Electronic Colloquium on Computational Complexity, Report No. 10 (2007)

Improved Lower Bounds for Resolution over Linear Inequalities *

Arist Kojevnikov

St.Petersburg Department of Steklov Institute of Mathematics
27 Fontanka, 191023 St.Petersburg, Russia
http://logic.pdmi.ras.ru/~arist/

Abstract. We continue a study initiated by Krajíček of a Resolution-like proof system working with clauses of linear inequalities, R(CP). For all proof systems of this kind Krajíček proved in [1] an exponential lower bound of the form:

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

where M is the maximal absolute value of coefficients in a given proof and W is the maximal clause width.
In this paper we improve this lower bound for two restricted versions of R(CP)-like proof systems. For tree-like R(CP)-like proof systems we remove a dependence on the maximal absolute value of coefficients M, hence, we give the answer to an open question from [2]. Proof follows from an upper bound on the real communication complexity of a polyhedra. For R(CP) we remove a dependence on the maximal clause width W. Proof follows from the fact that in R(CP) at each step we modify at most one inequality in a clause. Hence, we can use information about other inequalities from previous steps and do not need to check all inequalities in the clause.

Key words: propositional proof complexity, integer programming, cutting planes

Many well known methods in an area of pseudo-boolean constraints optimization like a branch-and-bound [3] and Cutting Planes with the deduction rule [4] can be defined in terms of Resolution proof system that operates with clauses of linear inequalities, R(CP) [1]. This proof system is a natural extension of Resolution and can be viewed as a generalization of Resolution over formulas in k-DNF, Res(k), that was introduced in [5]. In the last few years much attention was paid to complexity of Res(k) [6–8]. From the other hand, it is not much known about the complexity of R(CP), while it and similar proof systems are often used in practice [9–11].

Consider a R(CP)-like proof system as a system that work with clauses of linear inequalities using finite set of tautologically valid axioms and sound deriva-

* Supported in part by Russian Science Support Foundation, INTAS (grant 04-83-3836) and RFBR (grants 05-01-00932, 06-01-00502). The paper was done during the stay of the author at the Max-Planck-Institut für Mathematik, Bonn, Germany.

ISSN 1433-8092

tion rules with at most two hypotheses. The main goal of this paper is to improve lower bounds on restricted but still very important families of R(CP)-like proof systems. Namely, we proved better lower bounds for tree-like R(CP)-like proof systems and R(CP)-like proof systems with the following restriction on the derivation rule: all but at most one inequalities in any of two hypotheses are contained in the conclusion. The later restriction is very natural, for example, all rules of R(CP) satisfy it, and it is hard to design a derivation rule with two hypotheses that does not satisfy it. We denote all proof systems with the last restriction as *passive* R(CP)-like proof systems.

The main idea of exponential lower bounds that based on monotone interpolation theorem is a transformation of a proof P of the formula F into a monotone circuit C of size polynomial in $|P|$. If the formula F formalizes that the intersection of two disjoint NP-sets is not empty, then the circuit C separates these two disjoint NP-sets. For example, the pair of disjoint NP-sets, consisting of a set of graphs with a k-clique and the set of $(k-1)$-colorable graphs, the monotone circuit that separates one set from another has at least exponential size [12]. Hence, the size of proof P is exponential.

There is a very nice connection between boolean circuits and communication complexity [13], and sometimes it is more easier to think in terms of communication complexity then in terms of circuits. This idea was used by Krajíček to prove many important exponential lower bounds in [14, 1, 2]. He reduced the proof-into-circuit transformation problem into a problem of proving upper bounds on communication complexity of specific decision problems.

In this paper we give an answer to one of the open questions from [2]: we prove new upper bound on real monotone communication complexity of a polyhedra and, hence, a better lower bound for tree-like R(CP)-like proof systems. The proof is straightforward. The basic techniques are the same as in [14, 1, 2].

For passive R(CP)-like proof systems we introduce a minor modification in general semantic derivation protocol that allows us also to obtain better lower bounds. We explain the new idea in the following.

Let $U, V \subseteq \{0,1\}^n$ be two disjoint NP-sets. We define a formula $E(x,y) \wedge F(x,z)$ such that U is a set of partial assignments on x that can be extended to assignments satisfying E, and V is a set of partial assignments on x that can be extended to assignments satisfying F. Informally speaking, we use G to transform a refutation π of the formula $E(x,y) \wedge F(x,z)$ into the real game of two players A and B. The player A knowing a satisfying assignment (u,y) of subformula E and the player B knowing a satisfying assignment (v,z) of subformula F attempt to construct a path $P = P_0, \ldots, P_h$ through the refutation π to find such i that $u_i \neq v_i$.

The protocol G is defined by induction on a size of the refutation π. Players start from the last line of π, empty clause $\emptyset = P_0$ and P_{j+1} is one of the two clauses that are hypotheses of an inference rule

$$\frac{X \qquad Y}{P_j}$$

that derives P_j in π such that both tuples (u, y, z) and (v, y, z) *do not* satisfy P_{j+1}. Players first determine whether (u, y, z) and (v, y, z) satisfy X. Since the inference rule is sound, there are three possibilities:

1. both (u, y, z) and (v, y, z) satisfy X and therefore none of (u, y, z) and (v, y, z) satisfy Y,
2. none of (u, y, z) and (v, y, z) satisfy X,
3. only one of (u, y, z) and (v, y, z) satisfy X.

In the first case players' strategy $S(u, v, P_j)$ is to take Y, in the second case they take X. In the third case players stop constructing the path and find a natural number i that $u_i \neq v_i$. Such i must exists as necessarily $u \neq v$. As none of the E or F cannot be both satisfied by (u, y, z) and (v, y, z) the players must eventually enter the possibility 3 and find such i that $u_i \neq v_i$.

Actually, in Krajíček's proof of [14, Theorem 5.1] we need only to change a part of the strategy $S(u, v, P_j)$ testing that (u, y, z) and (v, y, z) satisfy X. Since X is a clause and $(|X| - p)$ of its inequalities are not satisfied by (u, y, z) and (v, y, z) (they are contained in P_i that is not satisfied by (u, y, z) and (v, y, z)) we need to check only the remaining p inequalities.

This simple idea allows us to improve the lower bound for the case of p-passive systems.

The paper is organized as follows. In Sect. 1 we give all necessary definitions, in Sect. 2 we recall the notion of interpolation and prove new lower bound on tree-like R(CP)-like proof systems. In Sect. 3 we propose the simple protocol modification to remove the dependence on the maximal clause width in the lower bound for passive R(CP)-like proof systems.

1 Definitions

In this paper we use the following notation: we typically denote integer vectors with letters a, b, c, their coordinates with a_i, b_i, c_i, vectors of Boolean variables with u, v, w, x, y, z and integers with A, B, C. We will write $a \cdot x$ instead of $\sum_i a_i x_i$.

1.1 Resolution over linear inequalities

Now we describe several propositional proof systems for the language of systems of linear inequalities that have no 0/1-solutions. A proof system R(CP) was defined in [1] as follows. The lines of the system are disjunctions of linear inequalities: $a \cdot x \geq A \vee \ldots \vee b \cdot x \geq B$. The derivation rules are (we denote by $\mathit{\Gamma}$ an arbitrary disjunction of linear inequalities)

$$\frac{a \cdot x \geq A \vee \mathit{\Gamma} \qquad b \cdot x \geq B \vee \mathit{\Gamma}}{(a+b) \cdot x \geq A + B \vee \mathit{\Gamma}} \ , \qquad \frac{a \cdot x \geq A \vee \mathit{\Gamma}}{Ca \cdot x \geq CA \vee \mathit{\Gamma}} \ , \quad \text{where } C \geq 0 \ ,$$

$$\frac{Ca \cdot x \geq A \vee \mathit{\Gamma}}{a \cdot x \geq \lceil A/C \rceil \vee \mathit{\Gamma}} \ , \qquad \frac{}{x_i \geq 0} \qquad \frac{}{-x_i \geq -1} \quad \text{for all variables } x_i \ ,$$

$$\frac{}{a \cdot x \geq A \vee (-a) \cdot x \geq 1 - A} \ , \quad \frac{\mathit{\Gamma}}{a \cdot x \geq A \vee \mathit{\Gamma}} \ , \quad \frac{a \cdot x \geq A \vee a \cdot x \geq A \vee \mathit{\Gamma}}{a \cdot x \geq A \vee \mathit{\Gamma}} \ .$$

Note that one can omit $0 \geq 1$ from $0 \geq 1 \vee \mathit{\Gamma}$ because the contradiction $0 \geq 1$ is easily transformable into any other inequality. The goal is to derive $0 \geq 1$.

We also define a family of R(CP)-like proof systems, that operate with disjunctions of linear inequalities by finite set of tautologically valid axioms and sound derivation rules that have at most two hypotheses. We are interested in its sub-family of *p-passive* R(CP)-like proof systems, where all derivation rules are of the form

$$\frac{\mathit{\Delta}_1 \vee \mathit{\Gamma}_1 \qquad \mathit{\Delta}_2 \vee \mathit{\Gamma}_2}{\mathit{\Delta}_3 \vee \mathit{\Gamma}_1 \vee \mathit{\Gamma}_2} \ ,$$

where $\mathit{\Delta}_i$ and $\mathit{\Gamma}_i$ are arbitrary disjunctions of linear inequalities and $|\mathit{\Delta}_i| \leq p$, for $i = 1, 2$.

1.2 Real Communication Complexity

The following set of definitions is an extension of boolean communication complexity [13, 15], that allows players to communicate with each other not only by bits, but with real numbers. It was introduced in [2].

Let I be finite set, $U, V \subset \{0,1\}^*$, $R \subseteq U \times V \times I$ be such that

$$\forall u \in U,\ v \in V\ \exists i \in I\ R(u,v,i)\ .$$

We will call relations satisfying this condition *multifunctions*.

Definition 1. *A* real game protocol *P over domain $U \times V$ with range I is a binary tree where each internal node v is labeled by two function $a_v : U \to \mathbb{R}$ and $b_v : V \to \mathbb{R}$ and each leaf is labeled with an element $i \in I$.*

The value *of the real game protocol P on input (x, y) is the label of the leaf reached by starting from the root, and walking on the tree. At each internal node v labeled by (a_v, b_v) we walk left if $a_v(x) < b_v(y)$ and right if $a_v(x) \geq b_v(y)$. The* number of rounds of the real game with protocol P on input (x, y) *is the length of the path taken on input (x, y). The* number of rounds of the real game with protocol P *is the height of the tree. If for every $u \in U$ and $v \in V$ the value i of P satisfies $R(u, v, i)$, we say that P computes R.*

Definition 2. *The* real communication complexity *of a multifunction R, $CC^{\mathbb{R}}(R)$, is the minimal number of rounds of the real game with protocol P, over all P that compute R.*

Usually, sets U, V are defined by some partial Boolean function f that maps $W \subseteq \{0,1\}^n$ to $\{0,1\}$. We take $U := f^{-1}(1)$, $V := f^{-1}(0)$ and $I := \{1, \ldots, n\}$. Relation $R(u, v, i)$ is true if strings u and v differ in position i. We are interested in *monotone* partial Boolean functions, that have at least one extension to a monotone Boolean function [13]. For such a function f define $R_f^{mono} \subseteq U \times V \times I$ by

$$R_f^{mono}(u,v,i) \quad \text{iff} \quad u \in U \wedge v \in V \wedge u_i = 1 \wedge v_i = 0\ .$$

As it happens with monotone boolean functions and Boolean communication complexity, there is a relation between the real communication complexity of R_f^{mono} and the depth of monotone real circuit computing f.

1.3 Monotone Real Circuits

A *monotone real circuit* is a circuit of fan-in 2 computing with real numbers where every gate computes a nondecreasing real function [16]. Since monotone real circuits are generalization of monotone boolean circuits, we require that they output 0 or 1 on every input from $\{0,1\}^*$. The depth and size of the monotone real circuit are defined as for boolean circuits.

Lemma 1 (Lemma 1.4, [2]). *Let f be a partial monotone boolean function. Then $CC^{\mathbb{R}}(R_f^{mono})$ is at most the minimal depth of a monotone real circuit C that computes the function f. Moreover,*

$$CC^{\mathbb{R}}(R_f^{mono}) \leq \log_{3/2} S^{\mathbb{R}}(f) \ ,$$

where $S^{\mathbb{R}}(f)$ is the minimal size of a monotone real formula computing f.

There is an important open question about the converse statement. A positive answer on it would immediately imply an extension of lower bound proved in this paper from tree-like R(CP) to general R(CP) [2].

1.4 Protocols

The notions of *protocol* and *monotone protocol* were defined in [14]. We need them for transformation of a refutation in some proof system into the real game in a natural and intuitive way.

Definition 3 (Definition 2.1, [2]). *Let $U, V \subseteq \{0,1\}^n$ be two sets and let $R \subseteq U \times V \times I$ be a multifunction. A protocol for R is a labeled directed graph G satisfying the following conditions:*

1. *Graph G is acyclic and has one source denoted by $\emptyset$. The nodes with zero out-degree are leaves, all other are inner nodes. All inner nodes have out-degree 2.*
2. *All leaves are labeled by elements of I.*
3. *There is a* strategy *$S(u,v,x)$ such that S assigns to a node x and a pair $u \in U$ and $v \in V$ one of the two children $S(u,v,x)$ of y.*
4. *For every pair $u \in U$, $v \in V$ there is a set $F(u,v)$ of nodes of G satisfying:*
   (a) $\emptyset \in F(u,v)$.
   (b) $x \in F(u,v) \rightarrow S(u,v,x) \in F(u,v)$.
   (c) If i is the label of a leaf from $F(u,v)$ then $R(u,v,i)$ holds.
   We call such set F the consistency condition.

The protocol is tree-like *iff the underlying graph is a tree.*

A protocol for a particular multifunction $R = \{(u,v,i) | u_i = 1 \wedge v_i = 0\}$ is called a monotone protocol *for U, V.*

Definition 4 (Definition 2.2, [2]). *Let G be a protocol for R. Let $S(u, v, x)$ be the strategy and $F(u, v)$ be the consistency condition of G.*

The real communication complexity *of G, denoted $CC^{\mathbb{R}}(G)$, is the minimal t such that for every $x \in G$ the players (first knows pair (u, x), the second knows (v, x)) decide $x \in F(u, v)$ and compute $S(u, v, x)$ in at most t round of the real game.*

For tree-like protocol it is possible to prove an exponential lower bounds on the following set of functions:

Let I, J be sets of size n. Consider a monotone Boolean function BPM that gives to a bipartite graph $\Gamma \subseteq I \times J$ the value 1 iff Γ contains a perfect matching. Inputs to BPM are n^2 variables x_{ij}, $i \in I, j \in J$. Their truth evaluations are in one to one correspondence with bipartite graphs.

Theorem 1 (Theorem 2.5, [2]). *Let G be a tree-like protocol for BPM of size S, such that $CC^{\mathbb{R}}(G) = t$. Then*

$$S = exp(\Omega((\frac{n}{t \log n})^{1/2})) \ .$$

2 Lower bound for tree-like R(CP)-like proof systems

The following definition was introduced in [14] and is a generalization of usual derivation in a proof system. A sequence of sets $D_1, \ldots, D_k \subseteq \{0,1\}^N$ is a *semantic derivation* of D_k from $A_1, \ldots, A_m$ if each D_i is either one of A_j, or contains $D_{i_1} \cap D_{i_2}$ for some $i_1, i_2 < i$. Till the end of this section we use $N = n + s + t$. Let us consider the following problem for two players:

Definition 5 (Definition 3.1, [2]). *For set $A \subseteq \{0,1\}^N$ we fix $u, v \in \{0,1\}^n$, $y \in \{0,1\}^s$ and $z \in \{0,1\}^t$. Consider the following three tasks:*

1. *Decide whether $(u, y, z) \in A$.*
2. *Decide whether $(v, y, z) \in A$.*
3. *If $(u, y, z) \in A$ and $(v, y, z) \notin A$, then find such $i \leq n$ that*

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

or find some u' satisfying

$$u' \geq u \wedge (u', y, z) \notin A \qquad (\text{where } u' \geq u \text{ means } \bigwedge_{i \leq n}(u'_i \geq u_i)) \ .$$

These tasks can be solved by two players, one knowing (u, y) and another one knowing (v, z).

A monotone real communication complexity *of A, $MCC^{\mathbb{R}}(A)$ is the minimal t such that tasks 1-3 have real communication complexity at most t.*

We define subset $Q(b)$ of $\mathbb{Z}^W$ as follows

$$Q(b) = \{a \in \mathbb{Z}^W | \forall i \leq W \ (a_i \leq b_i - 1)\} \ .$$

We need to prove the following lemma to improve the lower bound for tree-like R(CP)-like proof systems. It extends Lemma 5.1, [14] to real communication complexity.

Lemma 2. *Let linear mapping*

$$H : \{0,1\}^N \to \mathbb{Z}^W$$

be defined by a matrix with elements from $\mathbb{Z}$.

Let $Y \subseteq \mathbb{Z}^W$ be any set defined as

$$Y = \mathbb{Z}^W \setminus Q(b) \ ,$$

for some $b \in \mathbb{Z}^W$. We fix $X := H^{-1}(Y)$.

Then

$$MCC^{\mathbb{R}}(X) = O(W) + O(\log(n)) \ .$$

Proof. 1. To decide whether $(u, y, z) \in X$ we need to find such $i \in 1, ..., W$ that

$$\sum_{j=1}^{n} h_{ij} \cdot u_j + \sum_{j=n+1}^{n+s} h_{ij} \cdot y_j + \sum_{j=n+s+1}^{n+s+t} h_{ij} \cdot z_j \geq b_i \ . \tag{1}$$

Player A knows all elements in this sum except z. Let integer z_i satisfy the equality

$$\sum_{j=1}^{n} h_{ij} \cdot u_j + \sum_{j=n+1}^{n+s} h_{ij} \cdot y_j + z_i = b_i \ .$$

The players compare z_i and $z'_i = \sum_{j=n+s+1}^{n+s+t} h_{ij} \cdot z_j$ for all $i \in 1, ..., W$ and if for some i the inequality $z_i \leq z'_i$ holds, then (1) is also holds and therefore $(u, y, z) \in X$. Otherwise, $(u, y, z) \notin X$.

To decide whether $(u, y, z) \in X$ players need W rounds.

2. Similarly, in W rounds we can decide whether $(v, y, z) \in X$.
3. Assume that $(u, y, z) \in X$ and $(v, y, z) \notin X$. It means that for some $i \in 1, ..., W$ is

$$\sum_{j=1}^{n} h_{ij} \cdot u_j + \sum_{j=n+1}^{n+s} h_{ij} \cdot y_j + \sum_{j=n+s+1}^{n+s+t} h_{ij} \cdot z_j \geq b_i \ ,$$

and also

$$\sum_{j=1}^{n} h_{ij} \cdot v_j + \sum_{j=n+1}^{n+s} h_{ij} \cdot y_j + \sum_{j=n+s+1}^{n+s+t} h_{ij} \cdot z_j < b_i \ .$$

From the last two inequalities it follows that

$$\sum_{j \in J} h_{ij} \cdot u_j > \sum_{j \in J} h_{ij} \cdot v_j \ \ ,$$

where $J = \{1, \ldots, n\}$.
For all j such that $h_{ij} < 0$ first player assigns 1 to u_j. If for some $u' \geq u$ the triple $(u', y, z) \notin X$, then he communicates one bit of the answer to second player, and they stop if it is equal to 1. Otherwise,

$$\sum_{j \in J} h_{ij} \cdot u'_j > \sum_{j \in J} h_{ij} \cdot v_j \ \ , \tag{2}$$

where $J = \{1, \ldots, n\}$.
Let fix $J_1 = \{1, \ldots, \lfloor n/2 \rfloor\}$ and $J_2 = \{\lfloor n/2 \rfloor + 1, \ldots, n\}$. Note that it is holds either

$$\sum_{j \in J_1} h_{ij} \cdot u'_j > \sum_{j \in J_1} h_{ij} \cdot v_j \qquad \text{or} \qquad \sum_{j \in J_2} h_{ij} \cdot u'_j > \sum_{j \in J_2} h_{ij} \cdot v_j \ \ ,$$

otherwise (2) is not satisfying. Continue with one of the satisfied inequalities and find such j that $(u'_j = 1 \wedge v_j = 0)$ or $(u'_j = 0 \wedge v_j = 1)$. Since in this case, $h_{ij} > 0$ (otherwise u'_j is equal to 1), we have that $u'_j = u_j = 1 \wedge v_j = 0$. The real communication complexity of described binary search procedure is equal to $O(\log(n))$.

□

Following [2] we define a set $\tilde{A}$ for the $A \subseteq \{0,1\}^{n+s}$ as follows:

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

where a, b, c are from $\{0,1\}^n, \{0,1\}^s$ and $\{0,1\}^t$ respectively. For $B \subseteq \{0,1\}^{n+t}$ we define in the same way $\tilde{B}$:

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

Theorem 2 (Theorem 3.2, [2]). *Let $A_1, \ldots, A_m \subseteq \{0,1\}^{n+s}$ and $B_1, \ldots, B_\ell \subseteq \{0,1\}^{n+t}$ be two set families. Assume that there is a semantic derivation $\pi = D_1, \ldots, D_k$ of the empty set $\emptyset = D_k$ from $A_1, \ldots, A_m, B_1, \ldots, B_\ell$. Assume also that all the sets $A_1, \ldots, A_m$ satisfy the following monotone condition:*

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

and $MCC^{\mathbb{R}}(D_i) \leq t$ for all $i \leq k$.

Define sets U and V as follows:

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

and

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

Then there is a monotone protocol G for the sets U, V of size at most $k+n$ with real communication complexity $CC^{\mathbb{R}}$ at most t.

Moreover, if the semantic derivation π is tree-like, then protocol G is also tree-like.

The following theorem extends [2, Theorem 3.3] from CP-like proof systems to R(CP)-like proof systems.

Theorem 3. *Let a system of linear inequalities $E_1(x,y)$, $\ldots$, $E_m(x,y)$, $F_1(x,z)$, $\ldots$, $F_\ell(x,z)$ contain only variables $(x_1,\ldots,x_n)$, $(y_1,\ldots,y_s)$ and $(z_1,\ldots,z_t)$. Assume that there is a refutation π of the system in* R(CP)*-like proof system with k lines. Let every clause in π have at most W occurrences of linear inequalities. Assume also that x_i occur in all $E_1,\ldots,E_m$ only with non-negative coefficients.*

Then there is a monotone protocol G for U, V:

$$U = \{u \in \{0,1\}^n \mid \exists y \in \{0,1\}^s; (u,y) \text{ satisfying } \bigwedge_{i \leq m} E_i(u,y)\} \ ,$$
$$V = \{v \in \{0,1\}^n \mid \exists z \in \{0,1\}^t; (v,z) \text{ satisfying } \bigwedge_{j \leq \ell} F_j(v,z)\} \ ,$$

such that the size of G is at most $k+n$ and its real communication complexity is $O(W) + O(\log(n))$.

Moreover, if the refutation π is tree-like, then protocol G is also tree-like.

Proof. Consider a clause $D = \{h_i \cdot (x,y,z)^T \geq b_i \mid i \leq W\}$ in the refutation π. Then assignment (x,y,z) satisfies it iff

$$H \cdot (x,y,z) \in \mathbb{Z}^W \setminus Q((b_1,\ldots,b_W)) \ ,$$

where H is a $N \times W$-matrix with strings h_i. Replace each clause D in π by $\tilde{D} \subseteq \{0,1\}^N$ of assignments satisfying it to obtain a semantic refutation of $\tilde{E}_i$ and $\tilde{F}_i$. By Lemma 2 for every set S occurring in the refutation it holds that $MCC^{\mathbb{R}}(S) = O(W) + O(\log(n))$. To complete the proof apply Theorem 2. □

2.1 Exponential Lower Bounds

In [2] the following set of inequalities was introduced, $Hall_n$, that formalize Hall's theorem.

Let $|I| = |J| = n$.

1. $\sum_i y_{ki} \geq 1$, for all $1 \leq k \leq n$.
2. $y_{ki} + y_{k'i} \leq 1$, for all $1 \leq k < k' \leq n$.
3. $\sum_j y'_{kj} \geq 1$, for all $1 \leq k \leq n$.
4. $y'_{kj} + y'_{k'j} \leq 1$, for all $1 \leq k < k' \leq n$.
5. $y'_{kj} + y_{ki} - x_{ij} \leq 1$, for all $1 \leq k \leq n$, $i \in I$, $j \in J$.

Let $E_i(x, y, y')$ be all these linear inequalities. Note, that the set

$$U := \{x \in \{0,1\}^{n^2} \mid \exists y, y' (\bigwedge_i E_i(x, y, y'))\}$$

determines a set of graphs with BPM equal to 1.

The set V of graphs with BPM equal to 0 can be defined analogously by inequality system $F_j(x, z, z')$. The union set of all inequalities E_i and F_j is denoted by $Hall_n$.

Theorem 4. *Let π be a tree-like refutation of $Hall_n$ in any* R(CP)*-like proof system. Then $|\pi| \geq exp(\Omega((\frac{n}{W \log(n) + (\log(n))^2})^{1/2}))$.*

Proof. By Theorem 3 there is a tree-like monotone protocol G for BPM problem of size $k + n$ and real communication complexity $t = O(W) + O(\log(n))$. The required lower bound follows from Theorem 1. □

3 Lower bound for p-passive R(CP)-like proof systems

In this section we improve currently known lower bounds for the family of p-passive R(CP)-like systems, where for each derivation rule all but at most p inequalities in any of two hypotheses are contained in the conclusion.

Theorem 5. *Let a system of linear inequalities $S = E_1(x, y)$, $\ldots$, $E_m(x, y)$, $F_1(x, z)$, $\ldots$, $F_\ell(x, z)$ be as in Theorem 3 and a refutation π of the system S in p-passive* R(CP)*-like system be of the size k. Then there is a monotone protocol G for U, V:*

$$U = \{u \in \{0,1\}^n \mid \exists y \in \{0,1\}^s; (u, y) \textit{ satisfying } \bigwedge_{i \leq m} E_i(u, y)\} \ ,$$

$$V = \{v \in \{0,1\}^n \mid \exists z \in \{0,1\}^t; (v, z) \textit{ satisfying } \bigwedge_{j \leq \ell} F_j(v, z)\} \ ,$$

such that the size of G is at most $k + n$ and its real communication complexity is $O(p) + O(\log(n))$.

Moreover, if the refutation π is tree-like then protocol G is also tree-like.

Proof. The proof is just the same as for [14, Theorem 5.1], except that we use the main property of p-passive R(CP)-like systems and, hence, in each clause we need to check only p, but not W inequalities.

Let $\pi = C_1, \ldots, C_k$ be a refutation of the system S in p-passive R(CP)-like system. We construct a monotone protocol G for the real game on U, V as follows.

Assume that player A receives $u \in U$ and player B receives $v \in V$. Player A fixes some y such that $\bigwedge_{i\leq m} E_i(u,y)$ holds and player B fixes some z such that $\bigwedge_{j\leq \ell} F_j(v,z)$ holds. Protocol G has $(k+n)$ nodes, k for all steps of refutation π and n additional nodes labeled by formulas $u_i = 1 \wedge v_i = 0$, $i = 1,\ldots,n$. The consistency condition $F(u,v)$ consists of clauses C_j such that (v,y,z) and (u',y,z) for some $u' \geq u$ are not satisfying C_j and of those of the additional n nodes whose label is valid for the particular pair (u,v).

Let C_j be derived from X and Y by an inference rule

$$\frac{X \qquad Y}{C_j} \ .$$

The strategy function for C_j is defined as follows:

1. If (v,y,z) does not satisfy X and
   (a) if for some $u' \geq u$ (u',y,z) does not satisfy X then put $S(u,v,C_j) := X$,
   (b) otherwise, players find such i that $u_i = 1 \wedge v_i = 0$ and $S(u,v,C_j)$ is the node labeled by $u_i = 1 \wedge v_i = 0$.
2. Otherwise (v,y,z) does not satisfy Y (since the inference rule is sound) and
   (a) if for some $u' \geq u$ (u',y,z) does not satisfy Y then put $S(u,v,C_j) := Y$,
   (b) otherwise, players find such i that $u_i = 1 \wedge v_i = 0$ and $S(u,v,C_j)$ is the node labeled by $u_i = 1 \wedge v_i = 0$.

Since all x_s occur in all E_i, $1 \leq i \leq m$ only with non-negative coefficients, then for every $u' \geq u$ it holds that tuple (u',y,z) satisfies $\bigwedge_{i\leq m} E_i(u,y)$. Also tuple (v,y,z) satisfies all F_i, $1 \leq i \leq \ell$. Thus, none of the E_i, $1 \leq i \leq m$ and F_i, $1 \leq i \leq \ell$ is included in $F(u,v)$. This implies that players eventually have to find such i that $u_i = 1 \wedge v_i = 0$ holds.

Players can compute the relation $x \in F(u,v)$ and the function $S(u,v,x)$ in at most $O(p)+O(\log(n))$ rounds of real game, using the protocol from Lemma 2 for H defined by variables coefficients and b by free coefficients in p inequalities that are new in X and Y. □

Since R(CP) proof system is a 1-passive proof system, we have the following statement similar to Theorem 4.

Corollary 1. *Let π be a tree-like refutation of $Hall_n$ in* R(CP)*. Then $|\pi| \geq exp(\Omega(\frac{\sqrt{n}}{\log(n)}))$.*

Remark 1. Using the same idea we can remove the dependence on the maximal clause width from Krajíček's lower bound for general R(CP) and obtain lower bound of the form

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

To do that we only need to modify the protocol in [1, Theorem 6.1].

Acknowledgments

The author is very grateful to Dima Grigoriev, Jan Krajíček and Alexander S. Kulikov for helpful comments and is indebted to Edward A. Hirsch for enlightening discussions.

References

1. Krajíček, J.: Discretely ordered modules as a first-order extension of the cutting planes proof system. Journal of Symbolic Logic **63**(4) (1998) 1582–1596
2. Krajíček, J.: Interpolation by a game. Mathematical Logic Quarterly **44**(40) (1998) 450–458
3. Land, H., Doig, A.G.: An automatic method for solving discrete programming problems. Econometrica **28** (1960) 497–520
4. Bonet, M., Pitassi, T., Raz, R.: Lower bounds for cutting planes proofs with small coefficients. The Journal of Symbolic Logic **62**(3) (1997) 708–728
5. Krajíček, J.: On the weak pigeonhole principle. Fundamenta Mathematicæ **170**(1-3) (2001) 123–140
6. Atserias, A., Bonet, M.L., Esteban, J.L.: Lower bounds for the weak pigeonhole principle and random formulas beyond resolution. Information and Computation **176**(2) (2002) 136–152
7. Segerlind, N., Buss, S.R., Impagliazzo, R.: A Switching Lemma for Small Restrictions and Lower Bounds for k-DNF Resolution. SIAM Journal on Computing **33**(5) (2004) 1171–1200
8. Alekhnovich, M.: Lower bounds for k-DNF resolution on random 3-CNFs. In: STOC '05: Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, New York, NY, USA, ACM Press (2005) 251–256
9. Prestwich, S.: Incomplete dynamic backtracking for linear pseudo-boolean problems. Annals of Operations Research **130** (2004) 57–73
10. Chai, D., Kuehlmann, A.: A fast pseudo-boolean constraint solver. IEEE Trans. on CAD of Integrated Circuits and Systems **24**(3) (2005) 305–317
11. Manquinho, V.M., Marques-Silva, J.: On using cutting planes in pseudo-boolean optimization. Journal of Satisfiability, Boolean Modeling and Computation **2** (2006) 209–219
12. Razborov, A.A.: Lower bounds on the monotone complexity of some Boolean functions. Dokl. Akad. Nauk SSSR **281**(4) (1985) 798–801 In Russian: English translation in *Soviet Math. Dokl.* 31:354–357, 1985.
13. Karchmer, M., Wigderson, A.: Monotone circuits for connectivity require super-logarithmic depth. SIAM Journal on Discrete Mathematics **3**(2) (1990) 255–265
14. Krajíček, J.: Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. Journal of Symbolic Logic **62**(2) (1997) 457–486
15. Kushilevitz, E., Nisan, N.: Communication Complexity. Cambridge University Press (1997)
16. Pudlák, P.: Lower bounds for resolution and cutting plane proofs and monotone computations. Journal of Symbolic Logic **62**(3) (1997) 981–998