Monotone Simulations of Nonmonotone Proofs

Albert Atserias[*]
Universitat Politècnica de Catalunya
Barcelona, Spain
atserias@lsi.upc.es

Nicola Galesi[†]
Universitat Politècnica de Catalunya
Barcelona, Spain
University of Toronto
Toronto, Canada (ON)
galesi@lsi.upc.es

Pavel Pudlák[‡]
Mathematical Institute AVČR
Prague, Czech Republic
pudlak@math.cas.cz

Abstract

We show that an LK proof of size m of a monotone sequent (a sequent that contains only formulas in the basis $\wedge, \vee$) can be turned into a proof containing only monotone formulas of size $m^{O(\log m)}$ and with the number of proof lines polynomial in m. Also we show that some interesting special cases, namely the functional and the onto versions of PHP and a version of the Matching Principle, have polynomial size monotone proofs. We prove that LK is polynomially bounded if and only if its monotone fragment is.

1 Introduction

The main subject of proof complexity is the study of the lengths of proofs in propositional calculus. The ultimate goal is to prove that in no proof system the lengths of proofs can be bounded by a polynomial, which would prove $NP \neq coNP$, cf. [6]. Similarly as in other areas of complexity theory, we are able to prove exponential lower bounds only for very restricted proof systems. The most known is the exponential lower bound for propositional Resolution [7]. Using a different method, the so called *feasible interpolation,* one can reduce proving a lower bound for Resolution to the well-known exponential lower bounds on monotone boolean circuits [9, 11]. Thus it is natural to look for more relations between monotone computations and propositional proof systems, in particular, to look for a proof system that would correspond to monotone boolean circuits. The most obvious idea is to restrict some proof systems that use all boolean formulas only to monotone formulas. Recall that a monotone formula is a formula in the basis $\{\vee, \wedge\}$. Since no monotone

[*] This work was done while the author was supported by the CUR, Generalitat de Catalunya, through grant 1999FI 00532. The work was also partially supported by ALCOM-FT, IST-99-14186.

[†] This work was done while the author was a member of the School of Mathematics of the Institute for Advanced Study (Princeton) supported by the NSF grant n. CCR-9987845. Partially supported by Spanish grant TIC2001-1577-C03-02 and by CSERC Canadian funds

[‡] This work was done while the author was a member of the Institute for Advanced Study, Princeton, supported by a grant of the State of New Jersey. Partially supported by grant A1019901 of the Academy of Sciences of the Czech Republic and by project LN00A056 of the Ministry of Education of the Czech Republic.

formula is a tautology, one cannot use to this end proof systems in which the proof steps consist of single formulas. In proof theory the most used system is the *sequent calculus* LK. In sequent calculus a proof line, called a *sequent*, consists of two sequences of formulas separated by $\vdash$. The meaning is that the conjunction of the first set implies the disjunction of the second set. Now the restriction to sequents that contain only monotone formulas is very natural. One can express almost all the studied tautologies as monotone sequents. Further motivation for this calculus is given by the fact that it can be viewed as an extension of resolution and as a subsystem of the intuitionistic propositional calculus (see [3]).

The study of the propositional monotone sequent calculus (MLK) was proposed in [12]. As there are monotone functions that can be computed by monotone circuits of exponential size only, while they can be computed by polynomial size circuits if negation is allowed [15], it was conjectured that a similar gap should be between proof systems that do not use negation and those that do. Contrary to this expectation we show that the gap is at most quasipolynomial. More precisely, a general proof of size m of a monotone sequent can be transformed into a monotone proof of size at most $m^{O(\log m)}$. Furthermore, if one counts only the number of proof lines, then our simulation is polynomial. Our proof uses an idea from circuit complexity, the so called *slice functions* (see [17]). These are monotone functions such that, for some k, the value of the function is 0 on all inputs with less than k ones and it is 1 on all inputs with more than k ones. For such functions their circuit complexity does not depend essentially on whether we use negations or not. While slice functions are very special monotone boolean functions, we apply the idea to arbitrary monotone sequents.

We also show that in some special cases the simulation is in fact polynomial. We consider two well-known variants of the pigeonhole principle (PHP). The Onto PHP (OPHP) states that there is no one-to-one correspondence from a set of $n+1$ elements *onto* a set of n elements. The Functional PHP (FPHP) states that there is no one-to-one *function* from a set of $n+1$ elements into a set of n elements (a correspondence differs from a function in that each element may have more than one image in the former, but not in the latter). All three principles PHP, OPHP, and FPHP, have been used, often interchangeably, in the literature. As a matter of fact, Cook and Reckhow considered the FPHP in their original paper. We show that for proofs of OPHP and FPHP the monotone simulation of LK proofs is polynomial. Thus, using a result of Buss [4] that (all versions of) PHP have polynomial proofs in the sequent calculus, we get also polynomial size monotone proofs of the two versions of PHP. Finally, we consider the monotone formulation of the Matching Principle that appears in [10] and get polynomial size monotone proofs as well.

Using our technique we derive the following interesting result: MLK is polynomially bounded if and only if LK is. Recall that a system is called polynomially bounded if there is a polynomial bound to the minimal proof of every tautology. Thus, our result says that proving that MLK is not polynomially bounded is as hard as the same for LK, and consequently as for any Frege system [6].

The paper is structured as follows. In Section 2 we define the sequent calculus LK and its monotone restriction MLK. In Section 3 we show that MLK quasipolynomially simulates LK on monotone sequents. Section 4 is devoted to show polynomial size MLK proofs for some restricted versions of the Pigeonhole Principle and the Matching principle. In Section 5 we prove that MLK is polynomially bounded if and only if LK is. In the last section we conclude with some open problems.

2 Monotone Calculus

All our propositional formulas are over the basis $\{0, 1, \wedge, \vee, \neg\}$. We will assume some familiarity with the propositional fragment of the Gentzen sequent calculus LK as defined, e.g., in the book by Takeuti [14]. By an abuse of notation we use LK for the propositional fragment, as we do not consider other than propositional proofs (this concerns also other notation). For completeness, we present the rules and axioms of LK. For formulas φ and ψ, and sequences of formulas Γ, Γ', Δ, and Δ':

Axioms:

$$\frac{}{\varphi \vdash \varphi} \qquad \frac{}{0 \vdash \Gamma} \qquad \frac{}{\Gamma \vdash 1}$$

Left Structural Rules

$$\frac{\Gamma, \varphi, \varphi, \Delta \vdash \Gamma'}{\Gamma, \varphi, \Delta \vdash \Gamma'} \qquad \frac{\Gamma, \varphi, \psi, \Delta \vdash \Gamma'}{\Gamma, \psi, \varphi, \Delta \vdash \Gamma'} \qquad \frac{\Gamma \vdash \Gamma'}{\varphi, \Gamma \vdash \Gamma'}$$

Right Structural Rules

$$\frac{\Gamma' \vdash \Gamma, \varphi, \varphi, \Delta}{\Gamma' \vdash \Gamma, \varphi, \Delta} \qquad \frac{\Gamma' \vdash \Gamma, \varphi, \psi, \Delta}{\Gamma' \vdash \Gamma, \psi, \varphi, \Delta} \qquad \frac{\Gamma' \vdash \Gamma}{\Gamma' \vdash \Gamma, \varphi}$$

Cut Rule

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

Left Logical Rules

$$\frac{\varphi, \psi, \Gamma \vdash \Delta}{(\varphi \wedge \psi), \Gamma \vdash \Delta} \qquad \frac{\varphi, \Gamma \vdash \Delta \quad \psi, \Gamma' \vdash \Delta'}{(\varphi \vee \psi), \Gamma, \Gamma' \vdash \Delta, \Delta'} \qquad \frac{\Gamma \vdash \varphi, \Delta}{\neg\varphi, \Gamma \vdash \Delta}$$

Right Logical Rules

$$\frac{\Gamma \vdash \Delta, \varphi, \psi}{\Gamma \vdash \Delta, (\varphi \vee \psi)} \qquad \frac{\Gamma \vdash \Delta, \varphi \quad \Gamma' \vdash \Delta', \psi}{\Gamma, \Gamma' \vdash \Delta, \Delta', (\varphi \wedge \psi)} \qquad \frac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$$

As usual, a proof in LK 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 LK 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 *size* of a formula φ, denoted by $|\varphi|$, is the overall number of *symbols* used in it. The *size* of the proof is the sum of the sizes of the formulas in it.

The Monotone Sequent Calculus (MLK) is the subsystem of LK in which all formulas are positive; that is, all formulas are over the monotone basis $\{\wedge, \vee\}$, thus the negation rules are prohibited. Note that there are no monotone formulas that are tautologies (except for the truth constant 1), so the concept of a monotone true statement makes sense only in the sequent calculus. On the other hand most of the studied tautologies can easily be presented as monotone sequents. A typical example is the Pigeonhole Principle which can be encoded as a monotone sequent in the following form:

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

3 Monotone simulation of LK

The key idea to prove that negations are powerless to compute k-slice boolean functions f_k is as follows. Prove that in a De Morgan circuit (a circuit over the basis $\{\wedge, \vee, \neg\}$ with all negations in front of the variables) we can replace every negated variable $\neg x_i$ by a polynomial size monotone circuit C_i, called the *pseudocomplement of x_i with respect to f_k*, which is equivalent to $\neg x_i$ on all inputs with exactly k ones (see [17]).

We use this idea to obtain MLK simulations of LK. First, we define a system, LK-De Morgan, in which negations are applied only to variables. Then, we show that in proving monotone sequents, LK-De Morgan efficiently simulates LK. Finally we prove that whenever we know how to replace negated variables by monotone formulas (the *pseudocomplements*), then LK-De Morgan proofs of monotone sequents can be easily transformed into MLK proofs (Theorem 1).

This last result will be then be used: (1) to give monotone simulations of LK by proving that we can always define quasipolynomial size pseudocomplement formulas for any negated variable (subsection 3.2), and (2) to give polynomial size MLK proofs of some specific classes of monotone tautologies for which we can improve the size of the pseudocomplements to a polynomial (Section 4).

3.1 De Morgan Sequent Calculus

We say that a formula is in De Morgan normal form if all the negations occur in front of the variables. For every formula φ, let $p(\varphi)$ be a formula in De Morgan normal form that is equivalent to φ. Observe that $p(\varphi)$ is uniformly obtained from φ by pushing the negations to the atoms according to the De Morgan rules. Observe that $p(\neg\neg\varphi) = p(\varphi)$, and that the size of $p(\varphi)$ is linear in the size of φ.

We define LK-De Morgan to be the subsystem of LK in which all formulas are in De Morgan normal form; that is, all formulas have the negations pushed down to the atoms, and the negation rules are only allowed over variables.

Lemma 1 *The sequents $\vdash p(\varphi), p(\neg\varphi)$ and $p(\varphi), p(\neg\varphi) \vdash$ have tree-like* LK*-De Morgan proofs of size $O(|\varphi|^2)$.*

Proof: The proof is by induction on the structure of φ. If φ is atomic, say x, then the sequents $\vdash x, \neg x$ and $x, \neg x \vdash$ are derivable in one step from the axiom $x \vdash x$. Suppose next that φ is of the form $\psi \wedge \theta$. By induction hypothesis, the sequents $\vdash p(\psi), p(\neg\psi)$ and $\vdash p(\theta), p(\neg\theta)$ have tree-like LK-De Morgan proofs of size quadratic in the sizes of ψ and θ respectively. By means of weakening we derive $\vdash p(\psi), p(\neg\psi), p(\neg\theta)$ and $\vdash p(\theta), p(\neg\psi), p(\neg\theta)$. Right $\wedge$-introduction followed by right $\vee$-introduction gives $\vdash p(\psi) \wedge p(\theta), p(\neg\psi) \vee p(\neg\theta)$. The size of the proof is clearly quadratic in the size of φ. The sequent $p(\psi) \wedge p(\theta), p(\neg\psi) \vee p(\neg\theta) \vdash$ is derived similarly. When φ is of the form $\psi \vee \theta$ reason dually. Finally, suppose that φ is of the form $\neg\psi$. By induction hypothesis, the sequent $\vdash p(\psi), p(\neg\psi)$ has a tree-like LK-De Morgan proof of size quadratic in the size of ψ. Since $p(\neg\neg\psi) = p(\psi)$, we immediately have a tree-like LK-De Morgan proof of $\vdash p(\neg\psi), p(\neg\neg\psi)$ of the same size. Reason similarly for the sequent $p(\neg\psi), p(\neg\neg\psi) \vdash$. □

Theorem 1 *Let Σ and Γ be sequences of formulas. If $\Sigma \vdash \Gamma$ has a tree-like* LK*-proof of size S, then $p(\Sigma) \vdash p(\Gamma)$ has a tree-like* LK*-De Morgan proof of size $O(S^2)$.*

Proof: Suppose that $\Sigma \vdash \Gamma$ has a tree-like LK-proof P of size S. By induction on P, for each sequent $\Sigma' \vdash \Gamma'$ in P we obtain an LK-De Morgan proof of $p(\Sigma') \vdash p(\Gamma')$. Observe that the only

LK rules that do not preserve the De Morgan restriction are the two negation rules. For each right $\neg$-introduction rule in P of the form

$$\frac{\Sigma', \varphi \vdash \Gamma'}{\Sigma' \vdash \neg\varphi, \Gamma',}$$

we simulate the inference

$$\frac{p(\Sigma'), p(\varphi) \vdash p(\Gamma')}{p(\Sigma') \vdash p(\neg\varphi), p(\Gamma')}$$

in the new proof by means of a cut with $\vdash p(\varphi), p(\neg\varphi)$, which can be derived in $O(|\varphi|^2)$ steps according to Lemma 1. Similarly, each left $\neg$-introduction rule in P is replaced by an inference involving a cut with $p(\varphi), p(\neg\varphi) \vdash$. The size of the new proof is clearly $O(S^2)$. □

Theorem 2 *Let Σ and Γ be sequences of monotone formulas with all variables within $x_1, \ldots, x_n$. Suppose that for every $i \in \{1, \ldots, n\}$ there exists a monotone formula φ_i such that the sequents $\Sigma \vdash x_i, \varphi_i, \Gamma$ and $\Sigma, \varphi_i, x_i \vdash \Gamma$ have tree-like* MLK*-proofs of size at most R. Then, if $\Sigma \vdash \Gamma$ has a tree-like* LK*-proof of size S, then it has a tree-like* MLK*-proof of size $O(S^2 + RS^2)$.*

Proof: Suppose that $\Sigma \vdash \Gamma$ has a tree-like LK-proof of size S. Since Σ and Γ are sequences of monotone formulas, we have that $p(\Sigma) = \Sigma$ and $p(\Gamma) = \Gamma$. Therefore, by Theorem 1, the sequent $\Sigma \vdash \Gamma$ has a tree-like LK-De Morgan proof P of size $O(S^2)$. Consider the following transformation on P. First, add Σ to the left of each sequent and Γ to the right of each sequent by weakening on the axioms. Then, replace each occurrence of $\neg x_i$ in P by φ_i. It remains to see how to simulate the rules of $\neg$-introduction. Consider such an application in P

$$\frac{\Sigma', x_i \vdash \Gamma'}{\Sigma' \vdash \neg x_i, \Gamma'.}$$

We need to simulate the inference

$$\frac{\Sigma, \Sigma', x_i \vdash \Gamma', \Gamma}{\Sigma, \Sigma' \vdash \varphi_i, \Gamma', \Gamma.}$$

This is straightforward: derive $\Sigma \vdash x_i, \varphi_i, \Gamma$, cut on x_i, and apply some structural rules. The simulation of a left $\neg$-introduction rule is symmetrical by means of a cut with $\Sigma, \varphi_i, x_i \vdash \Gamma$. The size of the new proof is clearly $O(S^2 + RS^2)$. □

3.2 Using Threshold Formulas to Simulate LK

Recall the following definitions from [2].

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.

The threshold functions are central in the monotone simulation of non monotone circuits computing slice functions. First they can be computed by polynomial size monotone circuits (see [16]). Moreover it is possible to show (see [17]) that $\mathrm{TH}^{n-1}_k(a_1, \ldots a_{i-1}, a_{i+1}, \ldots, a_n)$ is the pseudocomplement of x_i with respect to computations of the k-slice function over n variables.

We follow a similar approach to prove a monotone simulation of non monotone proofs. Consider the definition of monotone threshold formulas: $\mathrm{th}^1_0(x) := 1$, $\mathrm{th}^1_1(x) := x$, $\mathrm{th}^1_k(x) := 0$ for every $k > 1$, and for every $n > 1$ and $k \geq 0$, define the formula

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

where $I_k^n = \{(i,j) : 0 \le i \le n/2,\ 0 \le j \le n - n/2,\ i+j \ge k\}$ and $n/2$ is an abbreviation for $\lfloor n/2 \rfloor$. It is straightforward to prove that $\mathrm{th}_k^n(x_1,\ldots,x_n)$ computes the boolean function TH_k^n. On the other hand, it is easy to prove, by induction on n, that the size of $\mathrm{th}_k^n(x_1,\ldots,x_n)$ is bounded by $n^{O(\log n)}$.

We use the threshold formulas to define the pseudocomplement formulas in the sequent calculus in a way similar to the circuits simulation. The main property we prove (see Lemma 5) says that, when exactly k among all the variables are true, the formula $\mathrm{th}_k^n(x_1,\ldots,x_i/0,\ldots,x_n)$ is the pseudocomplement of x_i. Since we prove this property for each $k = 1,\ldots,n$, it follows that we can always replace a negated variable by a monotone formula.

We start by giving some preliminary properties of the threshold formulas. Recall that if φ and ψ are formulas and x is a variable, the notation $\varphi(x/\psi)$ stands for the formula that results of replacing every occurrence of x (if any) in φ by ψ.

Lemma 2 **([2])** *If φ is a monotone formula, the sequents (i) $\varphi \vdash x, \varphi(x/0)$, (ii) $\varphi(x/1), x \vdash \varphi$ have tree-like* MLK*-proofs of size $O(|\varphi|^2)$.*

Lemma 3 **([2])** *For every n, m, and l with $0 < m \le n$ and $0 \le l \le n$, the sequent*

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

has tree-like MLK*-proofs with $n^{O(1)}$ lines and size $n^{O(\log n)}$.*

The polynomial bound on the number of proof lines is not stated explicitly in [2], but an easy inspection of the proof gives it. The next lemma easily follows from the definitions of the threshold formulas.

Lemma 4 *For every n and k with $k > n$, the sequents*

(i) $\mathrm{th}_k^n(x_1,\ldots,x_n) \vdash$*, and*

(ii) $\vdash \mathrm{th}_0^n(x_1,\ldots,x_n)$

have tree-like MLK *proofs with $n^{O(1)}$ lines and size $n^{O(\log n)}$.*

For k and i with $0 \le k \le n$ and $1 \le i \le n$, the k-pseudocomplement of x_i is, by definition, the monotone formula $\mathrm{th}_k^n(x_1,\ldots,x_i/0,\ldots,x_n)$. The next Lemma guarantees that the hypothesis of Theorem 2 hold for any of the k-pseudocomplement formulas and any monotone sequent $\Sigma \vdash \Gamma$ with variables within $x_1,\ldots,x_n$ such that Σ contains $\mathrm{th}_k^n(x_1,\ldots,x_n)$ and Γ contains $\mathrm{th}_{k+1}^n(x_1,\ldots,x_n)$.

Lemma 5 *For every k and i with $0 \le k \le n$ and $1 \le i \le n$ the sequents:*

(i) $\mathrm{th}_k^n(x_1,\ldots,x_n) \vdash \mathrm{th}_{k+1}^n(x_1,\ldots,x_n), \mathrm{th}_k^n(x_1,\ldots,x_i/0,\ldots,x_n), x_i$

(ii) $x_i, \mathrm{th}_k^n(x_1,\ldots,x_i/0,\ldots,x_n), \mathrm{th}_k^n(x_1,\ldots,x_n) \vdash \mathrm{th}_{k+1}^n(x_1,\ldots,x_n)$

have tree-like MLK*-proofs with $n^{O(1)}$ lines and size $n^{O(\log n)}$.*

Proof: The first sequent follows from right weakening on Lemma 2 (i). For the second, from Lemma 2 (ii) we have $x_i, \mathrm{th}_{k+1}^n(x_1,\ldots,x_i/1,\ldots,x_n) \vdash \mathrm{th}_{k+1}^n(x_1,\ldots,x_n)$. Moreover, Lemma 3 gives $\mathrm{th}_k^n(x_1,\ldots,x_i/0,\ldots,x_n) \vdash \mathrm{th}_{k+1}^n(x_1,\ldots,x_i/1,\ldots,x_n)$. The sequent in (ii) is obtained by cutting and then adding $\mathrm{th}_k^n(x_1,\ldots,x_n)$ by left weakening. □

Theorem 3 *Let $\Sigma \vdash \Gamma$ be a monotone sequent with n variables. If $\Sigma \vdash \Gamma$ has an* LK*-proof of size S, then $\Sigma \vdash \Gamma$ has a tree-like* MLK*-proof with $S^{O(1)}$ lines and size $S^{O(1)} \cdot n^{O(\log n)}$.*

Proof: By Theorem 2 and the well known result that tree-like LK polynomially simulates LK [8], it will be sufficient to simulate tree-like LK-De Morgan proofs by tree-like MLK proofs. Let P be a tree-like LK-De Morgan proof of $\Sigma \vdash \Gamma$ of size S. By the previous lemma and Theorem 2, for each $k \in \{0, \dots, n\}$ we obtain tree-like MLK proofs of the sequents $\mathrm{th}_k^n(x_1, \dots, x_n), \Sigma \vdash \Gamma, \mathrm{th}_{k+1}^n(x_1, \dots, x_n)$ each one with $S^{O(1)}$ lines and size $S^{O(1)} \cdot n^{O(\log n)}$. Finally, n consecutive cuts give us a proof of the sequent $\mathrm{th}_0^n(x_1, \dots, x_n), \Sigma \vdash \Gamma, \mathrm{th}_{n+1}^n(x_1, \dots, x_n)$ from which we obtain the theorem using Lemma 4. □

Corollary 1 *Tree-like* MLK *quasipolynomially simulates* LK *on monotone sequents. In particular, tree-like* MLK *quasipolynomially simulates* MLK.

Notice that the proof of Theorem 3 shows that the number of lines of the resulting MLK proof is polynomial in n and the number of lines of the original LK proof. This observation reveals that any proof of a superpolynomial gap between LK and MLK, if any, should focus on size and not on the number of lines.

Finally, since every MLK-proof can be polynomially simulated by a proof in the intuitionistic calculus JK (see [3]) we get the following.

Corollary 2 *The intuitionistic calculus* JK *quasipolynomially simulates* LK *on monotone sequents.*

Note, however, that this is unlikely for intuitionistically valid *nonmonotone* sequents, see [5].

4 Pigeonhole and Matching Principles

The *Pigeonhole Principle* states that if $n+1$ pigeons go into n holes, then there is some hole with more than one pigeon sitting in it. Recall its definition as a monotone sequent in Section 2. We consider two well-known variants of this principle. The Onto PHP, denoted OPHP, requires the mapping to be onto the set of holes. The Functional PHP, denoted FPHP, requires the mapping to send every pigeon to exactly one hole. Their propositional formulations as monotone sequents are as follows:

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

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

Using Corollary 1 and Buss' polynomial size LK proofs of the PHP_n^{n+1} we give another proof of the main result of [2].

Theorem 4 ([2]) PHP_n^{n+1} *has* MLK*-proofs of size quasipolynomial in n.*

We can improve this result showing that the principles OPHP, FPHP and a Perfect Matching Principle PM that we introduce later admit polynomial size MLK-proofs.

Theorem 5 FPHP_n^{n+1} *and* OPHP_n^{n+1} *have tree-like* MLK*-proofs of size polynomial in n.*

Proof: Buss proved that PHP_n^{n+1} has a Frege proof of size polynomial in n, and therefore, so do FPHP_n^{n+1} and OPHP_n^{n+1}. Since tree-like LK polynomially simulates any Frege system [8], they also have polynomial-size tree-like LK-proofs. We first consider FPHP_n^{n+1}. For every $i \in \{1, \ldots, n+1\}$ and $j \in \{1, \ldots, n\}$, let φ_{ij} be the formula $\bigvee_{j' \neq j} p_{i,j'}$ where j' ranges over $\{1, \ldots, n\}$. Let LFPHP be the left hand side of the sequent FPHP_n^{n+1}, and let RFPHP be the right hand side of the sequent FPHP_n^{n+1}. We claim that the sequents

$$\mathrm{LFPHP} \vdash p_{i,j}, \varphi_{ij}, \mathrm{RFPHP} \tag{1}$$

$$\mathrm{LFPHP}, \varphi_{ij}, p_{i,j} \vdash \mathrm{RFPHP} \tag{2}$$

have tree-like MLK-proofs of size polynomial in n. The result will follow for FPHP_n^{n+1} by Theorem 2. For sequent (1) reason as follows. For every $j' \in \{1, \ldots, n\}$, we have $p_{i,j'} \vdash p_{i,1}, \ldots, p_{i,n}, \mathrm{RFPHP}$ by right weakening on the axiom $p_{i,j'} \vdash p_{i,j'}$ and structural rules. By left $\vee$-introduction we get $\bigvee_{j=1}^n p_{i,j} \vdash p_{i,1}, \ldots, p_{i,n}, \mathrm{RFPHP}$. Left weakening and left $\wedge$-introduction gives $\mathrm{LFPHP} \vdash p_{i,1}, \ldots, p_{i,n}, \mathrm{RFPHP}$. Finally, some structural rules and right $\vee$-introduction give sequent (1). For sequent (2) reason as follows. For every $j, j' \in \{1, \ldots, n+1\}$ such that $j \neq j'$, we have $p_{i,j}, p_{i,j'} \vdash p_{i,j} \wedge p_{i,j'}$ easily. Left weakening, right weakening and right $\vee$-introduction gives $\mathrm{LFPHP}, p_{i,j}, p_{i,j'} \vdash \mathrm{RFPHP}$. Finally, left $\vee$-introduction for every $j' \neq j$ gives sequent (2). As regards OPHP_n^{n+1}, one simply needs define φ_{ij} as $\bigvee_{i' \neq i} p_{i',j}$ where i' ranges over $\{1, \ldots, n+1\}$, and reason analogously. □

Let us be given a graph $G = (V, E)$ on $n = 3m$ nodes. We consider the following matching principle PM_n formulated in [10]. If X is a set of m edges forming a perfect matching in G and Y is an $m-1$ subset of V, then there is some edge $(u, v) \in X$ such that neither u nor v are in V. To encode this principle as a monotone sequent we use variables $x_{i,k}$ for $i \in [m]$ and $k \in [3m]$ whose intended meaning is that the node k is in the i-th edge of the matching, and variables $\neg y_{i,k}$ for $i \in [m-1]$ and $k \in [3m]$ whose intended meaning is that the node k is the i-th element in Y. We will encode the fact that there is a perfect matching on m edges in G by an $m \times 3m$ matrix such that in each row there are exactly two 1's and in each column there is at most one 1. Notice that our formula has depth 3.

$$X(1) := \bigwedge_{i \in [m]} \bigvee_{k,k' \in [3m], k \neq k'} (x_{i,k} \wedge x_{i,k'})$$

$$X(2) := \bigwedge_{i \in [m]} \bigwedge_{k,l,h \in [3m], k \neq l \neq h \neq k} (\neg x_{i,k} \vee \neg x_{i,l} \vee \neg x_{i,h})$$

$$X(3) := \bigwedge_{i,i' \in [m], i \neq i'} \bigwedge_{k \in [3m]} (\neg x_{i,k} \vee \neg x_{i',k})$$

Similarly, we will encode that Y is an $m-1$ subset of V, by an $(m-1) \times 3m$ matrix in which for each row there is exactly one 0 and in each column there is at most one 0 (recall that the presence of a node in Y is indicated by a negated variable).

$$Y(1) := \bigwedge_{i,i' \in [m-1], i \neq i'} \bigwedge_{k \in [3m]} (y_{i,k} \vee y_{i',k})$$

$$Y(2) := \bigwedge_{i, \in [m-1]} \bigwedge_{k,k' \in [3m], k \neq k'} (y_{i,k} \vee y_{i,k'})$$

$$Y(3) := \bigwedge_{i \in [m-1]} \bigvee_{k \in [3m]} \neg y_{i,k}$$

The last formula that we introduce means that there is an edge such that neither of its endpoints is in Y.

$$XY := \bigvee_{i\in[m]} \bigvee_{k,k'\in[3m],k\neq k'} (x_{i,k} \wedge x_{i,k'} \bigwedge_{i\in[m-1]} y_{i,k} \bigwedge_{i\in[m-1]} y_{i,k'})$$

Then the PM_{3m} principle is expressed by the following sequent:

$$(1) \quad X(1), X(2), X(3), Y(1), Y(2), Y(3) \vdash XY$$

It is easy to see that this sequent can be transformed in a monotone sequent. Consider the formulas $X(i)^{\perp} := \neg X(i)$ for $i = 2, 3$, and $Y(3)^{\perp} := \neg Y(3)$. Then (1) is equivalent to the monotone sequent

$$X(1), Y(1), Y(2) \vdash X(2)^{\perp}, X(3)^{\perp}, Y(3)^{\perp}, XY$$

Notice that, as observed in [10], PM_{3m} can be reduced to OPHP^{m}_{m-1}. However we need to define the PHP variables $p_{i,j}$ as $p_{i,j} := \bigvee_{k\in[3m]}(x_{i,k} \wedge \neg y_{j,k})$ which is not a monotone formula. Therefore the reduction cannot be proved in MLK. In any case, we can get polynomial size MLK proofs for PM_{3m} principle directly.

Theorem 6 PM_n *has tree-like* MLK*-proofs of size polynomial in* n.

Proof: The proof follows the same lines of the previous Theorem given that [10] gave polynomial size LK proofs for PM_n. Define for each $i \in [m]$ and for each $k \in [3m]$ the pseudocomplement formula $\varphi^{x}_{i,k}$ for $x_{i,k}$ as:

$$\varphi^{x}_{i,k} := \bigvee_{k',k''\in[3m],k'\neq k'',\, k',k''\neq k} (x_{i,k'} \wedge x_{i,k''})$$

For each $i \in [m-1]$ and for each $k \in [3m]$ define the pseudocomplement formula $\varphi^{y}_{i,k}$ for $y_{i,k}$ as

$$\varphi^{y}_{i,k} := \bigwedge_{k'\in[3m],k'\neq k} y_{i,k'}$$

We prove that for each $i \in [m]$, for each $j \in [m-1]$ for each $k \in [3m]$ the following sequents have polynomial size tree-like MLK proofs:

(1) $X(1), x_{i,k}, \varphi^{x}_{i,k} \vdash X(2)^{\perp}, X(3)^{\perp}$
(2) $X(1) \vdash x_{i,k}, \varphi^{x}_{i,k}, X(2)^{\perp}, X(3)^{\perp}$
(3) $Y(1), Y(2), y_{j,k}, \varphi^{y}_{j,k} \vdash Y(3)^{\perp}$
(4) $Y(1), Y(2) \vdash y_{j,k}, \varphi^{y}_{j,k}, Y(3)^{\perp}$

The theorem then follows by the same argument used in the previous Theorem. We prove sequents (1) and (2). Sequents (3) and (4) follow by an argument similar to that of FPHP. Observe that $X(2)^{\perp}, X(3)^{\perp}$ are the following formulas

$$X(2)^{\perp} := \bigvee_{i\in[m]} \bigvee_{k,l,h\in[3m],k\neq l\neq h\neq k} (x_{i,k} \wedge x_{i,l} \wedge x_{i,h})$$

$$X(3)^{\perp} := \bigvee_{i,i'\in[m] i\neq i'} \bigvee_{k\in[3m]} (x_{i,k} \wedge x_{i',k})$$

For sequent (1) reason as follows: for each $k' \neq k$ we have proofs of the sequents $x_{i,k} \wedge x_{i,k'} \vdash x_{i,k}$. By left $\vee$-introduction on all the previous proofs, we can derive $\bigvee_{k' \in [3m],\, k' \neq k}(x_{i,k} \wedge x_{i,k'}) \vdash x_{i,k}$. From this, by right weakening we have

$$(5) \qquad \bigvee_{k' \in [3m]\ ,k' \neq k} (x_{i,k} \wedge x_{i,k'}) \vdash x_{i,k}, \varphi^x_{i,k}$$

For each $k' \neq k'' \in [3m]$, with $k', k'' \neq k$ we can derive $x_{i,k'} \wedge x_{i,k''} \vdash x_{i,k'} \wedge x_{i,k''}$. From this, by right weakenings, we can derive $x_{i,k'} \wedge x_{i,k''} \vdash x_{i,k}, \varphi^x_{i,k}$. By left $\vee$-introductions on these proofs we obtain

$$(6) \qquad \bigvee_{k',k'' \in [3m]\ k',k'' \neq k} (x_{i,k'} \wedge x_{i,k''}) \vdash x_{i,k}, \varphi^x_{i,k}$$

Finally by left $\vee$-introduction between (5) and (6), left weakening, and left $\wedge$-introduction we obtain $X(1) \vdash x_{i,k}, \varphi^x_{i,k}$, from which (1) follows by right weakenings.

For sequent (2) reason as follows: for each $k' \neq k'' \in [3m]$, $k', k'' \neq k$, we have proofs of the sequents $x_{i,k}, (x_{i,k'} \wedge x_{i,k''}) \vdash (x_{i,k} \wedge x_{i,k'} \wedge x_{i,k''})$. By weakenings and right $\vee$-introduction we obtain $x_{i,k}, (x_{i,k'} \wedge x_{i,k''}) \vdash X(3)^{\perp}$. By right $\vee$-introductions on all previous proofs we have $x_{i,k}, \varphi^x_{i,k} \vdash X(3)^{\perp}$ from which the sequent (2) follows by two weakenings, left and right. □

5 MLK is polynomially bounded if and only if LK is.

In this section we prove the above statement. The main part of the proof is the following lemma.

Lemma 6 *Let $\tau^n_k(x_1, \ldots, x_n)$ be polynomial-size monotone formulas for* TH^n_k. *If the sequents of Lemmas 4 and 5 have polynomial-size* LK*-proofs with $\tau^n_k(x_1, \ldots, x_n)$ instead of $\mathrm{th}^n_k(x_1, \ldots, x_n)$, then* MLK *polynomially simulates* LK *on monotone sequents.*

Proof: Let $p(n)$ be a bound on the size of $\tau^n_k(x_1, \ldots, x_n)$. Suppose we have LK-proofs of all the sequents in Lemmas 4 and 5 in a single proof of size at most $q(n)$. These $2(n+1)n+2$ sequents are called the *pseudocomplement properties.* We prove, by induction on n, that all $2(n+1)n+2$ pseudocomplement properties of $\tau^n_k(x_1, \ldots, x_n)$ can be obtained in a single MLK-proof of polynomial-size. This will be enough since then we can apply the same argument as in Theorem 3 with $\tau^n_k(x_1, \ldots, x_n)$ instead of $\mathrm{th}^n_k(x_1, \ldots, x_n)$.

We will obtain a recurrence $s(n)$ for the size of the MLK-proofs of the pseudocomplement properties of τ^n_k. For $n = 1$, the proofs are just constant size and $s(n) = O(1)$. Suppose $n > 1$ next. Define auxiliary formulas as follows. Let $\sigma^n_0 = 1$, $\sigma^n_n = \bigwedge^n_{i=1} x_i$, and for every $i \in \{1, \ldots, n-1\}$, let σ^n_i be the formula

$$\tau^{n-1}_i(x_1, \ldots, x_{n-1}) \vee (\tau^{n-1}_{i-1}(x_1, \ldots, x_{n-1}) \wedge x_n).$$

Observe that the size of σ^n_k is bounded by $2p(n-1)+3$. It is easy to get MLK-proofs of the sequents of the pseudocomplement properties for σ^n_i from those of τ^{n-1}_i. The size of these proofs is at most $l(n)$ for some polynomial $l(n)$. With these, we use the argument of Theorem 3 with $\sigma^n_0, \ldots, \sigma^n_n$ as threshold formulas to turn the LK-proofs of the properties of τ^n_i into MLK-proofs of size $q(n) + 2q(n)(2p(n-1)+3) + s(n-1) + l(n)$. To see this bound on the size, observe that the proof is built as follows. For each $k \in \{0, \ldots, n\}$, take the LK-De Morgan proofs of the $2(n+1)n+2$ properties for τ^n_i and add σ^n_k to the left and σ^n_{k+1} to the right by weakening. This gives size $q(n) + 2q(n)(2p(n-1)+3)$. Then replace each negated variable $\neg x_i$ by $\sigma^n_k(x_i/0)$. This gives $q(n)(2p(n-1)+3)$ additional symbols. Then derive the pseudocomplement properties of

τ_i^{n-1} monotonically in size $s(n-1)$, and those of σ_k^n from these in $l(n)$ additional symbols. Finally, the rules of $\neg$-introduction are simulated by cuts on these sequents. This analysis gives us the recurrence $s(n) = q(n) + 3q(n)(2p(n-1)+3) + s(n-1) + l(n)$ which is easily seen to give a polynomial. We note that the proofs are not tree-like at all. □

We are now ready to prove the main result of this section.

Theorem 7 LK *is polynomially bounded if and only if* MLK *is polynomially bounded.*

Proof: Suppose that LK is polynomially bounded. Let τ_k^n be Valiant's monotone formulas for all threshold functions [16]. Any other polynomial-size monotone formulas computing TH_k^n would do as well. Since we are assuming that LK is polynomially bounded, the pseudocomplement properties of τ_k^n have polynomial-size LK-proofs. Hence, by Lemma 6, MLK polynomially simulates LK. In particular, MLK is polynomially bounded.

For the other direction, suppose that MLK is polynomially bounded. We shall use the following translation of nonmonotone sequents to monotone ones. Suppose we have a formula that uses only variables $x_1, \ldots, x_n$. Take another set of variables $y_1, \ldots, y_n$ that will represent the negations of the x_i's. Given a sequent

$$\Sigma \vdash \Gamma,$$

in De Morgan normal form, we shall translate it into the following monotone sequent

$$(x_1 \vee y_1), \ldots, (x_n \vee y_n), \Sigma' \vdash \Gamma', (x_1 \wedge y_1), \ldots, (x_n \wedge y_n), \tag{3}$$

where Σ', Γ' are obtained from Σ, Γ by replacing all $\neg x_i$ by y_i, for $i = 1, \ldots, n$. Clearly, the first sequent is a tautology if and only if the second is. Hence, if $\Sigma \vdash \Gamma$ is a tautology, we have, by our assumption, a polynomial size MLK proof of the second sequent. Thus it remains to show that a proof of the translation in MLK can be transformed into at most polynomially larger proof of the original sequent in LK. But this is trivial. First replace y_i's back to $\neg x_i$'s in the whole MLK proof. Then add proofs of sequents $\vdash x_i \vee \neg x_i$ and apply cuts to remove these disjunctions from (3). Do the same thing (more precisely, the dual thing) with the consequent. □

6 Conclusions and open problems

We do not know if our simulation of LK by MLK (of monotone sequents) can be improved to a polynomial simulation. The bottleneck of our proof are the threshold formulas. By Lemma 6 to get a polynomial simulation it would suffice to replace them by monotone formulas of polynomial size and find polynomial size proofs of the properties of these formulas in LK. While there are explicit constructions of polynomial size monotone threshold formulas (an easy corollary of the construction of log-depth sorting network [1]), it is at all not clear whether the conditions can be proven for such formulas by polynomial size proofs. The most direct approach would be to formalize the proof of [1] in LK. This would require, in particular, to prove that the expander graphs used in the construction have the expansion properties. We are not aware of any 'low level' proof of the expansion properties, thus this seems to be an essential obstacle.

As expander graphs proved to be very useful in many applications, it may be of independent interest to know if a tautology expressing such a property for some graph has polynomial size proofs. Let ρ_k^n be (nonmonotone) formulas expressing TH_k^n and such that the basic conditions (the sequents of Lemmas 4 and 5) have polynomial size LK proofs for these formulas. (Such formulas are well-known [4]; it does not matter which we choose, since their equivalence is provable by polynomial size proofs.) Let G be a graph such that for some k and l, every set of vertices X of size k expands to size l by G, which means that there are at least l vertices that either belong to X or are connected by an edge to X. Let the set of vertices of G be $\{1, \ldots, n\}$ and the set of edges of G be E. The following tautology expresses the expansion property of G:

$$\rho_k^n(x_1, \ldots, x_n) \to \rho_l^n(x_1 \vee \bigvee_{(1,j)\in E} x_j, \ldots, x_n \vee \bigvee_{(n,j)\in E} x_j) \tag{4}$$

The interesting case is when the degree of G is constant and for some constants $0 < \epsilon < \delta < 1$, k is asymptotically ϵn and l is asymptotically δn. Does there exist a graph G such that for such parameters the sequent (4) has a polynomial size LK proof?

The complexity of MLK proofs of the general PHP is also an open problem. Thus it is not totally excluded that this tautology can be used to show a superpolynomial gap between LK and MLK.

References

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

[2] A. Atserias, N. Galesi, and R. Gavaldà. Monotone proofs of the pigeon-hole principle. *Mathematical Logic Quarterly*, 47(4), pp. 461–474, 2001.

[3] M. Bílková, Monotone sequent calculus and resolution. *Comment. Math. Univ. Carolinae*, 42(3), pp. 575–582, 2001.

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

[5] S. R. Buss and P. Pudlák. On the computational content of intuitionistic propositional proofs. *Annals of Pure and Applied Logic*, 109, pp. 49-64, 2001.

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

[7] A. Haken. The intractability of resolution. *Theoretical Computer Science*, 39, 297-308, 1985.

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

[9] J. Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *Journal of Symbolic Logic*, 62(2), 457-486, 1997.

[10] R. Impagliazzo, T. Pitassi, A. Urquhart. Upper and Lower Bounds for Tree-like Cutting Planes Proofs. In *Proceedings of Ninth Annual IEEE Symposium on Logic in Computer Science (LICS)*, pp. 220-228, 1994.

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

[12] P. Pudlák. On the complexity of the propositional calculus. *Sets and Proofs, Invited Papers from Logic Colloquium '97.* Cambridge University Press, pp. 197-218, 1999.

[13] A.A. Razborov. Lower bounds on the monotone complexity of some boolean functions. *Doklady Akad. Nauk SSSR*, 282, pp. 1033–1037, 1985.

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

[15] E. Tardos. The gap between monotone and non-monotone circuit complexity is exponential. *Combinatorica*, 7(4), pp. 141–142, 1987.

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

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