{SAT}^*, \mathrm{REF}_f) \equiv_m^{pp} (A, B)$. 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* $(\mathrm{SAT}^*, \mathrm{REF}_f) \equiv_m^{pp} (A, B)$.

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 $A \leq_m^p \mathrm{SAT}$ via g. Let M be an NP-machine that accepts B in time p. Define the following function f.

$$f(z) \stackrel{df}{=} \begin{cases} \neg g(x) & : \text{ if } z = \langle x, w \rangle,\ |w| = p(|x|),\ M(x) \text{ accepts along path } w \\ \neg x & : \text{ if } z = \langle x, w \rangle,\ |w| \neq p(|x|),\ |z| \geq 2^{|x|},\ x \notin \mathrm{SAT} \\ \neg \mathrm{false} & : \text{ otherwise} \end{cases}$$

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

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

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 y = false then output b
3   if n ≥ 2^|y| then
4      if y ∈ SAT then output a else output b
5   endif
6   if g^-1(y) exists then output g^-1(y)
7   output a
```

The exhaustive search in line 4 is possible in quadratic time in n. So $h \in \mathrm{PF}$.

Assume $(y, 0^n) \in \mathrm{SAT}^*$. So we reach line 3. If we reach line 4, then we output $a \in A$. Otherwise we reach line 6. If $g^{-1}(y)$ exists, then it belongs to A. Therefore, in either case (output in line 6 or in line 7) 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 the output is made in line 2, then we are done. If we reach line 4, then we output b. Otherwise we reach line 6. So far we have $y \neq$ false and $|z| \leq n < 2^{|y|}$. 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. $\square$

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 pps. 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 $r(x, 0^n) \stackrel{df}{=} (x, 0^{p(n)})$. 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 $y' \stackrel{df}{=} h(x)$ it holds that $|y'| \leq p(n)$ and $g(y') = \neg x$ which shows $(x, 0^{p(n)}) \in \mathrm{REF}_g$. $\square$

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* 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

Let $\{M_i\}_i$ be a standard effective enumeration of Turing machines. We require the following definition and theorems:

Definition 4.1 *We define a class $\mathcal{C}$ of nonempty disjoint* NP*-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 4.2 *For all $(A, B), (C, D) \in \mathrm{DisjNP}$, the following classes are effectively presentable.*

$$\begin{aligned}\mathcal{C}_1 &\stackrel{df}{=} \{(X, Y) \in \mathrm{DisjNP} \,\big|\, (C, D) \leq_T^{pp} (X \oplus A, Y \oplus B)\} \\ \mathcal{C}_2 &\stackrel{df}{=} \{(X, Y) \in \mathrm{DisjNP} \,\big|\, (X, Y) \leq_T^{pp} (A, B)\}\end{aligned}$$

Proof. Let $N_1, N_2, \dots$ be an effective enumeration of nondeterministic polynomial-time-bounded Turing machines such that N_k's running time on inputs of length n is $n^k + k$. Let $T_1, T_2, \dots$ be an effective enumeration of deterministic polynomial-time-bounded Turing machines such that T_l's running time on inputs of length n is $n^l + l$. We may assume that A, B, C, and D are infinite: Otherwise the corresponding pair is p-separable and therefore, if we use any p-separable pair of infinite sets instead, then we obtain the same classes $\mathcal{C}_1$ and $\mathcal{C}_2$. Define the predicate $\mathrm{Test}_1(i, j, k, m, x)$ 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. $L(N_i) \cap \Sigma^{\leq m} \neq \emptyset$ and $L(N_j) \cap \Sigma^{\leq m} \neq \emptyset$
3. for all y such that $|y|^k + k \leq |x|$ and for all $S \subseteq \Sigma^{\leq |x|}$ such that S separates $((L(N_i) \oplus A) \cap \Sigma^{\leq |x|}, (L(N_j) \oplus B) \cap \Sigma^{\leq |x|})$ it holds that $(y \in C \Rightarrow T_k^S(y)$ accepts) and $(y \in D \Rightarrow T_k^S(y)$ rejects)

Similarly, define the predicate $\mathrm{Test}_2(i, j, l, m, x)$ 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. $L(N_i) \cap \Sigma^{\leq m} \neq \emptyset$ and $L(N_j) \cap \Sigma^{\leq m} \neq \emptyset$
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)

The predicates Test_1 and Test_2 are certainly decidable. Define

$$f_1(\langle i, j, k, m \rangle) \stackrel{df}{=} (c_1, d_1)$$

where c_1 and d_1 are the indices of the machines described below.

- M_{c_1} on input x: If $\mathrm{Test}_1(i, j, k, m, x)$, then accept if and only if $x \in L(N_i) - L(N_j)$. Otherwise, accept if and only if $x \in C$.
- M_{d_1} on input x: If $\mathrm{Test}_1(i, j, k, m, x)$, then accept if and only if $x \in L(N_j) - L(N_i)$. Otherwise, accept if and only if $x \in D$.

Similarly, define

$$f_2(\langle i, j, l, m \rangle) \stackrel{df}{=} (c_2, d_2)$$

where c_2 and d_2 are the indices of the machines described below.

- M_{c_2} on input x: If $\mathrm{Test}_2(i, j, l, m, x)$, 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_2} on input x: If $\mathrm{Test}_2(i, j, l, m, x)$, 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 $\mathcal{C}_1$ is effectively presented by f_1, and $\mathcal{C}_2$ is effectively presented by f_2.

Clearly, f_1 and f_2 are total and computable. Also, M_{c_1}, M_{d_1}, M_{c_2}, and M_{d_2} halt on all inputs which shows statement 1 in Definition 4.1. Statement 2 is shown by the following claims.

Claim 4.3 *For all* $(c_1, d_1) \in \mathrm{range}(f_1)$, $(L(M_{c_1}), L(M_{d_1})) \in \mathrm{DisjNP}$ *and*

$$(C, D) \leq_T^{pp} (L(M_{c_1}) \oplus A, L(M_{d_1}) \oplus B).$$

Proof. Choose i, j, k, m such that $(c_1, d_1) = f_1(\langle i, j, k, m \rangle)$. By definition of M_{c_1} and M_{d_1} it holds that $L(M_{c_1}) \cap L(M_{d_1}) = \emptyset$.

Case 1: Assume $\mathrm{Test}_1(i, j, k, m, x)$ holds for all x. Hence $L(N_i) \cap L(N_j) = \emptyset$, $L(N_i) \neq \emptyset$, and $L(N_j) \neq \emptyset$. This shows $L(M_{c_1}) = L(N_i)$ and $L(M_{d_1}) = L(N_j)$, and so $(L(M_{c_1}), L(M_{d_1})) \in \mathrm{DisjNP}$.

We show $(C, D) \leq_T^{pp} (L(M_{c_1}) \oplus A, L(M_{d_1}) \oplus B)$ via machine T_k. Let S' be an arbitrary separator of $(L(M_{c_1}) \oplus A, L(M_{d_1}) \oplus B)$. Assume there exists $y \in C$ such that $T_k^{S'}(y)$ rejects. So $T_k^S(y)$ rejects where $S \stackrel{df}{=} S' \cap \Sigma^{\leq |y|^k + k}$. Hence statement 3 in the definition of Test_1 does not hold for $x = 0^{|y|^k + k}$. This contradicts our assumption in Case 1. It follows that if $y \in C$, then $T_k^{S'}(y)$ accepts. Analogously, if $y \in D$, then $T_k^{S'}(y)$ rejects. This shows that $L(T_k^{S'})$ is a separator of (C, D) and hence, $(C, D) \leq_T^{pp} (L(M_{c_1}) \oplus A, L(M_{d_1}) \oplus B)$.

Case 2: Assume there exists x such that $\mathrm{Test}_1(i, j, k, m, x)$ does not hold. Then $\mathrm{Test}_1(i, j, k, m, y)$ does not hold for all y such that $|y| \geq |x|$. So by definition of M_{c_1} and M_{d_1}, $L(M_{c_1})$ is a finite variation of C, and $L(M_{d_1})$ is a finite variation of D. So both sets are infinite and hence $(L(M_{c_1}) \oplus A, L(M_{d_1}) \oplus B) \in \mathrm{DisjNP}$. Also $(C, D) \leq_T^{pp} (L(M_{c_1}) \oplus A, L(M_{d_1}) \oplus B)$. This finishes the proof of Claim 4.3. $\square$

Claim 4.4 *For all* $(c_2, d_2) \in \text{range}(f_2)$*,* $(L(M_{c_2}), L(M_{d_2})) \in \text{DisjNP}$ *and*

$$(L(M_{c_2}), L(M_{d_2})) \leq_T^{pp} (A, B).$$

Proof. Choose i, j, l, m such that $(c_2, d_2) = f_2(\langle i, j, l, m \rangle)$. By definition of M_{c_2} and M_{d_2} it holds that $L(M_{c_2}) \cap L(M_{d_2}) = \emptyset$.

Case 1: Assume $\text{Test}_2(i, j, l, m, x)$ holds for all x. Hence $L(N_i) \cap L(N_j) = \emptyset$, $L(N_i) \neq \emptyset$, and $L(N_j) \neq \emptyset$. This shows $L(M_{c_2}) = L(N_i)$ and $L(M_{d_2}) = L(N_j)$, and so $(L(M_{c_2}), L(M_{d_2})) \in \text{DisjNP}$.

We show $(L(M_{c_2}), L(M_{d_2})) \leq_T^{pp} (A, B)$ via T_l. Let S' be any separator of (A, B). Assume there exists $y \in L(M_{c_2})$ such that $T_l^{S'}(y)$ rejects. So $T_l^S(y)$ rejects where $S \stackrel{df}{=} S' \cap \Sigma^{\leq |y|^l + l}$. Hence statement 3 in the definition of Test_2 does not hold for $x = 0^{|y|^l + l}$. This contradicts our assumption in Case 1. It follows that if $y \in L(M_{c_2})$, then $T_l^{S'}(y)$ accepts. Analogously, if $y \in L(M_{d_2})$, then $T_l^{S'}(y)$ rejects. This shows that $L(T_l^{S'})$ is a separator of $(L(M_{c_2}), L(M_{d_2}))$ and hence, $(L(M_{c_2}), L(M_{d_2})) \leq_T^{pp} (A, B)$.

Case 2: Assume there exists x such that $\text{Test}_2(i, j, l, m, x)$ does not hold. Then $\text{Test}_2(i, j, l, m, y)$ does not hold for all y such that $|y| \geq |x|$. So by definition of M_{c_2} and M_{d_2}, $L(M_{c_2})$ is a finite variation of A, and $L(M_{d_2})$ is a finite variation of B. So both sets are infinite and hence $(L(M_{c_2}), L(M_{d_2})) \in \text{DisjNP}$. Also $(L(M_{c_2}), L(M_{d_2})) \leq_T^{pp} (A, B)$. This finishes the proof of Claim 4.4. □

Claim 4.5 *For all* $(X, Y) \in \text{DisjNP}$ *such that* $(C, D) \leq_T^{pp} (X \oplus A, Y \oplus B)$*, there exists* n *such that* $f_1(n) = (c_1, d_1)$*,* $L(M_{c_1}) = X$*, and* $L(M_{d_1}) = Y$*.*

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 such that $(C, D) \leq_T^{pp} (X \oplus A, Y \oplus B)$ via T_k. Choose m large enough such that $X \cap \Sigma^{\leq m} \neq \emptyset$ and $Y \cap \Sigma^{\leq m} \neq \emptyset$. Define c_1 and d_1 such that $f_1(\langle i, j, k, m \rangle) = (c_1, d_1)$.

We claim that $\text{Test}_1(i, j, k, m, x)$ holds for all x. Clearly, statements 1 and 2 in the definition of Test_1 hold for all x. Assume statement 3 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 $((L(N_i) \oplus A) \cap \Sigma^{\leq |x|}, (L(N_j) \oplus B) \cap \Sigma^{\leq |x|})$ such that ($y \in C$ and $T_k^S(y)$ rejects) or ($y \in D$ and $T_k^S(y)$ accepts). Extend S to a separator S' of $(L(N_i) \oplus A, L(N_j) \oplus B)$ 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 ($y \in C$ and $T_k^{S'}(y)$ rejects) or ($y \in D$ and $T_k^{S'}(y)$ accepts). So $T_k^{S'}(y)$ is not a separator of (C, D) showing that (C, D) does not Turing reduce to $(X \oplus A, Y \oplus B)$ via machine T_k. This contradicts our assumption and therefore, statement 3 in the definition of Test_1 holds for all x. So we know that $\text{Test}_1(i, j, k, m, x)$ holds for all x, and $L(N_i) \cap L(N_j) = \emptyset$. It follows that $L(M_{c_1}) = L(N_i) = X$ and $L(M_{d_1}) = L(N_j) = Y$. This proves Claim 4.5. □

Claim 4.6 *For all* $(X, Y) \in \text{DisjNP}$ *such that* $(X, Y) \leq_T^{pp} (A, B)$*, there exists* n *such that* $f_2(n) = (c_2, d_2)$*,* $L(M_{c_2}) = X$*, and* $L(M_{d_2}) = Y$*.*

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 l such that $(X, Y) \leq_T^{pp} (A, B)$ via T_l. Choose m large enough such that $X \cap \Sigma^{\leq m} \neq \emptyset$ and $Y \cap \Sigma^{\leq m} \neq \emptyset$. Define c_2 and d_2 such that $f_2(\langle i, j, l, m \rangle) = (c_2, d_2)$.

We claim that $\text{Test}_2(i, j, l, m, x)$ holds for all x. Clearly, statements 1 and 2 in the definition of Test_2 hold for all x. Assume statement 3 does not hold. So there exist x and y such that $|y|^l + l \leq |x|$ and there exists $S \subseteq \Sigma^{\leq |x|}$ separating $(A \cap \Sigma^{\leq |x|}, B \cap \Sigma^{\leq |x|})$ such that ($y \in X$ and $T_l^S(y)$ rejects) or ($y \in Y$ and $T_l^S(y)$ accepts). Extend S to a separator S' of (A, B) such that $S = S' \cap \Sigma^{\leq |x|}$. The computation $T_l^S(y)$ cannot ask strings longer than $|y|^l + l \leq |x|$. Therefore, either ($y \in X$ and $T_l^{S'}(y)$ rejects) or ($y \in Y$ and $T_l^{S'}(y)$ accepts). So $T_l^{S'}(y)$ is not a separator of (X, Y) showing that (X, Y) does not Turing reduce to (A, B) via machine T_l. This contradicts our assumption and therefore, statement 3 in the definition of Test_2 holds for all x. So we know that $\text{Test}_2(i, j, l, m, x)$ holds for all x, and $L(N_i) \cap L(N_j) = \emptyset$. It follows that $L(M_{c_2}) = L(N_i) = X$ and $L(M_{d_2}) = L(N_j) = Y$. This proves Claim 4.6. □

This finishes the proof of Theorem 4.2. □

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 pairs is *closed under finite variations* if for all disjoint 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 $(A', B') \in \mathcal{C}$.

For any function, define $f^n(x)$ to be the n-fold iteration of f on x ($f^0(x) = x$, $f^1(x) = f(x)$, and $f^{n+1}(x) = f(f^n(x))$). For any function f defined on the set of natural numbers, define

$$G[f] = \{x \in \Sigma^* \mid f^n(0) \leq |x| < f^{n+1}(0), \text{ for even } n\}.$$

The following theorem is a version of Schöning's method [Sch82] for uniform diagonalization, applied to disjoint NP-pairs.

Theorem 4.7 *Let A, B, C, and D be infinite decidable sets such that (A, B) and (C, D) are disjoint pairs. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be classes of disjoint pairs with the following properties:*

- *$(A, B) \notin \mathcal{C}_1$ and $(C, D) \notin \mathcal{C}_2$;*
- *$\mathcal{C}_1$ and $\mathcal{C}_2$ are effectively presentable; and*
- *$\mathcal{C}_1$ and $\mathcal{C}_2$ are closed under finite variations.*

Then there exists a set $T \in \mathrm{P}$ such that the disjoint pair (E, F), where $E = (T \cap A) \cup (\overline{T} \cap C)$ and $F = (T \cap B) \cup (\overline{T} \cap D)$, has the following properties:

- *$T \cap A$, $\overline{T} \cap A$, $T \cap B$, $\overline{T} \cap B$, $T \cap C$, $\overline{T} \cap C$, $T \cap D$, $\overline{T} \cap D$ are infinite,*
- *$(E, F) \notin \mathcal{C}_1 \cup \mathcal{C}_2$, and*
- *if (A, B) is P-separable, then $(E, F) \leq_m^{pp} (C, D)$.*

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 the following functions:

$$\begin{aligned}
g_1(n) &= \max\{|\min\{z \,\big|\, |z| \geq n \text{ and } z \in L(M_i) \triangle A \cup L(M_j) \triangle B \text{ and } (i,j) = f_1(k)\}| \,\big|\, k \leq n\} \\
g_2(n) &= \max\{|\min\{z| \,\big|\, z| \geq n \text{ and } z \in L(M_i) \triangle C \cup L(M_j) \triangle D \text{ and } (i,j) = f_2(k)\}| \,\big|\, k \leq n\} \\
g_3(n) &= \min\{m \,\big|\, m \geq n \text{ and } \exists u,v,w,x \in \Sigma^{\geq n} \cap \Sigma^{\leq m} \text{ such that } u \in A, v \in B, w \in C, x \in D\}
\end{aligned}$$

We prove that g_1, g_2, and g_3 are total computable functions. Since $(A,B) \notin \mathcal{C}_1$, for all $(i,j) \in \text{range}(f_1)$, $(A,B) \neq (L(M_i), L(M_j))$. As $\mathcal{C}_1$ is closed under finite variations, $L(M_i) \triangle A \cup L(M_j) \triangle B$ is an infinite set. Thus, for all k, and for all $n \geq k$, there is a string z such that $|z| \geq n$ and $z \in L(M_i) \triangle A \cup L(M_j) \triangle B$, where $(i,j) = f_1(k)$. Observe that the relation defined by "$z \in L(M_i) \triangle A \cup L(M_j) \triangle B$ and $(i,j) = f_1(k)$" is decidable, because both A and B are decidable, both M_i and M_j halt on all inputs and f_1 is total computable. Min is a computable operator and taking the maximum over a finite set is a computable operator, so g_1 is computable. Similar arguments show that g_2 and g_3 are total and computable (for g_3 we need A, B, C, and D to be infinite).

Since $\max(g_1, g_2, g_3) + 1$ is a total computable function, there exists a fast function[1] g such that for all n, $g(n) > \max(g_1(n), g_2(n), g_3(n))$ (We refer to Proposition 7.3 of the text by Homer and Selman [HS01].) Also, $G[g] \in \mathrm{P}$ (Lemma 7.1, [HS01]). Now take $T = G[f]$. We prove that the pair (E,F), where $E = (T \cap A) \cup (\overline{T} \cap C)$ and $F = (T \cap B) \cup (\overline{T} \cap D)$, has the desired properties.

Suppose $T \cap A$ is finite. Choose an even integer n such that all words in $T \cap A$ are of length less than $g^n(0)$. Substituting $g^n(0)$ for n in the definition of g_3 implies that there exists a word $u \in A$ such that $g^n(0) \leq |u| \leq g_3(g^n(0)) < g^{n+1}(0)$. So $u \in A \cap T$ which contradicts the choice of n. Hence $T \cap A$ must be infinite. Similar arguments show that $\overline{T} \cap A$, $T \cap B$, $\overline{T} \cap B$, $T \cap C$, $\overline{T} \cap C$, $T \cap D$, $\overline{T} \cap D$ are infinite.

We turn to the second consequence. The definition of g_1 implies the following:

$$k \leq n \Rightarrow \exists z[n \leq |z| \leq g_1(n) \text{ and } z \in L(M_i) \triangle A \cup L(M_j) \triangle B, \text{ where } f_1(k) = (i,j)]. \tag{1}$$

Suppose $(E,F) \in \mathcal{C}_1$. Then, there exists k such that $(E,F) = (L(M_i), L(M_j))$, where $f_1(k) = (i,j)$. Select n to be an even positive integer such that $g^n(0) \geq k$. Substituting $g^n(0)$ for n in Equation (1), there is a string z such that $g^n(0) \leq |z| \leq g_1(g^n(0)) < g^{n+1}(0)$ and $z \in L(M_i) \triangle A \cup L(M_j) \triangle B$. Thus, $z \in T$ and $z \in L(M_i) \triangle A \cup L(M_j) \triangle B$, which implies, using the definition of (E,F), that $z \in L(M_i) \triangle E \cup L(M_j) \triangle F$. This is a contradiction. We conclude that $(E,F) \notin \mathcal{C}_1$. A similar argument shows that $(E,F) \notin \mathcal{C}_2$.

[1] A function $g : \mathbb{N} \to \mathbb{N}$ is called *fast* if (i) for all $n \in \mathbb{N}$, $f(n) > n$, and (ii) 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.

Now we show that the third consequence holds. Suppose (A, B) is P-separable. Let S be a separator of (A, B) that belongs to P. Let c and d be fixed words that belong to C and D, respectively. Consider the following function h:

$$h(x) = \begin{cases} x & \text{if } x \in \overline{T}, \\ c & \text{if } x \in T \text{ and } x \in S, \\ d & \text{if } x \in T \text{ and } x \notin S. \end{cases}$$

We claim that $(E, F) \leq_m^{pp} (C, D)$ via h. First it is clear that h is polynomial time computable since both T and S belong to P. Now suppose $x \in E$. If $x \in \overline{T}$, then $x \in C$. Hence, $h(x) = x \in C$. Otherwise $x \in A \subseteq S$. Hence, $h(x) = c \in C$. So in either case we have $h(x) \in C$. Therefore, $h(E) \subseteq C$. Similarly we can show that $h(F) \subseteq D$. $\square$

Now we apply Theorem 4.7 to obtain the following result about the degree structure of disjoint NP-pairs. Observe that the premise of the following theorem is true as long as there exist P-inseparable disjoint NP-pairs. For under this hypothesis, we can take (A, B) to be P-separable and (C, D) to be P-inseparable. We obtain the full generality of the theorem, in which we do not assume that (A, B) is P-separable, by using a technique of Regan [Reg83, Reg88].

Theorem 4.8 *Suppose there exist disjoint* NP*-pairs* (A, B) *and* (C, D) *such that* A, B, C, *and* D *are infinite,* $(A, B) \leq_T^{pp} (C, D)$, *and* $(C, D) \not\leq_T^{pp} (A, B)$. *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:*

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

Proof. Define

$$\begin{aligned} \mathcal{C}_1 &= \{(X, Y) \in \text{DisjNP} \,|\, (C, D) \leq_T^{pp} (X \oplus A, Y \oplus B)\} \quad \text{and} \\ \mathcal{C}_2 &= \{(X, Y) \in \text{DisjNP} \,|\, (X, Y) \leq_T^{pp} (A, B)\}. \end{aligned}$$

Clearly, $(A, B) \notin \mathcal{C}_1$ and $(C, D) \notin \mathcal{C}_2$. By Theorem 4.2, both $\mathcal{C}_1$ and $\mathcal{C}_2$ are effectively presentable. Also, it is obvious that $\mathcal{C}_1$ and $\mathcal{C}_2$ are closed under finite variations. Thus by Theorem 4.7, there exists a set $T \in \text{P}$ such that $(E', F') \notin \mathcal{C}_1 \cup \mathcal{C}_2$, where $E' = (T \cap A) \cup (\overline{T} \cap C)$ and $F' = (T \cap B) \cup (\overline{T} \cap D)$ are infinite sets. Clearly, $(E', F') \in \text{DisjNP}$, since both (A, B) and (C, D) belong to DisjNP and $T \in \text{P}$. Define $E = E' \oplus A$ and $F = F' \oplus B$. It is straightforward to see that (E, F) also belongs to DisjNP and $(A, B) \leq_m^{pp} (E, F)$. By the definition of $\mathcal{C}_1$ and $\mathcal{C}_2$, $(C, D) \not\leq_T^{pp} (E, F)$ and $(E, F) \not\leq_T^{pp} (A, B)$. In addition, we have the following claim:

Claim 4.9 $(E, F) \leq_T^{pp} (C, D)$.

Proof. Let S be a separator of (C, D). Since $(A, B) \leq_T^{pp} (C, D)$, there is a separator S_1 of (A, B) such that $S_1 \leq_T^p S$. Then $S_2 = (S_1 \cap T) \cup (S \cap \overline{T})$ is a separator of (E', F') and $S_2 \leq_T^p S_1 \oplus S \leq_T^p S$. Thus $S_3 = S_2 \oplus S_1$ is a separator of (E, F) and $S_3 \leq_T^p S$. □

The following summarizes the properties we proved so far:

- $(A, B) \leq_m^{pp} (E, F) \leq_T^{pp} (C, D)$;
- $(C, D) \not\leq_T^{pp} (E, F) \not\leq_T^{pp} (A, B)$.

Now we define the pair (G, H). It follows from the proof of Theorem 4.7 that if we take $T' = \overline{T} = \overline{G[f]}$, then all the consequences of the theorem are satisfied as well. So we define

$$G' = (T' \cap A) \cup (\overline{T'} \cap C) = (\overline{T} \cap A) \cup (T \cap C)$$

and

$$H' = (T' \cap B) \cup (\overline{T'} \cap D) = (\overline{T} \cap B) \cup (T \cap D).$$

Then we have $(G', H') \notin \mathcal{C}_1 \cup \mathcal{C}_2$. Similarly we define $G = G' \oplus A$ and $H = H' \oplus B$. By the same arguments as above, the following properties hold for (G, H):

- $(A, B) \leq_m^{pp} (G, H) \leq_T^{pp} (C, D)$;
- $(C, D) \not\leq_T^{pp} (G, H) \not\leq_T^{pp} (A, B)$.

It remains to show $(E, F) \not\leq_T^{pp} (G, H)$ and $(G, H) \not\leq_T^{pp} (E, F)$. We show only that $(E, F) \not\leq_T^{pp} (G, H)$ since the proof of the latter is identical. The proof follows from the following two claims:

Claim 4.10 $(C, D) \leq_m^{pp} (E \oplus G, F \oplus H)$.

Proof. We define the reduction f as follows: On input x, if $x \in T$, then $f(x) = 10x$, and, if $x \notin T$, then $f(x) = 00x$. We need to prove that $f(C) \subseteq E \oplus G$ and $f(D) \subseteq F \oplus H$. Suppose that $x \in C$. Consider the case that $x \in T$. By definition of G', $x \in G'$. So $0x \in G$. Hence, $f(x) = 10x \in E \oplus G$. In the case that $x \notin T$, we have $x \in E'$. So $0x \in E$. Hence, $f(x) = 00x \in E \oplus G$. Thus, $f(C) \subseteq E \oplus G$. The proof that $f(D) \subseteq F \oplus H$ is similar. □

Claim 4.11 *If* $(E, F) \leq_T^{pp} (G, H)$ *then* $(E \oplus G, F \oplus H) \leq_T^{pp} (G, H)$

Proof. Let S be a separator of (G, H). By the hypothesis, there is a separator S' of (E, F) such that $S' \leq_T^p S$. Then $S' \oplus S$ is a separator of $(E \oplus G, F \oplus H)$ and $S' \oplus S \leq_T^p S$. □

Now we see that if $(E, F) \leq_T^{pp} (G, H)$, then $(C, D) \leq_m^{pp} (E \oplus G, F \oplus H) \leq_T^{pp} (G, H)$, which is a contradiction. □

Corollary 4.12 *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 Theorem 4.8, and in addition, satisfy the following conditions:*

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

The proof follows readily.

Corollary 4.13 *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 4.12, Theorem 3.1, and Proposition 3.5. □

Acknowledgements. The authors thank Kenneth W. Regan for informing them of the methods in his papers [Reg83, Reg88].

References

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

[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.

[HS01] S. Homer and A. Selman. *Computability and Complexity Theory.* Texts in Computer Science. Springer, New York, 2001.

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

[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.

[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 Foundations of Computation Theory*, 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.