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

September 18th, 2000

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 prove a size-depth trade-off upper bound for monotone proofs of the standard encoding of the PHP as a monotone sequent. At one extreme of the trade-off we get quasipolynomial-size monotone proofs, and at the other extreme we get subexponential-size bounded-depth monotone proofs. This result is a consequence of deriving the basic properties of certain monotone formulas computing the boolean threshold functions. We also consider the monotone sequent expressing the Clique-Coclique Principle (CLIQUE) 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 of our results, Resolution, Cutting Planes with polynomially bounded coefficients, and Bounded-Depth Frege are 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.

[*] Partially supported by the IST Programme of the EU under contract number IST-1999-14186 (ALCOM-FT), by FRESCO PB98-0937-C04-04 and by SGR CIRIT 1997SGR–00366.

[†] Supported by the CUR, Generalitat de Catalunya, through grant 1999FI 00532.

[‡] From September 2000 at Institute for Advanced Study. Olden Lane, Princeton 08450 New Jersey, USA. e-mail: galesi@ias.edu

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 [17] 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 admittedly far at present from proving that these systems are not polynomially bounded. Surprisingly, one of the main difficulties is that there are not very many tautologies candidate to be hard for these systems.

Nevertheless several important results have been obtained for less powerful but nontrivial proof systems. Strong lower bounds are actually known for systems such as Resolution [19, 14, 6, 36, 15], Bounded-Depth Frege [1, 7, 27, 24, 4] and Polynomial Calculus [32]. 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, whenever $m > n$. 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 [19]. This result was generalized to PHP^m_n, for m linear in n, by Buss and Turan [14]. 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 a subexponential lower bound by Beame et al. [7, 27, 24, 4]. The complexity of the PHP^m_n is also well-studied in algebraic-style propositional proof systems. Recently, Razborov [32] (see also [20]) showed that PHP^m_n is also hard for the Polynomial Calculus (notice that Riis [34] showed that a different encoding of PHP^{n+1}_n restricted to bijective maps has constant degree proofs in the Polynomial Calculus). Actually, the exact complexity of Resolution refutations of PHP^m_n, $\frac{}{\log n}$, remains an interesting open problem [6, 13, 33]. Thus, in spite of its simple intuitive meaning, PHP^{n+1}_n is one of the most fruitfully 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 [10], 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 [18], and that the slightly weaker form PHP^{2n}_n has quasipolynomial-size proofs in Bounded Depth Frege [26, 25].

Monotone proof systems, that is, proof systems restricted to propositional formulas over the monotone basis $\{\wedge, \vee\}$, were considered by Pudlák and Buss [30], and more recently, by Pudlák [28], and Clote and Setzer [16]. There are several alternative definitions of monotone proof systems. Here we consider the Monotone Gentzen Calculus, called *Geometric Logic* in [28]. Although the only monotone tautological formula is the true constant 1, Pudlák suggests the study of tautological sequents of the form $A \rightarrow B$, where A and B are boolean formulas built over the monotone basis $\{\wedge, \vee\}$. Several interesting combinatorial principles can be put in this form, among them PHP_n^{n+1}.

The correspondence 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 [11] 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 [31, 3], non-trivial lower bounds 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 [10] formalize a counting argument, and it is not clear how to formalize counting arguments into short monotone proofs. See the paper by Pudlák [28] for a further discussion on this topic (see also [16]).

In this work we exhibit a size-depth trade-off upper bound for monotone proofs of PHP_n^{n+1} in the Monotone Gentzen Calculus. At one extreme of the trade-off we get quasipolynomial-size monotone proofs of PHP_n^{n+1}. At the other extreme of the trade-off we get subexponential-size bounded-depth monotone proofs of PHP_n^{n+1}. This comes close to known lower bounds for bounded-depth Frege (or LK) of the pigeonhole principle [22], although the dependence on the depth parameter is still substantially different in upper and lower bounds.

In general, the trade-off may be expressed as follows: for every $s \leq n$, the PHP_n^{n+1} admits monotone proofs of size $n^{s \log_s(n)}$ and depth $2\log_s(n)$. The abovementioned extremes occur when $s = 2$ and $s = n^\epsilon$ respectively. To obtain this result, we consider explicit monotone formulas to compute the boolean threshold functions, that in the extreme cases mentioned above, have quasipolynomial-size in one case, and subexponential-size and bounded-depth in the other. While polynomial-size monotone formulas are known for these functions [37, 2], Pudlák remarks that it is not clear whether their basic properties have short monotone proofs. First, Valiant's construction [37] is probabilistic, and therefore, it does not provide any explicit formula to work with. Second, the sorting network of Ajtai, Komloś, and Szemerédi [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 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 monotone proofs within the specified trade-offs. 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 monotone proofs of the required size.

We remark that our proofs can be put in tree-like form, but the straightforward details are left to the interested reader. For non-monotone Gentzen Calculi, Krajíček [21] proved that tree-like proofs are as powerful as the unrestricted ones. It is not known at present, however, whether this holds for the monotone case since 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 exponential lower bound in Cutting Planes with polynomially bounded coefficients (poly-CP) was proved [9] (notice the difference with the Clique Principle with common variables introduced by Krajíček in [23], and used by Pudlák in [29] to obtain exponential lower bounds for Cutting Planes with unrestricted coefficients. The latter is not a monotone tautology of the form $A \to B$). We show that monotone proofs for the monotone sequent obtained from the formula CLIQUE^n_k can be reduced to monotone proofs of the *onto* version of PHP^k_{k-1}, which in turn can be easily reduced to the standard PHP^k_{k-1}. This way, we obtain quasipolynomial-size monotone proofs of CLIQUE^n_k

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 [28], 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.

2 Preliminaries

A *monotone formula* is a propositional formula without negations. The *Monotone Gentzen Calculus* (MLK), also called *Geometric Logic* [28], is obtained from the standard Gentzen Calculus (LK [35]) 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:

$$\overline{A \vdash A} \qquad \overline{0 \vdash \Gamma} \qquad \overline{\Gamma \vdash 1}$$

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 a premise in a rule of the proof, we say that the system is tree-like.

The *depth* of a formula is the maximum number of alternations between conjunctions and disjunctions. The *depth* of the proof is the maximum depth of a formula in it. The *size* of the proof is the overall number of *symbols* used in it. 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 $A(x_1/B_1, \ldots, x_n/B_n)$ 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 [8, 11] (monotonicity is only needed in part (v), and the proof is straightforward).

Lemma 1 *If A is a monotone formula, the sequents (i) $A, x \vdash A(x/1)$, (ii) $A \vdash x, A(x/0)$, (iii) $A(x/1), x \vdash A$, (iv) $A(x/0) \vdash x, A$, and (v) $A(x/0) \vdash A(x/1)$, have* MLK*-proofs of size quadratic in the size of A and the same depth as A.*

For every n and $k \in \{0, \ldots, n\}$, let $\mathrm{TH}^n_k : \{0,1\}^n \to \{0,1\}$ be the boolean function such that $\mathrm{TH}^n_k(a_1, \ldots, a_n) = 1$ if and only if $\sum_{i=1}^k a_i \geq k$, for every $(a_1, \ldots, a_n) \in \{0,1\}^n$. Each TH^n_k is called a threshold function. Valiant [37] proved that every threshold function TH^n_k is computable by a monotone formula of size polynomial in n. The proof is probabilistic, and so 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 [39], and in the more recent book by Vollmer [38]. Here we revisit that construction with a minor modification to achieve a size-depth trade-off.

Let s be a natural number. In the following, we use the notation $\bar{\imath}$ to denote a sequence $(i_1, \ldots, i_l)$. The length l of the sequence will be clear from context. Define $\mathrm{th}^1_{1,s}(x) := x$ and $\mathrm{th}^1_{0,s}(x) := 1$. For every exact power of s, say $n = s^r$, and for every $k \leq n$, we let $\mathrm{th}^n_{k,s}(x_1, \ldots, x_n)$ be the formula

$$\bigvee_{\bar{\imath} \in I^n_{k,s}} \bigwedge_{j=1}^{s} \mathrm{th}^{n/s}_{i_j,s}(x_{(j-1)n/s+1}, \ldots, x_{jn/s}),$$

where $I^n_{k,s} = \{(i_1, \ldots, i_s) \in \mathbb{N}^s : 0 \leq i_j \leq n/s, \sum_j i_j \geq k\}$. It is straightforward to prove that when n is an exact power of s, the formula $\mathrm{th}^n_{k,s}(x_1, \ldots, x_n)$ computes the boolean function TH^n_k. The depth of $\mathrm{th}^n_{k,s}(x_1, \ldots, x_n)$ is bounded by $2\log_s(n)$. Moreover, the maximum size of $\mathrm{th}^n_{k,s}(x_1, \ldots, x_n)$, say $S(n,s)$, satisfies the recurrence

$$S(n,s) \leq n^s S(n/s, s),$$

so we have $S(n,s) \leq n^{s \log_s(n)}$. Observe that when $s = 2$, the depth is bounded by $2\log_2(n)$ and the size is bounded by $n^{2\log_2(n)}$, and that when $s = n^{2/d}$ for a constant $d > 2$, the depth is bounded by d and the size is bounded $2^{n^{3/d}}$.

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 $\mathrm{th}^n_{k,s}(x_1, \ldots, x_n)$.

To simplify notation, in this and following sections we omit the the subscript s in proofs, as it is always the same.

The first properties are easy:

Lemma 2 *Let $s \in \mathbb{N}$ and let $n \in \mathbb{N}$ be an exact power of s. Let $i_1, \ldots, i_s \leq n/s$, let $k = \sum_{j=1}^{s} i_j$, and let $h, l \in \mathbb{N}$ with $n \geq h \geq l$. The sequents*

(i) $\vdash \mathrm{th}^n_{0,s}(x_1, \ldots, x_n)$,

(ii) $\mathrm{th}^n_{n,s}(x_1, \ldots, x_n) \vdash \bigwedge_{i=1}^{n} x_i$,

(iii) $\bigwedge_{j=1}^{s} \mathrm{th}^n_{i_j,s}(x_{(j-1)n/s+1}, \ldots, x_{jn/s}) \vdash \mathrm{th}^n_{k,s}(x_1, \ldots, x_n)$,

(iv) $\mathrm{th}^n_{h,s}(x_1, \ldots, x_n) \vdash \mathrm{th}^n_{l,s}(x_1, \ldots, x_n)$,

have MLK*-proofs of size polynomial in $n^{s \log_s(n)}$ and depth $2 \log_s(n)$.*

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 *Let $s \in \mathbb{N}$ and let $n \in \mathbb{N}$ be an exact power of s. Let $m, k, l \in \mathbb{N}$ with $0 < m \leq n$, $0 \leq k < n$, and $0 \leq l \leq n$. The sequents*

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

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

have MLK*-proofs of size polynomial in $n^{s \log_s(n)}$ and depth $2 \log_s(n)$.*

Proof: In the following, let $\overline{x}_j = (x_{(j-1)n/s+1}, \ldots, x_{jn/s})$ for every $j \in \{1, \ldots, s\}$, and let $\overline{x}'_j$ be the result of replacing x_l by 0 in $\overline{x}_j$. 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 $l \leq n/s$, that is, x_l is in the first block of variables $\overline{x}_1$. Recall the definition of $\mathrm{th}^n_{k+1}(x_1, \ldots, x_n)$:

$$\bigvee_{\overline{i} \in I^n_{k+1}} \bigwedge_{j=1}^{s} \mathrm{th}^{n/s}_{i_j}(\overline{x}_j).$$

Fix $(i_1, \ldots, i_s) \in I^n_{k+1}$. If $i_1 = 0$, then $\sum_{j=2}^{s} i_j \geq k+1$ so that $i_q > 0$ for some $q \in \{2, \ldots, s\}$. Then, $\mathrm{th}^{n/s}_{i_q}(\overline{x}_q) \vdash \mathrm{th}^{n/s}_{i_q-1}(\overline{x}_q)$ by part (iv) of Lemma 2. On the other hand, clearly $\mathrm{th}^{n/s}_{i_j}(\overline{x}_j) \vdash \mathrm{th}^{n/s}_{i_j}(\overline{x}_j)$ for every $j \in \{2, \ldots, s\} - \{q\}$. Moreover, we have $\vdash \mathrm{th}^{n/s}_0(\overline{x}'_1)$ by part (i) of Lemma 2. Note, by the way, that $\overline{x}'_j = \overline{x}_j$ for every $j \in \{2, \ldots, s\}$. Right $\wedge$-introduction, left weakening, and left $\wedge$-introduction gives then

$$\bigwedge_{j=1}^{s} \mathrm{th}^{n/s}_{i_j}(\overline{x}'_j) \vdash \mathrm{th}^{n/s}_0(\overline{x}'_1) \wedge \bigwedge_{2 \leq j < q} \mathrm{th}^{n/s}_{i_j}(\overline{x}'_j) \wedge \mathrm{th}^{n/s}_{i_q-1}(\overline{x}'_q) \wedge \bigwedge_{q < j \leq s} \mathrm{th}^{n/s}_{i_j}(\overline{x}'_j).$$

A cut with part (iii) of Lemma 2 gives $\bigwedge_{j=1}^{s} \mathrm{th}_{i_j}^{n/s}(\overline{x}'_j) \vdash \mathrm{th}_{t-1}^{n}(\overline{x}'_1, \ldots, \overline{x}'_s)$, where $t = \sum_{j=1}^{s} i_j$. Finally, since $t - 1 \geq k + 1 - 1 = k$, a cut with part (iv) of Lemma 2 gives the result.

If $i_1 > 0$, we use the induction hypothesis on n to get $\mathrm{th}_{i}^{n/s}(\overline{x}'_1) \vdash \mathrm{th}_{i-1}^{n/s}(\overline{x}'_1)$. Easy manipulation as before gives

$$\bigwedge_{j=1}^{s} \mathrm{th}_{i_j}^{n/s}(\overline{x}'_j) \vdash \mathrm{th}_{i_1-1}^{n/s}(\overline{x}'_1) \wedge \bigwedge_{2 \leq j \leq s} \mathrm{th}_{i_j}^{n/s}(\overline{x}'_j).$$

Finally an application of parts (iii) and (iv) of Lemma 2 gives the desired result. The proof of (ii) is very similar. □

Lemma 4 *Let $s \in \mathbb{N}$ and let $n \in \mathbb{N}$ be an exact power of s. Let $m, k, l \in \mathbb{N}$ with $1 \leq k < l \leq n$, and $m \leq n$, the sequents*

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

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

have MLK*-proofs of size polynomial in $n^{s \log_s(n)}$ and depth $2\log_s(n)$.*

Proof: We use the same notation as in the proof of Lemma 3. Both proofs are identical. It is enough to prove (i) when x_k and x_l fall in different blocks of variables. The complete proof of (i) would then be a simple induction on the recursive definition of $\mathrm{th}_{m}^{n}(x_1, \ldots, x_n)$ whose base case is when that happens. Notice that the base case is eventually reached, at latest, when $n = s$. So assume x_k and x_l fall in blocks a and b respectively. In the following, let $\overline{x}_a/1$ be the result of replacing x_k by 1 in $\overline{x}_a$, and define the notation $\overline{x}_a/0$, $\overline{x}_b/1$ and $\overline{x}_b/0$ analogously. Recall the definition of $\mathrm{th}_{m}^{n}(\overline{x}_1, \ldots, \overline{x}_s)$:

$$\bigvee_{\overline{i} \in I_m^n} \bigwedge_{j=1}^{s} \mathrm{th}_{i_j}^{n/s}(\overline{x}_j)$$

Fix $(i_1, \ldots, i_s) \in I_m^n$. If $i_a > 0$, then Lemma 3 shows that $\mathrm{th}_{i_a}^{n/s}(\overline{x}_a/1) \vdash \mathrm{th}_{i_a-1}^{n/s}(\overline{x}_a/0)$. Similarly, whenever $i_b < n/s$ we have $\mathrm{th}_{i_b}^{n/s}(\overline{x}_b/0) \vdash \mathrm{th}_{i_b+1}^{n/s}(\overline{x}_b/1)$. From these two sequents, the result follows easily when $i_a > 0$ and $i_b < n/s$. Consider next the case in which either $i_a = 0$ or $i_b = n/s$. If $i_b = n/s$, then $\mathrm{th}_{i_b}^{n/s}(\overline{x}_b/0)$ is just provably false by part (ii) of Lemma 2, and the result follows easily. If $i_a = 0$, then $\mathrm{th}_{i_a}^{n/s}(\overline{x}_{i_a}/1)$ is just provably true by part (i) of Lemma 2. On the other hand, $\mathrm{th}_{i_b}^{n/s}(\overline{x}_b/0) \vdash \mathrm{th}_{i_b}^{n/s}(\overline{x}_b/1)$ follows by part (v) of Lemma 1, and the result follows too. □

Lemma 5 *Let $s \in \mathbb{N}$ and let $n \in \mathbb{N}$ be an exact power of s. Let $m, i, j \in \mathbb{N}$, with $m \leq n$ and $1 \leq i < j \leq n$. The sequent*

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

has an MLK*-proof of size polynomial in $n^{s \log_s(n)}$ and depth $2\log_s(n)$.*

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) $\mathrm{th}^n_{m,s}(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n),x_i,x_j \vdash \mathrm{th}^n_{m,s}(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$,

(ii) $\mathrm{th}^n_{m,s}(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n),x_i \vdash x_j,\mathrm{th}^n_{m,s}(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$,

(iii) $\mathrm{th}^n_{m,s}(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n),x_j \vdash x_i,\mathrm{th}^n_{m,s}(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$,

(iv) $\mathrm{th}^n_{m,s}(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n) \vdash x_i,x_j,\mathrm{th}^n_{m,s}(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$.

We only show sequent (ii), the rest of sequents have similar proofs. Two applications of Lemma 1 give $\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n),x_i \vdash x_j,\mathrm{th}^n_m(x_1,\ldots,1,\ldots,0,\ldots,x_n)$. Lemma 4 gives $\mathrm{th}^n_m(x_1,\ldots,x_i,\ldots,x_j,\ldots,x_n),x_i \vdash x_j,\mathrm{th}^n_m(x_1,\ldots,0,\ldots,1,\ldots,x_n)$. Two more applications of Lemma 1 give $\mathrm{th}^n_m(x_1,\ldots,0,\ldots,1,\ldots,x_n),x_i \vdash x_j,\mathrm{th}^n_m(x_1,\ldots,x_j,\ldots,x_i,\ldots,x_n)$. Finally, a cut between the last two sequents gives (ii). □

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 *Let $s \in \mathbb{N}$ and let $n \in \mathbb{N}$ be an exact power of s. Let $m \in \mathbb{N}$, with $m \leq n$, and let π be a permutation over $\{1,\ldots,n\}$. The sequent $\mathrm{th}^n_{m,s}(x_1,\ldots,x_n) \vdash \mathrm{th}^n_{m,s}(x_{\pi(1)},\ldots,x_{\pi(n)})$ has an* MLK*-proof of size polynomial in $n^{s\log_s(n)}$ and depth $2\log_s(n)$.*

The next two properties state that the smallest threshold formulas are provably equivalent to their usual formulas. The proof is omitted.

Lemma 6 *Let $s \in \mathbb{N}$ and let $n \in \mathbb{N}$ be an exact power of s. The sequents*

(i) $\bigvee_i x_i \dashv\vdash \mathrm{th}^n_{1,s}(x_1,\ldots,x_n)$;

(ii) $\bigvee_{i\neq j}(x_i \wedge x_j) \dashv\vdash \mathrm{th}^n_{2,s}(x_1,\ldots,x_n)$;

have MLK*-proofs of size polynomial in $n^{s\log_s(n)}$ and depth $2\log_s(n)$.*

The next lemma states that threshold functions split by cases:

Lemma 7 *Let $s \in \mathbb{N}$ and let $n \in \mathbb{N}$ be an exact power of s. Let $m \in \mathbb{N}$ be an exact multiple of s with $m \leq n$. The sequents*

(i) $\mathrm{th}^n_{m+1,s}(x_1,\ldots,x_n) \vdash \mathrm{th}^{n/s}_{m/s+1,s}(\overline{x}_1),\ldots,\mathrm{th}^{n/s}_{m/s+1,s}(\overline{x}_s)$,

(ii) $\mathrm{th}^n_{m,s}(x_1,\ldots,x_n) \vdash \mathrm{th}^{n/s}_{m/s+1,s}(\overline{x}_1),\ldots,\mathrm{th}^{n/s}_{m/s+1,s}(\overline{x}_{s-1}),\mathrm{th}^{n/s}_{m/s,s}(\overline{x}_s)$,

where $\overline{x}_j = (x_{(j-1)n/s+1},\ldots,x_{jn/s})$, have MLK*-proofs of size polynomial in $n^{s\log_s(n)}$ and depth $2\log_s(n)$.*

Proof: We first prove (i). Fix $(i_1, \ldots, i_s) \in I^n_{m+1}$. Since m is an exact multiple of s, there must exist a $q \in \{1, \ldots, s\}$ such that $i_q \geq m/s + 1$ for otherwise $\sum_{j=1}^s i_j \leq m$. Then, $\mathrm{th}^{n/s}_{i_q}(\overline{x}_q) \vdash \mathrm{th}^{n/s}_{m/s+1}(\overline{x}_q)$ by part (iv) of Lemma 2. The sequent

$$\bigwedge_{j=1}^{s} \mathrm{th}^{n/s}_{i_j}(\overline{x}_j) \vdash \mathrm{th}^{n/s}_{m/s+1}(\overline{x}_1), \ldots, \mathrm{th}^{n/s}_{m/s+1}(\overline{x}_s)$$

follows by right weakening, left weakening, and left $\wedge$-introduction. Since this happens for every $\overline{i} \in I^n_{m+1}$, the result follows by left $\vee$-introduction. The proof of (ii) is extremely similar. Given $(i_1, \ldots, i_s) \in I^n_m$, either $i_q \geq m/s + 1$ for some $q \in \{1, \ldots, s-1\}$, or $i_s \geq m/s$ for otherwise $\sum_{j=1}^s i_j < m$. Manipulation as in part (i) gives property (ii). □

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

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

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 need a technical lemma saying that PHP_n can be reduced to the case in which n is an exact power of s.

Lemma 8 *There exists a polynomial $p(n)$ such that, for every $m, S \in \mathbb{N}$, if the sequent* PHP_m *has an* MLK*-proof of size at most S, then, for every $n \leq m$, the sequent* PHP_n *has an* 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 *Let $s\in\mathbb{N}$ and let $n\in\mathbb{N}$ be such that $s\le n$. The sequents PHP_n have* MLK*-proofs of size polynomial in $n^{s\log_s(n)}$ and depth $2\log_s(n)$.*

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 (in symbols, $\mathrm{th}_1^{n+1}(p_{i,1},\ldots,p_{i,n})$). We deduce that among all variables grouped by pigeons, at least $n+1$ are true (in symbols, $\mathrm{th}_{n+1}^{n(n+1)}(p_{1,1},\ldots,p_{1,n},\ldots,p_{n+1,1},\ldots,p_{n+1,n})$). The symmetry of the threshold allows us to show that the same holds when the variables are grouped by holes (in symbols, $\mathrm{th}_{n+1}^{n(n+1)}(p_{1,1},\ldots,p_{n+1,1},\ldots,p_{1,n},\ldots,p_{n+1,n})$). From this, at least one hole contains two pigeons (in symbols, $\mathrm{th}_2^{n+1}(p_{1,i},\ldots,p_{n+1,i})$ for some $i\in\{1,\ldots,n\}$), and this implies RPHP_n.

According to Lemma 8, we may assume that $n+1$ is an exact power of s since there always is such a number between n and sn. So let us assume that $n=s^r-1$ 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.

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

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

$$\mathrm{th}_{n+1}^{(n+1)^2}(p_1,\ldots,p_{n+1})\vdash\mathrm{th}_{n+1}^{(n+1)^2}(q_1,\ldots,q_{n+1})\tag{3}$$

$$\mathrm{th}_{n+1}^{(n+1)^2}(q_1,\ldots,q_{n+1})\vdash\mathrm{RPHP}_n\tag{4}$$

In the next lemmas we show how to prove these sequents in MLK. An MLK-proof of $\mathrm{LPHP}_n\vdash\mathrm{RPHP}_n$ will follow by three applications of the cut rule. □

Lemma 9 *Sequent (1) has* MLK*-proofs of size polynomial in $n^{s\log_s(n)}$ and depth $2\log_s(n)$.*

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 $\mathrm{LPHP}_n\vdash\bigwedge_{i=1}^{n+1}\mathrm{th}_1^{n+1}(p_i)$ by the definition of LPHP_n and cuts on part (i) of Lemma 6. □

Lemma 10 *Sequent (2) has* MLK*-proofs of size polynomial in $n^{s\log_s(n)}$ and depth $2\log_s(n)$.*

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

$$\bigwedge_{w \in \Sigma^t} \mathrm{th}^{N/s^t}_{(n+1)/s^t}(p^w) \vdash \bigwedge_{w \in \Sigma^{t-1}} \mathrm{th}^{N/s^{t-1}}_{(n+1)/s^{t-1}}(p^w). \tag{5}$$

Once we have all these proofs, we only have to cut sequentially to obtain the lemma. We prove sequent (5). For a fixed $t \in \{1, \ldots, r\}$ and a fixed $w \in \Sigma^{t-1}$, an application of part (iii) of Lemma 2 gives

$$\bigwedge_{i=0}^{s-1} \mathrm{th}^{N/s^t}_{(n+1)/s^t}(p^{wi}) \vdash \mathrm{th}^{N/s^{t-1}}_{(n+1)/s^{t-1}}(p^w).$$

We put all these formulas in a unique conjunction using $\wedge$-introduction to get sequent (5). □

Lemma 11 *Sequent (3) has* MLK*-proofs of size polynomial in* $n^{s \log_s(n)}$ *and depth* $2\log_s(n)$.

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

Lemma 12 *Sequent (4) has* MLK*-proofs of size polynomial in* $n^{s \log_s(n)}$ *and depth* $2\log_s(n)$.

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 s-ary tree of height $\log_s(n+1) = r$ in reverse order of that of Lemma 10. We use properties (i) and (ii) of Lemma 7 to perform this process.

Recall that $n+1 = s^r$. Let $N = (n+1)^2$. Let $\Sigma = \{0, \ldots, s-1\}$. Define $q^w = q_{\overline{w}}$ for every $w \in \Sigma^r$, where $\overline{w}$ is defined as in the proof of Lemma 10. For every $w \in \Sigma^{<r}$, define $q^w = (q^{w0}, \ldots, q^{w(s-1)})$. Observe that $q^\lambda = (q_1, \ldots, q_{n+1})$. For every $t \in \{0, \ldots, r-1\}$ and $w \in \Sigma^t$, properties (ii) and (i) of Lemma 7 give

$$\begin{gathered}
\mathrm{th}^{N/s^t}_{(n+1)/s^t}(q^w) \vdash \mathrm{th}^{N/s^{t+1}}_{(n+1)/s^{t+1}+1}(q^{w0}), \ldots, \mathrm{th}^{N/s^{t+1}}_{(n+1)/s^{t+1}+1}(q^{w(s-2)}), \mathrm{th}^{N/s^{t+1}}_{(n+1)/s^{t+1}}(q^{w(s-1)}) \\
\mathrm{th}^{N/s^t}_{(n+1)/s^t+1}(q^w) \vdash \mathrm{th}^{N/s^{t+1}}_{(n+1)/s^{t+1}+1}(q^{w0}), \ldots, \mathrm{th}^{N/s^{t+1}}_{(n+1)/s^{t+1}+1}(q^{w(s-1)}).
\end{gathered}$$

Appropriate cuts and the definition of q^w for $w \in \Sigma^r$ show then that

$$\mathrm{th}^{N}_{n+1}(q^\lambda) \vdash \mathrm{th}^{n+1}_2(q_1), \mathrm{th}^{n+1}_2(q_2), \ldots, \mathrm{th}^{n+1}_2(q_n), \mathrm{th}^{n+1}_1(q_{n+1}).$$

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

Setting $s = 2$ and $s = n^{2/d}$ in Theorem 2, we obtain the main results of this section.

Corollary 1 *The sequent* PHP_n *has* MLK*-proofs of size* $n^{O(\log n)}$.

Corollary 2 *The sequent* PHP_n *has depth-*d MLK*-proofs of size* $2^{O(n^{3/d})}$ *for every constant* $d > 2$.

Corollaries 1 and 2 obviously hold also for bounded-depth LK. The lower bound for the size of d-depth LK proofs of the pigeonhole principle is $\Omega(2^{n^{(1/6)^d}})$ [22]. Thus, the dependence on d is an exponential higher than in Corollary 2. This makes a noticeable difference: Corollary 2 implies that there are proofs of quasipolynomial size and depth $O(\log n / \log\log n)$; the lower bound implies only that proofs of quasipolynomial size must have depth $\Omega(\log\log n)$. It would be interesting to narrow this gap.

5 Separation Results

A graph G is a 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 [9] 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_k^n as follows. For every $l \in \{1,\ldots,k\}$ and $i \in \{1,\ldots,n\}$, let x_{li} 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_{li} 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

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

We show how to reduce CLIQUE_k^n to PHP_{k-1} in the monotone sequent calculus. The reduction was first given in [9]; here we provide proofs of correctness for completeness. The strategy will be to show that the sequents

$$\mathrm{LCLIQUE}_k^n \vdash \mathrm{LPHP}'_{k-1} \tag{6}$$
$$\mathrm{RPHP}'_{k-1} \vdash \mathrm{RCLIQUE}_k^n \tag{7}$$

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 $\bigvee_{i=1}^{n}(x_{li} \wedge y_{l'i})$ for every $l \in \{1,\ldots,k\}$ and $l' \in \{1,\ldots,k-1\}$.

Lemma 13 *Sequent (6) 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 $A \vdash B$, $B \vdash C$):

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

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 $\bigvee_{i=1}^{n}(x_{li} \wedge y_{l'i})$). □

Lemma 14 *Sequent (7) has* MLK-*proofs of size polynomial in* n.

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

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

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. □

Corollary 3 *The sequents* CLIQUE_k^n *have* MLK-*proofs of size* $n^{O(\log n)}$.

Putting together our upper bounds for PHP_n^{n+1} and for CLIQUE_k^n with the exponential lower bounds in Resolution [19], Bounded Depth Frege [1, 4], and poly-CP [9], 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 [35] for a precise definition). As observed by Pudlák [28], 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 [28], Pudlák proves that the Intuitionistic Gentzen Calculus enjoys a feasible interpolation property. It is also asked in [28] whether the feasible interpolation can be made monotone. While we have been able to provide a quasipolynomial upper bound for the size of intuitionistic proofs of an encoding of the Clique-Coclique 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 [23]) 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 [12] for a proof of this fact), but would not be computable by a monotone polynomial-size circuit, since otherwise, the Intuitionistic Gentzen Calculus would admit the monotone feasible interpolation property.

Acknowledgments We thank Maria L. Bonet for helpful comments and insights, Pavel Pudlák for comments on a preliminary version and pointing out that our proofs also holds for the tree-like case. Toni Pitassi has informed us that she obtained Corollary 1 independently. We thank her for reading a preliminary version of this paper. We also thank the anonymous ICALP'2000 referees for useful comments.

References

[1] M. Ajtai. The complexity of the pigeonhole principle. *Combinatorica* **14** (1994), 417–433.

[2] M. Ajtai, J. Komlós, E. Szemerédi. An $O(n \log n)$ sorting network. *Combinatorica* **3**(1) (1993), 1–19.

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

[4] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, P. Pudlák, A. Woods. Exponential lower bounds for the Pigeon Hole Principle. *Proc. 24th ACM Symp. on Theory of Computing* (1992), 200–220.

[5] P. Beame, T. Pitassi. Propositional Proof Complexity: Past, Present and Future. *Bulletin of the European Association for Theoretical Computer Science* **65** (1998), 66–89.

[6] P. Beame, T. Pitassi. Simplified and Improved Resolution Lower Bound. *Proc. 37th IEEE Annual Symposium on Foundations of Computer Science* (1996), 274–282.

[7] S. Bellantoni, T. Pitassi, A. Urquhart. Approximation and Small Depth Frege Proofs. *Siam Journal on Computing* **21**(6) (1992), 1161–1179.

[8] M. Bonet, C. Domingo, R. Gavaldà, A. Maciel, T. Pitassi. Non-automatizability of Bounded-Depth Frege Proofs. *Proc. 17th IEEE Conference on Computational Complexity* (1998), 15–23.

[9] M. Bonet, T. Pitassi, R. Raz. Lower Bounds for Cutting Planes Proofs with small Coefficients. *Journal of Symbolic Logic* **62**(3) (1997), 708–728.

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

[11] S. Buss. Some remarks on length of proofs. *Archive for Mathematical Logic* **34** (1995), 377–394.

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

[13] S. Buss, T. Pitassi. Resolution and the weak Pigeonhole principle. In: *Selected Papers of the 11th CSL*, Springer-Verlag Lecture Notes in Computer Science vol. 1414 (1998), 149–156.

[14] S. R. Buss, G. Turan. Resolution proofs of generalized pigeonhole principles. *Theoretical Computer Science* **62**(3) (1998), 311–317.

[15] V. Chvátal E. Szemerédi. Many hard examples for resolution. *Journal of the Association for Computer Machinery* **35** (1988), 759–768.

[16] 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.

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

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

[19] A. Haken. The intractability of resolution. *Theoretical Computer Science* **39** (1985), 297–305.

[20] R. Impagliazzo, P. Pudlak, J. Sgall. Lower Bounds for the Polynomial Calculus and the Groebner basis Algorithm. *Computational Complexity* **8**(2) (1999), 127–144.

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

[22] J. Krajíček. *Bounded Arithmetic, Propositional Logic and Complexity Theory.* Cambridge University Press, 1995.

[23] J. Krajíček. Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic. *Journal of Symbolic Logic* **62** (1997), 457–486.

[24] J. Krajíček, P. Pudlak, A. Woods. Exponential lower bound to the size of bounded depth Frege proofs of the pigeonhole principle. *Random Structures and Algorithms* **7/1** (1995), 15–39.

[25] A. Maciel, T. Pitassi, and A. R. Woods. A New Proof of the Weak Pigeonhole Principle. *Proc. 32th ACM Symp. on Theory of Computing* (2000), 368–377.

[26] 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) (1988), 1235–1244.

[27] T. Pitassi, P. Beame, R. Impagliazzo. Exponential Lower bounds for the Pigoenhole Principle. *Computational Complexity* **3**(2) (1993), 97–140.

[28] P. Pudlák. On the complexity of the propositional Calculus. *Sets and Proofs*, invited paper from *Logic Colloquium '97*. Cambridge University Press (1999), 197–218.

[29] P. Pudlák. Lower bounds for resolutions and cutting planes proofs and monotone computations. *Journal of Symbolic Logic* **62**(3) (1997), 981–998.

[30] 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 Lecture Notes in Computer Science 995 (1995), 151–162.

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

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

[33] A. A. Razborov, A. Wigderson, A. Yao. Read Once Branching Programs, Rectangular Proofs of the Pigeonhole Principle and the Transversal Calculus. *Proc. 29th ACM Symp. on Theory of Computing* (1997), 739–748.

[34] S. Riis. A Complexity Gap for Tree-Resolution. *BRICS Report Series, RS-99-29*, 1999.

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

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

[37] L. Valiant. Short monotone formulae for the majority function. *Journal of Algorithms* **5** (1984), 363–366.

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

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