Monotone Simulations of Nonmonotone Proofs

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

Nicola Galesi†
Institute for Advanced Study
Princeton, USA
galesi@ias.edu

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.

1 Introduction

The study of the propositional monotone sequent calculus was proposed in [9] in an attempt to find a proof complexity version of the monotone Boolean circuits. This calculus is simply the restriction of the full propositional sequent calculus to formulas in basis $\{\vee, \wedge\}$. 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 [3].

Classical results of Razborov [10] and others in computational complexity theory show that monotone Boolean circuits are substantially less powerful than circuits that use also negation. 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 [12]. Therefore 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 proof of size m 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 [13]). 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.

*Supported by the CUR, Generalitat de Catalunya, through grant 1999FI 00532, and partially supported by ALCOM-FT, IST-99-14186.

†Supported by the NSF grant n. CCR-9987845

‡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 project LN00A056 of the Ministry of Education of the Czech Republic.

We also show that in some special cases the simulation is in fact polynomial. We consider two well-known variants of the Pigeon Hole 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 [8] and get polynomial size monotone proofs as well.

2 Monotone Calculus

All our propositional formulas are over the basis $\{\wedge, \vee, \neg\}$. 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 will assume some familiarity with the propositional fragment of the Gentzen sequent calculus as defined, eg., in the book by Takeuti [11]. 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). 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, 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.

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.

The size of a proof is the number of symbols in it. We say that a proof is tree-like if each sequent is used at most once as a premise of a rule.

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 linear in the size of* φ.

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 linear 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 linear 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 linear size 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* $O(S)$.

Proof: Suppose that $\Sigma \vdash \Gamma$ has a tree-like LK-proof P of size S. Consider the following transformation of

P. First, replace each formula φ in P by $p(\varphi)$. 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 $O(S)$ 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 $O(S)$. □

Theorem 2 *Let Σ and Γ be sequences of monotone formulas with all variables within $x_1, \dots, x_n$. Suppose that for every $i \in \{1, \dots, n\}$ 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 $O(S + RS)$.*

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 $O(S)$. 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 $O(S + RS)$. □

3 Monotone simulation of LK

Recall the following definitions and Lemmas from [2]. 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 $\mathrm{TH}^n_k(a_1, \dots, a_n) = 1$ if and only if $\sum_{i=1}^k a_i \geq k$, for every $(a_1, \dots, a_n) \in \{0,1\}^n$. Each TH^n_k is called a threshold function.

Monotone threshold formulas are defined the following way: $\mathrm{th}^1_0(x) := 1$, $\mathrm{th}^1_1(x) := x$, $\mathrm{th}^1_k(x) := 0$ for every $k > 1$, and for every $n > 1$ and $k \geq 0$, define the formula

$$\mathrm{th}^n_k(x_1, \dots, x_n) :=$$

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

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 prove, by induction on n, that the size of $\mathrm{th}^n_k(x_1, \dots, x_n)$ is bounded by $n^{O(\log n)}$.

Recall that if A and B are formulas and x is a variable that may or may nor occur in A, the notation $A(x/B)$ stands for the formula that results of replacing every occurrence of x in A by B (simultaneously).

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

Lemma 3 ([2]) *For every $n, m, l \in \mathbb{N}$ with $0 < m \leq n$ and $0 \leq l \leq n$, the sequent*

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

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 $n, k \in \mathbb{N}$ with $k > n$, the sequents*

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

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

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

For $k, i \in \mathbb{N}$ with $0 \leq k \leq n$ and $1 \leq i \leq n$, the k-pseudocomplement of x_i is, by definition, the monotone formula $\mathrm{th}^n_k(x_1, \ldots, x_i/0, \ldots, x_n)$. 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 $\mathrm{th}^n_k(x_1, \ldots, x_n)$ and Γ contains $\mathrm{th}^n_{k+1}(x_1, \ldots, x_n)$.

Lemma 5 *For every $k, i \in \mathbb{N}$ with $0 \leq k \leq n$ and $1 \leq i \leq n$ the sequents:*

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

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

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 sequent observe that from Lemma 2 (ii) we have $x_i, \mathrm{th}^n_{k+1}(x_1, \ldots, x_i/1, \ldots, x_n) \vdash \mathrm{th}^n_{k+1}(x_1, \ldots, x_n)$. Moreover, Lemma 3 gives $\mathrm{th}^n_k(x_1, \ldots, x_i/0, \ldots, x_n) \vdash \mathrm{th}^n_{k+1}(x_1, \ldots, x_i/1, \ldots, x_n)$. The sequent in (ii) is obtained by cutting and then adding $\mathrm{th}^n_k(x_1, \ldots, x_n)$ 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 [7], 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 $k \in \{0, \ldots, n\}$ we obtain tree-like MLK proofs of the sequents $\mathrm{th}^n_k(x_1, \ldots, x_n), \Sigma \vdash \Gamma, \mathrm{th}^n_{k+1}(x_1, \ldots, x_n)$ each one with S lines and size $S \cdot n^{O(\log n)}$. Finally, n consecutive cuts give us a proof of the sequent $\mathrm{th}^n_0(x_1, \ldots, x_n), \Sigma \vdash \Gamma, \mathrm{th}^n_{n+1}(x_1, \ldots, x_n)$ 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.

The careful reader will 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 intuitionisitic calculus* JK *quasipolynomially simulates* LK *on monotone sequents.*

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

4 Pigeon-hole and Matching Principles

We consider the following propositional formulations of PHP, OPHP and FPHP: We let PHP^{n+1}_n be the sequent

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

We let OPHP^{n+1}_n be the sequent

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

Finally, we let FPHP_n^{n+1} be the sequent

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

Using Corollary 2 and Buss' polynomial size LK proofs of the PHP 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 [7], they also have polynomial-size tree-like LK-proofs. We first consider FPHP_n^{n+1}. For every $i \in \{1,\dots,n+1\}$ and $j \in \{1,\dots,n\}$, let φ_{ij} be the formula $\bigvee_{j'\neq j} p_{i,j'}$ where j' ranges over $\{1,\dots,n\}$. Let LFPHP_n^{n+1} be the left hand side of the sequent FPHP_n^{n+1}, and let RFPHP_n^{n+1} be the right hand side of the sequent FPHP_n^{n+1}. We claim that the sequents

$$\mathrm{LFPHP}_n^{n+1} \vdash p_{i,j}, \varphi_{ij}, \mathrm{RFPHP}_n^{n+1} \qquad (1)$$
$$\mathrm{LFPHP}_n^{n+1}, \varphi_{ij}, p_{i,j} \vdash \mathrm{RFPHP}_n^{n+1} \qquad (2)$$

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 $j' \in \{1,\dots,n\}$, we have $p_{i,j'} \vdash p_{i,1},\dots,p_{i,n}, \mathrm{RFPHP}_n^{n+1}$ by right weakening on the axiom $p_{i,j'} \vdash p_{i,j'}$ and structural rules. By left $\vee$-introduction we get $\bigvee_{j=1}^{n} p_{i,j} \vdash p_{i,1},\dots,p_{i,n}, \mathrm{RFPHP}_n^{n+1}$. Left weakening and left $\wedge$-introduction gives $\mathrm{LFPHP}_n^{n+1} \vdash p_{i,1},\dots,p_{i,n}, \mathrm{RFPHP}_n^{n+1}$. Finally, some structural rules and right $\vee$-introduction give sequent (1). For sequent (2) reason as follows. For every $j, j' \in \{1,\dots,n+1\}$ 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 $\mathrm{LFPHP}_n^{n+1}, p_{i,j}, p_{i,j'} \vdash \mathrm{RFPHP}_n^{n+1}$. 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 $\{1,\dots,n+1\}$, 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 [8]. 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.

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

Then the 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 $X^{\perp}(i) := \neg X(i)$ for $i = 2, 3$, and $Y^{\perp}(3) := \neg Y(3)$. Then (1) is equivalent to the monotone sequent

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

Notice that, as observed in [8], 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. Either way 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 [8] 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

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

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

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

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

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

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

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 $x_{i,k}, (x_{i,k'} \wedge x_{i,k''}) \vdash X^{\perp}(3)$. By right $\vee$-introductions on all previous proofs we have $x_{i,k}, \varphi^x_{i,k} \vdash X^{\perp}(3)$ from which the sequent (2) follows by two weakenings, left and right. □

5 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. 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 (lemmas 3 and 4). 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 (in fact, even in full LK). The most direct approach would be to formalize the proof of [1] in MLK. 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. The following observation may be helpful for proving that MLK polynomially simulates LK.

Proposition 1 *Suppose that it is possible to construct polynomial size* monotone *threshold formulas such that the sequents of Lemmas 3 and 4 have polynomial size proofs in* LK. *Then* MLK *polynomially simulates* LK *(with respect to monotone tautological sequents).*

Proof: Suppose we have such formulas and proofs. We will show how to transform the nonmonotone proofs of the sequents of Lemmas 3 and 4 into monotone ones. Then the theorem follows using the same proof as in Theorem 3.

Let us denote by τ_k^n the formula for TH_k^n, with variables $x_1, \dots, x_n$. We prove by induction on n that for the formulas $\tau_0^n, \dots, \tau_n^n$ the sequents have monotone polynomial size proofs. For $n = 1$ the proofs are just constant size. Assume we have proven this statement for n. Then we first define auxiliary formulas σ_i^{n+1} by

$$\sigma_i^{n+1} := \tau_i^n \vee (\tau_{i-1}^n \wedge x_{n+1})$$

for $i = 1, \dots, n$, $\sigma_0^{n+1} := 1$ and σ_{n+1}^{n+1} is the conjunction of $n + 1$ variables. To get polynomial size monotone proofs of the properties of $\sigma_0^n, \dots, \sigma_{n+1}^{n+1}$ from those of $\tau_0^n, \dots, \tau_n^n$ is a simple task. Then we use the argument of Theorem 3 with $\sigma_0^n, \dots, \sigma_{n+1}^{n+1}$ to construct polynomial size monotone proofs of $\tau_0^n, \dots, \tau_{n+1}^{n+1}$. $\square$

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 a (nonmonotone) formulas expressing TH_k^n and such that the basic conditions have polynomial size LK proofs for these formulas. 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 $\{1, \dots, n\}$ and the set of edges of G be E. The following tautology expresses the expansion property of G:

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

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.

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. In *27th International Colloquium on Automata, Languages and Programming*, pp.151–162, 2000. To appear in Mathematical Logic Quarterly.

[3] M. Bílková, Monotone sequent calculus and resolution, preprint.

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

[5] S. R. Buss and P. Pudlák. On the computational content of intuitionistic propositional proofs. *Annals of Pure and Applied Logic,* to appear.

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

[7] J. Krajíček. Bounded Arithmetic, Propositional Logic and Complexity Theory, Cambridge Univ. Press, 1985.

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

[9] 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.

[10] A.A. Razborov, Lower bounds on the monotone complexity of some Boolean functions. Doklady Akad. Nauk SSSR 282, (1985), 1033–1037.

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

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

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