Marta Bílková

Monotone sequent calculus and resolution

Commentationes Mathematicae Universitatis Carolinae, Vol. 42 (2001), No. 3, 575--582

Persistent URL: `http://dml.cz/dmlcz/119272`

Monotone sequent calculus and resolution

Marta Bílková

Abstract. We study relations between propositional Monotone Sequent Calculus (MLK — also known as Geometric Logic) and Resolution with respect to the complexity of proofs, namely to the concept of the polynomial simulation of proofs. We consider Resolution on sets of monochromatic clauses. We prove that there exists a polynomial simulation of proofs in MLK by intuitionistic proofs. We show a polynomial simulation between proofs from axioms in MLK and corresponding proofs of contradiction (refutations) in MLK. Then we show a relation between a resolution refutation of a set of monochromatic clauses (CNF formula) and a proof of the sequent (representing corresponding DNF formula) in MLK. Because monotone logic is a part of intuitionistic logic, results are relevant for intuitionistic logic too.

Keywords: intuitionistic propositional logic, monotone logic, sequent calculus, resolution, complexity of proofs

Classification: 03F07, 03F20, 03B20, 03F55

1. Introduction

In this article we consider some proof systems for propositional logic. One of them is the *Monotone Sequent Calculus* — MLK ([4], [1]). This is the classical sequent calculus LK restricted to monotone formulas — formulas in the basis $\vee$, $\wedge$. Monotone logic is also known as Geometric Logic. Rules of MLK are structural rules, logical rules for $\wedge$ and $\vee$, and the cut rule. The only monotone tautological formula is the constant of truth T (because there is no rule of $\neg$ or $\rightarrow$ in MLK, we cannot get any tautological sequent with an empty antecedent); proofs in MLK are proofs of tautological sequents or proofs of contradiction — proofs of the empty sequent from assumptions. We measure the complexity of a proof by the number of uses of rules, i.e. steps of a proof.

We say that there exists a *polynomial simulation* ([3]) between two proof systems if one can construct in polynomial time a proof in one system from a proof in the other. It provides a more subtle relation between proof systems than comparison of lengths of proofs does. In Section 2 we prove (by polynomial simulation of proofs) that monotone logic is a part of intuitionistic logic. Let us recall that *Intuitionistic Sequent Calculus*–LJ is obtained from the classical one by admitting at most one formula in succedent of each sequent ([5]). The idea of the proof is simple: we interpret the succedent as a disjunction. Let us note that our simulations actually change the number of steps also only polynomially.

The second proof system we consider here is the *Resolution*. This is a refutation system for formulas in CNF which are represented as sets of *clauses* (resolution can be seen as a proof system for tautologies in DNF). Clauses are disjunctions of *literals*, we consider them as sets of literals. Literals are propositional variables and their negations. The only rule is the *resolution rule*:

$$\frac{A \cup \{p\} \quad B \cup \{\neg\, p\}}{A \cup B}\,.$$

Resolution has no axioms, a proof starts with a set of clauses which is intended to be refuted. This is done by deriving the empty clause. A resolution proof can be represented by a tree, then the complexity of a proof is the number of nodes.

2. Monotone and intuitionistic proofs

In the following theorem we show polynomial simulation of proofs in MLK by intuitionistic proofs.

Theorem 2.1. *Let P be a proof of the sequent $\Gamma \Rightarrow A_1, A_2, \ldots, A_n$ in MLK. Then there exists a proof Q of the sequent $\Gamma \Rightarrow A_1 \vee A_2 \vee \cdots \vee A_n$ in MLK, which is an intuitionistic proof. Q can be constructed in polynomial time from P. Moreover, if P is in a tree form than Q is in a tree form too.*

Proof: First we prove the principle of associativity for $\vee$:

$$\vee\text{-l}\,\dfrac{\vee\text{-l}\,\dfrac{\dfrac{A \Rightarrow A}{A \Rightarrow A \vee (B \vee C)} \qquad \dfrac{\dfrac{B \Rightarrow B}{B \Rightarrow B \vee C}}{B \Rightarrow A \vee (B \vee C)}}{(A \vee B) \Rightarrow A \vee (B \vee C)} \qquad \dfrac{\dfrac{C \Rightarrow C}{C \Rightarrow B \vee C}}{C \Rightarrow A \vee (B \vee C)}}{(A \vee B) \vee C \Rightarrow A \vee (B \vee C)}$$

$$\vee\text{-l}\,\dfrac{\dfrac{\dfrac{A \Rightarrow A}{A \Rightarrow A \vee B}}{A \Rightarrow (A \vee B) \vee C} \qquad \vee\text{-l}\,\dfrac{\dfrac{\dfrac{B \Rightarrow B}{B \Rightarrow A \vee B}}{B \Rightarrow (A \vee B) \vee C} \qquad \dfrac{C \Rightarrow C}{C \Rightarrow (A \vee B) \vee C}}{B \vee C \Rightarrow (A \vee B) \vee C}}{A \vee (B \vee C) \Rightarrow (A \vee B) \vee C}$$

Now we can omit parentheses from descriptions of formulas in which only $\vee$ occurs. This makes the proof more transparent.

Let P be a proof of the sequent $\Gamma \Rightarrow \Delta$, where $\Delta \equiv \{A_1, A_2, \ldots, A_n\}$, $A_i \in \Delta$, in MLK. We want to get a proof Q of the sequent $\Gamma \Rightarrow A_1 \vee A_2 \vee \cdots \vee A_n$. We replace right sides of all sequents in P which are sets of formulas by disjunction of these formulas. Because there is no possibility of passage between the left

side and the right side of sequents in MLK, we leave left sides without change. The resulting sequence is not yet a proof. We have to modify it as follows.
AXIOMS: axioms remain without change (as in P).
STRUCTURAL RULES
WEAKENING–r: we replace it by $\vee$-r
CONTRACTION–r: we want to get:

$$\frac{\Gamma \Rightarrow A \vee A \vee D}{\Gamma \Rightarrow A \vee D}$$

We get it in this way (we insert the following part):

$$\dfrac{\vee\text{-l}\;\dfrac{\vee\text{-r}\;\dfrac{A \Rightarrow A}{A \Rightarrow A \vee D} \qquad A \vee D \Rightarrow A \vee D}{A \vee A \vee D \Rightarrow A \vee D} \qquad \Gamma \Rightarrow A \vee A \vee D}{\Gamma \Rightarrow A \vee D}\;\text{cut}$$

EXCHANGE–r: we want to get:

$$\frac{\Gamma \Rightarrow G \vee A \vee B \vee D}{\Gamma \Rightarrow G \vee B \vee A \vee D}$$

We insert the following part:

$$\vee\text{-r}\;\dfrac{\vee\text{-l}\;\dfrac{\vee\text{-l}\;\dfrac{\vee\text{-r}\;\dfrac{G \Rightarrow G}{G \Rightarrow G \vee B \vee A} \qquad \dfrac{A \Rightarrow A}{A \Rightarrow G \vee B \vee A}}{G \vee A \Rightarrow G \vee B \vee A} \qquad \dfrac{\dfrac{B \Rightarrow B}{B \Rightarrow G \vee B}\;\vee\text{-r}}{B \Rightarrow G \vee B \vee A}\;\vee\text{-r}}{G \vee A \vee B \Rightarrow G \vee B \vee A}}{G \vee A \vee B \Rightarrow G \vee B \vee A \vee D}$$

$$\vee\text{-l}\;\dfrac{G \vee A \vee B \Rightarrow G \vee B \vee A \vee D \qquad \dfrac{D \Rightarrow D}{D \Rightarrow G \vee B \vee A \vee D}\;\vee\text{-r}}{G \vee A \vee B \vee D \Rightarrow G \vee B \vee A \vee D}$$

$$\text{cut}\;\dfrac{G \vee A \vee B \vee D \Rightarrow G \vee B \vee A \vee D \qquad \Gamma \Rightarrow G \vee A \vee B \vee D}{\Gamma \Rightarrow G \vee B \vee A \vee D}$$

LOGICAL RULES
$\vee$–r: we want to get:

$$\frac{\Gamma \Rightarrow A \vee D}{\Gamma \Rightarrow A \vee B \vee D}$$

We insert the following part:

$$\vee\text{-l}\;\dfrac{\vee\text{-l}\;\dfrac{\vee\text{-r}\;\dfrac{A \Rightarrow A}{A \Rightarrow A \vee B \vee D} \qquad \dfrac{D \Rightarrow D}{D \Rightarrow A \vee B \vee D}}{A \vee D \Rightarrow A \vee B \vee D} \qquad \dfrac{\dfrac{B \Rightarrow B}{B \Rightarrow A \vee B}\;\vee\text{-r}}{B \Rightarrow A \vee B \vee D}\;\vee\text{-r}}{A \vee D \vee B \Rightarrow A \vee B \vee D}$$

$$\text{cut}\ \dfrac{A \vee D \vee B \Rightarrow A \vee B \vee D \qquad \dfrac{\Gamma \Rightarrow A \vee D}{\Gamma \Rightarrow A \vee D \vee B}\ \vee\text{-r}}{\Gamma \Rightarrow A \vee B \vee D}$$

We want to get:

$$\dfrac{\Gamma \Rightarrow A \vee D}{\Gamma \Rightarrow B \vee A \vee D}$$

We leave it without change.

THE CUT RULE: we want to get:

$$\dfrac{\Gamma \Rightarrow A \vee D \qquad A, \Gamma \Rightarrow D}{\Gamma \Rightarrow D}$$

We insert the following part:

$$\dfrac{\vee\text{-l}\ \dfrac{A, \Gamma \Rightarrow D \qquad \dfrac{D \Rightarrow D}{D, \Gamma \Rightarrow D}\ \text{weakening-l}}{A \vee D, \Gamma \Rightarrow D} \qquad \Gamma \Rightarrow A \vee D}{\Gamma \Rightarrow D}\ \text{cut}$$

$\wedge$–r: we want to get:

$$\dfrac{\Gamma \Rightarrow A \vee D \qquad \Gamma \Rightarrow B \vee D}{\Gamma \Rightarrow (A \wedge B) \vee D}$$

We insert the following part:

$$\vee\text{-l}\ \dfrac{\vee\text{-r}\ \dfrac{\dfrac{\dfrac{A \Rightarrow A}{A, B \Rightarrow A} \qquad \dfrac{B \Rightarrow B}{A, B \Rightarrow B}}{A, B \Rightarrow A \wedge B}\ \wedge\text{-r}}{A, B \Rightarrow (A \wedge B) \vee D} \qquad \dfrac{D \Rightarrow D}{D \Rightarrow (A \wedge B) \vee D}\ \vee\text{-r}}{A \vee D, B \Rightarrow (A \wedge B) \vee D}$$

$$\dfrac{A \vee D, B \Rightarrow (A \wedge B) \vee D \qquad D \Rightarrow (A \wedge B) \vee D}{A \vee D, B \vee D \Rightarrow (A \wedge B) \vee D}\ \vee\text{-l}$$

$$\text{cut}\ \dfrac{\wedge\text{-l}\ \dfrac{A \vee D, B \vee D \Rightarrow (A \wedge B) \vee D}{(A \vee D) \wedge (B \vee D) \Rightarrow (A \wedge B) \vee D} \qquad \dfrac{\Gamma \Rightarrow A \vee D \qquad \Gamma \Rightarrow B \vee D}{\Gamma \Rightarrow (A \vee D) \wedge (B \vee D)}\ \wedge\text{-r}}{\Gamma \Rightarrow (A \wedge B) \vee D}$$

Thus we have got a proof Q with only one formula in the succedent of each sequent, i.e. intuitionistic proof. We have constructed Q polynomially because every inserted part has a constant number of uses of rules and the new steps use only old formulas and, hence, the size of each step (considering lengths of formulas) can be bounded in terms of the original proof P. Since we have inserted just tree-like parts it is easy to see that if P is in a tree-form then Q is in a tree-form too.

$\square$

3. Monotone and resolution proofs

The following definition introduces a special form of clauses.

Definition 3.1. A *monochromatic clause* is a clause containing only positive or only negative literals.

We present two examples of tautologies, whose negations can be represented as sets of monochromatic clauses — PHP and CLIQUE.

An interesting tautology the negation of which can be represented as a set of monochromatic clauses is PHP_n^{n+1}. This is the *Pigeon Hole Principle*, which states that if $n+1$ pigeons go into n holes, then there is some hole with more than one pigeon in it. We can represent PHP_n^{n+1} by the following monotone sequent ([1]):

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

In Resolution we get:

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

It is known ([1]) that PHP has quasipolynomial-size proofs in MLK whereas in resolution it has only exponential proofs ([4]). Thus resolution is exponentially separated from MLK.

Another example is CLIQUE_k^n. For $k \leq n$, the (n,k)-Clique Principle states that a graph on $1,\dots,n$ containing a k-clique cannot be colored with $k-1$ colors. In the article [1] the Clique principle CLIQUE_k^n is expressed by a monotone sequent slightly stronger to make possible to reduce it to PHP_{k-1} in MLK. One can say that this is another tautology; however, from point of view of true values all tautologies are the same. We want to express it as a set of monochromatic clauses by using two functions — the clique function and the function of coloring. We have a graph G on $1,\dots,n$. For every $i,j \in \{1,\dots,n\}$ let $x_{i,j}$ be a propositional variable whose meaning is that there is an edge between i-th and j-th node in G. A clique is coded by a mapping from $\{1,\dots,k\}$ into $\{1,\dots,n\}$. For every $i \in \{1,\dots,n\}$ and every $l \in \{1,..,k\}$ let $\neg y_{l,i}$ be a literal whose meaning is that i-th node of G is l-th node of the clique. We define it negatively to get a set of monochromatic clauses. For every $i \in \{1,\dots,n\}$ and every $l \in \{1,\dots,k-1\}$ let $z_{l,i}$ be a propositional variable whose meaning is that i-th node of G is colored by l-th color. Now we code the clique function as follows:

$$\bigwedge_{i,j=1\ i\neq j}^{n} \bigwedge_{m,l=1}^{k} (y_{m,i} \vee y_{l,j} \vee x_{i,j}) \wedge \bigwedge_{m=1}^{k} \bigvee_{i=1}^{n} \neg y_{m,i} \wedge \bigwedge_{i=1}^{n} \bigwedge_{m,l=1\ m\neq l}^{k} (y_{m,i} \vee y_{l,i})$$

and the function of the coloring as follows:

$$\bigwedge_{i,j=1\ i\neq j}^{n} \bigwedge_{l=1}^{k-1} (\neg x_{i,j} \vee \neg z_{l,i} \vee \neg z_{l,j}) \wedge \bigwedge_{i=1}^{n} \bigvee_{l=1}^{k-1} z_{l,i}.$$

Thus we have got the set of monochromatic clauses.

In the following proposition we show a relation between proofs and refutations in Monotone Sequent Calculus.

Proposition 3.2. (i) *Let P be a proof of the sequent $A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$ in MLK. Then there exists a proof P' of contradiction (the empty sequent) in MLK from assumptions*

$$\Rightarrow A_1 \ , \ldots , \ \Rightarrow A_n \ , \ B_1 \Rightarrow \ , \ldots , \ B_m \Rightarrow$$

P' can be constructed in polynomial time from P.

(ii) *Let Q be a proof of contradiction from assumptions*

$$\Rightarrow A_1 \ , \ldots , \ \Rightarrow A_n \ , \ B_1 \Rightarrow \ , \ldots , \ B_m \Rightarrow$$

in MLK. Then there exists a proof Q' of the sequent $A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m$ in MLK. Q' can be constructed in polynomial time from Q.

Proof: (i) Suppose a proof P and assumptions as in the theorem are given. We use step by step cuts of the form:

$$\frac{A_1, \ldots, A_n \Rightarrow B_1, \ldots, B_m \qquad \Rightarrow A_1}{A_2, \ldots, A_n \Rightarrow B_1, \ldots, B_m}$$

$$\ldots$$

$$\ldots$$

$$\frac{A_n \Rightarrow B_1, \ldots, B_m \qquad \Rightarrow A_n}{\Rightarrow B_1, \ldots, B_m}$$

$$\frac{\Rightarrow B_1, \ldots, B_m \quad B_1 \Rightarrow}{\Rightarrow B_2, \ldots, B_m}$$

$$\ldots$$

$$\ldots$$

$$\frac{\Rightarrow B_m \quad B_m \Rightarrow}{\Rightarrow}$$

We take the proof P with added assumptions and cuts as the proof P'.
$|P'| = |P| + m + n$.

(ii) Suppose a proof Q of the empty sequent is given. We get a proof Q' by the following modification of the proof Q: we add $A_1,\dots,A_n$ into the antecedent of each sequent in Q and $B_1,\dots,B_m$ into the succedent of each sequent in Q. By this modification we get sequents of the following form from previous assumptions: for $i\in\{1,\dots,m\},\ j\in\{1,\dots,n\}$

$$A_1,\dots,A_n,B_i\Rightarrow B_1,\dots,B_m$$
$$A_1,\dots,A_n\Rightarrow A_j,B_1,\dots,B_m.$$

These sequents are provable from axioms by using the rule of weakening (in $(m+n)\cdot(m+n-1)$ steps). The endsequent of the proof Q' is $A_1,\dots,A_n\Rightarrow B_1,\dots,B_m$. $|Q'|=|Q|+(m+n)\cdot(m+n-1)$. □

In the next corollary we show an application of this proposition to the Resolution. (Limit c_i (d_k) denotes length of i-th positive (k-th negative) clause. $p_{i,j},\ q_{k,l}$ denote propositional variables that need not be distinct).

Corollary. *Let us have a resolution proof P of the contradiction from the formula $\neg\varphi\ :\ (\bigwedge_{i=1}^{m}\bigvee_{j=1}^{c_i}p_{i,j})\wedge(\bigwedge_{k=1}^{n}\bigvee_{l=1}^{d_k}\neg q_{k,l})$, (i.e., from the set of monochromatic clauses). We represent the formula φ by the following monotone sequent:*

$$\bigvee_{j=1}^{c_1}p_{1,j},\dots,\bigvee_{j=1}^{c_m}p_{m,j}\Rightarrow\bigwedge_{l=1}^{d_1}q_{1,l},\dots,\bigwedge_{l=1}^{d_n}q_{n,l}\,. \tag{1}$$

Then the sequent (1) *has in the Monotone Sequent Calculus a proof Q. Q can be constructed in polynomial time from the resolution proof P. Consequently, the same is true for Intuitionistic Sequent Calculus.*

Proof: We translate the proof P as follows:
(i) instead of each clause $\bigvee_{j=1}^{c_i}p_{i,j}$, we take the sequent $\Rightarrow p_{i,1},\dots,p_{i,c_i}$;
(ii) instead of each clause $\bigvee_{l=1}^{d_k}\neg q_{k,l}$, we take the sequent $q_{k,1},\dots,q_{k,d_k}\Rightarrow$;
(iii) instead of each use of the resolution rule on $p_{i,j}$ (resp. $q_{k,l}$), we use the cut on $p_{i,j}$ (resp. $q_{k,l}$).
Thus we get a proof of the empty sequent in Monotone Sequent Calculus. Now we use the part (ii) of the proposition to get the proof Q. We add $\bigvee_{j=1}^{c_1}p_{1,j},\dots,\bigvee_{j=1}^{c_m}p_{m,j}$ into the antecedent of each sequent and $\bigwedge_{l=1}^{d_1}q_{1,l},\dots,\bigwedge_{l=1}^{d_n}q_{n,l}$ into the succedent of each sequent. We continue as in the proof (ii). □

We have shown that there is some connection between Monotone Sequent Calculus and Resolution (and thus between Intuitionistic Sequent Calculus and Resolution, too) in the sense of the polynomial simulation of proofs. It is a new result of A. Atserias [2] that onto and functional versions of PHP have polynomial proofs in MLK and hence in Intuitionistic Sequent Calculus. It is an open question if the Clique Principle has at least quasipolynomial proofs in these systems. Another question is if there exist sequents with short proofs in LJ but not in MLK.

References

[1] Atserias A., Galesi N., Gavalda R., *Monotone Proofs of the Pigeon Hole Principle*, preprint, Barcelona University, 1999.

[2] Atserias A., Galesi N., Pudlák P., *Monotone Simulations of Nonmonotone Propositional Proofs*, ECCC Report TR00-087, 2000.

[3] Cook S.A., Reckhow R.A., *The relative efficiency of propositional proof systems*, J. Symbolic Logic **44** (1979), 36-50.

[4] Pudlák, P., *On the complexity of the propositional calculus*, in Sets and Proofs, Invited papers from Logic Colloquium 1997, S.B. Cooper and J.K. Truss eds., Cambridge University Press, 1999, pp . 197–218.

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

Department of Logic, Faculty of Philosophy, Charles University, nám. Jana Palacha 2, 116 38 Prague 1, Czech Republic

(*Received* August 7, 2000)