Monotone Proofs of the Pigeon Hole Principle

Albert Atserias[*†] Nicola Galesi [†] Ricard Gavaldà [†]

Departament de Llenguatges i Sistemes Informàtics
Universitat Politècnica de Catalunya
Barcelona, Spain
{atserias,galesi,gavalda}@lsi.upc.es

November 16, 1999

Abstract

We study the complexity of proving the Pigeon Hole Principle (PHP) in a monotone variant of the Gentzen Calculus, also known as Geometric Logic. We show that the standard encoding of the PHP as a monotone sequent admits quasipolynomial-size proofs in this system. This result is a consequence of deriving the basic properties of certain quasipolynomial-size monotone formulas computing the boolean threshold functions. Since it is known that the shortest proofs of the PHP in systems such as Resolution or Bounded Depth Frege are exponentially long, it follows from our result that these systems are exponentially separated from the monotone Gentzen Calculus. We also consider the monotone sequent (CLIQUE) expressing the *clique-coclique* principle defined by Bonet, Pitassi and Raz (1997). We show that monotone proofs for this sequent can be easily reduced to monotone proofs of the one-to-one and onto PHP, and so CLIQUE also has quasipolynomial-size monotone proofs. As a consequence, Cutting Planes with polynomially bounded coefficients is also exponentially separated from the monotone Gentzen Calculus. Finally, a simple simulation argument implies that these results extend to the Intuitionistic Gentzen Calculus. Our results partially answer some questions left open by P. Pudlák.

[*]Supported by the CUR, Generalitat de Catalunya, through grant 1999FI 00532.
[†]Partially supported by DGES PB95–0787 (KOALA Project) and by SGR CIRIT 1997SGR–00366.

1 Introduction

One of the main approaches to attack the **NP** $\neq$ co-**NP** question is that of studying the length of proofs in propositional calculi. In a well-known result, Cook and Reckhow [16] proved that if all propositional proof systems are not *polynomially bounded*, that is, if they have families of tautologies whose shortest proofs are superpolynomial in the size of the formulas, then **NP** $\neq$ co-**NP**. In spite of the simplicity of propositional proof systems such as the Hilbert Calculus (Frege system) or the Gentzen sequent Calculus, we are admitedly far at present from proving that these systems are not polynomially bounded. Surprisingly, one of the main difficulties is the lack of families of tautologies candidate to be hard for these systems.

Nevertheless several important results have been obtained for less powerful but not trivial proof systems. Strong lower bounds are actually known for systems such as Resolution [18, 13, 5, 31, 14], Bounded Depth Frege [1, 4] and Polynomial Calculus [28]. The common point among these results is the family of formulas that is considered to give the exponential lower bounds. These formulas encode a basic combinatorial principle known as the Pigeon Hole Principle (PHP^m_n), saying that there is no one-to-one mapping from a set of m elements to a set of n elements, provided $m > n$. Resolution was the first proof system for which an exponential lower bound was proved for the size of refutations of the PHP^{n+1}_n, a well-known result due to Haken [18]. This result was generalized to PHP^m_n, for m linear in n, by Buss and Turan [13]. The same formula, PHP^{n+1}_n, was later used by Ajtai [1] to give a superpolynomial size lower bound for a system that subsumes Resolution: Bounded Depth Frege. This result was simplified and improved up to an exponential lower bound by Beame et al. [4]. The complexity of the PHP^m_n is also well-studied in algebraic-style propositional proof systems. Recently, Razborov [28] (see also [19]) showed that PHP^{n+1}_n is also hard for the Polynomial Calculus. Actually one of the most interesting problems is to know the exact complexity of Resolution refutations of PHP^m_n, when $m \geq \frac{n^2}{\log n}$ [6, 12, 29]. Thus, in spite of its simple combinatorial nature, PHP^{n+1}_n is one of the most commonly used principles to give proof complexity lower bounds. For this reason, in studying the complexity of a new proof system, it is important to consider the complexity of proving PHP^{n+1}_n as a first step. After Haken's lower bound, it was conjectured that PHP^{n+1}_n would also be hard to prove for more powerful proof systems, such as Frege. The conjecture was refuted by Buss [9], who exhibited polynomial-size proofs in Frege, or equivalently, in the Gentzen Calculus. It is also known that PHP^{n+1}_n has polynomial-size proofs in Cutting Planes [17], and that the slightly weaker form PHP^{2n}_n has quasipolynomial-size proofs in Bounded Depth Frege [23, 22].

Monotone proof systems, that is, proof systems restricted to propositional formulas over the monotone basis $\{\wedge, \vee\}$, were considered by Pudlák and Buss [26], and more recently, by Pudlák [24], and Clote and Setzer [15]. There are several alternative definitions of monotone proof systems. Here we consider the Monotone Gentzen Calculus, called *Geometric Logic* in [24]. Although the only monotone tautological formula is the true constant 1, Pudlák suggests the study of tautological sequents of the form $A \to B$, where A and B are boolean formulas built over the monotone basis $\{\wedge, \vee\}$. Several interesting combinatorial principles can be put in this form; for example, PHP^{n+1}_n.

The correpondence between circuit complexity classes and proof systems inspires new techniques to obtain both upper and lower bounds for proofs. Examples are the lower bound of Beame et. al. [4] for Bounded Depth Frege (also known as $\mathbf{AC}_0$ Frege), in which they used an adaptation of Hastad's Switching Lemma, and the polynomial upper bound of Buss ([10]) for PHP_n^m in Frege (or $\mathbf{NC}_1$-Frege) using an $\mathbf{NC}_1$ circuit for addition. While strong lower bounds for monotone circuits were given more than ten years ago (see [27, 3]), non-trivial lower bound for monotone proof systems are not known yet. Hence, one of the basic questions is whether PHP_n^{n+1} can be used to obtain exponential lower bounds for these systems. This question is also important since the (non-monotone) Frege proofs of PHP_n^{n+1} given by Buss [9] formalize a counting argument, and it is not clear how to formalize counting arguments into short monotone proofs. See the paper by Pudlák [24] for a further discussion on this topic (see also [15]).

In this work we exhibit quasipolynomial-size proofs of PHP_n^{n+1} in the Monotone Gentzen Calculus. To obtain this result, we consider quasipolynomial-size monotone formulas to compute the boolean threshold functions. While polynomial-size monotone formulas are known for these functions [32, 2], Pudlák remarks that it is not clear whether their basic properties have short monotone proofs. First, Valiant's construction [32] is probabilistic, and therefore, it does not provide any explicit formula to work with. Second, the sorting network of Ajtai, Komloś, and Szemeredi [2] makes use of expanders graphs, and there is little hope that their basic properties will have short monotone proofs. Here we address the difficulty raised by Pudlák by considering explicit quasipolynomial-size monotone formulas $\mathrm{th}_k^n(x_1, \ldots, x_n)$ to compute threshold functions. We show that the basic properties of $\mathrm{th}_k^n(x_1, \ldots, x_n)$ admit quasipolynomial-size monotone proofs. In particular, we prove that for any permutation π the sequent $\mathrm{th}_k^n(x_1, \ldots, x_n) \vdash \mathrm{th}_k^n(x_{\pi(1)}, \ldots, x_{\pi(n)})$ has quasipolynomial-size monotone proofs.

We remark that our proofs can be made tree-like, but details are omitted in this version. For non-monotone Gentzen Calculi, J. Krajíček [20] proved that tree-like proofs are as powerful as the unrestricted ones. But it is not known at present whether this holds for the monotone case, as the same technique does not apply.

We also consider the formula CLIQUE_k^n expressing the (n, k)-Clique-Coclique Principle, used by Bonet, Pitassi and Raz, and for which an exponentialy lower bound in Cutting Planes with polynomially bounded coefficients (poly-CP) was proved [8] (notice the difference with the Clique Principle with common variables introduced by J. Krajíček in [21], and used by Pudlák in [25] to obtain exponential lower bounds for Cutting Planes with unrestricted coefficients. The latter is not a monotone tautology of the form $A \rightarrow B$). We show that monotone proofs for the monotone sequent obtained from the formula CLIQUE_k^n can be reduced to monotone proofs of the *onto* version of PHP_{k-1}^k, which in turn can be easy reduced to the standard PHP_{k-1}^k. This way, we obtain quasipolynomial-size monotone proofs of CLIQUE_k^n.

Our results imply that Resolution, Bounded-depth Frege, and poly-CP are exponentially separated from the (tree-like) Monotone Gentzen Calculus. Finally, as remarked in [24], a simple simulation argument shows that every proof in the Monotone Gentzen Calculus, is also a proof in the Intuitionistic Gentzen Calculus. Hence, all our results also hold for this system.

The paper is organized in the following way. In Section 2 we define the Monotone Gentzen Calculus, and the quasipolynomial-size monotone formulas to compute the threshold functions. In Section 3 we give monotone proofs for the basic properties of the threshold formulas. In Setion 4 we build the quasipolynomial-size monotone proofs of PHP_n^{n+1}. In Section 5 we show the result for CLIQUE_k^n, and we discuss the consequences of extending our result to different encodings of this principle.

2 Preliminaries

A *monotone formula* is inductively defined as follows: a propositional constant or variable is a monotone formula; if A and B are monotone formulas, then $A \wedge B$ and $A \vee B$ are monotone formulas; nothing else is a monotone formula. The *Monotone Gentzen Calculus* (MLK), also called *Geometric Logic* [24], is obtained from the standard Gentzen Calculus when only monotone formulas are considered, and the negation rules are ignored. For completeness, we present the rules and axioms of MLK. For monotone formulas A and B, and sequences of monotone formulas Γ, Γ', Δ, and Δ':

Axioms:

$$\frac{}{A \vdash A} \qquad \frac{}{0 \vdash A} \qquad \frac{}{A \vdash 1}$$

Left Structural Rules

$$\frac{\Gamma, A, A, \Delta \vdash \Gamma'}{\Gamma, A, \Delta \vdash \Gamma'} \qquad \frac{\Gamma, A, B, \Delta \vdash \Gamma'}{\Gamma, B, A, \Delta \vdash \Gamma'} \qquad \frac{\Gamma \vdash \Gamma'}{A, \Gamma \vdash \Gamma'}$$

Right Structural Rules

$$\frac{\Gamma' \vdash \Gamma, A, A, \Delta}{\Gamma' \vdash \Gamma, A, \Delta} \qquad \frac{\Gamma' \vdash \Gamma, A, B, \Delta}{\Gamma' \vdash \Gamma, B, A, \Delta} \qquad \frac{\Gamma' \vdash \Gamma}{\Gamma' \vdash \Gamma, A}$$

Cut Rule

$$\frac{\Gamma \vdash \Delta, A \quad A, \Gamma' \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}$$

Left Logical Rules

$$\frac{A, B, \Gamma \vdash \Delta}{(A \wedge B), \Gamma \vdash \Delta} \qquad \frac{A, \Gamma \vdash \Delta \quad B, \Gamma' \vdash \Delta'}{(A \vee B), \Gamma, \Gamma' \vdash \Delta, \Delta'}$$

Right Logical Rules

$$\frac{\Gamma \vdash \Delta, A, B}{\Gamma \vdash \Delta, (A \vee B)} \qquad \frac{\Gamma \vdash \Delta, A \quad \Gamma' \vdash \Delta', B}{\Gamma, \Gamma' \vdash \Delta, \Delta', (A \wedge B)}$$

As usual, a proof in MLK is a sequence of *sequents*, or lines, of the form $\Gamma \vdash \Delta$ each of which is either an initial axiom, or has been obtained by a rule of MLK from two previous lines in the sequence. The sequence constitutes a proof of the last sequent. When we restrict the proofs in such a way that each derived sequent can be used only once as premise in a rule, we say that the system is tree-like.

The overall number of *symbols* used in a proof is the *size* of the proof. Let A and $B_1, \ldots, B_n$ be formulas, and let $x_1, \ldots, x_n$ be propositional variables that may or may not occur in A. We let $A(x_1/B_1, \dots, x_n/B_n)$ denote the formula that results from A when all occurrences of x_i (if any) are replaced by B_i (replacements are made simultaneously). Observe that if A and B are monotone formulas, then $A(x/B)$ is also monotone. The non-monotone version of the following Lemma appears in [7].

Lemma 1 *For every monotone formula A, the sequents*

(i) $A, x \vdash A(x/1)$;
(ii) $A \vdash x, A(x/0)$;
(iii) $A(x/1), x \vdash A$;
(iv) $A(x/0) \vdash x, A$;
(v) $A(x/0) \vdash A(x/1)$;

have MLK*-proofs of size quadratic in the size of A.*

Proof: All five sequents have straightforward proofs built by induction on the structure of A. Since the number of subformulas of A is at most quadratic in the size of A, the result follows. Observe that the monotonicity of A is only needed in part (v). □

For every n and $k \in \{0, \dots, n\}$, let $\mathrm{TH}^n_k : \{0,1\}^n \to \{0,1\}$ be the boolean function such that for every $(a_1, \dots, a_n) \in \{0,1\}^n$, we have that $\mathrm{TH}^n_k(a_1, \dots, a_n) = 1$ if and only if $\sum_{i=1}^k a_i \geq k$. Each TH^n_k is called a threshold function. Valiant [32] proved that every threshold function TH^n_k is computable by a monotone formula of size polynomial in n. The proof being probabilistic, the construction is not explicit. In the same paper, Valiant mentioned that a divide and conquer strategy leads to explicit quasipolynomial-size monotone formulas for all threshold functions. The same construction appears in the book by Wegener [34], and in the more recent book by Vollmer [33]. Here we revisit that construction with a minor modification. We define monotone formulas

$$\mathrm{th}^1_0(x) := 1, \qquad \mathrm{th}^1_1(x) := x,$$

and for every $n > 1$ and $k \in \{0, \dots, n\}$, define the formula

$$\mathrm{th}^n_k(x_1, \dots, x_n) \quad := \quad \bigvee_{(i,j) \in I^n_k} (\mathrm{th}^{n/2}_i(x_1, \dots, x_{n/2}) \wedge \mathrm{th}^{n-n/2}_j(x_{n/2+1}, \dots, x_n)),$$

where $I^n_k = \{(i,j) : 0 \leq i \leq n/2,\ 0 \leq j \leq n - n/2,\ i + j \geq k\}$ and $n/2$ is an abbreviation for $\lfloor n/2 \rfloor$. It is straightforward to prove that $\mathrm{th}^n_k(x_1, \dots, x_n)$ computes the boolean function TH^n_k. On the other hand, it is easy to check that the maximum number of connectives of $\mathrm{th}^n_k(x_1, \dots, x_n)$, say $S(n)$, satisfies the following recurrence:

$$S(n) \quad \leq \quad n^2 \cdot S(n/2).$$

Since $S(1) \leq 1$, it follows at once that the size of the formula $\mathrm{th}^n_k(x_1, \dots, x_n)$ is bounded by $n^{c \log_2(n)}$ for some constant $c > 0$; that is, the size of $\mathrm{th}^n_k(x_1, \dots, x_n)$ is quasipolynomial in n.

3 Basic properties of threshold formulas

We establish a number of lemmas stating that the elementary properties of the threshold formulas admit short MLK-proofs. Here, short means size polynomial in the size of the formula $\mathrm{th}^n_k(x_1,\ldots,x_n)$, and therefore, size quasipolynomial in n.

Lemma 2 *For every $n,m,k \in \mathbb{N}$ with $m \le n/2$, and $k \le n-n/2$, and for every $h,s \in \mathbb{N}$ with $n \ge h \ge s$, the sequents*

(i) $\vdash \mathrm{th}^n_0(x_1,\ldots,x_n)$;

(ii) $\mathrm{th}^n_n(x_1,\ldots,x_n) \vdash \bigwedge_i x_i$;

(iii) $\mathrm{th}^{n/2}_m(x_1,\ldots,x_{n/2}) \wedge \mathrm{th}^{n-n/2}_k(x_{n/2+1},\ldots,x_n) \vdash \mathrm{th}^n_{m+k}(x_1,\ldots,x_n)$;

(iv) $\mathrm{th}^n_h(x_1,\ldots,x_n) \vdash \mathrm{th}^n_s(x_1,\ldots,x_n)$;

have MLK-*proofs of size quasipolynomial in n.*

Proof: Recall that $\mathrm{th}^1_0(x_1)$ is 1, and $\vdash 1$; property (i) follows easily by induction on n. Similarly, recall that $\mathrm{th}^1_1(x_1)$ is x_1; property (ii) follows again easily by induction on n. For property (iii), the left-hand side is a disjunct of the right-hand side, and the sequent follows by an application of the axiom $A \vdash A$, right weakening, and right $\vee$-introduction. For property (iv), reason as follows. When $s=0$, the sequent is trivial by property (i) and left weakening. When $s>0$, every disjunct of $\mathrm{th}^n_h(x_1,\ldots,x_n)$ is also a disjunct of $\mathrm{th}^n_s(x_1,\ldots,x_n)$, so that the sequent follows easily as before. □

In the next lemmas we give MLK-proofs of the basic properties relative to the symmetry of the threshold formulas (Theorem 1 below).

Lemma 3 *For every $n,m,k,l \in \mathbb{N}$, with $0 < m \le n$, $0 \le k < n$, and $0 \le l \le n$, the sequents*

(i) $\mathrm{th}^n_{k+1}(x_1,\ldots,x_l/1,\ldots,x_n) \vdash \mathrm{th}^n_k(x_1,\ldots,x_l/0,\ldots,x_n)$

(ii) $\mathrm{th}^n_{m-1}(x_1,\ldots,x_l/0,\ldots,x_n) \vdash \mathrm{th}^n_m(x_1,\ldots,x_l/1,\ldots,x_n)$

have MLK-*proofs of size quasipolynomial in n.*

Proof: We first show (i). We use induction on n, where the base case is $\mathrm{th}^1_1(1) \vdash \mathrm{th}^1_0(0)$. Assume without loss of generality that $l \le n/2$, that is, x_l is in the first half of the variables. Recall the definition of $\mathrm{th}^n_{k+1}(x_1,\ldots,x_l/1,\ldots,x_n)$:

$$\bigvee_{(i,j)\in I^n_{k+1}} (\mathrm{th}^{n/2}_i(x_1,\ldots,x_l/1,\ldots,x_{n/2}) \wedge \mathrm{th}^{n-n/2}_j(x_{n/2+1},\ldots,x_n)).$$

Fix $(i,j) \in I^n_{k+1}$. If $i=0$, then $j \ge k+1$ and $\mathrm{th}^{n-n/2}_j(x_{n/2+1},\ldots,x_n) \vdash \mathrm{th}^{n-n/2}_k(x_{n/2+1},\ldots,x_n)$ by part (iv) of Lemma 2. Since $\vdash \mathrm{th}^{n/2}_0(x_1,\ldots,x_l/0,\ldots,x_{n/2})$ by part (i) of Lemma 2, right $\wedge$-introduction gives

$$\mathrm{th}^{n-n/2}_j(x_{n/2+1},\ldots,x_n) \vdash \mathrm{th}^{n/2}_0(x_1,\ldots,x_l/0,\ldots,x_{n/2}) \wedge \mathrm{th}^{n-n/2}_k(x_{n/2+1},\ldots,x_n),$$

and a cut with part (iii) of Lemma 2 gives $\mathrm{th}_j^{n-n/2}(x_{n/2+1},\ldots,x_n) \vdash \mathrm{th}_k^n(x_1,\ldots,x_l/0,\ldots,x_n)$. Left weakening and left $\wedge$-introduction gives then

$$\mathrm{th}_i^{n/2}(x_1,\ldots,x_l/1,\ldots,x_{n/2}) \wedge \mathrm{th}_j^{n-n/2}(x_{n/2+1},\ldots,x_n) \vdash \mathrm{th}_k^n(x_1,\ldots,x_l/0,\ldots,x_n)$$

as desired. If $i > 0$, then $\mathrm{th}_i^{n/2}(x_1,\ldots,x_l/1,\ldots,x_{n/2}) \vdash \mathrm{th}_{i-1}^{n/2}(x_1,\ldots,x_l/0,\ldots,x_{n/2})$ by induction hypothesis on n. Easy manipulation using part (iii) of Lemma 2 as before gives

$$\mathrm{th}_i^{n/2}(x_1,\ldots,x_l/1,\ldots,x_{n/2}) \wedge \mathrm{th}_j^{n-n/2}(x_{n/2+1},\ldots,x_n) \vdash \mathrm{th}_{i-1+j}^n(x_1,\ldots,x_l/0,\ldots,x_n).$$

Finally, since $i-1+k \geq k$, a cut with part (iv) of Lemma 2 gives the result. The proof of (ii) is very similar. $\square$

Lemma 4 *For every $m,n,k,l \in \mathbb{N}$ with $1 \leq k < l \leq n$, and $m \leq n$, the sequents*

(i) $\mathrm{th}_m^n(x_1,\ldots,x_k/1,\ldots,x_l/0,\ldots,x_n) \vdash \mathrm{th}_m^n(x_1,\ldots,x_k/0,\ldots,x_l/1,\ldots,x_n)$
(ii) $\mathrm{th}_m^n(x_1,\ldots,x_k/0,\ldots,x_l/1,\ldots,x_n) \vdash \mathrm{th}_m^n(x_1,\ldots,x_k/1,\ldots,x_l/0,\ldots,x_n)$

have MLK-*proofs of size quasipolynomial in n.*

Proof: Both proofs are identical. It is enough to prove (i) when $k \leq n/2 < l$, that is, when x_k falls in the first half of the variables and x_l falls in the second half of the variables. The complete proof of (i) would then be a simple induction on the recursive definition of $\mathrm{th}_m^n(x_1,\ldots,x_k/1,\ldots,x_l/0,\ldots,x_n)$ whose base case is $k \leq n/2 < l$. So assume $k \leq n/2 < l$ and recall the definition of $\mathrm{th}_m^n(x_1,\ldots,x_k/1,\ldots,x_l/0,\ldots,x_n)$:

$$\bigvee_{(i,j)\in I_m^n} (\mathrm{th}_i^{n/2}(x_1,\ldots,x_k/1,\ldots,x_{n/2}) \wedge \mathrm{th}_j^{n-n/2}(x_{n/2+1},\ldots,x_l/0,\ldots,x_n)).$$

Fix $(i,j) \in I_m^n$. If $i > 0$ and $j < n-n/2$, then Lemma 3 shows that

$$\mathrm{th}_i^{n/2}(x_1,\ldots,x_k/1,\ldots,x_{n/2}) \vdash \mathrm{th}_{i-1}^{n/2}(x_1,\ldots,x_k/0,\ldots,x_{n/2})$$
$$\mathrm{th}_j^{n-n/2}(x_{n/2+1},\ldots,x_l/0,\ldots,x_n) \vdash \mathrm{th}_{j+1}^{n-n/2}(x_{n/2+1},\ldots,x_l/1,\ldots,x_n),$$

from which the result follows easily. Consider next the case in which either $i = 0$ or $j = n-n/2$. If $j = n-n/2$, then $\mathrm{th}_{n-n/2}^{n-n/2}(x_{n/2+1},\ldots,x_l/0,\ldots,x_n)$ is just provably false by part (ii) of Lemma 2, and the result follows easily. If $i = 0$, then $\mathrm{th}_i^{n/2}(x_1,\ldots,x_k/0,\ldots,x_{n/2})$ is just provably true by part (i) of Lemma 2. On the other hand, $\mathrm{th}_j^{n-n/2}(x_{n/2+1},\ldots,x_l/0,\ldots,x_n) \vdash \mathrm{th}_j^{n-n/2}(x_{n/2+1},\ldots,x_l/1,\ldots,x_n)$ follows by part (v) of Lemma 1, and the result follows too. $\square$

Lemma 5 *For every $m,n,i,j \in \mathbb{N}$, with $m \leq n$ and $1 \leq i < j \leq n$, the sequent*

$$\mathrm{th}_m^n(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n) \vdash \mathrm{th}_m^n(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$$

has MLK-*proofs of size quasipolynomial in n.*

Proof: We split the property according to the four possible truth values of x_i and x_j. Namely, we will give proofs of the following four sequents from which the lemma is immediately obtained by the cut rule.

(i) $\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n), x_i, x_j \vdash \mathrm{th}^n_m(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$,
(ii) $\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n), x_i \vdash x_j, \mathrm{th}^n_m(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$,
(iii) $\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n), x_j \vdash x_i, \mathrm{th}^n_m(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$,
(iv) $\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n) \vdash x_i, x_j, \mathrm{th}^n_m(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$.

We only show (ii), the rest are similar. Two applications of Theorem 1 with the formula $\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n)$ and a cut give

$$\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n), x_i \vdash x_j, \mathrm{th}^n_m(x_1,\ldots,1,\ldots,0,\ldots,x_n). \tag{1}$$

A cut with part (i) of Lemma 4 gives

$$\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n), x_i \vdash x_j, \mathrm{th}^n_m(x_1,\ldots,0,\ldots,1,\ldots,x_n). \tag{2}$$

Two more applications of Theorem 1 on $\mathrm{th}^n_m(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$ and a cut give

$$\mathrm{th}^n_m(x_1,\ldots,0,\ldots,1,\ldots,x_n), x_i \vdash x_j, \mathrm{th}^n_m(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n) \tag{3}$$

Finally, a cut between 2 and 3 gives (ii). The size of the proof is quasipolynomial since we are applying Theorem 1 on $\mathrm{th}^n_m()$ whose size is quasipolynomial in n. □

Since every permutation on $\{1,\ldots,n\}$ can be obtained as the composition of (polynomially many) permutations in which only two elements are permuted (transpositions), Lemma 5 easily implies the following theorem.

Theorem 1 *For every $m, n \in \mathbb{N}$, with $m \le n$, and for every permutation π over $\{1,\ldots,n\}$ the sequent*

$$\mathrm{th}^n_m(x_1,\ldots,x_n) \vdash \mathrm{th}^n_m(x_{\pi(1)},\ldots,x_{\pi(n)})$$

has MLK*-proofs of size quasipolynomial in n.*

The last two properties state that the smallest threshold formulas are equivalent to their usual formulas:

Lemma 6 *For every $n \in \mathbb{N}$, the sequents*

(i) $\bigvee_i x_i \vdash \mathrm{th}^n_1(x_1,\ldots,x_n)$;
(ii) $\mathrm{th}^n_1(x_1,\ldots,x_n) \vdash \bigvee_i x_i$;
(iii) $\bigvee_{i\neq j}(x_i \wedge x_j) \vdash \mathrm{th}^n_2(x_1,\ldots,x_n)$;
(iv) $\mathrm{th}^n_2(x_1,\ldots,x_n) \vdash \bigvee_{i\neq j}(x_i \wedge x_j)$;

have MLK*-proofs of size polynomial in n.*

Proof: All proofs are by induction on n. For (i), reason as follows. Clearly, $x_1 \vdash \mathrm{th}_1^1(x_1)$ so that the base case holds. Assume then $n > 1$, and that the claim holds for smaller n. Since $\vdash \mathrm{th}_0^{n-n/2}(x_{n/2+1}, \ldots, x_n)$ by part (i) of Lemma 2, right $\wedge$-introduction on the induction hypothesis for $\mathrm{th}_1^{n/2}(x_1, \ldots, x_{n/2})$ gives

$$\bigvee_{i=1}^{n/2} x_i \vdash \mathrm{th}_1^{n/2}(x_1, \ldots, x_{n/2}) \wedge \mathrm{th}_0^{n-n/2}(x_{n/2+1}, \ldots, x_n).$$

Similarly,

$$\bigvee_{i=n/2+1}^{n} x_i \vdash \mathrm{th}_0^{n/2}(x_1, \ldots, x_{n/2}) \wedge \mathrm{th}_1^{n-n/2}(x_{n/2+1}, \ldots, x_n).$$

In both cases, a cut with part (iii) of Lemma 2 gives $\mathrm{th}_1^n(x_1, \ldots, x_n)$. Left $\vee$-introduction gives then (i). The proof of (ii) is also by induction on n. In fact, we prove the slightly stronger statement: $\mathrm{th}_s^n(x_1, \ldots, x_n) \vdash \bigvee_i x_i$ for every $s \in \{1, \ldots, n\}$. Fix $(i,j) \in I_1^n$, so that either $i \geq 1$ or $j \geq 1$ for otherwise $i + j = 0$. Then, by induction hypothesis, either $\mathrm{th}_i^{n/2}(x_1, \ldots, x_{n/2}) \vdash \bigvee_i x_i$ or $\mathrm{th}_j^{n-n/2}(x_{n/2+1}, \ldots, x_n) \vdash \bigvee_i x_i$. In any case,

$$\mathrm{th}_i^{n/2}(x_1, \ldots, x_{n/2}) \wedge \mathrm{th}_j^{n-n/2}(x_{n/2+1}, \ldots, x_n) \vdash \bigvee_i x_i$$

by left weakening and left $\wedge$-introduction. The proof of properties (iii) and (iv) are every similar. $\Box$

The next lemma states that threshold functions split by cases:

Lemma 7 *For every $m, n \in \mathbb{N}$ with m even, $m \leq n$, and n an exact power of two, the sequents*

(i) $\mathrm{th}_{m+1}^n(x_1, \ldots, x_n) \vdash \mathrm{th}_{m/2+1}^{n/2}(x_1, \ldots, x_{n/2}), \mathrm{th}_{m/2+1}^{n/2}(x_{n/2+1}, \ldots, x_n)$,

(ii) $\mathrm{th}_m^n(x_1, \ldots, x_n) \vdash \mathrm{th}_{m/2+1}^{n/2}(x_1, \ldots, x_{n/2}), \mathrm{th}_{m/2}^{n/2}(x_{n/2+1}, \ldots, x_n)$,

have MLK-*proofs of size quasipolynomial in n.*

Proof: We first prove (i). Fix $i, j \leq n/2$ such that $i + j \geq m + 1$. Since m is even, either $i \geq m/2 + 1$ or $j \geq m/2 + 1$ for otherwise $i + j \leq m$. In the former case we get

$$\mathrm{th}_i^{n/2}(x_1, \ldots, x_{n/2}) \vdash \mathrm{th}_{m/2+1}^{n/2}(x_1, \ldots, x_{n/2}), \mathrm{th}_{m/2+1}^{n/2}(x_{n/2+1}, \ldots, x_n)$$

by part (iv) of Lemma 2 and the rule of right weakening. In the latter case we get

$$\mathrm{th}_j^{n/2}(x_{n/2+1}, \ldots, x_n) \vdash \mathrm{th}_{m/2+1}^{n/2}(x_1, \ldots, x_{n/2}), \mathrm{th}_{m/2+1}^{n/2}(x_{n/2+1}, \ldots, x_n),$$

and so the rule of left $\wedge$-introduction puts these together in a single sequent. Since this happens for every pair $i, j \leq n/2$ such that $i + j \geq m + 1$, we get $\mathrm{th}_{m+1}^n(x_1, \ldots, x_n) \vdash$

$\mathrm{th}^{n/2}_{m/2+1}(x_1, \ldots, x_{n/2}), \mathrm{th}^{n/2}_{m/2+1}(x_{n/2+1}, \ldots, x_n)$ as required. The proof of (ii) is extremely similar. Given $i, j \leq n/2$ such that $i + j \geq m$, either $i \geq m/2 + 1$ or $i < m/2 + 1$. In the former case, as before using part (iv) of Lemma 2, we have

$$\mathrm{th}^{n/2}_{i}(x_1, \ldots, x_{n/2}) \vdash \mathrm{th}^{n/2}_{m/2+1}(x_1, \ldots, x_{n/2}), \mathrm{th}^{n/2}_{m/2}(x_{n/2+1}, \ldots, x_n).$$

In the latter case we have that $j \geq m/2$ because $i + j \geq m$, and we can proceed as before to get

$$\mathrm{th}^{n/2}_{j}(x_{n/2+1}, \ldots, x_n) \vdash \mathrm{th}^{n/2}_{m/2+1}(x_1, \ldots, x_{n/2}), \mathrm{th}^{n/2}_{m/2}(x_{n/2+1}, \ldots, x_n),$$

Manipulation as in part (i) gives property (ii). $\square$

4 Monotone proofs of PHP

The *Pigeon Hole Principle* states that if $n + 1$ pigeons go into n holes, then there is some hole with more than one pigeon sitting in it. It is encoded by the following (non-monotone) formula

$$\mathrm{PHP}^{n+1}_{n} \quad := \quad \bigwedge_{i=1}^{n+1} \bigvee_{j=1}^{n} p_{i,j} \rightarrow \bigvee_{k=1}^{n} \bigvee_{\substack{i,j=1 \\ i \neq j}}^{n+1} (p_{i,k} \wedge p_{j,k}).$$

Observe that the Pigeon Hole Principle can be obtained as a monotone sequent simply replacing the symbol $\rightarrow$ above by the symbol $\vdash$. From now on we refer to the left part of the sequent as LPHP_n, and to the right part of the sequent as RPHP_n. The sequent itself is denoted PHP_n.

We first establish that PHP_n can be reduced to the case in which n is an exact power of two.

Lemma 8 *There exists a polynomial $p(n)$ such that, for every $m, S \in \mathbb{N}$, if the sequent PHP_m has a* MLK*-proof of size at most S, then, for every $n \leq m$, the sequent PHP_n has a* MLK*-proof of size at most $S + p(n)$.*

Proof: Suppose that there is a monotone proof $\Psi_1, \Psi_2, \ldots, \mathrm{PHP}_m$ of size at most S, where each Ψ_i is a monotone sequent $\Sigma_i \vdash \Gamma_i$. We get a proof of PHP_n from the proof of PHP_m by replacing some variables by constants as follows. Define a partial truth assignment σ as indicated next. Let $\sigma(p_{k+1,k}) = 1$ for every $k \in \{n+1, \ldots, m\}$. Similarly, for every $k \in \{n+2, \ldots, m+1\}$ and $i \in \{1, \ldots, k-2\}$, let $\sigma(p_{k,i}) = 0$; and for every $i \in \{n+1, \ldots, m\}$ and $k \in \{1, \ldots, i\}$, let $\sigma(p_{k,i}) = 0$. Any other variable remains undefined by σ. Given a sequent $\Sigma \vdash \Gamma$, let $[\Sigma \vdash \Gamma][\sigma]$ be the result of replacing each occurrence of the variable $x \in \mathrm{Dom}(\sigma)$ in Σ or Γ by $\sigma(x)$. The sequence $[\Sigma_1 \vdash \Gamma_1][\sigma], [\Sigma_2 \vdash \Gamma_2][\sigma], \ldots, [\mathrm{PHP}_m][\sigma]$ is a valid proof of $[\mathrm{PHP}_m][\sigma]$. To see this, observe that the initial axioms of the form $p_{i,j} \vdash p_{i,j}$ become $0 \vdash 0$, $1 \vdash 1$, or stay $p_{i,j} \vdash p_{i,j}$, which are all true sequents. Moreover, it is not difficult to give a proof of

$$\left[\bigwedge_{i=1}^{n+1} \bigvee_{j=1}^{n} p_{i,j} \vdash \bigwedge_{i=1}^{m+1} \bigvee_{j=1}^{m} p_{i,j}\right][\sigma]$$

and

$$\left[\bigvee_{k=1}^{m}\bigvee_{\substack{i,j=1\\ j\neq i}}^{m+1}(p_{i,k}\wedge p_{j,k})\vdash\bigvee_{k=1}^{n}\bigvee_{\substack{i,j=1\\ j\neq i}}^{n+1}(p_{i,k}\wedge p_{j,k})\right][\sigma]$$

from the axioms $0\vdash$ and $\vdash 1$. For example, $[\vdash\bigvee_{j=1}^{m}p_{n+2,j}][\sigma]$ is derivable since $\sigma(p_{n+2,n+1})=1$. Two cuts give a proof of PHP_n of size at most $S+p(n)$ for some polynomial $p(n)$, as desired. □

Theorem 2 *The sequents* PHP_n *have* MLK*-proofs of size quasipolynomial in* n*.*

Proof: We first outline the idea of the proof. From the antecedent of PHP_n we immediately derive that for each pigeon i there is at least one variable $p_{i,j}$ that is true $(\mathrm{th}_1^{n+1}(p_{i,1},\ldots,p_{i,n}))$. In turn, we deduce that among all variables grouped by pigeons, at least $n+1$ are true $(\mathrm{th}_{n+1}^{n(n+1)}(p_{1,1},\ldots,p_{1,n},\ldots,p_{n+1,1},\ldots,p_{n+1,n}))$. The symmetry of the threshold formulas will allow us to show that the same holds when the variables are grouped by holes $(\mathrm{th}_{n+1}^{n(n+1)}(p_{1,1},\ldots,p_{n+1,1},\ldots,p_{1,n},\ldots,p_{n+1,n}))$. Finally, from this we get that there is at least one hole with two pigeons ($\mathrm{th}_2^{n+1}(p_{1,i},\ldots,p_{n+1,i})$ for some $i\in\{1,\ldots,n\}$), and this implies RPHP_n.

According to Lemma 8, it is enough to give quasipolynomial size proofs of PHP_n when $n+1$ is a power of two, since there always is a power of two between n and $2n$. So let us assume $n=2^r-1$ for some $r\in\mathbb{N}$. For technical reasons in the proof we will consider a *squared* form (instead of rectangular form) of PHP_n where we assume the existence of an $(n+1)$-st hole in which no pigeon can go. So, we introduce $n+1$ new symbols $p_{1,n+1},\ldots,p_{n+1,n+1}$ that will stand for the constant 0. For every $i\in\{1,\ldots,n+1\}$, let $p_i=(p_{i,1},\ldots,p_{i,n+1})$, and let $q_i=(p_{1,i},\ldots,p_{n+1,i})$ (hence $q_{n+1}=(0,\ldots,0)$ is the sequence of $n+1$ zeros). Consider the following four sequents.

$$\mathrm{LPHP}_n\vdash\textstyle\bigwedge_{i=1}^{n+1}\mathrm{th}_1^{n+1}(p_i)\tag{4}$$

$$\textstyle\bigwedge_{i=1}^{n+1}\mathrm{th}_1^{n+1}(p_i)\vdash\mathrm{th}_{n+1}^{(n+1)^2}(p_1,\ldots,p_{n+1})\tag{5}$$

$$\mathrm{th}_{n+1}^{(n+1)^2}(p_1,\ldots,p_{n+1})\vdash\mathrm{th}_{n+1}^{(n+1)^2}(q_1,\ldots,q_{n+1})\tag{6}$$

$$\mathrm{th}_{n+1}^{(n+1)^2}(q_1,\ldots,q_{n+1})\vdash\mathrm{RPHP}_n\tag{7}$$

In the next lemmas we show how to prove these sequents with quasipolynomial size MLK-proofs. A MLK-proof of $\mathrm{LPHP}_n\vdash\mathrm{RPHP}_n$ of size quasipolynomial in n will follow by four applications of the cut rule. □

Lemma 9 *Sequent 4 has* MLK*-proofs of size polynomial in* n*.*

Proof: For each $i\in\{1,\ldots,n+1\}$ derive the sequents $\bigvee_{j=1}^{n}(p_{i,j})\vdash\bigvee_{j=1}^{n}p_{i,j}\vee 0$ using right weakening and right $\vee$-introduction. Then, n right $\wedge$-introductions and n left $\wedge$-introductions give $\mathrm{LPHP}_n\vdash\bigwedge_{i=1}^{n+1}\mathrm{th}_1^{n}(p_i)$ by the definition of LPHP_n and a cut on part (i) of Lemma 6. The size of the whole proof is quadratic in n. □

Lemma 10 *Sequent 5 has* MLK*-proofs of size quasipolynomial in* n*.*

Proof: Recall that $n+1=2^r$. Let $N=(n+1)^2$. The idea of this proof is to succesively pack the conjuncts of the antecedent into a unique threshold formula, following a complete binary tree structure of height $\log_2(n+1)=r$. For every $w\in\{0,1\}^r$, let $p^w=p_{\overline{w}}$, where $\overline{w}$ is the position of w in the lexicographical order on $\{0,1\}^r$. Thus, $p^{0^r}=p_1$ and $p^{1^r}=p_{n+1}$. For every $w\in\{0,1\}^{<r}$, let $p^w=(p^{w0},p^{w1})$. Observe that $p^\lambda=(p_1,\ldots,p_{n+1})$. For each $t\in\{1,\ldots,r\}$, we exhibit a MLK-proof of

$$\bigwedge_{w\in\{0,1\}^t}\mathrm{th}^{N/2^t}_{(n+1)/2^t}(p^w)\vdash\bigwedge_{w\in\{0,1\}^{t-1}}\mathrm{th}^{N/2^{t-1}}_{(n+1)/2^{t-1}}(p^w) \tag{8}$$

of size quasipolynomial in n. Observe that for $t=r$, we are proving the sequent

$$\bigwedge_{i=1}^{n+1}\mathrm{th}^{n+1}_1(p_i)\vdash\bigwedge_{i=1}^{(n+1)/2}\mathrm{th}^{2(n+1)}_2(p_{2i-1},p_{2i}),$$

while for $t=1$, we are proving the sequent

$$\mathrm{th}^{(n+1)^2/2}_{(n+1)/2}(p_1,\ldots,p_{(n+1)/2})\wedge\mathrm{th}^{(n+1)^2/2}_{(n+1)/2}(p_{(n+1)/2+1},\ldots,p_{n+1})\vdash\mathrm{th}^{(n+1)^2}_{n+1}(p_1,\ldots,p_{n+1}).$$

Once we have all these proofs, we only have to cut sequentially to obtain the lemma. It remains to show how to obtain sequent 8. For a fixed $t\in\{1,\ldots,r\}$ and a fixed $w\in\{0,1\}^{t-1}$, an application of part (iii) of Lemma 2 gives

$$\mathrm{th}^{N/2^t}_{(n+1)/2^t}(p^{w0})\wedge\mathrm{th}^{N/2^t}_{(n+1)/2^t}(p^{w1})\vdash\mathrm{th}^{N/2^{t-1}}_{(n+1)/2^{t-1}}(p^w).$$

We put all these formulas in a unique conjunction using left and right $\wedge$-introduction to get sequent 8. The size of the proof is clearly quasipolynomial in n. $\Box$

Lemma 11 *Sequent 6 has* MLK*-proofs of size quasipolynomial in n.*

Proof: Immediate from Theorem 1 because $q_1,\ldots,q_{n+1}$ is a permutation of $p_1,\ldots,p_{n+1}$. $\Box$

Lemma 12 *Sequent 7 has* MLK*-proofs of size quasipolynomial in n.*

Proof: The idea of this proof is to unfold the threshold formula in the antecedent into disjunctions of threshold formulas computing the number of pigeons going into each hole. The unpacking process follows the structure of a complete binary tree of height $\log_2(n+1)=r$ in reverse order of that of Lemma 10. We use properties (ii) and (iii) of Lemma 7 to perform this process.

Recall that $n+1=2^r$. Let $N=(n+1)^2$. The first step of the unfolding process is given by property (iii) of Lemma 7:

$$\mathrm{th}^N_{n+1}(q_1,\ldots,q_{n+1})\vdash\mathrm{th}^{N/2}_{(n+1)/2+1}(q_1,\ldots,q_{(n+1)/2}),\ \mathrm{th}^{N/2}_{(n+1)/2}(q_{(n+1)/2+1},\ldots,q_{n+1}).$$

For the general case, define $q^w=q_{\overline{w}}$ for every $w\in\{0,1\}^r$, where $\overline{w}$ is defined as in the proof of Lemma 10. For every $w\in\{0,1\}^{<r}$, define $q^w=(q^{w0},q^{w1})$. Observe that $q^\lambda=(q_1,\ldots,q_{n+1})$. For every $t\in\{0,\ldots,r-1\}$ and $w\in\{0,1\}^t$, properties (iii) and (ii) of Lemma 7 give

$$\mathrm{th}^{N/2^t}_{(n+1)/2^t}(q^w)\vdash\mathrm{th}^{N/2^{t+1}}_{(n+1)/2^{t+1}+1}(q^{w0}),\ \mathrm{th}^{N/2^{t+1}}_{(n+1)/2^{t+1}}(q^{w1})$$
$$\mathrm{th}^{N/2^t}_{(n+1)/2^t+1}(q^w)\vdash\mathrm{th}^{N/2^{t+1}}_{(n+1)/2^{t+1}+1}(q^{w0}),\ \mathrm{th}^{N/2^{t+1}}_{(n+1)/2^{t+1}+1}(q^{w1}).$$

Appropriate cuts and the definition of q^w for $w \in \{0,1\}^r$ show then that

$$\mathrm{th}^N_{n+1}(q^\lambda) \vdash \mathrm{th}^{n+1}_2(q_0), \mathrm{th}^{n+1}_2(q_1), \ldots, \mathrm{th}^{n+1}_2(q_n), \mathrm{th}^{n+1}_1(q_{n+1}).$$

Since $q_{n+1} = (0, \ldots, 0)$, we immediately have that $\mathrm{th}^{n+1}_1(q_{n+1}) \vdash 0$ by part (ii) of Lemma 6, so that the result follows by a cut on $0 \vdash$, successive cuts on part (iv) of Lemma 6, and right $\vee$-introduction. The size of the proof is again quasipolynomial in n. $\Box$

5 Separation Results

A graph G is k-clique if there is a set of k nodes of G such that any two distinct nodes of the set are connected by an edge, and no other edge is present in G. A graph G is a k-coclique if there is a partition of the nodes of G into k disjoint sets in such a way that any two nodes that belong to different sets are connected by an edge, and no other edges are present in G.

The (n,k)-clique-coclique principle of [8] says that, given a set V of n nodes, if G is a k-clique over V and H is a $(k-1)$-coclique over V, then there is an edge in G that is not present in H. This principle may be stated as a monotone sequent CLIQUE^n_k as follows. For every $l \in \{1, \ldots, k\}$ and $i \in \{1, \ldots, n\}$, let $x_{l,i}$ be a propositional variable whose intended meaning is that i is the l-th largest node of the fully connected set which forms a fixed k-clique over $\{1, \ldots, n\}$. Similarly, for every $l \in \{1, \ldots, k-1\}$ and $i \in \{1, \ldots, n\}$, let $y_{l,i}$ be a propositional variable whose intended meaning is that the i-th node is in the l-th disjoint set of a fixed $(k-1)$-coclique over $\{1, \ldots, n\}$. The principle is then expressed as follows

$$\bigwedge_{l=1}^{k} \bigvee_{i=1}^{n} x_{l,i} \wedge \bigwedge_{i=1}^{n} \bigvee_{l'=1}^{k-1} y_{l',i} \vdash \bigvee_{t=1}^{k-1} \bigvee_{\substack{l,l'=1 \\ l \neq l'}}^{k} \bigvee_{\substack{i,j=1 \\ i \neq j}}^{n} (x_{l,i} \wedge x_{l',j} \wedge y_{t,i} \wedge y_{t,j}) \vee \bigvee_{\substack{l,l'=1 \\ l \neq l'}}^{k} \bigvee_{i=1}^{n} (x_{l,i} \wedge x_{l',i}).$$

Strictly speaking, this sequent expresses a principle slightly stronger than the principle above since the variables $y_{l,i}$ are not restricted to encode a one-to-one function. Let $\mathrm{LCLIQUE}^n_k$ be the left-hand side of this sequent and let $\mathrm{RCLIQUE}^n_k$ be its right-hand side.

We show how to reduce CLIQUE^n_k to PHP_{k-1} in the monotone sequent calculus. The reduction was first given in [8]; here we provide proofs of correctness for completeness. The strategy will be to show that the sequents

$$\mathrm{LCLIQUE}^n_k \vdash \mathrm{LPHP}'_{k-1} \tag{9}$$
$$\mathrm{RPHP}'_{k-1} \vdash \mathrm{RCLIQUE}^n_k \tag{10}$$

have MLK-proofs of size polynomial in n, where LPHP'_{k-1} and RPHP'_{k-1} are obtained from LPHP_{k-1} and RPHP_{k-1} respectively by replacing the variable $p_{l,l'}$ by the formula $\bigvee_{i=1}^n (x_{l,i} \wedge y_{l',i})$ for every $l \in \{1, \ldots, k\}$ and $l' \in \{1, \ldots, k-1\}$.

Lemma 13 *Sequent 9 has* MLK*-proofs of size polynomial in* n.

Proof: Consider the following sequence of sequents with easy MLK-proofs (the notation $A \vdash B \vdash C$ stands for the sequence $A \vdash B$, $B \vdash C$):

$$\bigwedge_{l=1}^{k} \bigvee_{i=1}^{n} x_{l,i} \wedge \bigwedge_{i=1}^{n} \bigvee_{l'=1}^{k-1} y_{l',i} \vdash \bigwedge_{l=1}^{k} \left(\bigvee_{i=1}^{n} x_{l,i} \wedge \bigwedge_{i=1}^{n} \bigvee_{l'=1}^{k-1} y_{l',i} \right) \vdash \bigwedge_{l=1}^{k} \bigvee_{i=1}^{n} \left(x_{l,i} \wedge \bigvee_{l'=1}^{k-1} y_{l',i} \right) \vdash$$

$$\vdash \bigwedge_{l=1}^{k}\bigvee_{i=1}^{n}\bigvee_{l'=1}^{k-1}(x_{l,i}\wedge y_{l',i}) \vdash \bigwedge_{l=1}^{k}\bigvee_{l'=1}^{k-1}\bigvee_{i=1}^{n}(x_{l,i}\wedge y_{l',i}).$$

The first derivation follows by left weakening, left $\wedge$-introduction, and commutativity; for the second derivation use distributivity and the derivable sequent $A \wedge B \vdash A$; for the third derivation use distributivity; and for the last derivation use commutativity. Finally observe that the first formula is $\mathrm{LCLIQUE}_k^n$ and the last formula is LPHP'_{k-1} (recall the substitution of $p_{l,l'}$ by $\bigvee_{i=1}^{n}(x_{l,i}\wedge y_{l',i})$). $\square$

Lemma 14 *Sequent 10 has* MLK*-proofs of size polynomial in n.*

Proof: Let us write down the full expression for RPHP'_{k-1}:

$$\bigvee_{t=1}^{k-1}\bigvee_{\substack{l,l'=1\\ l\neq l'}}^{k}\left[\bigvee_{i=1}^{n}(x_{l,i}\wedge y_{t,i})\wedge\bigvee_{j=1}^{n}(x_{l',j}\wedge y_{t,j})\right] \vdash \bigvee_{t=1}^{k-1}\bigvee_{\substack{l,l'=1\\ l\neq l'}}^{k}\bigvee_{i,j=1}^{n}(x_{l,i}\wedge y_{t,i}\wedge x_{l',j}\wedge y_{t,j}) \vdash$$

$$\vdash \left[\bigvee_{t=1}^{k-1}\bigvee_{\substack{l,l'=1\\ l\neq l'}}^{k}\bigvee_{\substack{i,j=1\\ i\neq j}}^{n}(x_{l,i}\wedge y_{t,i}\wedge x_{l',j}\wedge y_{t,j})\right]\vee\left[\bigvee_{t=1}^{k-1}\bigvee_{\substack{l,l'=1\\ l\neq l'}}^{k}\bigvee_{i=1}^{n}(x_{l,i}\wedge y_{t,i}\wedge x_{l',i}\wedge y_{t,i})\right] \vdash$$

$$\vdash \left[\bigvee_{t=1}^{k-1}\bigvee_{\substack{l,l'=1\\ l\neq l'}}^{k}\bigvee_{\substack{i,j=1\\ i\neq j}}^{n}(x_{l,i}\wedge y_{t,i}\wedge x_{l',j}\wedge y_{t,j})\right]\vee\left[\bigvee_{\substack{l,l'=1\\ l\neq l'}}^{k}\bigvee_{i=1}^{n}(x_{l,i}\wedge x_{l',i})\right].$$

The first derivation follows by distributivity, the second derivation follows by commutativity, and the third one follows by straightforward manipulation and the use of $A\wedge B\vdash A$. Observe that the last formula is simply $\mathrm{RCLIQUE}_k^n$, and the proof is complete. $\square$

Corollary 1 *The sequents* CLIQUE_k^n *with $k\leq n$ have* MLK*-proofs of size quasipolynomial in n.*

Putting together our upper bounds for PHP_n^{n+1} and for CLIQUE_k^n with the exponential lower bounds in Resolution [18] and in poly-CP [8], we obtain the following separations result:

Theorem 3 *Resolution, Bounded-Depth Frege and poly-CP are exponentially separated from the Monotone Gentzen Calculus.*

The Intuitionistic Gentzen Calculus forbids sequents with more than one formula in their consequent (see [30] for a precise definition). As observed by Pudlák [24], there is a simple simulation of the Monotone Gentzen Calculus by the Intuitionistic Gentzen Calculus. The simulation consists in replacing consequents with more than one formula by the disjunction of these formulas. This simple simulation implies that all our results also hold for the Intuitionistic Gentzen Calculus.

In [24], Pudlák proves that the Intuitionistic Gentzen Calculus enjoys a feasible interpolation property. It is also asked in [24] whether the feasible interpolation can be made monotone. While we have been able to provide a quasipolynomial upper bound for the size of intuitionisitic proofs of an encoding of the Clique Principle, it is not clear whether the encoding of the Clique Principle on which to apply the interpolation property (the one with common variables as in [21]) enjoys the same upper bound. The reason is that the resulting sequent is not monotone anymore, and our reduction method does not apply. On the other hand, a positive answer would imply that the disjointness property for the Intuitionistic Gentzen Calculus would belong to **P/poly − mP/poly**. In fact, the disjointness property would be computable by a (uniform) polynomial-size circuit (see [11] for a proof of this fact), but would not be computable by a monotone polynomial-size circuit, since otherwise, the Intuitionistc Gentzen Calculus would admit the monotone feasible interpolation property.

Acknowledgments The would like to thank the following people: Maria L. Bonet for helpful comments and insights; Pavel Pudlák fo reading a preliminary version, sending us interesting comments and pointing out the our proofs also holds for the tree-like case. Toni Pitassi has informed us that she obtained Theorem 2 independently. We thank her for reading a preliminary version of this paper.

References

[1] M. Ajtai. The complexity of the pigeonhole principle. *Combinatorica*, 14, pp. 417-433, 1994.

[2] M. Ajtai, J. Komlós, E. Szemerédi. An $O(n \log n)$ sorting network. *Combinatorica*, 3(1), pp. 1-19, 1983.

[3] N. Alon, R. B. Boppana. The monotone circuit complexity of boolean functions. *Combinatorica*, 7, pp. 1-22, 1987.

[4] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, P. Pudlák, A. Woods. Exponential lower bounds for the Pigeon Hole Principle. *Proc. of the 24-th STOC*, pp.200-220, 1992.

[5] P. Beame, T. Pitassi. Propositional Proof Complexity: Past, Present and Future. *Bulletin of the European Association for Theoretical Computer Science*, 65, 1998.

[6] P. Beame, T. Pitassi. Simplified and Improved Resolution Lower Bound. *Proc. of the FOCS'96*, pp. 274-282, 1996.

[7] M. Bonet, C. Domingo, R. Gavaldà, A. Maciel, T. Pitassi. Non-automatizability of Bounded-Depth Frege Proofs. *IEEE Conference on Computational Complexity*, 1998.

[8] M. Bonet, T. Pitassi, R. Raz. Lower Bounds for Cutting Planes Proofs with small Coefficients. *Journal of Symbolic Logic*, 62 (3), pp. 708-728, 1997. A preliminary version appeared STOC'95.

[9] S. R. Buss. Polynomial size proofs of the propositional pigeon hole principle. *Journal of Symbolic Logic*, 52 (4), pp. 916-927, 1987.

[10] S. Buss. Some remarks on length of proofs. *Archive for Mathematical Logic*, 34, pp. 377-394, 1995.

[11] S. Buss, G. Mints. The complexity of disjunction and existence properties in intuitionistc logic. Preprint, 1998.

[12] S. Buss, T. Pitassi. Resolution and the weak Pigeonhole principle. *Invited Talk to CSL 97. To appear in Selected Papers of the 11-th CSL*, Lecture Notes in Computer Science, 1998.

[13] S. R. Buss, G. Turan. Resolution proofs of generalized pigeonhole principles. *Theoretical Computer Science*, 62 (3), pp. 311-317, 1988.

[14] V. Chvátal E. Szemerédi. Many hard examples for resolution. *Journal of the Association for Computer Machinery*, 35, pp. 759-768, 1988.

[15] P. Clote, A. Setzer. On PHP, st-connectivity and odd charged graphs. *Proof Complexity and Feasible Arithmetics*, 93-118, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol 39, eds. Paul W. Beame and Samuel R. Buss, 1998.

[16] S. Cook, R. Reckhow. The relative efficiency of propositional proof systems. *Journal of Symbolic Logic*, 44, pp. 36-50, 1979.

[17] W. Cook, C. R. Coullard, G. Turán. On the complexity of Cutting Plane proofs. *Discrete Applied Mathematics*, 18, pp. 25-38, 1987.

[18] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39 (2-3), pp. 297-305, 1985.

[19] R. Impagliazzo, P. Pudlak, J. Sgall. Lower Bounds for the Polynomial Calculus and the Groebner basis Algorithm. ECCC TR97-042. To appear in *Computational Complexity.*

[20] J. Krajíček. Speed-up for propositional Frege systems via generalizations of proofs, *Commentationes Mathematicae Universiatatis Carolinae*,30, 1989, pp. 137-140.

[21] J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *Journal of Symbolic Logic*, 62, pp. 457-486, 1997.

[22] A. Maciel, T. Pitassi, and A. R. Woods. A New Proof of the Weak Pigeonhole Principle. To appear in STOC'00.

[23] J. B. Paris, A. J. Wilkie, and A. R. Woods. Provability of the pigeonhole principle and the existence of infinitely many primes. *Journal of Symbolic Logic*, 53 (4), pp. 1235-1244, 1988.

[24] P. Pudlák. On the complexity of the propositional Calculus. *Logic Colloquium '97.* To appear.

[25] P. Pudlák. Lower bounds for resolutions and cutting planes proofs and monotone computations. *Journal of Symbolic Logic*, 62 (2), pp. , 1997.

[26] P. Pudlák, S. Buss. How to lie without being (easily) convicted and the lengths of proofs in propositional calculus. *8th Workshop on CSL, Kazimierz, Poland, September 1994*, Springer Verlag LNCS n.995, pp. 151-162, 1995.

[27] A. Razborov. Lower bounds for the monotone complexity of some boolean functions. *Soviet Math. Doklady*, 31 (2), pp. 354-357, 1985.

[28] A. Razborov. Lower bounds for the Polynomial Calculus. *Computational Complexity*, 7 (4), pp. 291-324, 1998.

[29] A. A. Razborov, A. Wigderson, A. Yao. Read Once Branching Programs, Rectangular Proofs of the Pigeonhole Principle and the Transversal Calculus. *Proceedings of the 29-th STOC*, pp. 739-748, 4-6 May 1997.

[30] G. Takeuti. *Proof Theory.* North-Holland, second edition, 1987.

[31] A. Urquhart. Hard examples for Resolution. *Journal of the Association for Computing Machinery*, 34 (1), pp. 209-219, 1987.

[32] L. Valiant. Short monotone formulae for the majority function. *Journal of Algorithms*, 5, pp. 363-366, 1984.

[33] H. Vollmer. *Introduction to Circuit Complexity.* Springer, 1999.

[34] I. Wegener. *The Complexity of Boolean Functions.* J. Wiley and Sons, 1987.