Lower Bounds for Monotone Real Circuit Depth and Formula Size and Tree-like Cutting Planes

Jan Johannsen*
Department of Mathematics
University of California, San Diego

July 11, 1997

Abstract

Using a notion of real communication complexity recently introduced by J. Krajíček, we prove a lower bound on the depth of monotone real circuits and the size of monotone real formulas for st-connectivity. This implies a super-polynomial speed-up of dag-like over tree-like Cutting Planes proofs.

Keywords: monotone circuit, communication complexity, propositional proof system, Cutting Planes

Introduction

A *monotone real circuit* is a circuit computing with real numbers in which every gate computes a nondecreasing binary real function. This class of circuits was introduced in [8]. We require that such a circuit outputs 0 or 1 on every input of 0's and 1's only. Clearly, monotone boolean circuits are a special case of monotone real circuits.

The depth and size of a monotone real circuit are defined as usual, and we call it a *formula* if every gate has fan-out at most 1.

We generalize the lower bounds on the depth of monotone boolean circuits and the size of monotone boolean formulas for st-connectivity of [6] to monotone real circuits. By the main result of [8], this also implies a superpolynomial lower bound on the size of tree-like Cutting Planes proofs, thereby separating these from their dag-like counterparts.

*Supported by DFG grant No. Jo 291/1-1

We denote by $d_{\mathbb{R}}(f)$ the minimal depth of a monotone real circuit computing f, and by $s_{\mathbb{R}}(f)$ the minimal size of a monotone real formula computing f. For a natural number n, $[n]$ denotes the set $\{1, \dots, n\}$.

Real Communication Complexity

We recall the notion of real games and real communication complexity introduced in [7]. Let U, V be finite sets. A *real game* on U, V is played by two players I and II, where I computes a function $f_I : U \times \{0,1\}^* \to \mathbb{R}$ and II computes a function $f_{II} : V \times \{0,1\}^* \to \mathbb{R}$. Given inputs $u \in U$, $v \in V$, the players generate a sequence w of bits as follows:

$$w_0 := \lambda$$
$$w_{k+1} := \begin{cases} w_k 0 & \text{if } f_I(u, w_k) > f_{II}(v, w_k) \\ w_k 1 & \text{else} \end{cases}$$

Let I be another finite set, and let $R \subseteq U \times V \times I$ be a multifunction, i.e. $\forall u \in U\, \forall v \in V\, \exists i \in I\; (u, v, i) \in R$. The *real communication complexity* $cc_{\mathbb{R}}(R)$ is the minimal number k such that there is a real game on U, V and a function $g : \{0,1\}^k \to I$ such that

$$\forall u \in U\, \forall v \in V\; (u, v, g(w_k)) \in R\,.$$

If this holds then we also say that the game in question solves R in k rounds.

Let $f : \{0,1\}^n \to \{0,1\}$ be a monotone boolean function, let $U := f^{-1}(1)$ and $V := f^{-1}(0)$, and let the multifunction $R_f \subseteq U \times V \times [n]$ be defined by

$$(u, v, i) \in R_f \quad \text{iff} \quad u_i = 1 \text{ and } v_i = 0\,.$$

Then there is a relation between the real communication complexity of R_f and the depth of a monotone real circuit or the size of a monotone real formula, similar to the boolean case:

Lemma 1 (Krajíček [7]). *Let f be a monotone boolean function. Then*

$$cc_{\mathbb{R}}(R_f) \le d_{\mathbb{R}}(f) \qquad \text{and} \qquad cc_{\mathbb{R}}(R_f) \le \log_{3/2} s_{\mathbb{R}}(f)\,.$$

Proof. Let the value at gate g on input $u \in U$ be greater than the value at g on input $v \in V$. As the function computed by g is nondecreasing, the same must hold for at least one of the gates immediately below g. By playing the value of, say, the left gate below g on input u and v, respectively, the players can determine for which of the two gates this is the case. Hence given a circuit of depth k computing f, the players can find an input gate i with $u_i > v_i$ in k rounds. This proves the first inequality.

For the second inequality, let $f(x)$ be a formula of size s with $f(u) > f(v)$. The players determine a subformula $g(x)$ with $\frac{1}{3}|f(x)| \leq |g(x)| < \frac{2}{3}|f(x)|$, then play the values $g(u)$ and $g(v)$, respectively. If $g(u) > g(v)$, they continue with the formula $g(x)$. Otherwise let $f(x) = f'(x, g(x))$, then the players continue with the formula $f'(x, c)$, where c is the constant $g(u)$ for player I and $g(v)$ for player II respectively. After $\log_{3/2} s$ rounds, the players will have found an input i with $u_i > v_i$. □

For a monotone boolean function f, let $\min(f)$ denote the set of minterms of f, and $\max(f)$ the set of maxterms of f. Since f is monotone, we can represent these as sets of index sets. We define the relation $R_f^m \subseteq \min(f) \times \max(f) \times [n]$ by

$$(p, q, i) \in R_f \quad \text{iff} \quad i \in p \cap q \; .$$

Then as in the boolean case (see [5]), a real game solving R_f can be used to solve R_f^m, and vice versa, hence we have

$$cc_{\mathbb{R}}(R_f^m) = cc_{\mathbb{R}}(R_f) \; .$$

Let $stconn_n$ be the monotone function on $\binom{n+2}{2}$ variables, representing the edges of an undirected graph G on the set of nodes $N := [n] \cup \{s, t\}$, that gives 1 if there is a path in G from s to t, and 0 else. As an example, we shall give a real game for $R^m_{stconn_n}$, giving an upper bound $cc_{\mathbb{R}}(R^m_{stconn_n}) = O(\log^2 n)$.

A minterm of $stconn_n$ is a simple path from s to t, and a maxterm can be represented by a coloring of N by two colors 0,1 such that s gets color 0 and t gets color 1. The aim of the game is to find a bicolored edge in the path.

Let m be the number of the middle node of I's path. For $\lceil \log n \rceil$ rounds, player I keeps playing m, while player II uses binary search to determine m. After that, both players know m, and I plays 0 while II plays m's color, thereby communicating that color to I. If the color is 1, then the players repeat this procedure with the half of the path from s to m, otherwise with the half from m to t. After at most $\lceil \log n \rceil$ repetitions, the length of the current path is 1, hence the players have found a bicolored edge.

We shall show that also $cc_{\mathbb{R}}(R^m_{stconn_n}) = \Omega(\log^2 n)$, thus by Lemma 1, monotone real circuits for $stconn_n$ have to have depth $\Omega(\log^2 n)$, and monotone real formulas for $stconn_n$ are of size $n^{\Omega(\log n)}$.

The Lower Bound

The proof of the lower bound on $cc_{\mathbb{R}}(R^m_{stconn_n})$ follows closely the proof of the Karchmer/Wigderson monotone circuit depth lower bound as presented in [2, section 5.2].

Let a game solving $R \subseteq U \times V \times I$ in $k+1$ rounds be given. Let $\alpha_u := f_I(u, \lambda)$ and $\beta_v := f_{II}(v, \lambda)$. W.l.o.g. we can assume that $\alpha_u \neq \alpha_{u'}$ for $u \neq u' \in U$ and $\beta_v \neq \beta_{v'}$ for $v \neq v' \in V$. Now consider a matrix whose columns are indexed by the α_u's and whose rows are indexed by the β_v's, both in increasing order, and let the entry in position (α_u, β_v) be 0 if $\alpha_u > \beta_v$ and 1 else. Then it is easily seen that either the upper right $\lceil\frac{|U|}{2}\rceil \times \lceil\frac{|V|}{2}\rceil$-submatrix is entirely filled with 0's, or the lower left $\lceil\frac{|U|}{2}\rceil \times \lceil\frac{|V|}{2}\rceil$-submatrix is entirely filled with 1's. Hence there are $U' \subseteq U$ and $V' \subseteq V$ with $|U'| \geq \frac{1}{2}|U|$ and $|V'| \geq \frac{1}{2}|V|$ such that for every input $(u, v) \in U' \times V'$, the first bit played is the same, say b. Hence there is a game that solves R restricted to $U' \times V'$ in k rounds: pretend that in the first round, the bit b was played, and then continue as in the original game. This motivates the following definition:

We call a real game an $(n, \ell, \epsilon, \delta)$-game of length k, if there is a set U of paths from s to t of length $\ell + 1$, represented as vectors in $[n]^\ell$, and a set $V \subseteq \{0,1\}^{[n]}$ of colorings with $|U| \geq \epsilon n^\ell$ and $|V| \geq \delta 2^n$ such that the game solves $R^m_{stconn_n}$ restricted to $U \times V$ in k rounds. The considerations above prove the following

Lemma 2. *If there is an $(n, \ell, \epsilon, \delta)$-game of length k, then there also is an $(n, \ell, \frac{\epsilon}{2}, \frac{\delta}{2})$-game of length $k - 1$.*

The following lemma is the heart of the argument:

Lemma 3. *If there is an $(n, \ell, \epsilon, \delta)$-game of length k, and r is such that $\frac{100\ell}{\epsilon} \leq r \leq \frac{n}{100\ell}$ and $\delta \geq 2(\frac{3}{4})^{\frac{n}{r}}$, then there is an $(n - r, \frac{\ell}{2}, \frac{\sqrt{\epsilon}}{2}, \frac{r\delta}{2n})$-game of length k.*

Proof. Define a set of random restrictions R_r as follows: to choose $\rho \in R_r$, first choose a set $W_\rho \subseteq [n]$ of size $|W_\rho| = r$ randomly and uniformly, and then choose a coloring $c_\rho : W_\rho \to \{0,1\}$ randomly and uniformly. Let $S_\rho := \{\, x \in W_\rho \,;\, c_\rho(x) = 0 \,\}$ and $T_\rho := \{\, x \in W_\rho \,;\, c_\rho(x) = 1 \,\}$. The idea is that ρ maps S_ρ to s and T_ρ to t, and every other node to itself.

Let U_0 and V_0 be the sets for which the game solves $R^m_{stconn_n}$, with $|U_0| \geq \epsilon n^\ell$

and $|V_0| \geq \delta 2^n$. Define

$$U_L := \left\{ u \in [n]^{\frac{\ell}{2}} \; ; \; \left| \left\{ u' \in [n]^{\frac{\ell}{2}} \; ; \; (u,u') \in U_0 \right\} \right| > \frac{\epsilon}{4} n^{\frac{\ell}{2}} \right\}$$

and U_R analogously. If $(u,u') \in U_0$, then either $u \in U_L$ and $u' \in U_R$, or $u \notin U_L$, or $u' \notin U_R$. Now at most $|U_L| \cdot |U_R|$ elements can be of the first type, and there can be at most $n^{\frac{\ell}{2}} \cdot \frac{\epsilon}{4} n^{\frac{\ell}{2}} = \frac{\epsilon}{4} n^\ell$ elements of each of the latter two types. Hence we get $\epsilon n^\ell \leq |U_0| \leq |U_L| \cdot |U_R| + \frac{\epsilon}{2} n^\ell$, and thus $|U_L| \cdot |U_R| \geq \frac{\epsilon}{2} n^\ell$. Therefore one of U_L or U_R has to be of size at least $\sqrt{\frac{\epsilon}{2}} n^{\frac{\ell}{2}}$. W.l.o.g. let it be U_L.

For a restriction $\rho \in R_r$, let

$$U_\rho := \left\{ u \in U_L \; ; \; u \in ([n] \setminus W_\rho)^{\frac{\ell}{2}} \text{ and } \exists u' \in T_\rho^{\frac{\ell}{2}} \; (u,u') \in U_0 \right\}$$
$$V_\rho := \left\{ v \in \{0,1\}^{[n] \setminus W_\rho} \; ; \; (v \cup c_\rho) \in V_0 \right\}$$

We obtain a game solving $R^m_{stconn_n}$ restricted to $U_\rho \times V_\rho$ as follows: on input $(u,v) \in U_\rho \times V_\rho$, player I computes a vector $u' \in T_\rho^{\frac{\ell}{2}}$ such that $(u,u') \in U_0$, then the players play the original game on input $((u,u'),(v \cup c_\rho))$. It remains to show that there is a $\rho \in R_r$ with $|U_\rho| \geq \frac{\sqrt{\epsilon}}{2}(n-r)^{\frac{\ell}{2}}$ and $|V_\rho| \geq \frac{r\delta}{2n} 2^{n-r}$.

Now the same calculations as in [2, section 5.2] show that each of the inequalitites $|U_\rho| \geq \frac{\sqrt{\epsilon}}{2}(n-r)^{\frac{\ell}{2}}$ and $|V_\rho| \geq \frac{r\delta}{2n} 2^{n-r}$ holds with probability at least $\frac{3}{4}$. Hence the probability that both inequalities hold is at least $\frac{1}{2}$. □

Theorem 4. *For sufficiently large n, $cc_{\mathbb{R}}(R^m_{stconn_n}) > \frac{1}{100} \log^2 n$.*

Proof. Suppose there is a game solving $R^m_{stconn_n}$ in $\frac{1}{100} \log^2 n$ rounds, for some large n, and let $\ell := n^{\frac{1}{4}}$. Then in particular, this is an $(n, \ell, \frac{1}{4} n^{-\frac{1}{10}}, 1)$-game. We divide the game in $\frac{1}{10} \log n$ stages of $\frac{1}{10} \log n$ rounds each.

Lemma 2 applied $\frac{1}{10} \log n$ times then gives us an $(n, \ell, \frac{1}{4} n^{-\frac{1}{5}}, n^{-\frac{1}{10}})$-game having one stage fewer. Since n is large, the conditions of Lemma 3 are met for $r = \sqrt{n}$, hence we obtain an $(n - \sqrt{n}, \frac{\ell}{2}, \frac{1}{4} n^{-\frac{1}{10}}, \frac{1}{2} n^{-\frac{3}{5}})$-game having one stage fewer that the original game.

Repeating this for all the $\frac{1}{10} \log n$ stages yields an $(m, \ell', \frac{1}{4} n^{-\frac{1}{10}}, n^{-\frac{3}{50} \log n - \frac{1}{10}})$-game of length 0, where $m := n - \frac{1}{10} \log n \sqrt{n}$ and $\ell' := n^{\frac{3}{20}}$. Now a game of length 0 gives the same edge for every pair of inputs. But the number of paths of length ℓ' in $[m]$ containing one particular edge is at most $m^{\ell'-1}$, whereas the game has to solve the problem for a set of size $\frac{1}{4}n^{-\frac{1}{10}}m^{\ell'}$. But for large n, the latter quantity is strictly larger than the former, hence a game solving $R^m_{stconn_n}$ in $\frac{1}{100}\log^2 n$ rounds cannot exist. □

Lemma 1 now gives us the desired lower bound:

Corollary 5. *$d_{\mathbb{R}}(stconn_n) = \Omega(\log^2 n)$ and $s_{\mathbb{R}}(stconn_n) = n^{\Omega(\log n)}$.*

Cutting Planes

Cutting Planes (CP) are a proof system operating with linear inequalities of the form $\sum_{i\in I} a_i x_i \geq k$, where the coefficients a_i and k are integers. The rules of CP are addition of two inequalities, multiplication by a positive integer and division by a positive integer that evenly divides all coefficients on the left hand side, whereby the right hand side is divided by that integer and rounded up.

A CP refutation of a set E of inequalities is a derivation of $0 \geq 1$ from the inequalities in E and the axioms $x \geq 0$ and $-x \geq -1$ for any variable x, using the rules of CP. It can be shown that a set of inequalities has a CP-refutation iff it has no $\{0,1\}$-solution.

Cutting Planes can be used as a refutation system for propositional formulas in conjunctive normal form: note that a clause $\bigvee_{i\in P} x_i \vee \bigvee_{j\in N} \neg x_j$ is satisfiable iff the inequality $\sum_{i\in P} x_i - \sum_{j\in N} x_j \geq 1 - |N|$ has a $\{0,1\}$-solution. It is also easily seen that CP can simulate resolutions. For more information on Cutting Planes, see the references cited below.

A CP-refutation is called tree-like if every line in the refutation is used at most once as a premise to an application of a rule, so that the derivation can be represented as a tree. Exponential lower bounds for tree-like CP-refutations were given in [4]. That paper left open the question whether tree-like CP can polynomially simulate arbitrary CP, i.e. whether for some polynomial $p(x)$, every set of inequalities that has a CP refutation of size s also has a tree-like CP refutation of size $p(s)$.

The question was answered for the subsystem CP^*, where every coefficient appearing in a refutation must be bounded by a polynomial in the size of the original inequalitites, by [1]: they showed that CP^* cannot be simulated by tree-like CP^*. We shall show the same for CP with arbitrary coefficients.

Cutting Planes refutations are linked to monotone real circuits by the following interplation theorem due to Pudlák:

Theorem 6 (Pudlák [8]). *Let $\bar{p}, \bar{q}, \bar{r}$ be disjoint vectors of variables, and let $A(\bar{p}, \bar{q})$ and $B(\bar{p}, \bar{r})$ be sets of inequalities in the indicated variables such that the variables $\bar{p}$ either have only nonnegative coefficients in $A(\bar{p}, \bar{q})$ or have only nonpositive coefficients in $B(\bar{p}, \bar{r})$.*

Suppose there is a CP refutation R of $A(\bar{p}, \bar{q}) \cup B(\bar{p}, \bar{r})$. Then there is a monotone real circuit $C(\bar{p})$ of size $O(|R|)$ such that for any vector $\bar{a} \in \{0,1\}^{|\bar{p}|}$

$$\begin{array}{lcl} C(\bar{a}) = 0 & \rightarrow & A(\bar{a}, \bar{q}) \text{ is unsatisfiable} \\ C(\bar{a}) = 1 & \rightarrow & B(\bar{a}, \bar{r}) \text{ is unsatisfiable} \end{array}$$

Furthermore, if R is tree-like, then $C(\bar{p})$ is a monotone real formula.

The following sets of clauses representing st-connectivity were considered in [3]: In the set $A(\bar{p}, \bar{q})$, the variables $\bar{q}$ code a path from s to t in the graph given by prositional variables $p_{\{i,j\}}$ with $i, j \in N$, where we set $s = 0$ and $t = n + 1$:

$$\begin{array}{ll} q_{0,s}, \qquad q_{n+1,t} & \\ \neg q_{i,j} \vee \neg q_{i,k} & \text{for } 0 \leq i \leq n+1 \text{ and } 0 \leq j < k \leq n+1 \\ q_{i,1} \vee \ldots \vee q_{i,n} & \text{for } 1 \leq i \leq n \\ \neg q_{i,j} \vee \neg q_{i+1,k} \vee p_{\{j,k\}} & \text{for } 0 \leq i < n+1 \text{ and } j, k \in N \text{ with } j \neq k \, . \end{array}$$

In the set $B(\bar{p}, \bar{r})$, the variables $\bar{r}$ code a partition of N into two classes with s and t being in different classes and no edge between nodes in different classes. It is given as

$$\neg r_s \, , \qquad r_t \, , \qquad \neg r_i \vee \neg p_{\{i,j\}} \vee r_j \quad \text{for } i, j \in N \text{ with } i \neq j \, .$$

Observe that the variables $p_{\{i,j\}}$ occur only positively in $A(\bar{p}, \bar{q})$ and only negatively in $B(\bar{p}, \bar{r})$, which makes Theorem 6 applicable. Now the formula $C(\bar{p})$ obtained from a tree-like CP-refutation in this case has to compute $stconn_n$, and hence has to be of size $n^{\Omega(\log n)}$, which gives:

Theorem 7. *A tree-like CP refutation of the (inequalities representing) clauses $A(\bar{p}, \bar{q}) \cup B(\bar{p}, \bar{r})$ has to be of size $n^{\Omega(\log n)}$.*

On the other hand, it was shown in [3] that the clauses $A(\bar{p}, \bar{q}) \cup B(\bar{p}, \bar{r})$ have resolution refutations of size $O(n^4)$. Hence tree-like Cutting Planes cannot polynomially simulate (non-tree-like) resolutions, and in particular, they cannot polynomially simulate non-tree-like Cutting Planes.

Acknowledgements: The author would like to thank Jan Krajíček, who discovered an error in an earlier alleged proof of Theorem 4, and Sam Buss for several helpful discussions.

References

[1] M. L. Bonet, T. Pitassi, and R. Raz. Lower bounds for cutting planes proofs with small coefficients. In *Proc. 27th STOC*, pages 575–584, 1995.

[2] R. B. Boppana and M. Sipser. The complexity of finite functions. In J. van Leeuwen (ed.), *Handbook of Theoretical Computer Science Vol. A*, chapter 14, pages 757–804. Elsevier, Amsterdam, 1990.

[3] P. Clote and A. Setzer. A note on Degen's generalization of the pigeonhole principle, *st*-connectivity, and odd charged graphs. In: P. Beame and S. Buss (eds.), *Feasible Arithmetics and Proof Complexity*, to appear

[4] R. Impagliazzo, T. Pitassi, and A. Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Proc. 9th LICS*, pages 220–228, 1994.

[5] M. Karchmer. *Communication Complexity: A New Approach to Circuit Depth.* MIT Press, Cambridge, 1989.

[6] M. Karchmer and A. Wigderson. Monotone circuits for connectivity require super-logarithmic depth. In *Proc. 20th STOC*, pages 539–550, 1988.

[7] J. Krajíček. Interpolation by a game. Submitted for publication, 1997. Available as ECCC TR97-015.

[8] P. Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symb. Logic*, to appear.