Interpolation by a game

Jan Krajíček*

Mathematical Institute, Oxford†

Abstract

We introduce a notion of a *real game* (a generalisation of the Karchmer - Wigderson game, cf.[3]) and *real communication complexity*, and relate them to the size of monotone real formulas and circuits. We give an exponential lower bound for tree-like monotone protocols (defined in [4, Def. 2.2]) of small real communication complexity solving the monotone communication complexity problem associated with the bipartite perfect matching problem.

This work is motivated by a research in interpolation theorems for propositional logic (by a problem posed in [5, Sec. 8], in particular). Our main objective is to extend the communication complexity approach of [4, 5] to a wider class of proof systems. In this direction we obtain an effective interpolation in a form of a protocol of small real communication complexity. Together with the above mentioned lower bound for tree - like protocols this yields as a corollary a lower bound on the number of steps for particular semantic derivations of Hall's theorem (these include tree-like cutting planes proofs for which an exponential lower bound was demonstrated by [2]).

Various interesting unsatisfiable propositional formulas occurring in length-of-proofs lower bounds can be formulated in the following form. Let $U, V \subseteq \{0,1\}^*$ be two disjoint NP-sets. The formula formalises that the intersection of $U_n := U \cap \{0,1\}^n$ and of $V_n := V \cap \{0,1\}^n$ is not empty. A best example is perhaps the pair consisting of the set of graphs with a k-clique and the set of $(k-1)$-colorable graphs.

An effective interpolation for a proof system P means that a good upper bound on the complexity of sets $W_n \subseteq \{0,1\}^n$ separating U_n from V_n can be given in terms of the minimal size of P-refutations of $U_n \cap V_n \neq \emptyset$. The complexity of W_n is often measured by circuit-size. In this note we shall measure

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

†On leave from the Mathematical Institute at Prague. This work was done while at the Mathematical Institute and at the Institute of Computer Science of the Academy of Sciences, Prague.

it in terms of a particular communication complexity. This is motivated by an approach to interpolation developed in [4, 5] and it bypasses in a sense the problem singled out in [5, Sec. 8][1]. The approach of [4, 5] relies on communication complexity concepts and our main objective is to extend the concepts so that the same method applies to a wider class of proof systems. In particular, to cutting planes, to resolution combined with cutting planes, or even to their first-order extensions (see [5] for definitions). This was achieved in [5] via Boolean communication complexity for the proof systems provided the absolute values of coefficients occurring in inequalities in proofs is small (cf. [5] for details). Our hope is that a generalisation of the concept of a communication game defined here will allow analogous results for the unrestricted case. In this paper we make a first step towards this goal.

This paper is a continuation of the research pursued in [4, 5], and we do not give any background information, motivations, or references to related work. All this can be found in detail in [4, 5]. However, all details of the new material are given. Vectors of integers are denoted $a, b, \ldots, x, y, \ldots$ and their coordinates $a_i, \ldots, x_i, \ldots$.

1 Real game

Let U and V be two subsets of $\{0,1\}^*$.

Definition 1.1 *A* real game *on the pair U, V is played by two players I and II. Player I gets $u \in U$ and II gets $v \in V$. At every round each player announces one real number.*

A position *in a play is a binary word*

$$w$$

whose length is the number of steps need to reach the position.

The initial position *is*

$$\emptyset$$

where $\emptyset$ is the empty word.

In $(k+1)^{st}$ step player I announces a real α and player II announces a real β. The position after the $(k+1)^{st}$ step is

$$w0 \quad \textit{if}\, \alpha > \beta$$

or

$$w1 \quad \textit{if}\, \alpha \leq \beta$$

The move α (resp. β) is computed by I (resp. by II) from u (resp. from v) and the position w only.

[1] That problem, calling for a particular upgrading of the communication complexity part of the interpolation theorem for semantic derivations ([4, Thm. 5.1]), is still open.

Let I be a finite set and let $R \subseteq U \times V \times I$ be any relation such that

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

Relations satisfying this condition will be called *multifunctions.*

Definition 1.2 *The* real communication complexity *of a multifunction R, denoted $CC^{\mathbf{R}}(R)$, is the minimal number h such that there are strategies for the players of the real game on U, V, and there is a function*

$$g : \{0,1\}^h \to I$$

such that for every $u \in U, v \in V$, if the position in the game after the h^{st} step is w then

$$R(u,v,g(w))$$

A partial Boolean function is monotone if it has at least one extension to a total monotone Boolean function. Let $W \subseteq \{0,1\}^n$ be a set and let $f : W \to \{0,1\}$ be a partial monotone Boolean function. Put $U := f^{(-1)}(1)$, $V := f^{(-1)}(0)$ and $I := \{1, \ldots, n\}$. Following [3] define $R_f^{mono} \subseteq U \times V \times I$ by

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

Definition 1.3 ([7]) 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.*

Lemma 1.4 *$CC^{\mathbf{R}}(R_f^{mono})$ is at most the minimal depth of a monotone real circuit C that computes (on W) the function f. In fact,*

$$CC^{\mathbf{R}}(R_f^{mono}) \leq \log_{3/2} FS_{mon}^{\mathbf{R}}(f)$$

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

Proof :
The first inequality is trivial. In particular, at a node of a circuit the players announce the values at the left incoming subcircuit. In this way they construct a path through the circuit such that in every node the value at u is bigger than the value at v. Hence at an input node this gives i such that $u_i = 1 \wedge v_i = 0$.

The strategies of the players yielding the second inequality are similar, except that they use Spira's trick. At a node corresponding to the output of a formula F they find a node ξ splitting F in the 1/3 - 2/3 fashion. They announce the values on u and v at ξ.

If $\xi(u) > \xi(v)$, they go to the subformula determined by ξ. If $\xi(u) \leq \xi(v)$, they take a formula $F'(x_1, \ldots, x_n, y)$ such that

$$F(x_1, \ldots, x_n) = F'(x_1, \ldots, x_n, y/\xi(x_1, \ldots, x_n))$$

Then they continue with the game analogously, with player I substituting the value $\xi(u)$ for y in F' and II substituting $\xi(v)$. Hence the players need $\log_{3/2}|F|$ rounds.

q.e.d.

A probabilistic communication complexity of a multifunction R with public coins and error ϵ is denoted $C^{pub}_{\epsilon}(R)$. Denote by $R^{<}_{m} \subseteq \{0,1\}^m \times \{0,1\}^m \times \{0,1\}$ the set of all triples (α, β, δ) such that $\delta = 0$ if $\alpha > \beta$ in the lexico-graphic ordering and $\delta = 1$ otherwise.

Theorem 1.5 (Nissan [6]) *For $\epsilon < \frac{1}{2}$, $C^{pub}_{\epsilon}(R^{<}_{m}) = O(\log m + \log \epsilon^{-1})$.*

Lemma 1.6 *Let $R \subseteq U \times V \times I$ be a multifunction. Then for $\epsilon < \frac{1}{2}$ it holds*

$$C^{pub}_{\epsilon}(R) \leq CC^{\mathbf{R}}(R) \cdot O(\log n + \log \epsilon^{-1})$$

Proof :

In a real game with h rounds at most $|U| \cdot |V| \cdot 2 \cdot (2^h - 1) < 2^{2n+h+1}$ different reals occur. Let $\alpha_0 < \alpha_1 < \ldots < \alpha_k$, $k < 2^{2n+h+1}$, be their enumeration in an increasing order. The players may use i in place of α_i without affecting the game.

One step in such a game can be simulated by $O(\log m + \log(\epsilon^{-1}h))$, $m = 2n + h + 1$, steps of probabilistic Karchmer - Wigderson game with error ϵh^{-1} (Theorem 1.5). Hence the whole real game can be simulated by a probabilistic game with error ϵ of length

$$h \cdot O(\log m + \log(\epsilon^{-1}h) = h \cdot O(\log n + \log \epsilon^{-1})$$

as we may assume that $h \leq n$.

q.e.d.

2 Protocols

We use the notion of a *monotone protocol* for a game on pair U, V defined in [4, Def. 2.2]; we only measure its monotone communication complexity differently. We define first protocols for general multifunctions; a monotone protocol will be then just a protocol for a particular multifunction.

Definition 2.1 *Let $U, V \subseteq \{0,1\}^n$ be two sets. Let $R \subseteq U \times V \times I$ be a multifunction. A* protocol *for R is a labelled directed graph G satisfying the following four conditions:*

1. *G is acyclic and has one source (the in-degree 0 node) denoted $\emptyset$.*

   The nodes with the out-degree 0 are leaves, *all other are* inner nodes.

   All inner nodes have out-degree 2 (this condition was not present in [4] and it is added here for technical reasons only).

2. *All leaves are labelled by elements of I.*

3. *There is a function $S(u,v,x)$ (the* strategy*) such that S assigns to a node x and a pair $u \in U$ and $v \in V$ the edge $S(u,v,x)$ leaving from the node x.*

Every pair $u \in U$ and $v \in V$ defines for every node x a directed path P^x_{uv} in G from the node x to a leaf: $P^x_{uv} = x_1, \ldots, x_h$, where $x_1 = x$, the edge $S(u,v,x_i)$ goes from x_i to x_{i+1}, and x_h is a leaf.

4. *For every $u \in U$ and $v \in V$ there is a set $F(u,v) \subseteq G$ satisfying:*

   (a) $\emptyset \in F(u,v)$

   (b) $x \in F(u,v) \rightarrow P^x_{u,v} \subseteq F(u,v)$

   (c) *If i is the label of a leaf from $F(u,v)$ then $R(u,v,i)$ holds.*

   Such a set F is called the consistency condition.

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

A protocol for a particular multifunction R

$$\{(u,v,i) \mid u_i = 1 \wedge v_i = 0\}$$

is called a monotone protocol *for U, V.*

Note that some $S(u,v,x)$ could be defined in terms if $F(u,v)$ (as the leftmost son that is also in $F(u,v)$). In applications however, some other definition may be more natural, cf. [4].

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

The real communication complexity *of G, denoted $CC^{\mathbf{R}}(G)$, is the minimal t such that for every $x \in G$ the players (one knowing u and x, the other v and x) decide whether $x \in F(u,v)$ and compute $S(u,v,x)$ in at most t rounds of the real game.*

Lemma 2.3 *Let $U, V \subseteq \{0,1\}^n$ be two disjoint sets. Any monotone real circuit C of size S separating U from V determines a monotone protocol G for U, V with S nodes whose real communication complexity is 1.*

Proof :

G is the underlying graph of C. The consistency condition $F(u,v)$ contains all subcircuits x such that the value at x for u is bigger than for v. The strategy $S(u,v,x)$ assigns to x one of its two subcircuits that is also in $F(u,v)$ (monotonicity of C guarantees its existence).

q.e.d.

In Boolean case a form of a converse statement holds, see [4, Thm. 2.3] that restates [10, Thm. 3.1] in terms of protocols.

Theorem 2.4 *Let G be a tree-like protocol of size S for a multifunction R and assume that $CC^{\mathbf{R}}(G) = t$. Then*

$$C_{\epsilon}^{pub}(R) \leq \log S \cdot t \cdot O(\log n + \log \epsilon^{-1} + \log S)$$

Proof :

The protocol G is a binary tree that the players use to find $i \in I$ such that $R(u,v,i)$ holds. We shall transform it into a balanced binary tree G^* that will serve as a strategy for the probabilistic Karchmer - Wigderson game.

In the first step we transfer G into G' that will have the tree height $O(\log S)$ and the same real communication complexity as G. The players take a node x dividing G in the 1/3 - 2/3 fashion. They decide (in t rounds at most) whether $x \in F(u,v)$. If the answer is affirmative they will concentrate on the subtree of G with root x. Otherwise the remain in the same root and delete the subtree from G. This procedure defines G'.

By Lemma 1.6 the strategy function in G' can be computed by a probabilistic game with error ϵS^{-1} and length $t \cdot O(\log n + \log \epsilon^{-1} + \log S)$. Hence the whole tree G', with the original edges replaced by the binary trees of height $t \cdot O(\log n + \log \epsilon^{-1} + \log S)$, works as a strategy for the probabilistic game with total error ϵ.

This new tree G^* has height $O(\log S \cdot t \cdot (\log n + \log \epsilon^{-1} + \log S))$.

q.e.d.

Using Theorem 2.4 we shall be able to transfer a lower bound from [9] to a lower bound for tree-like protocols of small real communication complexity. We use the same Boolean function as [9].

Let I, J be two sets of size n. Consider a monotone Boolean function BPM that gives to a bipartite graph $G \subseteq I \times J$ the value 1 iff G 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 2.5 *Let G be a tree-like protocol for BPM of size S, and such that $CC^{\mathbf{R}}(G) = t$. Then*

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

Proof :
By Theorem 2.4

$$C_\epsilon^{pub}(R_{BPM}^{mono}) \leq \log S \cdot t \cdot O(\log n + \log \epsilon^{-1} + \log S)$$

By [9, Thm. 4.4]

$$C_0^{pub}(R_{BMP}^{mono}) = \Omega(n)$$

while by [8, Lemma 1.4] for any R

$$C_0^{pub}(R) \leq (C_\epsilon^{pub}(R) + 2)(\log_{1/\epsilon} n + 1)$$

Taking $\epsilon := n^{-1}$ we get

$$\log^2 S = \Omega(\frac{n}{t \log n})$$

q.e.d.

3 An interpolation theorem

The notion of a semantic derivation was defined in [4, Def. 4.1]. A sequence of sets $D_1, \ldots, D_k$ (tacitly all subsets of some $\{0,1\}^N$) is a semantic derivation of D_k from $A_1, \ldots, A_m$ if each D_i is either one of A_j's or contains $D_{i_1} \cap D_{i_2}$, for some $i_1, i_2 < i$. We modify the definition of its communication complexity ([4, Def. 4.3]) to accommodate new communication complexity over reals. We consider only the monotone case, as that is the case potentially yielding lower bounds.

Definition 3.1 *Let $N = n + s + t$ be fixed and let $A \subseteq \{0,1\}^N$. Let $u, v \in \{0,1\}^n$, $y^u \in \{0,1\}^s$ and $z^v \in \{0,1\}^t$.*

Consider three tasks:

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

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

or learn that there is some u' satisfying

$$u' \geq u \wedge (u', y^u, z^v) \notin A$$

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

These tasks can be solved by two players, one knowing u, y^u and the other one knowing v, z^v.
The monotone real communication complexity w.r.t. *U of A, $MCC_U^{\mathbf{R}}(A)$, is the minimal t such that the tasks 1.-3. have real communication complexity $\leq t$.*

The word monotone in $MCC_U^{\mathbf{R}}$ refers to the form of task 3..

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 3.2 *Let $A_1, \ldots, A_m \subseteq \{0,1\}^{n+s}$ and $B_1, \ldots, B_\ell \subseteq \{0,1\}^{n+t}$. Assume that there is a semantic derivation $\pi = D_1, \ldots, D_k$ of the empty set $\emptyset = D_k$ from the sets $\tilde{A}_1, \ldots, \tilde{A}_m, \tilde{B}_1, \ldots, \tilde{B}_\ell$.*
Assume that the sets $A_1, \ldots, A_m$ satisfy the following monotonicity condition:

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

and that $MCC_U^{\mathbf{R}}(D_i) \leq t$ for all $i \leq k$
Define two sets

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

and

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

Then there is a monotone protocol G for U, V of size at most $k + n$ whose real communication complexity $CC^{\mathbf{R}}(G)$ is at most t.

Moreover, if the semantic derivation is tree-like then so is G.

Proof :

The proof of the theorem entirely parallels the proof of the monotone part of [4, Thm. 5.1].

q.e.d.

CP is the cutting planes proof system, R is the resolution, and R(CP) is a proof system introduced in [5] combining naturally R with CP (working with clauses formed by integer inequalities). We shall not repeat the formal definitions here as we wish to stress that the method applies to all CP-like proof systems. These are proof systems satisfying the following conditions:

1. Proof-steps are integer inequalities of the form $a_1x_1 + \ldots + a_nx_n \geq b$, with a_i and b integers and x_i variables (called CP-inequalities).

2. All axioms are tautologically valid.

3. All inference rules are sound and have at most two hypotheses (the later condition is just a technical one).

Theorem 3.3 *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 only the displayed variables $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_s)$ and $z = (z_1, \ldots, z_t)$ occur. Let $N := n + s + t$. Assume that there is a refutation π of the system in a CP-like proof system such that π contains k steps. Assume also that x_i occur in all $E_1, \ldots, E_m$ with non-negative coefficients only.*
Then there is a monotone protocol G for U, V:

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

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

such that the size of G is at most $k + n$ and its real communication complexity is $O(1)$.

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

Proof :
Replace each CP-inequality D in π by the subset $\tilde{D}$ of $\{0,1\}^N$ of assignments satisfying it. This yields a semantic refutation of $\tilde{E}_i$'s and $\tilde{F}_j$'s. It is easy to see that for every set A occurring in the refutation it holds that $MCC_U^{\mathbf{R}}(A) = O(1)$. The rest follows from Theorem 3.2.

q.e.d.

4 Lower bounds for Hall's theorem

Impagliazzo, Pitassi and Urquhart [2] proved that a set of clauses related to BPM (similar to $Hall_n$ below) requires exponential size tree-like CP - refutations. In this section we derive a mild generalisation of their theorem (with

CP - like proof systems in place of just CP) as an immediate corollary of the monotone interpolation Theorem 3.3 and of Theorem 2.5.

We shall define two sets of CP-inequalities formalising Hall's theorem. Let y_{ai} and y'_{aj}, $a \in \{1,\ldots,n\}$, $i \in I$, $j \in J$ be $2n^2$ variables. Consider the inequalities:

1. $\sum_i y_{ai} \geq 1$, all $a \in \{1,\ldots,n\}$.
2. $1 - y_{ai} + 1 - y_{a'i} \geq 1$, all different $a, a' \in \{1,\ldots,n\}$.
3. $\sum_j y'_{aj} \geq 1$, all $a \in \{1,\ldots,n\}$.
4. $1 - y'_{aj} + 1 - y'_{a'j} \geq 1$, all different $a, a' \in \{1,\ldots,n\}$.
5. $1 - y_{ai} + 1 - y'_{aj} + x_{ij} \geq 1$, all $a \in \{1,\ldots,n\}$, $i \in I$ and $j \in J$.

The inequalities 1. and 2. force that y_{ai} determines a bijection $f : \{1,\ldots,n\} \to I$, and similarly 3. and 4. say that y'_{aj} determine a bijection $g : \{1,\ldots,n\} \to J$. Conditions 5. imply that the edges $\{(f(a), g(a)) \in I \times J \mid a \in \{1,\ldots,n\}\}$ form a perfect matching in G.

Let $E_i(x, y, y')$ be all these CP-inequalities. Clearly the set

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

is the set of graphs given 1 by BPM.

The set V of graphs given 0 by BPM can be defined analogously by CP-inequalities $F_j(x, z, z', z'')$ using Hall's theorem. They formalise that X is a subset of $\{1,\ldots,n\}$ containing n which is determined on $\{1,\ldots,n-1\}$ by $z''_1,\ldots,z''_{n-1}$, and that for some bijections $f : X \cap \{1,\ldots,n\} \to I$ and $g : X \cap \{1,\ldots,n-1\} \to J$ (or $f : X \cap \{1,\ldots,n\} \to J$ and $g : X \cap \{1,\ldots,n-1\} \to I$) determined by z_{ai} and z'_{aj}, all neighbors of nodes in $Rng(f)$ are in $Rng(g)$. The set of all these $O(n^4)$ inequalities E_i and F_j is denoted $Hall_n$.

Theorem 4.1 *Let π be a tree-like refutation of $Hall_n$ in any CP-like proof system. Assume that π has k steps.*
Then

$$k \geq \exp(\Omega((\frac{n}{\log n})^{1/2})$$

Proof :

By Theorem 3.3 there is a tree-like protocol G for BPM whose size is $k+n$ and whose real communication complexity is $O(1)$. The lower bound then follows by Theorem 2.5.

q.e.d.

5 Problems

An obvious problem is to generalize Theorem 2.5 and to prove strong lower bounds for general non - tree - like protocols (perhaps for a different monotone function than BPM as in Thm. 2.5, e.g. for the clique function). Using Theorem 3.3 this would give a new proof of the lower bound for CP proved in [7, 1] (in fact, for all CP - like proof systems). Assuming that Lemma 2.3 admits some form of a converse, the exponential lower bounds for monotone real circuits proved in [1, 7] would yield a ground for such a generalization.

Another problem is to extend Theorem 4.1 from tree - like CP-like proof systems to tree - like R(CP)-like proof systems (or even, together with a solution of the previous problem, to general R(CP) - like proof systems). In [5] a lower bound for R(CP) was given that depends on the maximum number W of CP-inequalities in a clause and on the maximum absolute value M of a coefficient in any CP-inequality. Theorem 4.1 drops the dependence on M for tree-like proofs, assuming $W = 1$. A similar bound for $W > 1$ could be deduced from an estimate of the real communication complexity of the following decision problem.

For $b \in \mathbf{Z}^W$ define

$$Q(b) := \{x \in \mathbf{Z}^W \mid x_i \leq b_i \text{ all } i \leq W\}$$

Player I gets $a, c_1, \ldots, c_n \in \mathbf{Z}^W$ while II gets $b \in \mathbf{Z}^W$. They should decide whether

$$a + \sum_{i \in I} c_i \in Q(b)$$

for some $I \subseteq \{1, \ldots, n\}$.

Let $t(W, n)$ be the real communication complexity of this decision problem[2]. Then if $A \subseteq \{0,1\}^N$ is defined by a disjunction of W CP-inequalities it holds that

$$MCC_U^{\mathbf{R}}(A) = O(t(W, n) \log n)$$

(this is analogous to [5, Lemma 5.1]). Hence we would get a lower bound of the form $\exp(\Omega(\frac{n^{1/2}}{t(W,n)^{1/2} \log n}))$.

Acknowledgements: I thank R. Impagliazzo for telling me about [6], and P. Pudlák and J. Sgall for several discussions about the problem from [5, Sec. 8].

References

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

[2] Added in proof: P. Pudlák showed recently that $t(2, n) = \Omega(n)$.

[2] Impagliazzo, R., Pitassi, T., and Urquhart, A. (1994) Upper and lower bounds for tree-like cutting planes proofs, in: Proc. of the 9th Annual IEEE Symposium on *Logic in Computer Science.* Piscataway, NJ, IEEE Computer Science Press. pp.220-228.

[3] 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.

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

[5] —— (1996) Discretely ordered modules as a first-order extension of the cutting planes proof system, *J. Symbolic Logic*, to appear.

[6] Nissan, N. (1993) The communication complexity of the threshold gates, in: *Combinatorics, P. Erdös is Eighty*, **Vol. 1**, Eds. Miklós et.al., Bolyai Math. Soc., pp.301-315.

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

[8] Raz, R., and Wigderson, A. (1989) Probabilistic communication complexity of Boolean relation, in: *Proc. IEEE* 30^{th} *Annual Symp. on Foundation of Computer Science*, pp.562-567.

[9] —— (1992) Monotone circuits for matching require linear depth, *J. of Assoc. for Computing Machinery*, **39(3)**, pp.736-744.

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

Current address:
Mathematical Institute
24-29 St.Giles'
Oxford, OX1 3LB, U.K.
`krajicek@maths.ox.ac.uk`