Discretely ordered modules as a first-order extension of the cutting planes proof system

Jan Krajíček*

Mathematical Institute and Institute of Computer Science
Academy of Sciences, Prague

Abstract

We define a first-order extension LK(CP) of the cutting planes proof system CP as the first-order sequent calculus LK whose atomic formulas are CP-inequalities $\sum_i a_i \cdot x_i \geq b$ (x_i's variables, a_i's and b constants). We prove an interpolation theorem for LK(CP) yielding as a corollary a conditional lower bound for LK(CP)-proofs. For a subsystem R(CP) of LK(CP), essentially resolution working with clauses formed by CP-inequalities, we prove a monotone interpolation theorem obtaining thus an unconditional lower bound (depending on the maximum size of coefficients in proofs and on the maximum number of CP-inequalities in clauses). We also give an interpolation theorem for polynomial calculus working with sparse polynomials.

The proof relies on a universal interpolation theorem for semantic derivations [16, Thm. 5.1].

LK(CP) can be viewed as a two-sorted first-order theory of $\mathbf{Z}$ considered itself as a discretely ordered $\mathbf{Z}$-module. One sort of variables are module elements, another sort are scalars. The quantification is allowed only over the former sort. We shall give a construction of a theory LK($\mathbf{M}$) for any discretely ordered module $\mathbf{M}$ (e.g., LK($\mathbf{Z}$) extends LK(CP)). The interpolation theorem generalizes to these theories obtained from discretely ordered $\mathbf{Z}$ -modules. We shall also discuss a connection to quantifier elimination for such theories.

We formulate a communication complexity problem whose (suitable) solution would allow to improve the monotone interpolation theorem and the lower bound for R(CP).

After lower bounds for the cutting planes proof system CP (defined in [8]), culminating in [21], various generalizations of CP were suggested. In particular, CP with the deduction rule. A proof in such a proof system allows to split

*Partially supported by the *US - Czechoslovak Science and Technology Program* grant # 93025, and by grant #*A*1019602 of the *AVČR*.

(repeatedly) the proof into two parts, depending on whether a CP-inequality is or is not satisfied (see Example 3 in Section 2 for a formalization due to [4]). A natural question arises to extend the lower bounds for CP to these presumably stronger proof systems.

It appeared to us that a convenient formalization of CP with the deduction rule is resolution working with clauses formed by CP-inequalities (see Section 3). In particular, it allows us to discuss also proofs in which the deduction formulas are not organized in a tree (as it is in [4]). We noticed that an interpolation theorem for such a proof system, and, in fact, for its first-order extension LK(CP), is an immediate consequence of a universal interpolation theorem for semantic derivations [16, Thm. 5.1] (the monotone interpolation for R(CP) needs an extra argument).

Let us explain first briefly how lower bounds for CP ([4, 16, 21]) were obtained. All these lower bounds use effective interpolation theorem. The idea of using effective interpolation for length-of-proofs lower bounds (proposed in [14]) is the following one. Let $A, B \subseteq \{0,1\}^*$ be two disjoint NP-sets. By NP-completeness of the satisfiability each set $A_n := A \cap \{0,1\}^n$ can be defined as

$$A_n := \{(x_1, \ldots, x_n) \in \{0,1\}^n \mid \exists y_1, \ldots, y_m \; \alpha_n(x, y)\}$$

where α_n is a CNF propositional formula of size (i.e., number of symbols) $n^{O(1)}$. Similarly $B_n := B \cap \{0,1\}^n$ is defined using $\beta_n(x, z)$. Then $A_n \cap B_n = \emptyset$ implies that

$$\alpha_n(x, y) \longrightarrow \neg\beta_n(x, z)$$

is a tautology, and any its interpolant $I(x)$ defines the set I separating A_n from B_n: $A_n \subseteq I \wedge I \cap B_n = \emptyset$. The idea of lower bounds is to find two disjoint NP-sets A, B such that any set separating A_n from B_n must be complex and, at the same time, to establish for a particular proof system P effective interpolation, i.e., to show that implications with short P-proofs must have interpolants of low complexity. This implies a lower bound for P-proofs of implications $\alpha_n \longrightarrow \neg\beta_n$ as otherwise A_n and B_n could be separated by a set of low complexity, contradicting thus the choice of A, B.

As noted in [14], the complexity of an interpolant must be measured in a computational model at least as strong as Boolean circuits (any circuit of size m is the unique interpolant of an implication with resolution proof of size $O(m)$). As no non-trivial lower bounds are known for the size of general circuits, it makes no sense to use any stronger model.

However, [23, 2, 1] provide lower bounds for monotone Boolean circuits and in the applications of effective interpolation to lower bounds monotone effective interpolation is thus used (cf.[4, 16, 21]). It says that if A is closed upwards (or B downwards) then a separating set exists that is closed upwards. It is natural then to measure its complexity in a monotone computational model. The ingredient allowing to improve in [21] upon [4, 16] is to consider monotone computations in a stronger model than is the Boolean. Namely, circuit computations over reals using non-decreasing functions. An important part of [21] is the proof of an exponential lower bound for such a model (cf. [11] for an independent proof).

In principle, one may try to use yet stronger models of monotone computations in estimating the complexity of monotone interpolants for stronger proof systems. In reality however, only one other model (monotone span programs) with relevant bounds is know in this connection ([3] provide the bounds, [22] provide the connection to interpolation).

The paper is organized as follows. In Section 1 we derive from [16, Thm. 5.1] an interpolation theorem for semantic derivations over discretely ordered $\mathbf{Z}$ -modules. The definitions of LK(CP) and R(CP) are given in Section 2, and we note there a connection to CP with the deduction rule. An interpolation theorem and a conditional lower bound for LK(CP) are proved in Section 3. In Section 4 we give another particular case of semantic derivations; namely for hypersurfaces defined by sparse polynomials (polynomials with few monomials). In Section 5 we prove a monotone interpolation for semantic derivations of polyhedra. This yields a monotone interpolation and an unconditional lower bound for R(CP) in Section 6. The proof system LK(CP) may be viewed as an example of two-sorted theories of discretely ordered modules. We discuss this, and related topics, in Section 7.

The lower bounds (and effective interpolation theorems) in Sections 3, 5 and 6 depend, in particular, on the maximum size of coefficients in proofs. This appears to be caused by the fact that the interpolation theorems we obtain use Boolean circuits. This, in turn, is because [16, Thm. 5.1] is based on Boolean communication complexity. If we could upgrade the monotone part of [16, Thm. 5.1] to use the power of monotone real circuits then we could improve the monotone interpolation theorem for R(CP) (Theorem 6.1) and the resulting lower bounds (Corollaries 6.2 and 6.3), making them independent of the size of coefficients in proofs. We discuss this in Section 8.

Propositional proof systems are deeply rooted in both mathematical logic and computational complexity theory. They provide several deep connections between the two fields. The reader may consult [15] for basic information on these topics.

Integers as well as their tuples will be denoted $a, b, \ldots$ (variables $x, y, \ldots$). If a is a tuple then its elements are denoted $a_1, \ldots, a_n$. The scalar product of tuples a and x is denoted $a \cdot x$.

1 Semantic derivations over discretely ordered $\mathbf{Z}$ -modules

Let us first recall the definition of semantic derivations introduced in [16] and the particular notion of the communication complexity of a set considered there (Definitions 4.1 and 4.3). A semantic rule allows to infer a set C from two sets A, B (tacitly all subsets of a fixed universe, most often $\{0,1\}^N$) provided $C \supseteq A \cap B$. A semantic derivation of a set C from sets A_i is a sequence $B_1, \ldots, B_k$ such that $B_k = C$ and every B_j is either one of A_i or derived from earlier B_{j_1}, B_{j_2} by the semantic rule. A semantic refutation is a semantic derivation of the empty set.

Let $N = n+s+t$ be fixed and let $A \subseteq \{0,1\}^N$. Let $u, v \in \{0,1\}^n$, $q^u \in \{0,1\}^s$ and $r^v \in \{0,1\}^t$. Consider three tasks:

1. Decide whether $(u, q^u, r^v) \in A$.
2. Decide whether $(v, q^u, r^v) \in A$.
3. If $(u, q^u, r^v) \in A \not\equiv (v, q^u, r^v) \in A$ find $i \leq n$ such that $u_i \neq v_i$.

These tasks can be solved by two players, one knowing u, q^u and the other one knowing v, r^v. The communication complexity of A, $CC(A)$, is the minimal number of bits they need to exchange in the worst case in solving any of these three tasks.

We shall denote the minimal positive element of a discretely ordered $\mathbf{Z}$ -module $\mathbf{M}$ by 1. This defines an embedding of $\mathbf{Z}$ in $\mathbf{M}$. In particular, we may think that $\{0,1\} \subseteq \mathbf{M}$.

Lemma 1.1 *Let $\mathbf{M}$ be a discretely ordered $\mathbf{Z}$ -module, let $N = n+s+t$ and let*

$$H : \{0,1\}^N \to \mathbf{M}^W$$

be a linear map given by a $\mathbf{Z}$ -matrix whose entries have the absolute value at most M.

Let $Y \subseteq \mathbf{M}^W$ be an arbitrary set and put

$$X := H^{(-1)}(Y)$$

Then

$$CC(X) = O(W \log(MN)) + \log(n)\log(Mn)$$

Proof :

Let the i^{th} coordinate of $H(x,y,z)$ be the scalar product

$$h_{i,-} \cdot (x,y,z)$$

where $h_{i,-}$ is the i^{th} row of H.

1. The players first compute $h_{1,-} \cdot (x, y, z)$ for $(x, y, z) := (u, q^u, r^v)$ and for $(x, y, z) := (v, q^u, r^v)$. This needs $O(\log(MN))$ bits. If these numbers agree, they move on to $h_{i,-} \cdot (x, y, z)$ for $i > 1$. There are W of them, so totally there are $O(W \log(MN))$ bits.

2. If they disagreed on the value of some $h_{i,-} \cdot (x, y, z)$, it means that they disagree about the value of $\sum_{j=1}^{n} h_{i,j} \cdot x_j$ for $x := u$ and $x := v$ respectively. Then they use binary search to find j s.t. $u_j \neq v_j$. This needs $\leq \log(n) \log(Mn)$ bits.

3. If they agreed on all values computed in part 1 then each player figures the truth-value of $H(x, y, z) \in Y$ on his own; no new bits of communication.

Thus $CC(X)$ is at most

$$O(W \log(MN)) + \log(n) \log(Mn)$$

q.e.d.

Let $N = n + s + t$ be fixed for the rest of the section. For $A \subseteq \{0,1\}^{n+s}$ define the set $\tilde{A}$ by:

$$\tilde{A} := \bigcup_{(a,b) \in A} \{(a, b, c) \mid c \in \{0,1\}^t\}$$

where a, b, c range over $\{0,1\}^n$, $\{0,1\}^s$ and $\{0,1\}^t$ respectively, and similarly for $B \subseteq \{0,1\}^{n+t}$ define $\tilde{B}$:

$$\tilde{B} := \bigcup_{(a,c) \in B} \{(a, b, c) \mid b \in \{0,1\}^s\} \ .$$

Theorem 1.2 *Let $A_1, \ldots, A_m \subseteq \{0,1\}^{n+s}$ and $B_1, \ldots, B_\ell \subseteq \{0,1\}^{n+t}$. Let $\mathbf{M}$ be a discretely ordered $\mathbf{Z}$ -module.*

Assume that $Y_1, \ldots, Y_k \subseteq \mathbf{M}^W$ are arbitrary sets and that

$$H_i : \{0,1\}^N \rightarrow \mathbf{M}^W$$

are linear maps given by $\mathbf{Z}$ -matrices with all entries having the absolute value at most M. Put $X_i := H_i^{(-1)}(Y_i)$.

If $X_1, \ldots, X_k$ is a semantic refutation of the sets $\tilde{A}_1, \ldots, \tilde{A}_m$, $\tilde{B}_1, \ldots, \tilde{B}_\ell$ then the two sets

$$U = \{u \in \{0,1\}^n \mid \exists q^u \in \{0,1\}^s; (u, q^u) \in \bigcap_{j \leq m} A_j\}$$

and

$$V = \{v \in \{0,1\}^n \mid \exists r^v \in \{0,1\}^t; (v, r^v) \in \bigcap_{j \leq \ell} B_j\}$$

can be separated by a Boolean circuit of size at most

$$(k+2n)(MN)^{O(W)}(Mn)^{O(\log n)}$$

Proof :
By Lemma 1.1 it holds that $CC(X_i) \leq \mu$ where

$$\mu = O(W \log(MN)) + \log(n)\log(Mn)$$

By [16, Thm. 5.1] the sets U, V can be separated by a circuit of size $(k+2n)2^{O(\mu)}$.

q.e.d.

To saturate the reader's curiosity let us outline briefly the proof of Theorem 5.1 in [16]. First a semantic refutation is turned into a general protocol (in a form of a particular directed acyclic graph) for the Karchmer - Wigderson game on U, V (cf.[13]). Using a construction due to Razborov [24] the protocol is further transformed into a circuit separating U from V.

2 Examples of proof systems

We shall consider several proof systems to which we shall be able to apply Theorem 1.2.

Definition 2.1 CP-inequality *is of the form* $a \cdot x \geq b$, *with* $a \in \mathbf{Z}^n$, $b \in \mathbf{Z}$, *and* x *ranging over* $\mathbf{Z}^n$. Free variables *in it are* $x = (x_1, \ldots, x_n)$. *Numbers* $a_1, \ldots, a_n, b$ *are* constants.

CP-formula *is any formula of first-order predicate calculus with atomic formulas being the CP-inequalities.*

In particular, a_i's and b are never quantified in CP-formulas.

Definition 2.2 LK(CP) *is the first-order sequent calculus working with CP-formulas whose inference rules are:*

1. *All LK-rules with the usual conventions on variables in the quantifier rules (cf. [26]).*
2. *All CP-rules:*

   (a)

$$\frac{\Gamma \longrightarrow \Delta, a \cdot x \geq b \qquad \Gamma \longrightarrow \Delta, a' \cdot x \geq b'}{\Gamma \longrightarrow \Delta, (a+a') \cdot x \geq (b+b')}$$

(b)

$$\frac{\Gamma \longrightarrow \Delta, a \cdot x \geq b}{\Gamma \longrightarrow \Delta, ca \cdot x \geq cb}$$

where $c \geq 0$

(c)

$$\frac{\Gamma \longrightarrow \Delta, a \cdot x \geq b}{\Gamma \longrightarrow \Delta, a' \cdot x \geq b'}$$

where all $a_i = n \cdot a'_i$ *and* $b' = \lceil \frac{b}{n} \rceil$ *for some natural number* $n \geq 1$.

(d)

$$\frac{}{\longrightarrow x_i \geq 0} \quad \textit{and} \quad \frac{}{\longrightarrow -x_i \geq -1}$$

(e) Two new rules (allowing to manipulate $\neg$*):*

$$\frac{}{\longrightarrow a \cdot x \geq b, (-a) \cdot x \geq -b+1}$$

and

$$\frac{}{a \cdot x \geq b, (-a) \cdot x \geq -b+1 \longrightarrow}$$

one for each $a \in \mathbf{Z}^n, b \in \mathbf{Z}$.

Definition 2.3 *R(CP) is the subsystem of LK(CP) that uses no logical connectives or quantifiers.*

Here are some examples of subsystems of LK(CP) and of proofs.

Example 1: CP itself is a subsystem of R(CP) and LK(CP).

Example 2: R(CP) is polynomially equivalent to resolution working with clauses formed by CP-inequalities, and admitting CP-rules. Here we define $\neg(a \cdot x \geq b)$ to be $(-a) \cdot x \geq -b+1$.

Example 3: CP *with the deduction rule* as defined in [4]. Refutations in such a system have two parts. The first part of a refutation of the set of CP-inequalities $\{B_1, \ldots, B_k\}$ consists of a balanced binary tree of height h with nodes labelled by CP-inequalities and outgoing edges labelled by YES/NO. Every path v_0(= the root)$, \ldots, v_h$ defines a set of CP-inequalities $\{A_0, \ldots, A_{h-1}\}$ such that A_i is the label (resp. its negation) of v_i if the edge (v_i, v_{i+1}) is labelled by YES (resp. by NO). The rest of the refutation consists of 2^h CP-refutations of all sets $\{B_1, \ldots, B_k\} \cup \{A_0, \ldots, A_{h-1}\}$, one for each path in the tree.
Clearly such refutation can be transformed into R(CP) - refutation of the set $\{B_1, \ldots, B_k\}$ with proportional number of proof steps. Note that the original splitting of the proof need not to be tree-like in the formalization via R(CP).

Example 4: LK(CP) can define the congruence relation modulo any fixed $m \in \mathbf{Z}$. It is then easy to see that LK(CP) proves all counting principles modulo m (see [15, Chpt. 12] or [5] for a definition) in polynomial size.

3 Interpolation theorem and conditional lower bound for LK(CP)

Now we derive a corollary of Theorem 1.2 for LK(CP).

Theorem 3.1 *Let $E_1(x,y),\ldots,E_m(x,y),F_1(x,z),\ldots,F_\ell(x,z)$ be a system of CP-inequalities in which occur only the displayed variables $x=(x_1,\ldots,x_n)$, $y=(y_1,\ldots,y_s)$ and $z=(z_1,\ldots,z_t)$. Let $N:=n+s+t$. Assume that there is an LK(CP)-refutation π of the system such that:*

1. *π contains $k(\pi)$ inferences.*
2. *Every coefficient occurring in a CP-inequality in π has the absolute value at most M.*
3. *Every sequent in π has at most W occurrences of atomic formulas.*

Then there is an interpolant $I(x)$ of the implication:

$$\bigwedge_{i\leq m} E_i(x,y) \longrightarrow \bigvee_{j\leq \ell} \neg F_j(x,z)$$

whose Boolean circuit-size is at most $(k(\pi)+2n)(MN)^{O(W)}(Mn)^{O(\log n)}$.

Proof :

Let S' denote the closure of a sequent S w.r.t. to all free variables other than x's, y's, and z's. Note that the atomic formulas in S and S' are the same. An atomic formula in such an S' has the form

$$e\cdot\xi + f\cdot\chi \geq d$$

where $\xi=(\xi_1,\xi_2,\ldots)$ are among the free variables of S' (and hence among x,y,z), and χ are the bounded variables. Thus $e\cdot\xi$ is just $h\cdot(x,y,z)$ for some integer vector h. Let $h^{S'}_{i,-}\cdot(x,y,z)$, $i=1,\ldots,W$, be all such expressions occurring in S' and let $H_{S'}$ be the $W\times N$-matrix with rows $h^{S'}_{i,-}$.

Let $S'(\alpha_1,\ldots,\alpha_W)$ be S' with terms $h^{S'}_{i,-}\cdot(x,y,z)$ replaced by variables α_i. Hence $S'=S'(\alpha_i/(h^{S'}_{i,-}\cdot(x,y,z)))$ and there are no other free variables in $S'(\alpha_1,\ldots,\alpha_W)$ other than $\alpha_1,\ldots,\alpha_W$. Define $Y_{S'}\subseteq \mathbf{M}^W$ to be the set of all $(a_1,\ldots,a_W)$ such that $S'(a_1,\ldots,a_W)$ is true.

If $\pi=S_1,\ldots,S_k$ is an LK(CP)-refutation of $E_1,\ldots,F_\ell$ then $X_1,\ldots,X_k$ with $X_i:=H^{(-1)}_{S'_i}(Y_{S'_i})$, is a semantic refutation of $\tilde{E}_1,\ldots,\tilde{F}_\ell$ (as all rules are sound).

Theorem 1.2 then implies the statement.

q.e.d.

Note that if the starting tree in a refutation in CP with the deduction rule (Example 3 in Section 2) has the height h than every clause in the R(CP)-translation has at most $W = h + 1$ elements. In particular, $W \leq \log_2 k(\pi)$ and we have a bound for interpolation for CP with the deduction rule. An interpolation theorem for CP with the deduction rule with the deduction assumptions arranged in a tree was proved in [12].

Effective interpolation yields proof-theoretic lower bounds as explained in the introduction.

Theorem 3.2 *Assume that there are two disjoint NP-sets U, V such that any set I separating U from V (i.e., $U \subseteq I \wedge V \cap I = \emptyset$) has the circuit-size at least $\exp(n^{\Omega(1)})$. Then for every n there is a set of $n^{O(1)}$ CP-inequalities in which all coefficients are $0, 1$ or -1 and such that for every LK(CP)-refutation π of the set the following holds. If every sequent in π has at most W atomic formulas and every coefficient in π has the absolute value at most M then*

$$k \cdot (Mn)^{O(W \log n)} \geq \exp(n^{\Omega(1)})$$

Proof :

Take $n^{O(1)}$ CP-inequalities E_i such that $U \cap \{0,1\}^n$ is defined as

$$U = \{x \in \{0,1\}^n \mid \exists y \in \{0,1\}^s; \bigwedge_i E_i(x, y)\}$$

and similarly F_j's for V. Any interpolant of the implication

$$\bigwedge_i E_i \rightarrow \bigvee_j \neg F_j$$

defines a set separating U from V.

The theorem then follows from Theorem 3.1.

q.e.d.

The hypothesis of Theorem 3.2 follows, for example, from the cryptographic conjectures assuming the existence of strong one-way functions. See [16, 18] for a discussion.

4 Interpolation for sparse polynomials

A sparse polynomial is a polynomial with few monomials.

Lemma 4.1 *Let R be a commutative ring with 1, let $N = n + s + t$, and let*

$$F : \{0,1\}^N \rightarrow R$$

be a polynomial map. Assume that the polynomial F has L monomials. Then

$$CC(Ker\ F) = O(L) + \log n$$

Proof :

The players first evaluate all monomials in F for $(x,y,z) = (u,q^u,r^v)$ and for $(x,y,z) = (v,q^u,r^v)$, distinguishing the x, y, and z parts of the monomials. This needs $O(L)$ bits.

If they disagree about the value of some monomial in x's then they use binary search (at most $\log n$ bits) to find i such that $u_i \neq v_i$.

q.e.d.

The following theorem provides an interpolation theorem for semantic derivations with hypersurfaces defined by sparse polynomials. It thus yields an interpolation and a conditional lower bound (analogously to Section 3) for polynomial calculus proofs over arbitrary ring R where all polynomials have few monomials (see [5] for polynomial calculus). [6] gave interpolation for constant degree polynomial calculus.

Theorem 4.2 *Let $A_1,\dots,A_m \subseteq \{0,1\}^{n+s}$ and $B_1,\dots,B_\ell \subseteq \{0,1\}^{n+t}$. Let R be a commutative ring with 1.*

Assume that

$$F_i : \{0,1\}^N \to R$$

are polynomial maps given by polynomials from $R[x,y,z]$ with all F_i having at most L monomials. Put $X_i := Ker\ F_i$.

If $X_1,\dots,X_k$ is a semantic refutation of the sets $\tilde{A}_1,\dots,\tilde{A}_m$, $\tilde{B}_1,\dots,\tilde{B}_\ell$ then the two sets

$$U = \{u \in \{0,1\}^n \mid \exists q^u \in \{0,1\}^s; (u,q^u) \in \bigcap_{j\le m} A_j\}$$

and

$$V = \{v \in \{0,1\}^n \mid \exists r^v \in \{0,1\}^t; (v,r^v) \in \bigcap_{j\le \ell} B_j\}$$

can be separated by a Boolean circuit of size at most

$$kn^{O(1)}2^{O(L)}$$

Proof :

By Lemma 4.1 $CC(X_i) \le O(L) + \log n$. By [16, Thm. 5.1] the sets U and V can be separated by a Boolean circuit of size $(k+2n)2^{O(L+\log n)} = kn^{O(1)}2^{O(L)}$.

q.e.d.

5 Monotone interpolation for semantic derivations of polyhedra

Let $N = n + s + t$ be fixed and let $A \subseteq \{0,1\}^N$. Let $u, v \in \{0,1\}^n$, $q^u \in \{0,1\}^s$ and $r^v \in \{0,1\}^t$. We shall recall now the definition of the monotone communication complexity of a set from [16, Def. 4.3]. Consider the following task for two players, a player I knowing $u \in \{0,1\}^n$ and $q^u \in \{0,1\}^s$, and player II knowing $v \in \{0,1\}^n$ and $r^v \in \{0,1\}^t$.

4. If $(u, q^u, r^v) \in A$ and $(v, q^u, r^v) \notin A$ either find $i \leq n$ such that

$$u_i = 1 \wedge v_i = 0$$

or decide that there is some u' satisfying

$$u' \geq u \wedge (u', q^u, r^v) \notin A$$

($u' \geq u$ means $\bigwedge_{i \leq n} u'_i \geq u_i$.)

The monotone communication complexity w.r.t. U of A, $MCC_U(A)$, is the minimal $\mu \geq CC(A)$ such that the task 4. can be solved by communicating at most μ bits in the worst case.

We shall denote by $Q(b)$ the subset of $\mathbf{M}^W$ of the form

$$Q(b) = \{a \in \mathbf{M}^W \mid \forall i \leq W; a_i \leq b_i - 1\}$$

Note that an inverse image of $Q(b)$ in any linear map $H : \mathbf{M}^N \to \mathbf{M}^W$ is a polyhedron in $\mathbf{M}^N$.

Lemma 5.1 *Let $\mathbf{M}$ be a discretely ordered $\mathbf{Z}$ -module, let $N = n+s+t$ and let*

$$H : \{0,1\}^N \to \mathbf{M}^W$$

be a linear map given by a $\mathbf{Z}$ -matrix whose entries have the absolute value at most M.

Let $Y \subseteq \mathbf{M}^W$ be any set of the form

$$Y = \mathbf{M}^W \setminus Q(b)$$

for some $b \in \mathbf{M}^W$. Put $X := H^{(-1)}(Y)$.

Then

$$MCC_U(X) = O(W \log(MN)) + O(W \log(n) \log(Mn))$$

Proof :

The players communicate as in the first step in the proof of Lemma 1.1 to establish the membership (u, q^u, r^v) and (v, q^u, r^v) in X. This needs

$$O(W \log(MN))$$

bits.

Assume $(u, q^u, r^v) \in X$ while $(v, q^u, r^v) \notin X$. Obviously we may disregard q^u, r^v, changing possibly b_i into

$$b_i' := b_i - \sum_{j=n+1}^{j=n+s} h_{i,j} q_j^u - \sum_{j=n+s+1}^{j=n+s+t} h_{i,j} r_j^v$$

as these sums are known to both players after the first step.

Let G be the $W \times n$ matrix consisting of the first n columns of H. The fact that $(u, q^u, r^v) \in X$ while $(v, q^u, r^v) \notin X$ is equivalent to $\bigvee_{i \leq W} g_{i,-} \cdot u \geq b_i'$ and $\bigwedge_{i \leq W} g_{i,-} \cdot v < b_i'$, i.e. $\bigwedge_{i \leq W} g_{i,-} \cdot v \leq b_i' - 1$, respectively (where $g_{i,-}$ is the i^{th} row of G).

To solve the problem 4. defining $MCC_U(X)$ the players communicate as follows.

Player I first figures out whether for some $u' \geq u$ $(u', q^u, r^v) \notin X$, i.e., $\bigwedge_{i \leq W} g_{i,-} \cdot u' \leq b_i' - 1$. He communicates 1 bit of the answer to II, and they stop if it is affirmative.

Assume that there is no such $u' \geq u$. Then they proceed as follows. Recall that we have $G \cdot v \in Q(b')$ while $G \cdot u' \notin Q(b')$ for all $u' \geq u$.

1. Let $g_{-,j}$, $j = 1, \ldots, n$ be the columns of G. For $I \subseteq \{1, \ldots, n\}$ define

   $$G^I \cdot x := \sum_{j : j \in I \wedge x_j = 1} g_{-,j}$$

   Then $G^I \cdot u = \sum_{j : u_j = 1} g_{-,j} = G \cdot u$ and likewise for $G \cdot v$, for $I = \{1, \ldots, n\}$.

2. Let $I_1 = \{1, \ldots, \lfloor n/2 \rfloor\}$ and $I_2 = \{1 + \lfloor n/2 \rfloor, \ldots, n\}$. For $j = 1, 2$ put $c^j := G^{I_j} \cdot v$. Player II sends to I the vector c^1. This needs $W \log(\frac{Mn}{2})$ bits at most.

3. Note that $c^1 \in Q(c^1 + (1, \ldots, 1))$ and $c^2 \in Q(b' - c^1)$, and that

   (a) either for no J_1: $I_1 \supseteq J_1 \supseteq \{i \leq \lfloor n/2 \rfloor \mid u_i = 1\}$ is $\sum_{j \in J_1} g_{-,j} \in Q(c^1 + (1, \ldots, 1))$

   (b) or for no J_2: $I_2 \supseteq J_2 \supseteq \{i > \lfloor n/2 \rfloor \mid u_i = 1\}$ is $\sum_{j \in J_2} g_{-,j} \in Q(b' - c^1)$

   as otherwise $u' \geq u$ defined by $J_1 \cup J_2$ would contradict that for no $u' \geq u$ is $G \cdot u' \in Q(b')$.

4. So the players settle either for interval I_1 (in case (a)) or for I_2 (in case (b)). This is decided by player I and it needs 1 bit of communication.

5. The players continue in this fashion for at most $\log n$ rounds, always dividing the current interval into halves. This needs no more than

$$O(W \log(Mn) \log(n))$$

bits.

6. The players stop when holding an interval $\{j\}$ of length 1. It is easy to see that conditions (a) and (b) in 3. imply that $v_j = 0 \wedge u_j = 1$.

q.e.d.

For the next theorem we shall use the same notation as in Theorem 1.2.

Theorem 5.2 *Let $A_1, \ldots, A_m \subseteq \{0,1\}^{n+s}$ and $B_1, \ldots, B_\ell \subseteq \{0,1\}^{n+t}$, and assume that the sets $A_1, \ldots, A_m$ satisfy the following monotonicity condition w.r.t. U:*

$$(u, q^u) \in \bigcap_{j \leq m} A_j \wedge u \leq u' \ \rightarrow \ (u', q^u) \in \bigcap_{j \leq m} A_j$$

Let $\mathbf{M}$ be a discretely ordered $\mathbf{Z}$ -module.

Assume that $Y_1, \ldots, Y_k \subseteq \mathbf{M}^W$ are arbitrary sets of the form

$$Y_i = \mathbf{M}^W \setminus Q(b^i)$$

for some $b^1, \ldots, b^k \in \mathbf{M}^W$. Let

$$H_i : \{0,1\}^N \rightarrow \mathbf{M}^W$$

be linear maps given by $\mathbf{Z}$ -matrices with all entries having the absolute value at most M. Put $X_i := H_i^{(-1)}(Y_i)$.

If $X_1, \ldots, X_k$ is a semantic refutation of sets $\tilde{A}_1, \ldots, \tilde{A}_m$, $\tilde{B}_1, \ldots, \tilde{B}_\ell$ then the two sets

$$U = \{u \in \{0,1\}^n \mid \exists q^u \in \{0,1\}^s; (u, q^u) \in \bigcap_{j \leq m} A_j\}$$

and

$$V = \{v \in \{0,1\}^n \mid \exists r^v \in \{0,1\}^t; (v, r^v) \in \bigcap_{j \leq \ell} B_j\}$$

can be separated by a monotone Boolean circuit of size at most

$$(k+n)(MN)^{O(W \log(n))}$$

Proof :

By Lemma 5.1 it holds that $MCC_U(X_i) \leq \mu$ for $\mu = O(W \log(Mn) \log(n))$. By [16, Thm. 5.1] the sets U and V can be separated by a monotone Boolean circuit of size $(k+n)2^{O(\mu)}$.

q.e.d.

6 Monotone interpolation and unconditional lower bound for R(CP)

As there are known strong lower bounds for monotone circuits we shall be able to obtain an unconditional lower bound from Theorem 5.2. First we need to prove a monotone interpolation theorem for R(CP). It implies, in particular, a monotone interpolation theorem for CP with the deduction rule (similarly with the argument after Theorem 3.1). No monotone interpolation theorem was proved for CP with the deduction rule in [12].

Theorem 6.1 *Let $E_1(x, y), \ldots, E_m(x, y), F_1(x, z), \ldots, F_\ell(x, z)$ be a system of CP-inequalities in which occur only the displayed variables $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_s)$ and $z = (z_1, \ldots, z_t)$. Assume that all x_i occur in all $E_1, \ldots, E_m$ with non-negative coefficients only.*
Let $N := n + s + t$. Assume that there is an R(CP)-refutation π of the system such that:

1. *π contains $k(\pi)$ inferences.*
2. *Every coefficient occurring in a CP-inequality in π has the absolute value at most M.*
3. *Every clause in π has at most W occurrences of CP-inequalities.*

Then there is an monotone interpolant $I(x)$ of the implication:

$$\bigwedge_{i \leq m} E_i(x, y) \longrightarrow \bigvee_{j \leq \ell} \neg F_j(x, z)$$

whose monotone Boolean circuit-size is at most $(k(\pi) + n)(MN)^{O(W \log n)}$.

Proof :
Let $\{h_{i,-} \cdot (x, y, z) \geq b_i \mid i \leq W\}$ be a clause in π. Then the vector (x, y, z) satisfies the clause iff

$$H(x, y, z) \in \mathbf{M}^W \setminus Q((b_1, \ldots, b_W))$$

where H is the $W \times N$-matrix with rows $h_{i,-}$.
Thus π determines a semantic refutation $X_1, \ldots, X_k$ of $\tilde{E}_1, \ldots, \tilde{F}_\ell$ satisfying the hypothesis of Theorem 5.2. This proves the theorem.

q.e.d.

Theorem 6.1 yields a lower bound for R(CP), using the strong lower bound of [23, 2, 1] for the size of monotone circuits separating graphs on n vertices with a clique of size $\xi + 1$ from those that are ξ-colorable, for particular ξ.

$Clique_{n,\omega}$ and $Color_{n,\xi}$ are the sets of CP-inequalities defined before [16, Cor. 7.3]. Namely, let $n, \omega, \xi \geq 1$ be natural numbers, and let $\binom{n}{2}$ denote the set of two-element subsets of $\{1, \ldots, n\}$. The set $Clique_{n,\omega}(x, y)$ is a set of the following CP-inequalities in the variables x_{ij}, $\{i, j\} \in \binom{n}{2}$, and y_{ui}, $u = 1, \ldots, \omega$ and $i = 1, \ldots, n$:

(1a) $\sum_{i \leq n} y_{ui} \geq 1$, all $u \leq \omega$,

(1b) $1 - y_{ui} + 1 - y_{vi} \geq 1$, all $u < v \leq \omega$ and $i = 1, \ldots, n$,

(1c) $1 - y_{ui} + 1 - y_{vj} + x_{ij} \geq 1$, all $u < v \leq \omega$ and $\{i, j\} \in \binom{n}{2}$.

The set $Color_{n,\xi}(x, z)$ is the set of the following formulas in the variables x_{ij}, $\{i, j\} \in \binom{n}{2}$, and z_{ia}, $i = 1, \ldots, n$ and $a = 1, \ldots, \xi$:

(2a) $\sum_{a \leq \xi} z_{ia} \geq 1$, all $i \leq n$,

(2b) $1 - z_{ia} + 1 - z_{ib} \geq 1$, all $a < b \leq \xi$ and $i \leq n$,

(2c) $1 - z_{ia} + 1 - z_{ja} + 1 - x_{ij} \geq 1$, all $a \leq \xi$ and $\{i, j\} \in \binom{n}{2}$.

Corollary 6.2 *Let n be sufficiently large, $\xi := \lfloor \frac{1}{8}(n/\log n)^{2/3} \rfloor$ and $\omega := \xi + 1$. Let π be an R(CP)-refutations of the set $Clique_{n,\omega} \cup Color_{n,\xi}$ with $k = k(\pi)$ sequents. Assume that in every clause in π occurs at most W CP-inequalities, and that all coefficients have the absolute value at most M.*

Then

$$kM^{O(W \log^2 n)} \geq \exp(n^{\Omega(1)})$$

Proof :

A circuit interpolating

$$\bigwedge Clique_{n,\omega} \rightarrow \bigvee \neg Color_{n,\xi}$$

separates graphs (on n vertices) with a clique of size ω from those that are ξ-colorable. By [1] any such monotone Boolean circuit must have the size $\exp(N^{\Omega(1)})$. Hence the corollary follows from Theorem 6.1, using $N = n^{O(1)}$.

q.e.d.

As the height h of the initial tree in a refutation in CP with the deduction rule (see Example 3 in Section 1 for the definition) necessarily satisfies $h \leq \log_2 k$, also $W \leq h + 1 \leq \log_2 k + 1$ and we immediately get the following corollary.

Corollary 6.3 *Let n, ω, ξ be as in Corollary 6.2. Then every refutation of the set $Clique_{n,\omega} \cup Color_{n,\xi}$ in CP with the deduction rule, in which all coefficients have the absolute value at most M, must have at least*

$$\frac{\exp(n^{\Omega(1)})}{M^{O(\log^2 n)}}$$

proof steps.

7 Two-sorted Presburger arithmetic and discretely ordered modules

We may view CP-inequalities

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n \geq b$$

as formulas in a two-sorted Presburger arithmetic, thinking about **Z** itself as a **Z**-module. In general, let **M** be any discretely ordered R-module, R a commutative ring with 1. (We shall think of R as being an implicit part of the definition of M.) Its two-sorted theory T_M has terms

$$a_1 \cdot x_1 + \ldots + a_n \cdot x_n + a_{n+1} \cdot 1$$

with $a_1, \ldots, a_{n+1}$ constants of the first sort, the sort of the ring elements, $x_1, \ldots, x_n$ variables ranging over the second sort, the sort of the module elements, and 1 denoting the minimal positive element of **M** . Atomic formulas are equalities and inequalities (in the module language) among terms. M-formulas are first-order formulas built from these atomic formulas. The theory $T_{\mathbf{M}}$ consists of all **M** -sentences true in **M** . Note that only module elements are quantified.

Define a proof system LK(**M**) to be the first-order sequent calculus LK working with **M**-formulas and augmented by extra initial sequents

$$\longrightarrow A \ , \quad \text{one for each } A \in T_{\mathbf{M}}$$

Note that LK(**Z**) contains LK(CP) as all CP-rules of LK(CP) are derived rules of LK(**Z**).

Also note that the proof of Theorem 3.1 extends without changes to LK(**M**).

LK(**Z**) is, however, not a propositional proof system in the sense of [7] (or see [15, Chpt. 4]) as the set of the new initial sequents is not polynomial-time decidable (cf. [10]). Interesting subsystems of LK(**Z**) can be obtained as follows.

Let $A(\alpha_1, \ldots, \alpha_m, x_1, \ldots, x_n)$ be a formula in the language of LK(**Z**) with variables α_i of the sort of scalars and variables x_j of the sort of module elements (and as before with no quantified scalars). Define LK($A(\alpha, x)$) to be LK(CP) augmented by the following initial sequents

$$\longrightarrow A(a, u)$$

for $a \in \mathbf{Z}^m$ and $u \in \mathbf{Z}^n$, whenever $\mathbf{Z} \models A(a_1, \ldots, a_m, u_1, \ldots, u_n)$.

In [9] a form of quantifier elimination was proved for formulas A that do not contain the $\leq$ sign (i.e., all its atomic formulas are equations among terms) so that the polynomial-time decidability of the set

$$\{(a, u) \in \mathbf{Z}^{m+n} \mid \mathbf{Z} \models A(a, u)\}$$

follows. Hence if $A(\alpha, x)$ does not contain the $\leq$ sign, $\mathrm{LK}(A(\alpha, x))$ is a propositional proof system in the sense of [7]. It is an interesting open problem whether a form of quantifier elimination holds also when the sign $\leq$ is present. As remarked in [9] this appears to be linked to a formalizability of the algorithm from [19] for integer programming in a fixed dimension (or some other algorithm for the same problem, cf. [20]).

8 A communication complexity problem

The problem is to generalize [24, Thm. 3.1(b)], a theorem giving a characterization of circuit size in terms of communication complexity and PLS-problems, to monotone circuits over reals. The first step should be to generalize Karchmer-Wigderson game (cf. [13]) to get a characterization of the depth of monotone real circuits in terms of the number of rounds in some *real communication game*.

Definition 8.1 ([21]) *A* monotone real circuit *is a circuit that computes with reals using constants and binary non-decreasing functions at gates, and that outputs* 0 *or* 1 *on all Boolean inputs.*

The restriction to constants and binary functions is inessential; it is enough to have a bound to the arity. The depth and the size of a circuit is defined as usual.

A suitable characterization of the size of monotone real circuits would presumably allow to upgrade [16, Thm. 5.1] (the monotone part). The proof of [16, Thm. 5.1] uses the notion of a monotone protocol for a game on pair U, V defined in [16, Def. 2.2]. One would only measure its monotone communication complexity differently, using the new real game. A notion of a *real game* is studied in this connection in [17].

The application would be that we could remove the dependence on M in Theorem 6.1, obtaining a monotone real circuit as an interpolant. Using the lower bound for monotone real circuit size obtained in [21, Thm. 6] for monotone real circuits separating graphs on n vertices with a clique of size $\xi+1$ from those that are ξ-colorable, for the same ξ as in Section 6 (or see [11] for another lower bound), we would get a strengthening of Corollaries 6.2 and 6.3 by removing the dependence on M.

As monotone real circuits are at least as strong as monotone circuits over any linear order we could, presumably, generalize Theorem 6.1 to $\mathrm{LK}(\mathbf{M})$, any $\mathbf{M}$.

Note that it makes no sense to consider real circuits computing with arbitrary functions as a real may encode any countable information. In fact, [25] implies that even circuits computing with non-decreasing functions from inputs $x_i, \neg x_i$ can compute every Boolean function in polynomial size (as noted by J. Sgall).

References

[1] Alon, N., and Boppana, R. (1987) The monotone circuit complexity of Boolean functions, *Combinatorica*, **7(1)** : 1-22.

[2] Andreev, A. E. (1985) On a method for obtaining lower bounds for the complexity of individual monotone functions (in Russian), *Doklady AN SSSR*, **282(5)** : 1033-1037.

[3] Babai, L., Gál, A., Kollár, J., Rónyai, L., Szabó, T., and Wigderson, A. (1996) Extremal bipartite graphs and superpolynomial lower bounds for monotone span programs, in: *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pp.603-611. ACM Press.

[4] Bonet, M. L., Pitassi, T., and Raz, R. (1994) Lower bounds for cutting planes proofs with small coefficients, preprint.

[5] Buss, S., Impagliazzo, R., Krajíček, J., Pudlák, P., Razborov, A. A., and Sgall, J. (1996) Proof complexity in algebraic systems and constant depth Frege systems with modular counting, *Computational Complexity*, to appear.

[6] Clegg, M., Edmonds, J., and Impagliazzo, R. (1996) Using the Groebner basis algorithm to find proofs of unsatisfiability, in: *Proc. the 28th Annual ACM Symp. on Theory of Computing*, ACM Press, pp.174-183.

[7] Cook, S. A., and Reckhow, A. R. (1979) The relative efficiency of propositional proof systems, *J. Symbolic Logic*, **44(1)**: 36-50.

[8] Cook, W., Coullard, C. R., and Turán, G. (1987) On the complexity of cutting plane proofs, *Discrete Applied Mathematics*, **18**: 25-38.

[9] van den Dries, L. and Holly, J. (1992) Quantifier elimination for modules with scalar variables, *Annals of Pure and Applied Logic*, **57**: 161-179.

[10] Fisher, M. J., and Rabin, M. O. (1974) Superexponential complexity of Presburger's arithmetic, *SIAM-AMS Proceedings*, **7**: 27-41.

[11] Haken, A. and Cook, S.A. (1995) An exponential lower bound for the size of monotone real circuits, *J. of Computer and System Science*, to appear.

[12] Impagliazzo, R. and Pitassi, T. (1996) Interpolation for generalized cutting planes proof systems, a report in the CZ-US email seminar written by T. Pitassi.

[13] Karchmer, M., and Wigderson, A. (1988) Monotone circuits for connectivity require super - logarithmic depth, in: *Proc.* 20^{th} *Annual ACM Symp. on Theory of Computing*, pp.539-550. ACM Press.

[14] Krajíček, J. (1994) Lower bounds to the size of constant-depth propositional proofs, *Journal of Symbolic Logic*, **59(1)**: 73-86.

[15] —— (1995) *Bounded arithmetic, propositional logic and complexity theory*, Cambridge University Press.

[16] —— (1997) Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, *J. Symbolic Logic*, **62(2)**: 457-486.

[17] —— (1996) Interpolation by a game, *Mathematical Logic Quarterly*, to appear.

[18] Krajíček, J., and Pudlák, P. (1995) Some consequences of cryptographical conjectures for S_2^1 and EF, in: *Logic and Computational Complexity* (Proc. of the meeting held in Indianapolis, October 1994), Ed. D. Leivant, Springer-Verlag, Lecture Notes in Computer Science, Vol. **960**: 210-220.

[19] Lenstra, H. W. (1983) Integer programming with a fixed number of variables, *Math. Oper. Research*, **8**: 538-548.

[20] Lovász, L. (1986) *Algorithmic theory of numbers, graphs and convexity*, CBMS-NSF Regional conferences series in applied mathematics, Soc. for Industr. and Applied mathematics, Philadelphia.

[21] Pudlák, P. (1995) Lower bounds for resolution and cutting planes proofs and monotone computations, *J. Symbolic Logic*, to appear.

[22] Pudlák, P. and Sgall, J. (1996) Algebraic models of computation, and interpolation for algebraic proof systems, preprint.

[23] Razborov, A. A. (1985) Lower bounds on the monotone complexity of some Boolean functions, *Soviet Mathem. Doklady*, **31** : 354-357.

[24] —— (1995) Unprovability of lower bounds on the circuit size in certain fragments of bounded arithmetic, *Izvestiya of the R.A.N.*, **59(1)**: 201-224.

[25] Rosenbloom, A. (1997) Monotone real circuits are more powerful than monotone boolean circuits, *Information Processing Letters*, **61**: 161-164.

[26] Takeuti, G. (1975) *Proof theory*, North-Holland.

Current address:
Mathematical Institute
Oxford University
24-29 St.Giles', Oxford
OX1 3LB, G.B.
`krajicek@math.cas.cz`