On reducibility and symmetry of disjoint NP-pairs

Pavel Pudlák*

Mathematical Institute, AV ČR and ITI**
Prague, Czech Republic

Abstract. We consider some problems about pairs of disjoint NP sets. The theory of these sets with a natural concept of reducibility is, on the one hand, closely related to the theory of proof systems for propositional calculus, and, on the other, it resembles the theory of NP completeness. Furthermore, such pairs are important in cryptography. Among others, we prove that the Broken Mosquito Screen pair of disjoint NP-sets can be polynomially reduced to Clique-Coloring pair and thus is polynomially separable and we show that the pair of disjoint NP-sets canonically associated with the Resolution proof system is symmetric.

1 Introduction

The subject of study of this paper is the concept of pairs of disjoint NP-sets. Thus instead of studying sets (or in other words, languages), the most common object in complexity theory, we study pairs of sets and we require, moreover, that they are disjoint and that they belong to NP. Pairs of disjoint sets have been studied by Grollmann and Selman in connection with complexity theoretical foundations of cryptography [7]. Razborov has shown that such pairs are naturally associated to some formal systems, in particular, proof systems for propositional calculus and systems of bounded arithmetic [15].

There is a natural concept of polynomial reducibility between pairs of disjoint sets. We say that a pair (A, B) is *polynomially reducible* to (C, D) if there is a polynomial time computable function f defined on all strings such that f maps A into C and B into D. (Note that polynomial reducibility does not imply that the corresponding sets are polynomially (Karp) reducible.) We say that two pairs are polynomially equivalent, if they are mutually polynomially reducible. Reducibility among pairs defines a quasiordering of pairs. The classes of equivalent elements in this quasiordering will be called, as usual, *degrees*. Thus the degree of a pair is the class of pairs that are equivalent to it. We say that a pair (A, B) is *polynomially separable*, if there exists a function f computable in polynomial time such that f is 0 on A and it is 1 on B.

* Partially supported by grant A1019901 of the AV ČR and grant 201/01/1195 of the GA ČR. Part of this reserch was done when visiting IAS, Princeton and being supported by a grant of the State of New Jersey.

** Project No. LN00A056 of the Ministry of Education of the Czech Republic.

We shall also study *propositional proof systems,* a concept that is very much related to pairs of disjoint NP-sets. A general propositional proof system, as defined by Cook and Reckhow [6], is simply a nondeterministic algorithm for the set of propositional tautologies. There are several well-studied concrete systems, coming from logic, automated reasoning and others. Proof systems can be compared using the relation of polynomial simulation (see Section 3 for definitions). It has been conjectured that there is no strongest propositional proof system.

Razborov [15] associated a pair of disjoint NP sets in a natural way to each proof system: roughly speaking, one set is the set of tautologies that have short proofs in the given system, the other is the set of non-tautologies. This relation gives a reason to believe that in the lattice of the degrees of pairs there is no biggest element. It seems that the lattice of degrees of pairs reflects the strength of the systems, hence there should not exist a biggest degree of a pair (unless we define it as the degree of pairs that are *not* disjoint), but we are not able to derive this statement from the standard complexity theoretical conjectures such as $P \neq NP$. Most people believe that $P \neq NP \cap coNP$, which implies that that there are pairs of disjoint NP sets that are not polynomially separable. However the only concrete sets in $NP \cap coNP$ that are conjectured not to belong to P come from cryptography. (In cryptography one assumes even more, namely, that there exists a set $A \in NP \cap coNP$ such that a random element of A cannot be distinguished from a random non-element of A using a probabilistic algorithm with probability significantly larger than $1/2$.) Also one can easily show that $P \neq UP$ implies the existence of a pair of polynomially inseparable NP sets [7].

In this paper we show that a pair called Broken Mosquito Screen, introduced by A. Haken [5] is polynomially separable. Pairs similar to BMS have been proposed for bit commitment schemas in cryptography. The polynomial separability implies that such schemas are not secure. Furthermore, we show simple monotone reductions between BMS and the Clique-Coloring pair. Hence one can deduce exponential lower bounds on monotone boolean circuits for BMS [5] and Clique-Coloring [14] one from the other. Note that all lower bounds on monotone computation models, with the exception of Andrejev's [2], are in fact lower bounds on devices separating two NP sets.

In section 3 we consider some basic relations between proof systems and disjoint NP-pairs. This section contains some new observations, but mostly it is a survey of simple basic facts. It is mainly intended as a brief introduction into the subject for those who are not experts in it.

In section 4 we shall show a symmetry property of the pair associated to the Resolution proof system. This is not a surprising result, as such properties have been already established in Razborov's original paper for stronger systems. The reason for presenting the reduction explicitly is that Resolution is relatively weak, so it does not share all good properties of strong systems. Furthermore, we would like to understand this pair and, possibly, to find a simpler combinatorial characterization of its degree.

2 The Broken Mosquito Screen pair

Definition 1. *The BMS pair is a pair of sets of graphs (BMS_0, BMS_1) such that*

- *BMS_0 is the set of graphs such that for some $k > 2$ the graph has $k^2 - 2$ vertices and contains k disjoint cliques with $k-1$ cliques of size k and one of size $k-2$,*
- *and BMS_1 is the set of graphs such that for some $k > 2$ the graph has k^2-2 vertices and contains k disjoint independent sets with $k-1$ independent sets of size k and one of size $k-2$.*

Clearly $BMS_0, BMS_1 \in NP$. To prove that the two sets are disjoint, suppose that a graph G satisfies both conditions at the same time. Each independent set of size k must contain a vertex that is not contained in any of the cliques of size k, since there are only $k-1$ such cliques and an independent set can have at most one vertex in common with a clique. But then we get $k-1$ vertices outside of the $k-1$ cliques of size k, so the graph has at least $(k-1)k+k-1 > k^2-1$ vertices, which is a contradiction. Thus $BMS_0 \cap BMS_1 = \emptyset$. This pair was introduced by A. Haken along with his new method for proving exponential lower bounds on the size of monotone boolean circuits. Then, in a joint paper with Cook [5], it was used to prove an exponential lower bound on the size of cutting planes proofs. We define a modification of the pair, denoted by BMS', by relaxing the conditions a little. In the BMS' pair (BMS'_0, BMS'_1) we ask for only $k-1$ cliques of size k, respectively, $k-1$ independent sets of size k (while the number of vertices is as in BMS, namely k^2-2). A very important pair is the following Clique-Coloring pair.

Definition 2. *The CC pair is a pair of sets (CC_0, CC_1) such that CC_0 and CC_1 are sets of pairs (G,k) with G a graph and $k \geq 2$ an integer such that*

- *CC_0 is the set of pairs (G,k) such that G contains a clique of size k*
- *and CC_1 is the set of pairs (G,k) such that G can be colored by $k-1$ colors.*

It is well-known that the CC pair is polynomially separable; the function that separates CC is the famous θ function of Lovász [12]. We will show a reduction of BMS' to CC, hence BMS' and BMS are also polynomially separable.

Proposition 1. *BMS' is polynomially reducible to CC.*

Proof. Let $G = (V,E)$ be a graph on k^2-2 vertices. We assign a graph H to G as follows. The vertices of H are (i,v), $1 \leq i \leq k-1$, $v \in V$; $((i,v),(j,u))$ is an edge in H, if $i = j$ and $(v,u) \in E$, or $i \neq j$ and $v \neq u$. If G contains $k-1$ disjoint cliques of size k, we can take one such clique in each copy, different cliques in different copies, and thus get a clique of size k^2-k in H. Now suppose G contains $k-1$ disjoint independent sets of size k. Let X be the union of these sets. Thus the graph induced on X by G can be colored by $k-1$ colors and the size of X is $k(k-1)$. Hence we can color the vertices $[1,k-1] \times X$ of H by

$(k-1)^2$ colors. The remaining vertices can be colored by $|V \setminus X| = k-2$ colors (by coloring (i, v) by v). Thus we need only $(k-1)^2 + k - 2 = k^2 - k - 1$ colors. Hence $G \mapsto (H, k^2 - k)$ is a reduction of BMS' to CC.

Corollary 1. *The BMS pair is polynomially separable.*

If a pair is polynomially separable, then, trivially, it can be polynomially reduced to any other pair. The algorithm for separation of the CC pair is, however, highly nontrivial, therefore the next proposition gives us additional information. Recall that a function f is a *projection*, if for every fixed input size n, the output size is a fixed number m and each bit of $f(x)$ is either constant or depends on only one bit of x. In other words, $f(x)$ is computed by depth 0 circuits. So far it was irrelevant in what form we represent the integers in the pairs. In the following we shall need that they are represented in unary.

Proposition 2. *CC is reducible to BMS' using a polynomial time computable projection.*

Proof. Let (G, k) be given, let $G = (V, E)$, $n = |V|$. We can assume w.l.o.g. that n is even $n \geq 4$ and $k = n/2$. We construct a graph H from $2k-2$ copies of G and some additional vertices. The edges connecting the copies and the edges connecting the additional vertices do not depend on G. Thus H is defined as a projection of G. The set of vertices of H is $\{0,1\} \times [1, k-1] \times V$ plus a set U of n elements and a set W of $n-2$ elements. A pair $((i, r, v), (j, s, u))$ is an edge in H, if either $i = j$ and $r = s$ and $(v, u) \in E$, or $i = j$ and $r \neq s$ and $v = u$, or $i \neq j$. On U we put a matching and W will be an independent set. Every vertex of $\{0,1\} \times [1, k-1] \times V$ will be connected with every vertex of U and W, and there will be no edges between U and W. The number of vertices of H is $2(k-1)n + n + n - 2 = 2(n/2 - 1)n + n + n - 2 = n^2 - 2$.

Assume that G has a clique K of size k. Then H has $k - 1 = n/2 - 1$ disjoint cliques of size $2k = n$ of the form $\{0,1\} \times \{r\} \times K$. Furthermore we get $n - k = n/2$ disjoint cliques of size n by taking $\{0,1\} \times [1, k-1] \times \{v\}$, $v \in V \setminus K$ together with a pair from U. Thus H contains $n-1$ disjoint cliques of size n.

Assume that $\chi(G) \leq k-1$. Then we can cover each of the two sets $\{i\} \times [1, k-1] \times V$ by $k-1$ independent sets of size n by uniting the independent sets diagonally. Thus we get $2(k-1) = n-2$ disjoint independent sets of size n. On $U \cup W$ we have another independent set of size $n/2 + n - 2 \geq n$.

Note that the reduction of BMS' to CC presented above is also a projection, thus the two pairs are very close to each other. We believe, though we do not have a proof yet, that a refinement of the proof will give the same for the original BMS. Furthermore, these projections are monotone (hence computable by linear size monotone circuits), thus one can get exponential lower bounds on the size of monotone boolean circuits for one pair from the other.

What are the pairs that we still believe that they are not polynomially separable? As noted above, the most likely inseparable pairs are from cryptography.

Any bit commitment schema that we believe is secure gives such a pair. For instance, the encryption schema RSA can be used to encode a single bit by using the parity of the encrypted number. Thus one set is the set of codes of odd numbers and the other consists of the codes of even numbers. Every one-way permutation can be used to define an inseparable pair. All these pairs are based on number theory. Pairs based on pure combinatorics are rather scarce. A somewhat combinatorial pair of disjoint NP sets is implicit in the lower bound on monotone span programs of [3]. This pair is based on bipartite graphs with special properties. There are two known constructions of such graphs. The first construction uses deep results from commutative algebra, the second uses deep results from number theory. We do not know a polynomial time separation algorithm for these pairs, but also we do not have any particular reasons to believe that they are not separable.

Razborov [15] defined another interesting type of pairs of disjoint NP sets. Let $t : N \rightarrow N$ be a polynomial time computable function; let $s_n : \{0,1\}^n \rightarrow \{0,1\}$, $n = 1, 2, \ldots$ be a sequence of boolean functions such that s_n cannot be computed by circuits of size $2t(n) + 1$. Denote by $SIMPLE_t$ the set of truth tables of boolean functions that can be computed by circuits of size $t(n)$, and by $SIMPLE_t^{\oplus s}$ the set of truth tables of boolean functions f such that, if $f : \{0,1\}^n \rightarrow \{0,1\}$, then $f \oplus s_n$ can be computed by circuits of size $t(n)$. Since $f \oplus (f \oplus s_n) = s_n$, the assumption on the complexity of s_n implies that the two sets are disjoint. As every boolean function has a circuit of size polynomial in the size of its truth table, $SIMPLE_t$ is in NP. If $x \mapsto s_n(x)$ is computable in $NTime(2^{O(n)})$, then also $SIMPLE_t^{\oplus s}$ is in NP. It is well-known that hardness of approximating the size of a minimal circuit from the truth table of a boolean function is equivalent to the existence of pseudorandom generators. As we believe that pseudorandom generators do exits, the later fact supports our belief that such pairs are polynomially inseparable.

Here is another pair that we do not know how to separate.

Definition 3. *The $MMMT$ (Monotone-Min-Max-Term) pair is the pair of sets $(MMMT_0, MMMT_1)$ in which both sets are sets of some pairs (C, k), C a monotone circuit and k a number and*

- *$MMMT_0$ is the set of pairs such that C has $k+1$ disjoint minterms,*
- *$MMMT_1$ is the set of pairs such that C has a maxterm of size k.*

We suspect, however, that $MMMT$ can be reduced to CC, since to prove the disjointness of the sets in the pair, essentially, only the pigeon hole principle is needed.

3 Propositional proof systems

In 1970's Cook initiated systematic study of the complexity of propositional proofs. In a joint paper with Reckhow [6] they defined a general concept of a propositional proof system: a *propositional proof system* is a polynomial time computable function S mapping all strings in a finite alphabet *onto* the set of all tautologies $TAUT$. To be precise one has to specify in what language the tautologies are. In this paper we will need only tautologies in DNF. The meaning of the definition is: *x is a proof of $S(x)$*. The fact that every string is a proof seems strange at first glance, but, clearly, it is only a technicality. The crucial property is that one can test in polynomial time whether a given string is a proof of a given formula.

Propositional proof systems are quasi-ordered by the relation of polynomial simulation. We say that P *polynomially simulates* S, if there exists a polynomial time computable function f such that $P(f(x)) = S(x)$ for all x. Thus given an S proof x of a formula ϕ (i.e. $\phi = S(x)$), f finds a P proof $f(x)$ of this formula (i.e. $\phi = P(f(x))$).

As in the next section we will consider the resolution proof system, which is a refutation system, we shall often talk about refutations, i.e., proofs of contradiction from a given formula, rather than direct proofs. Again, this is only *façon de parler*.

Disjoint NP pairs are closely related to propositional proof systems. Following [15] we define, for a proof system S, $REF(S)$ to be the set of pairs $(\phi, 1^m)$, where ϕ is a CNF formula that has a refutation of length $\leq m$ in S and 1^m is a string of 1's of length m. Furthermore, SAT^* is the set of pairs $(\phi, 1^m)$ where ϕ is a satisfiable CNF and m is an arbitrary natural number. We say that $(REF(S), SAT^*)$ is *the canonical NP-pair* for the proof system S.

The polynomial reducibility quasi-ordering of canonical pairs reflects the polynomial simulation quasi-ordering of proof systems.

Proposition 3. *If P polynomially simulates S, then the canonical pair of S is polynomially reducible to the canonical pair of P.*

Proof. The reduction is given by $(\phi, 1^m) \mapsto (\phi, 1^{p(m)})$, where p is a polynomial bound such that $|f(x)| \leq p(|x|)$ for all x.

It is possible, however, to give an example of two systems that are not equivalent with respect to polynomial simulation, but still have canonical pairs mutually polynomially reducible. We will give the example a few lines below.

The main problem about canonical pairs is, how hard it is to distinguish elements of one of the sets from the elements of the other set, in particular, is the pair polynomially separable? This question is related to the so called automatizability of a proof system. A proof system S is *automatizable*, if there exists a polynomial time algorithm that for a given formula ϕ and a number m finds a refutation of ϕ in time polynomial in m, provided a refutation of length at most m exists. The following is trivial:

Lemma 1. *If S is automatizable, then the canonical pair of S is polynomially separable.*

The converse may be not true, but the following weaker statement is true.

Lemma 2. *If the canonical pair of S polynomially separable, then there exists a proof system S' which polynomially simulates S and which is automatizable.*

Proof. Let f be a polynomial time computable function that is 0 on $REF(S)$ and 1 on SAT^*. In the proof system S' a refutation of ϕ is a sequence 1^m such that $f(\phi, 1^m) = 0$. Formally, we define S' by $S'(w) = \phi$, if $w = (\phi, 1^m)$ and $f(\phi, 1^m) = 0$; $S'(w) = x_1 \vee \neg x_1$ otherwise. A polynomial simulation of S by S' is the function $w \mapsto (S(w), 1^{|w|})$.

Corollary 2. *The canonical pair of a proof system S is polynomially separable iff there exists an automatizable proof system S' that polynomially simulates S.*

The last corollary shows that from the point of view of proof search the problem of the polynomial separation of the canonical pair is more important than automatizability. For example, assuming a reasonable complexity theoretical conjecture, it has been established that Resolution is not automatizable [1]. But this does not exclude the possibility that an extension of Resolution is automatizable. To show that the latter possibility is excluded means to prove that the canonical pair of Resolution is not polynomially separable. (Thus the relation of these two concepts is similar to *undecidability* and *essential undecidability* of first order theories in logic.)

Interpolation and reflection

We shall mention two more concepts that are connected with disjoint NP pairs. The first is the feasible interpolation property. We say that a system S has *the feasible interpolation property* if, given a proof of a formula

$$\phi(\bar{x}, \bar{y}) \vee \psi(\bar{x}, \bar{z}), \tag{1}$$

in which $\bar{x}, \bar{y}, \bar{z}$ are strings of distinct propositional variables, one can construct in polynomial time a boolean circuit C with the property

$$C(\bar{x}) = 0 \Rightarrow \phi(\bar{x}, \bar{y}) \quad \text{and} \quad C(\bar{x}) = 1 \Rightarrow \psi(\bar{x}, \bar{z}).$$

The meaning of this is that the sets $\{\bar{x}\ ;\ \exists \bar{y} \neg\phi(\bar{x}, \bar{y})\}$ and $\{\bar{x}\ ;\ \exists \bar{z} \neg\psi(\bar{x}, \bar{z})\}$, which have polynomial size nondeterministic boolean circuits, can be separated by a polynomial size (deterministic) circuit. If we had a sequence of formulas of the form above given uniformly in polynomial time and also their proofs given in this way, we would get, from the feasible interpolation property, a pair of disjoint NP-sets and a polynomial time separation algorithm for them. On the other hand, given an NP set A, we can construct (in fact, generate uniformly in polynomial time) a sequence of formulas α_n such that for $|\bar{x}| = n$, $\bar{x} \in A$ iff $\exists \bar{y}\ \alpha_n(\bar{x}, \bar{y})$. So the statement that two NP sets are disjoint can be expressed as a sequence of formulas of the form 1.

Consequently: *feasible interpolation means that whenever we have short proofs that two NP sets are disjoint, then they can be polynomially separated.*

Now we sketch the promised example of the two nonequivalent proof systems with essentially the same canonical pair. In [13] we have shown (using the feasible interpolation property) that in the cutting planes proof system CP the tautology expressing the disjointness of sets of the pair CC has only exponentially long proofs. Note that the disjointness of the CC pair is based on the pigeon hole principle: it is not possible to color a k-clique by $k-1$-colors. This may seem paradoxical, as the pigeon hole principle has polynomial size proofs in CP. The explanation is that in order to use the pigeon hole principle we need to define a mapping and the mapping from the clique to the colors cannot be defined using the restricted means of CP. In CP one can use only *linear* inequalities with propositional variables. To define the mapping we need quadratic terms, namely, terms of the form $x_i y_j$ for x_i coding a vertex of the clique and y_j coding a color.

So let us define an extension of CP, denoted by CP^2 that allows quadratic terms. What it means precisely is the following. Given a formula with variables $x_1, \dots, x_n$ we allow in its proofs inequalities with terms of the form x_i and $x_i x_j$ for $i < j$ (and, of course, constants). On top of the axioms ($0 \leq x_i \leq 1$) and rules (rational positive linear combinations and the rounding up rule) of CP the proofs of CP^2 may use the following axioms about the quadratic terms:

$$0 \leq x_i x_j \leq 1, \quad x_i x_j \leq x_i, \quad x_i x_j \leq x_j, \quad x_i + x_j \leq x_i x_j + 1.$$

In particular the rounding up rule states that given an inequality

$$\sum_i a_i x_i + \sum_{i,j} b_{i,j} x_i x_j \geq c,$$

with $a_i, b_{i,j}$ integers, we can derive

$$\sum_i a_i x_i + \sum_{i,j} b_{i,j} x_i x_j \geq \lceil c \rceil.$$

One can show that in this system the CC tautology has polynomial size proofs. Here is a hint. To construct the proof directly in CP^2 is not quite easy. Thus, instead, use the fact that CP simulates Resolution, hence CP^2 simulates Resolution augmented with conjunctions of pairs of variables. In such a system it is routine to derive the PHP clauses for the composition of the two mappings (the mapping from a k-element set into the graph and the mapping from the graph into $k-1$ colors). After translating the clauses back to CP^2 we can use the easy fact that CP (and hence CP^2 for inequalities with quadratic terms) proves PHP.

The key to prove that the canonical pair of CP^2 is polynomially reducible to the one of CP, is the observation that though the quadratic terms $x_i x_j$ are written as compound terms, they can be interpreted as just another type of variables (indexed by two indices). We can think of CP^2 as CP with an additional variable $x_{i,j}$ for each pair of variables x_i and x_j. Put differently, $x_{i,j}$ are extension variables representing the products. Thus the reduction is the following mapping: $(\phi, 1^m) \mapsto (\phi', 1^{p(m)})$ with ϕ' expressing that the above axioms for quadratic terms imply ϕ. Since CP is a refutation system, we can think of ϕ as a set of inequalities from which we want to derive a contradictory inequality and then ϕ' is the union of this set with the inequalities for all quadratic terms formed from variables occurring in ϕ. $p(m)$ is a suitable polynomial overhead.[1] Thus we have shown:

Proposition 4. *The proof system CP does not polynomially simulate the proof system CP^2, but their canonical pairs are polynomially equivalent.*

The last property of proof systems that we mention in this paper is the reflection property. We say that a system S has *the reflection property* if the formulas

$$\neg\rho_{S,n,m}(\bar{x},\bar{y}) \vee \neg\sigma_n(\bar{x},\bar{z})$$

have polynomial size proofs, where $\rho_{S,n,m}(\bar{x},\bar{y})$ is a propositional formula that expresses that *'y is an S refutation of length m of formula x of length n'* and $\sigma_n(\bar{x},\bar{z})$ is a propositional formula that expresses that *'z is a satisfying assignment of formula x of length n'*. Furthermore, we will assume that the proofs of these formulas are given uniformly by a polynomial time algorithm. The meaning of the formulas, actually tautologies, is that either the formula x has no refutation of length m or it is not satisfiable. Thus reflection of S means that we can generate in polynomial time proofs of propositional instances of the statement $REF(S) \cap SAT^* = \emptyset$.

Proposition 5. *If a proof system has both feasible interpolation and reflection properties, then its canonical pair is polynomially separable.*

Proof. Reflection means that one can efficiently generate proofs of the tautologies expressing the disjointness of the canonical pair. Feasible interpolation property means that any NP pair that has such proofs is polynomially separable. Hence the canonical pair is polynomially separable.

A version of the feasible interpolation by associating another pair of disjoint NP sets to a proof system. For a proof system P, let

$$D_P = \{(\phi,\psi,d);\ \phi \text{ and } \psi \text{ don't share variables and } d \text{ is a } P\text{-proof of } \phi\vee\psi\}.$$

We define the *interpolation pair* of P by (I_P^0, I_P^1) with

$$I_P^0 = \{(\phi,\psi,d) \in D_P;\ \neg\phi \in SAT\}, \quad I_P^1 = \{(\phi,\psi,d) \in D_P;\ \neg\psi \in SAT\}.$$

The version of the feasible interpolation property is the statement that the interpolation pair is polynomially separable. The above proposition can be interpreted as: if a system has reflection, then its canonical and interpolation pairs are polynomially equivalent.

[1] The Lovász-Schrijver system combined with CP that we considered in [13] seems not to be strong enough to polynomially simulate CP^2, as it does not allow applying the rounding up rule to quadratic inequalities.

We know of strong systems that have reflection property (see [8] Theorems 9.1.5 and 9.3.4),[2] we also know of weak systems that have feasible interpolation property, but we have no example of a proof system that has both properties. Note that the last proposition can be refined. Namely, to prove the polynomial separation of the canonical pair of a system S we only need to have short P proofs of the reflection principle for S in some, *possibly stronger*, system P that has the feasible interpolation property. We think that it is unlikely that for any of the studied systems the canonical pair is polynomially separable. In order to give a partial justification of this conjecture we shall show that CP does not have reflection property. In fact, we can show a little more.

Theorem 1. *Every CP proof proof of*

$$\neg\rho_{CP,n,m}(\bar{x},\bar{y}) \vee \neg\sigma_n(\bar{x},\bar{z}) \tag{2}$$

(the tautology expressing the reflection principle for CP) has size $2^{n^{\Omega(1)}}$.

The proof has two main steps. First, we observe that in Proposition 5, if the proof system satisfies *monotone* feasible interpolation (see [8] for the definition), then the conclusion can be strengthened to a separation by *monotone* boolean circuits of polynomial size. We recall that CP has the monotone feasible interpolation property. Second, we shall show a polynomial monotone reduction from BMS' to the canonical pair of CP. [3]

Let $G = (V, E)$ be a graph on $k^2 - 2$ vertices. We express the condition that $G \in BMS_0$ as the following set of linear inequalities. Let $A_1, \ldots, A_{k-1}$ be pairwise disjoint sets of size k. Let A denote their union. We use propositional variables $x_{i,v}$ for $i \in A$ and $v \in V$. These variable encode a one-to-one mapping from A to V, which is expressed by the clauses:

$$\text{(i)} \quad \sum_{v\in V} x_{i,v} \geq 1 \quad \text{for } i \in A,$$

$$\text{(ii)} \quad x_{i,v} + x_{j,v} \leq 1 \quad \text{for } i,j \in A,\ i \neq j,\ v \in V,$$

$$\text{(iii)} \quad x_{i,v} + x_{i,u} \leq 1 \quad \text{for } i \in A,\ v,u \in V,\ v \neq u.$$

The images of A_t determine cliques in G, which is expressed by:

$$\text{(iv)} \quad x_{i,v} + x_{j,u} \leq 1 \quad \text{for } i,j \in A_t,\ t = 1,\ldots,k-1,\ v,u \in V,\ (v,u) \notin E.$$

The reduction is based on the following lemma.

[2] For a logician this may look surprising, since reflection principles for first order theories are stronger than consistency and even the latter is unprovable by Gödel theorem. Furthermore, reflection for strong enough propositional proof systems is equivalent to their consistency [8].

[3] I could also use the CC pair, but I had written a piece of a proof for BMS' that I can use here now.

Lemma 3. *If $G \in BMS_1$ then there is a polynomial size proof of the fact that $G \notin BMS_0$ in CP.*

Lemma 4. *Given clauses $y_i + y_j \leq 1$ for $1 \leq i < j \leq n$, one can derive the clause*

$$\sum_{i=1}^{n} y_i \leq 1 \tag{3}$$

by a polynomial size CP proof. This holds also when y_i are linear terms with integer coefficients.

Proof. We prove (3) by induction on n. The base case is trivial. To prove the induction step we assume that we already have (3). Adding the clauses with y_{n+1} we get $\sum_{i=1}^{n}(y_i + y_{n+1}) \leq n$. Adding to it (3) multiplied by $n-1$ we get $n\sum_{i=1}^{n+1} y_i \leq 2n-1$. Dividing by n and rounding down the right hand side we get $\sum_{i=1}^{n+1} y_i \leq 1$. As we have added a piece of proof that is polynomial in n, the size of the proofs grows polynomially.

Proof of Lemma 3. Let $G \in BMS_1$, let $S_1, \ldots, S_{k-1}$ be the disjoint independent sets of size k. Let S_k be the remaining part of the vertices. The idea of the proof is as follows. The alleged mapping from A to V, for every $t, r < k$, can map at most one element from A_t to S_r. Therefore, by PHP, it has to map an element of A_t to S_k. As there are $k-1$ sets A_t and $|S_k| = k-2$, we get a contradiction by another application of PHP.

Here is how we do it formally in CP. First we get

$$\sum_{i \in A_t, v \in S_r} x_{i,v} \leq 1 \tag{4}$$

by applying the previous lemma to clauses (ii)-(iv) that are relevant for A_t and S_r. Adding them for a fixed t and $r = 1, \ldots, k-1$ we get

$$\sum_{i \in A_t, v \in S_1 \cup \ldots \cup S_{k-1}} x_{i,v} \leq k-1.$$

Adding (i) for $i \in A_t$, we get

$$\sum_{i \in A_t, v \in V} x_{i,v} \geq k.$$

Subtracting the previous inequality we get

$$\sum_{i \in A_t, v \in S_k} x_{i,v} \geq 1.$$

Adding these inequalities for $t = 1, \ldots, k-1$ we have

$$\sum_{i \in A, v \in S_k} x_{i,v} \geq k-1.$$

On the other hand, summing (4) for $v \in S_k$, we get

$$\sum_{i \in A, v \in S_k} x_{i,v} \le k - 2.$$

Thus $G \in BMS_0$ is refuted.

Now we can finish the proof of Theorem 1. Consider the mapping that to a given graph H on $k^2 - 2$ vertices assigns the set of inequalities (i)–(iv) above for $G = (V, E)$ the complement of H. This can, clearly, be done by a polynomial monotone projection (the more edges in H, the more equations in the set). This projection is a reduction of BMS' to the canonical pair of CP by Lemma 3. Indeed, if $H \in BMS'_0$, then $G \in BMS'_1$ and we get, by Lemma 3, a polynomial size refutation of the inequalities. If $H \in BMS'_1$, then $G \in BMS'_0$ and we get a satisfying assignment for the the inequalities, as they express the later fact.

Now suppose there is a CP proof of (2) of size s. Since $\sigma_n(\bar{x}, \bar{z})$ is monotone in $\bar{x}$, by the monotone feasible interpolation theorem we have a monotone circuit of size $s^{O(1)}$ that separates the instances of the canonical pair of the given length. Because of the reduction, we thus get a monotone circuit of size $s^{O(1)}$ that separates the instances of BMS'. By [5], we know that such a circuit must have size at least $2^{\Omega(k)}$, ($k^2 - 1$ is the number of vertices). Note that the n in $\sigma_n(\bar{x}, \bar{z})$ is polynomial in k. Hence $s = 2^{\Omega(n)}$, which finishes the proof.

A proof similar to the proof of Lemma 3 gives a reduction from $MMMT$ to the canonical pair of CP. Hence, if $MMMT$ is not polynomially separable, neither the canonical pair of CP is.

More recently Atserias and Bonet (personal communication) showed that also Resolution does not have polynomial size proofs of the reflection principle for Resolution.

Existential interpolation

Let us conclude by mentioning a weaker separation property. A pair (A, B) is called separable by *co*NP sets if there exist disjoint *co*NP sets A' and B' such that $A \subseteq A'$ and $B \subseteq B'$. We have much less evidence for believing that there exist disjoint NP pairs that are inseparable by *co*NP sets. Rudich has considered a related concept in cryptography and conjectured that the subset sum problem is an example of it [16]. Unfortunately, we do not see how to get a pair of disjoint NP sets from the subset sum problem. The problem is the disjointness. One can modify the concept of feasible interpolation to this kind of separability; such a property is called *existential interpolation*. It is not clear at all whether the classical systems, based on *modus ponens* and axiom schemas (the so called *Frege systems*, see [6, 8] for the exact definition of Frege systems) have this property.

The following natural property of a proof system implies existential interpolation. Say that a proof system P has *weak feasible disjunction property*, if there exists a polynomial p such that if a disjunction $\phi \vee \psi$, in which ϕ and ψ

do not share variables, has a P proof of length n, then either ϕ or ψ has a proof of length $p(n)$. (Clearly, if ϕ and ψ do not share variables, then the disjunction is a tautology iff one of the formulas is.) Feasible interpolation does not imply this property, but in all known cases the proof systems with feasible interpolation property have it. It is an interesting problem if any of the studied systems that *do not* have feasible interpolation property has this property. The following observation, however, suggest that the *weak feasible disjunction property* is very unlikely to occur, unless the system is very weak (for example that it satisfies the feasible interpolation property).

In the following proposition we need a proof system P satisfy a couple of simple natural properties. First, given a P proof of $\alpha(\bar{x}, \bar{y})$, and an arbitrary assignment $\bar{a}$ of true and false constants to variables $\bar{x}$, then there exists at most polynomially longer P proof of $\alpha(\bar{a}, \bar{y})$. The second property is a bit stronger. We require that given a P proof of the fact that $\neg\alpha$ is not satisfiable, then there is at most polynomially longer P proof α. The last property is the reflection. For example, Frege systems have all these properties.

Proposition 6. *Suppose a proof system P is sufficiently strong in the sense of the preceding paragraph and has the weak feasible disjunction property. Then for every proposition α and a natural number $m \geq |\alpha|$, either*

1. *there exists a P proof of α of length $m^{O(1)}$, or*
2. *there exists a P proof d of the nonexistence of a P proof of α of length m and the length of d is $m^{O(1)}$.*

Proof. Suppose P has all the properties required by the proposition. Let α and m be given. Let $\bar{a}$ be the truth assignment coding the proposition $\neg\alpha$. Substitute it into the formula expressing the reflection principle; thus we get

$$\neg\rho_{S,n,m}(\bar{a}, \bar{y}) \vee \neg\sigma_n(\bar{a}, \bar{z})$$

and this has a polynomial size P proof. Because we have substituted constants for the common variables, the two formulas do not share variables. Hence, by the weak feasible disjunction property, either the first one has a polynomial size proof or the second one has. The first one is the case 2 of the proposition, since $\neg\rho_{S,n,m}(\bar{a}, \bar{y})$ says that $\neg\alpha$ is not refutable. The second formula gives case 1, since $\neg\sigma_n(\bar{a}, \bar{z})$ says that $\neg\alpha$ is not satisfiable and we assume that this gives a polynomial size P proof of α.

The conclusion of the proposition seems unlikely, because it means that for every proposition we either get a short proof of it, or short proofs of lower bounds on the lengths of its proofs. But our experience rather suggests that proving lower bounds is difficult.

4 The NP-pair of Resolution

We shall consider the canonical pair of the Resolution proof system. Resolution uses only formulas that are disjunctions of variables and negated variables (called *literals*); these formulas are called *clauses*. The only rule of Resolution is the cut in which we combine two clauses with a complementary literal into one, omitting the complementary literal. A proof is a sequence of clauses such that at the beginning we have the clauses that we want to refute and then a sequence of clauses follows such that each of these clauses follows by an application of the resolution rule from two clauses before it. In general, the length of a proof is the length of a binary sequence that encodes the proof. In Resolution the size of each step of the proof, which is a clause, is bounded by the number of propositional variables that appear in the clauses to be refuted. Hence we can assume w.l.o.g. that the length is simply the number of clauses in the proof.

To get more information on the pair $(REF(R), SAT^*)$, where R stands for the resolution proof system, we prove the following symmetry property of it.

Definition 4. *A pair (A, B) is symmetric, if (A, B) is polynomially reducible to (B, A).*

This property has been shown for some stronger systems using first order theories associated to the proof systems [15]. Essentially, what is done there is proving the reflection property and deriving the symmetry of the canonical pair from it. Resolution is weaker than such systems, in particular it is unlikely that it possesses the reflection property. Therefore we give a direct proof of the symmetry of the canonical pair of Resolution. The idea of the proof is to show a property that is a little weaker than reflection, but still implies the symmetry.

Theorem 2. *The canonical pair of Resolution is symmetric.*

Proof. We need, for a given CNF ϕ and a number m, to construct in polynomial time a CNF ψ such that if ϕ is refutable by a resolution refutation of length m, then ψ is satisfiable and if ϕ is satisfiable, then ψ is refutable by a refutation with length polynomial in m. Let ϕ be the conjunction of clauses $C_1, \ldots, C_r$, let the variables in the clauses be $x_1, \ldots, x_n$. We shall represent a refutation of ϕ of length m by a $2n \times m$ matrix, plus some additional information. The columns of the matrix will encode the clauses of the refutation. The additional information will specify for each clause that is not an assumption, from which two clauses it has been derived. Furthermore we shall specify the variable that was resolved in this step of the refutation.

It will be clear from the construction of ψ that the formula is a correct description of a refutation, ie., if a refutation exists, then ψ is satisfiable. Thus the assignment $(\phi, 1^m) \mapsto (\psi, 1^{m'})$ maps $REF(R)$ into SAT^*, (whatever m' we choose).

The nontrivial part is to show that if ϕ is satisfiable, then there is a resolution refutation of ψ that is polynomial in the size of ϕ and m (the size of this proof will determine the m' and then we get that SAT^* is mapped to $REF(R)$). This will be proved as follows. We take a satisfying assignment and derive gradually, for each $j = r, r+1, \ldots, m$, the clause that says that the j-th clause of the proof agrees with the satisfying assignment at least in one literal. The contradiction is obtained by using the clauses of ψ that express that the last clause C_m should be empty (clauses (1) below). Here is a detailed proof.

Variables $y_{e,i,j}$, $e = 0, 1$, $i = 1, \ldots, n$, $j = 1, \ldots, m$ encode clauses. Namely, $y_{0,i,j}$ (resp. $y_{1,i,j}$) means that $\neg x_i$ (resp. x_i) is present in the clause C_j. Variables $p_{j,k}$ (resp. $q_{j,k}$) $1 \leq j < k$, $r < k \leq m$ say that C_k was obtained from C_j and C_j contains negated (resp. positively) the resolved variable. Finally, variables $v_{i,j}$ determine that C_j was obtained by resolving variable x_i. The following are the clauses of ψ.

(0) $y_{0,i,j}$ or $y_{1,i,j}$ for all i and all $j \leq r$, according to which literal occurs in C_j (recall that for $j \leq r$ the clauses are given by ϕ);

(1) $\neg y_{e,i,m}$, for all e, i (the last clause is empty);

(2) $\neg y_{0,i,j} \vee \neg y_{1,i,j}$, for all i, j (C_j does not contain x_i and $\neg x_i$ at the same time);

(3a) $\bigvee_{j<k} p_{j,k}$, (3b) $\bigvee_{j<k} q_{j,k}$, for $k > r$;

(4) $\neg p_{j,k} \vee \neg q_{j,k}$, for $j < k$, $r < k$;

(5) $\neg p_{j,k} \vee \neg p_{j',k}$, $\neg q_{j,k} \vee \neg q_{j',k}$ for $j, j' < k$, $j \neq j'$, $r < k$ ((3-5) say that there are exactly two clauses that are assigned to C_k);

(6a) $\neg p_{j,k} \vee \neg v_{i,k} \vee y_{0,i,j}$ (the C_j assigned to C_k contains literal $\neg x_i$);

(6b) $\neg q_{j,k} \vee \neg v_{i,k} \vee y_{1,i,j}$ (the C_j assigned to C_k contains literal x_i);

(7a) $\neg p_{j,k} \vee v_{i,k} \vee \neg y_{e,i,j} \vee y_{e,i,k}$ (C_k contains C_j except for $\neg x_i$);

(7b) $\neg q_{j,k} \vee v_{i,k} \vee \neg y_{e,i,j} \vee y_{e,i,k}$ (C_k contains C_j except for x_i);

(8a) $\bigvee_i v_{i,k}$ for $r < k$;

(8b) $\neg v_{i,k} \vee \neg v_{i',k}$ for $i \neq i'$, $r < k$ (the resolution variable x_i is uniquely assigned to C_k).

This finishes the description of the ψ that is assigned to $(\phi, 1^m)$. Now, given a satisfying assignment $(e_1, \ldots, e_n)$ for $C_1, \ldots, C_r$ we construct a polynomial size refutation from (0)-(8). We shall use the weakening rule, which is superfluous, but it simplifies notation. (The weakening rule is applied to add more literals to a derived clause.) Put

$$D_k := \; y_{e_1,1,k} \vee \ldots \vee y_{e_n,n,k}.$$

We shall gradually derive clauses $D_1, \ldots, D_m$. Once we have D_m, a contradiction follows immediately using clauses (1). Here is the detailed proof.

Clauses $D_1, \ldots, D_r$ follow immediately from (0) using weakening. To derive D_k, assuming D_j for $j < k$, we first derive clauses

(9) $\neg p_{j,k} \vee \neg q_{l,k} \vee D_k$

for $j \neq l$, $j, l < k$. To derive (9), we need to derive several clauses.

Fix i and l and assume w.l.o.g. $e_i = 0$. From (6b) and (2) we get $\neg q_{l,k} \vee \neg v_{i,k} \vee \neg y_{0,i,l}$. Resolving with D_l we get

(10) $\neg q_{l,k} \vee \neg v_{i,k} \vee (D_l \setminus \{y_{0,i,l}\})$.

From (7b) and (8b) we get

(11) $\neg q_{l,k} \vee \neg v_{i,k} \vee \neg y_{e_{i'},i',l} \vee y_{e_{i'},i',k}$,

for all $i' \neq i$. Resolving (10) with clauses in (11) we get $\neg q_{l,k} \vee \neg v_{i,k} \vee (D_k \setminus \{y_{0,i,k}\})$. Using weakening we get

(12) $\neg p_{j,k} \vee \neg q_{l,k} \vee \neg v_{i,k} \vee D_k$.

Having these for all i, we can resolve with (8a) and get (9).

To get D_k from (9), first resolve with (3a) to get $p_{l,k} \vee \neg q_{l,k} \vee D_k$. Then resolve with (4) to get $\neg q_{l,k} \vee D_k$. Finally resolve with (3b) and get D_k.

We have shown that if ϕ is satisfiable, then there exists a proof of ψ the size of which is polynomial in the size of ϕ and m. Let m' be the polynomial bound on this proof; we can compute this bound *without* having the proof of ψ. Thus, if we define the reduction by $(\phi, 1^m) \mapsto (\psi, 1^{m'})$, the set SAT^* will be mapped into $REF(R)$.

The following operation on pairs, clearly, defines the meet in the lattice of degrees of pairs,

$$(A, B) \wedge (C, D) = (A \times C, B \times D).$$

Given a pair (A, B) we can thus form a symmetric pair by taking $(A, B) \wedge (B, A)$. This symmetrization satisfies the following stronger property: there exists a polynomial time computable isomorphism that transposes the sets in the pair. An example of a concrete pair that has this property is BMS. We observe that the symmetry of a pair implies that there is an equivalent pair, namely $(A, B) \wedge (B, A)$, with the stronger property.

Proposition 7. *If (A, B) is symmetric, then (A, B) and $(A, B) \wedge (B, A)$ are polynomially equivalent.*

Proof. $(A, B) \wedge (B, A)$ is always reducible to (A, B) by the projection on the first coordinate. Let f be a polynomial reduction of (A, B) to (B, A). Then $x \mapsto (x, f(x))$ is a polynomial reduction of (A, B) to $(A, B) \wedge (B, A)$.

Consequently, there is a pair of disjoint NP sets that has this stronger symmetry property and that is polynomially equivalent to the canonical pair of Resolution.

5 Open problems and further research topics.

Our first result shows that seemingly different pairs may be in fact equivalent. Our second result shows that the canonical pair of Resolution is equivalent to a very symmetric pair. This gives some hope that a nice combinatorial characterization of the degree of the canonical pair of Resolution and other systems may be found. If the systems are natural and robust, there should be simple combinatorial principles on which they are based. Ideally, we would like to prove that some canonical pair is polynomially equivalent to some combinatorially defined pair. At present we only have reductions of cryptographic pairs to canonical pairs of proof systems [10, 4], but we do not have converse reductions. We do not have any reductions from canonical pairs to pairs defined in another way.

An important problem is to decide if the canonical pairs of weak systems are polynomially separable. In particular, prove or disprove (using plausible complexity theoretical assumptions) that the canonical pair of Resolution is polynomially separable. If it were polynomially separable, it might have practical consequences for automated theorem proving (see Lemma 2).

In this paper we have considered a concept of reduction between pairs that corresponds to many one reductions between sets. One can define also the concept corresponding to Turing reductions:

Definition 5. *(A, B) is polynomially Turing reducible to (C, D), if there exists a polynomial time oracle Turing machine M such that M^A separates (A, B) for every oracle A that separates (C, D).*

With this definition of reduction, it should be possible to show the equivalence of more pairs. Eg., every (A, B) is polynomially Turing equivalent to (B, A). Furthermore, given a pair (A, B), define $P_0^{A,B}, P_1^{A,B}$ by $(x_1, \ldots, x_n) \in P_i^{A,B}$ iff $x_1, \ldots, x_n \in A \cup B$ and the parity of the number of x_j's such that $x_j \in A_j$ is i. It is an easy exercise to show that this pair is polynomially Turing equivalent to (A, B).

It would be interesting to learn more about the lattice of degrees of disjoint NP pairs. We know about this structure even less than we know about the degrees of proof systems. Does there exist the biggest element in it? How is this question related to the same question about the degrees of proof systems? Etc.

References

1. M. Alekhnovich and A. A. Razborov, Resolution is Not Automatizable Unless W[P] is Tractable, http://genesis.mi.ras.ru/ razborov/
2. A. E. Andreev, On a method for obtaining lower bounds for the complexity of individual monotone functions. Soviet Math. Doklady 31, 1985, 530-534.
3. L. Babai, A. Gál and A. Wigderson, Superpolynomial lower bounds for monotone span programs, Combinatorica 19 (3), 1999, 301-319.
4. M. Bonet, T. Pitassi and R. Raz, On interpolation and automatization for Frege systems. SIAM J. on Computing 29(6), (2000), 1939-1967.
5. S.A. Cook and A. Haken, An exponential lower bound for the size of monotone real circuits, JCSS 58, (1999), 326-335.
6. S.A. Cook and Reckhow, The relative efficiency of propositional proof systems, J. of Symbolic Logic, **44(1)**, 36-50.
7. J. Grollmann and A. L. Selman, Complexity measures for public-key cryptosystems, SIAM J. Comput 17(2), 1988, 309-335.
8. J. Krajíček, Bounded arithmetic, propositional logic, and complexity theory, Cambridge Univ. Press, 1995.
9. J. Krajíček and P. Pudlák, Propositional proof systems, the consistency of first order theories and the complexity of computations, J. of Symbolic Logic, **54(3)**, 1063-1079.
10. J. Krajíček and P. Pudlák, Some consequences of cryptographical conjectures for S_2^1 and EF. Information and Computation 142, (1998), 82-94
11. L. Kučera, Cryptography and random graphs, preprint.
12. L. Lovász, On the Shannon capacity of graphs, *IEEE Trans. Inform. Theory* **25**, 1979, 1-7.
13. P. Pudlák, On the complexity of propositional calculus, Sets and Proofs, Invited papers from Logic Colloquium'97, Cambridge Univ. Press, 1999, 197-218
14. A.A. Razborov, Lower bounds on the monotone complexity of some Boolean functions, *Soviet Mathem. Doklady* **31,** 354-357.

15. A.A. Razborov, On provably disjoint NP-pairs, BRICS Report Series RS-94-36, 1994, http://www.brics.dk/RS/94/36/index.html.
16. S. Rudich, Super-bits, Demi-bits, and NP/poly-natual proofs, preprint, http://www.cs.cmu.edu/ rudich/papers/index.htm