Monotone Circuits for Matching Require Linear Depth

Ran Raz Avi Wigderson *

The Hebrew University

February 11, 2003

Abstract

We prove that monotone circuits computing the perfect matching function on n-vertex graphs require $\Omega(n)$ depth. This implies an exponential gap between the depth of monotone and nonmonotone circuits.

CR categories: F.1.1, Models of Computation, Unbounded Action Devices.

*This research was partially supported by the American-Israeli Binational Science Foundation grant number 87-00082

General Terms: THEORY

Key words: circuit depth, monotone computation, perfect matching

1 Introduction

In 1985 Razborov [R1] proved a superpolynomial lower bound on the **size** of monotone circuits computing the perfect matching function. As matching is in P, this result first showed a superpolynomial gap between the size of monotone and non-monotone circuits. This gap was shown to be exponential by Tardos [T] (with a different monotone function in P).

Another exponential gap for size, when the circuits are restricted to have constant depth, was proved by Ajtai and Gurevich [AG].

Karchmer and Wigderson [KW] studied the **depth** of boolean circuits, and characterized it in communication complexity terms. This approach was used in proving an $\Omega((logn)^2)$ lower bound on the depth of monotone circuits computing st-connectivity. No nontrivial gap was known between the depth of monotone and non-monotone circuits.

Our main result is that every monotone circuit that decides if an n node graph has a matching of size $n/3$ must have depth $\Omega(n)$. The proof uses the communication complexity approach of [KW]. It consists of a sequence of simple reductions from the probabilistic communication complexity of the set disjointness function, for which a linear lower bound was known [KS].

The same lower bound is derived for the bipartite perfect matching and clique functions.

From the main result we deduce a hierarchy theorem for monotone depth, and an exponential gap between monotone and nonmonotone depth.

The next section contains the necessary definitions. In section 3 we prove the main result, and in section 4 we describe some of its consequences.

2 Preliminaries

Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a monotone booelan function. We consider here boolean circuits for f over the boolean $\{\wedge, \vee, \neg\}$ and monotone $\{\wedge, \vee\}$ bases. All gates have fanin 2. Negations, if any, occur only at the inputs.

Let $d(f)$ (resp. $d^m(f)$) denote the minimal depth of any circuit (resp. monotone circuit) computing f.

Let X, Y, Z be finite sets, and let $R \subseteq X \times Y \times Z$ be a relation. A *deterministic communication protocol* A over (X, Y, Z) specifies the exchange of information bits by two players, I and II, that initially receive as inputs $x \in X$ and $y \in Y$, respectively, and finally agree on a value $A(x,y) \in Z$. Denote by $c_A(x,y)$ the number of bits exchanged by I and II on the input pair (x,y) when using protocol A. Let $c_A(R) = \max_{(x,y)\in X\times Y} c_A(x,y)$.

We say that A *computes* R if for all $(x,y) \in X \times Y$ we have $(x,y,A(x,y)) \in R$. Then the *deterministic communication complexity* of the relation R is $c(R) = min\{c_A(R)|A \text{ computes } R\}$.

We accomodate the more common notion of computing functions (rather than relations) in a natural way. If R has the property that for every (x,y) there is a unique $z(x,y) \in Z$ with $(x,y,z) \in R$, then we identify the relation R with the function $R : X \times Y \rightarrow Z$ where $R(x,y) = z(x,y)$.

A *probabilistic protocol* A is simply a probability distribution over deterministic protocols. Equivalently, we can think of A as a deterministic protocol in which the two players I and II *share* an (infinite) random string. Then $c_A(x,y)$ is the *expected* number of bits exchanged by I and II on input pair (x,y). As before, $c_A(R) = \max_{(x,y)\in X\times Y} c_A(x,y)$.

A probabilistic protocol A ϵ-*computes* the relation R if for all $(x,y) \in X \times Y$, $Prob[(x,y,A(x,y)) \in R] \geq 1-\epsilon$. The ϵ-*error probabilistic communication complexity* of R is thus defined by $c_\epsilon(R) = \min\{c_A(R) \mid A\ \epsilon - \text{computes } R\}$.

A trivial observation that we shall use is:

Fact 2.1 *If a relation R' is a restriction of a relation R to a subset $X' \subset X$, $Y' \subset Y$, then $c(R') \leq c(R)$, and for every ϵ, $c_\epsilon(R') \leq c_\epsilon(R)$.*

Our starting point for proving a monotone depth lower bound is the relationship, discovered by [KW], between circuit depth of a Boolean function and the communication complexity of an associated relation. Specifically, let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a monotone Boolean function. Recall that a minterm (resp. maxterm) of f is a minimal subset of $[n]$, such that setting the associated variables to 1 (resp. 0) forces the function f to take the value 1 (resp. 0). Let $MIN(f)$, $MAX(f)$ denote its sets of minterms and maxterms, respectively. Let the relation $R_f^m \subseteq MIN(f) \times MAX(f) \times [n]$ be defined by $(p, q, i) \in R_f^m \iff i \in p \cap q$. (In words, player I gets a minterm, player II gets a maxterm, and their task is to find a member of the intersection of these two sets, which always exists). Then

Theorem 2.1 (KW)

$$d^m(f) = c(R_f^m)$$

3 The Lower Bound

All functions and relations defined hereafter will be paramentrized by the integer m. Let N be a set of vertices, $|N| = n = 3m$. Let $MATCH$ be the monotone function that on input graph $G = (N, E)$, $MATCH(G) = 1$ iff G has a matching of m edges. Our goal is to prove:

Main Theorem:

$$d^m(MATCH) = \Omega(n)$$

Let $DISJ : \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}$ be the disjointness function, i.e. $DISJ(x, y) = 1$ iff $\forall i \in [m]\ x_i \wedge y_i = 0$. It was first proved by [KS] (and simplified in [R3]) that even probabilistic protocols for $DISJ$ require a linear number of bits.

Theorem 3.1 [KS]

$$c_{\frac{1}{3}}(DISJ) = \Omega(m)$$

We shall use a sequence of deterministic and probabilistic reductions to derive $d^m(MATCH) \geq c_{\frac{1}{3}}(DISJ)$, from which the Main Theorem follows.

Let P_N be the set of all m-matchings over N. (Each member of P_N is a set of m disjoint pairs (edges) from N). Let $\hat{Q}_N$ be the set of all $(m-1)$-subsets of N. Let E_N denote of all pairs (edges) from N. Finally define the relation $\hat{M} \subset P_N \times \hat{Q}_N \times E_N$ by $(p, \hat{q}, e) \in \hat{M}$ iff both $e \in p$ and $e \cap \hat{q} = \emptyset$.

Proposition 3.1

$$c(\hat{M}) \leq d^m(MATCH)$$

Proof: Note that P_N is the set of minterms of $MATCH$. Also, $\hat{q} \in \hat{Q}_N$, interpreted as a clique on the nodes $(N \setminus \hat{q})$ is a maxterm of $MATCH$. Finally, an edge e such that $e \in p$ and $e \cap \hat{q} = \emptyset$ is in the intersection of this minterm-maxterm pair. Hence $\hat{M}$ is a restriction of the relation R^m_{MATCH}, and the proposition follows from Theorem 2.1 and Fact 2.1.

♠

We will now define a decision problem (function) M related to the search problem (relation) $\hat{M}$. Let Q_N be the set of all m-subsets of N. Let $M : P_N \times Q_N \to \{0, 1\}$ be the function defined by $M(p, q) = 1$ iff there exists no edge $e \in p$ such that $e \cap q = \emptyset$. Before stating the formal relationship between M and $\hat{M}$ we need some more notation.

For $j \in \{0, 1, 2\}, p \in P_N, q \in Q_N$, let $\alpha_j(p, q) = |\{e \in p : |e \cap q| = j\}|$. For $0 \leq i \leq m$ define

$W_i = \{(p, q) \in P_N \times Q_N \mid \alpha_0(p, q) = i, \alpha_1(p, q) = m - i, (\alpha_2(p, q) = 0)\}$. Now

M can be defined equivalently by $M(p,q) = 1$ iff $(p,q) \in W_0$).

We say that a (probabilistic) communication protocol A is *good on average for M* if it has the following two properties: (which informally state that A is always correct on W_0, and is correct on half the inputs in each $W_i, i \geq 1$)

1. $Prob_{W_0}[A(p,q) = M(p,q) = 1] = 1$

2. For every i, $1 \leq i \leq m$, $Prob_{W_i}[A(p,q) = M(p,q) = 0] \geq \frac{1}{2}$

Here $Prob_{W_i}[A(p,q) = \ldots] = E[Prob[A(p,q) = \ldots]]$ where the expectation E is over the pairs $(p,q) \in W_i$ with the uniform distribution.
Let $\tilde{c}(M) = \min\{c_A(M) \mid A \text{ is good on average for } M\}$.

Proposition 3.2

$$\tilde{c}(M) \;\leq\; c(\hat{M}) + 1$$

Proof: We use an optimal deterministic protocol A for $\hat{M}$ to construct a probabilistic protocol B for M that is good on average and has essentially the same complexity.

Let $(p,q) \in P_N \times Q_N$ be an input of M. Recall that the players wish to determine if $(p,q) \in W_0$. The player holding q removes one point $u \in q$ at random, resulting in an $(m-1)$-subset $\hat{q}$. The players use the optimal protocol A on $(p, \hat{q})$ to find an edge $e = A(p, \hat{q})$ such that $e \in p$ and $e \cap \hat{q} = \emptyset$. Then they compute $B(p, q) = 1$ if $u \in e$ and $B(p, q) = 0$ otherwise.

Clearly, if $(p, q) \in W_0$, then $B(p, q) = 1$ (correctly). Consider now an input $(p, q) \in W_1$. (For $W_i, i > 1$ the proof is similar). If B is lucky enough to remove the unique "free" point in q (which misses all edges of p), then it answers '0' correctly.

Otherwise, in the resulting $(p, \hat{q})$ there are exactly two edges $e_1, e_2 \in p$ that are disjoint from $\hat{q}$. Exactly one of them is (consistently) returned by algorithm A (which is determinstic).

There are four possible (p, q) that could result in this $(p, \hat{q})$, namely when the removed point u is an endpoint of either e_1 or e_2. Then clearly in exactly two of these four cases B answers '0' (correctly).

♠

We will now define the 3-letter distinctness function $DIST$, that somewhat resembles the disjointness function $DISJ$. Let $V = \{a, b, c\}^m$. $DIST : V \times V \rightarrow \{0, 1\}$ is defined by $DIST(u, v) = 1$ iff

$\forall i \in [m]\ u_i \neq v_i$.

Proposition 3.3

$$c_{\frac{1}{3}}(DIST) \leq \tilde{c}(M)$$

Proof: For $u, v \in V$ we define $\beta(u,v) = |\{k \in [m] : u_k = v_k\}|$. For each i, $0 \leq i \leq m$ let $Z_i = \{(u,v) \in V \times V |\, \beta(u,v) = i\}$. (Note that $DIST$ can be equivalently defined by $DIST(u,v) = 1$ iff $(u,v) \in Z_0$.)

We use an optimal protocol B that is good on average for M, to construct a probabilistic protocol C that $\frac{1}{3}$-computes $DIST$, and has the same complexity.

The players consider their random string as an encoding of a pair (S, ρ), all pairs equally likely. $S = (S_1, S_2, \ldots S_m)$ is a partition of the vertex set N into a sequence of triples S_i, ($|S_i| = 3$).

$\rho = (\rho_1, \rho_2, \ldots \rho_m)$ is a sequence of random 1-1 mappings

$\rho_i : \{a, b, c\} \rightarrow S_i$. For $\gamma \in \{a, b, c\}$ define the "complementary" mapping

$\bar{\rho}_i(\gamma) = S_i \setminus \{\rho_i(\gamma)\}$.

Each pair (S, ρ) defines two mappings, $\sigma_I : V \rightarrow P_N$, $\sigma_{II} : V \rightarrow Q_N$ as follows.

$$\sigma_I(u) = \{\bar{\rho}_1(u_1), \bar{\rho}_2(u_2), \ldots \bar{\rho}_m(u_m)\}$$

$$\sigma_{II}(v) = \{\rho_1(v_1), \rho_2(v_2), \ldots \rho_m(v_m)\}$$

.

On input pair (u,v), player I computes $p = \sigma_I(u)$, player II computes $q = \sigma_{II}(v)$ and they use protocol B to compute $B(p,q)$. Now they flip a biased coin with $Prob[H] = \frac{1}{3}$, and decide as follows. If H then $C(u,v) = 0$ else $C(u,v) = B(p,q)$.

Claim: For every $(u,v) \in V \times V,\ Prob[C(u,v) = DIST(u,v)] \geq \frac{2}{3}$

Proof of Claim: Note that $V \times V$ is the disjoint union of the sets Z_i, $0 \leq i \leq m$. We prove the claim separately for each i.

For each $(u,v) \in Z_i$ note that $(p,q) = (\sigma_I(u), \sigma_{II}(v))$ is a uniformly distributed random variable in $W_i \subseteq P_N \times Q_N$. Recall that B is good on average for M, which means that it is always correct on W_0, and is correct with probability at least $\frac{1}{2}$ for random pairs in each $W_i, i \geq 1$. Hence we have:

$$Prob[C(u,v) = DIST(u,v)] = \frac{1}{3} \cdot 0 + \frac{2}{3} \cdot 1 = \frac{2}{3} \text{ when } (u,v) \in Z_0$$

$$Prob[C(u,v) = DIST(u,v)] \geq \frac{1}{3} \cdot 1 + \frac{2}{3} \cdot \frac{1}{2} = \frac{2}{3} \text{ when } (u,v) \in Z_i, 1 \leq i$$

♠

Finally we relate the probabilistic communication complexity of the functions $DIST$ and $DISJ$.

Proposition 3.4

$$c_{\frac{1}{3}}(DISJ) \leq c_{\frac{1}{3}}(DIST)$$

Proof: We describe a probabilistic protocol D for $DISJ$ that uses an optimal probabilistic protocol C for $DIST$. Players I and II get respectively inputs x and y from $\{0,1\}^m$. Define two mappings
$\tau_I, \tau_{II} : \{0,1\} \to \{a,b,c\}$ by $\tau_I(0) = a, \tau_{II}(0) = b, \tau_I(1) = \tau_{II}(1) = c$. These mappings naturally extend to $\tau_I, \tau_{II} : \{0,1\}^m \to V$.

Player I computes $u = \tau_I(x)$, player IIcomputes $\tau_{II}(y)$, and use protocol C to compute $D(x,y) = C(u,v)$. Clearly, $DISJ(x,y) = DIST(\tau_I(x), \tau_{II}(y))$, so if C ϵ-computes $DIST$ then D ϵ-computes $DISJ$.

♠

4 Consequences

4.1 Lower Bounds on Other Functions

Define three more monotone functions on graphs, with $|N| = n$:

- **PM**: Does G on vertex set N have a perfect matching?
- **BPM**: Does a bipartite G on vertices $N \bigcup \bar{N}$ have a perfect matching?

- **CL(k)**: Does G on vertex set N have a clique of size $> k$?

Theorem 4.1

$$d^m(PM) = \Omega(n)$$

Proof: Immediate from the Main Theorem by a standard reduction from $MATCH$: simply add m new vertices to the input graph, and connect each of them to all the original vertices. The new graph has a perfect matching iff the input graph had a matching of size m.

♠

Theorem 4.2

$$d^m(BPM) = \Omega(n)$$

Proof: The communication problem $\hat{M}$ on $(P_N, \hat{Q}_N)$ is easily reduced to the relation R^m_{BPM} associated with BPM on nodes $N \bigcup \bar{N}$: Duplicate each vertex ($\bar{i}$ for each original $i \in N$) and put edges $(i, \bar{j})$ and $(j, \bar{i})$ for each original (i, j). The two players transform their inputs accordingly, and any solution $(i, \bar{j})$ or $(j, \bar{i})$ to the new problem corresponds to a solution (i, j) for the original problem $\hat{M}$.

Warning: this is not a general reduction of PM to BPM (which could not work!). This reduction works only because the lower bound used just $\hat{Q}_N$ as maxterms (they are not all maxterms).

♠

Theorem 4.3

$$d^m(CL((2n/3)+1)) = \Omega(n)$$

Proof: A simple reduction from the search problem $\hat{M}$ to the relation R^m_{CL} associated with CL. All we have to observe is that $\hat{Q}_N$ are cliques of size $(2n/3)+1$, i.e. minterms of CL. Also, P_N is a subset of the maxterms of CL. Hence, a protocol for R^m_{CL} is in fact a protocol for $\hat{M}$, with the names of the players switched.

♠

As a corollary to Theorem 4.3 we get a depth bound on $CL(k)$, for every k. For large k it is better than the one derived from the size bounds of [R1] and [AB], and the direct bound of [GH].

Corollary 4.1 *For every $k = k(n) \le n/2$,*

$$d^m(CL(k)) = \Omega(k)$$

Finally, all these lower bounds hold even for the probabilistic communication complexity of the associated boolean relations. As in [RW], let $C_0(R)$ denote the Las Vegas (error free) probabilistic communication complexity of a relation R. Then, for example, we have:

Theorem 4.4 $C_0(R^m_{BPM}) = \Omega(n)$.
(In words, the probabilistic communication complexity of the monotone relation of BPM is $\Omega(n)$).

Similar results hold for the other functions discussed above, even in the Monte Carlo probabilistic model that allows ϵ error probability per input (see [RW]).

4.2 Hierarchy and Gap Theorems

Let $L \subseteq \{0,1\}^*$ be a language, and let $L_n : \{0,1\}^n \rightarrow \{0,1\}$ be the boolean function mapping exactly those strings in L of length n to '1'. Say that the language L is *monotone* if for every integer n the function L_n is monotone. For a function g on the integers we define two complexity classes of monotone languages, $MDEPTH(g(n))$ and $MDEPTH^m(g(n))$. A monotone language L is in $MDEPTH(g(n))$ (resp. $MDEPTH^m(g(n))$) iff $d(L_n) = O(g(n))$

(resp. $d^m(L_n) = O(g(n))$). The obvious inclusions between these classes is summarized below.

Fact 4.1 *For every two functions $h(n), g(n)$ with $h(n) \leq g(n)$ we have*

$$MDEPTH^m(h(n)) \subseteq MDEPTH^m(g(n)) \subseteq MDEPTH(g(n)) \subseteq MDEPTH^m(n)$$

Theorem 4.5 (Hierarchy theorem for monotone depth) *For every two functions $g(n) \leq \sqrt{n}$, and $h(n) = o(g(n))$,*

$$MDEPTH^m(h(n)) \not\supseteq MDEPTH^m(g(n)) \cap P$$

Proof: It is easy to see that $d^m(MATCH) = O(m)$, i.e. the lower bound of the main theorem is tight. The number of boolean variables in $MATCH$ is $O(m^2)$, so together with the lower bound we get the separation for $g(n) = \sqrt{n}$. For smaller functions $g(n)$ the result follows by padding.

♠

The theorem above shows that there are families of functions on n bits in P that are computable in monotone depth $g(n)$ but not $o(g(n))$ (for $g(n) < \sqrt{n}$). By counting we know that such families exist that separate monotone depth $g(n)$ from $g(n) - 1$. Can such a tight hierarchy be formed by explicit functions, say in P or NP ? Noga Alon [Al] recently used our results to give an answer which is almost as good - his separating functions are projections of NP functions.

Theorem 4.6 (Al) *There is a family of functions on $n(n+3)$ variables in NP, such that for every $1 \leq g(n) \leq n/1000$ there is a restriction of the nth function whose monotone depth is exactly $g(n)$.*

Proof sketch: The function is the following variant of the clique function: The input is a graph on n vertices, and two integers k and l (where both $n-k$ and $n-l$ are given in unary for monotonicity). The question is whether the graph has a k-clique containing the first (in some fixed ordering) l vertices.

The theorem follows easily from the following claim. For every t, the set of monotone depths of circuits for computing the functions with parameters $1 \leq l, k, n \leq t$ forms an interval of integers between 1 and at least $t/1000$. Clearly, taking $n = t, k = (2n/3) + 1, l = 0$ requires by theorem 4.3 depth at least $t/1000$. Also, the theorem clearly follows from the claim, as every depth in the interval is achieved.

The proof that indeed this set is an interval is by induction on t. For $t \leq 3$ it is easy to check. In moving from $t-1$ to t, proceed by backwards induction on $k+l$. When $l=k=n=t$, the question is whether the input graph is a clique, which needs depth $\log((n-1)n/2)$, and one can check that with all depths obtained from smaller values of t it is still an interval. This gives the base case, $l+k=2n$. When $l+k<2n$, the cases $k=n$ and $l=k$ are easy, and otherwise one can decrease $l+k$ by removing a vertex. The exact details are left to the reader.

♠

Razborov's lower bound [R2] on the size of monotone circuits for matching proved that for size, nonmonotone circuits are superpolynomially stronger than monotone circuits. Tardos [T] improved this to an exponential gap by considering a function in P related to the clique function. We prove a similar gap for circuit depth.

Theorem 4.7 (Exponential gap between monotone and nonmonotone depth) *For every function* $g(n) \leq \sqrt{n}$

$$MDEPTH^m(g(n)) \not\supseteq MDEPTH(\log^2 g(n))$$

Proof: Borodin, von zur Gathen and Hopcroft [BGH] observed that a randomized algorithm for matching, proposed by Lovasz [L], can be implemented by shallow circuits, i.e. $d(MATCH) = O(\log^2 m)$. This result with our lower bound give the separation for $g(n) = \sqrt{n}$. Again, for smaller functions $g(n)$ the result follows by padding.

♠

Corollary 4.2 *There is a monotone function in NC^1 that has no monotone NC circuits.*

Proof: Choose $g(n) = 2^{\sqrt{\log n}}$ in the gap theorem.

♠

4.3 Branching Programs

A monotone branching program over $X = \{x_1, \ldots, x_n\}$ is a directed graph H with distinguished nodes s, t, and some arcs labeled with elements from X. An assignment σ to the variables in X defines in a natural way a subgraph H_σ of H. Let $H(\sigma) = 1 \iff H_\sigma$ has an $s - t$ path. Then H defines a monotone boolean function, and for every monotone function f, let *mbp(f)* be the size of the smallest H computing f.

Theorem 4.8

$$mbp(BPM) = 2^{\Omega(\sqrt{n})}$$

Proof: A monotone branching program of size s can be easily converted into a monotone circuit of f of depth $O((\log s)^2)$.

♠

REFERENCES

[**A**] A. E. Andreev, "On a Method for Obtaining Lower Bounds on the Complexity of Individual Monotone Functions", *Dokl. Ak. Nauk. SSSR*, Vol 282, pp. 1033-1037, 1985 (in Russian). English translation in: *Sov. Math. Dokl.*, Vol 31, pp. 530-534, 1985.

[**Al**] N. Alon, Private communication.

[**AB**] N. Alon and R. Boppana, "The Monotone Circuit Complexity of Boolean Functions", *Combinatorica*, Vol 7, No. 1, pp. 1-22, 1987.

[**AG**] M. Ajtai and Y. Gurevich, "Monotone versus Positive", *JACM*, Vol. 34, No. 4, pp. 1004-1015, 1987.

[**BGH**] A. Borodin, J. von zur Gathen and J. Hopcroft, "Fast parallel Matrix and GCD Computations", *Proceedings of the 23rd STOC*, pp. 65-71, 1982.

[**GH**] M. Goldmann and J. Hastad, "A Lower Bound for Monotone Clique using a Communication Game", Manuscript.

[**K**] M. Karchmer "The Complexity of computation and restricted Machines" *Ph.D Thesis, The Hebrew University,* 1988.

[**KS**] B. Kalyanasundaram and G. Schnitger "The Probabilistic Communication Complexity of Set Intersection", *Proceedings Structure in Complexity Theorey* pp.41-49, 1987.

[**KW**] M. Karchmer and A. Wigderson "Monotone Circuits for Connectivity Require Super-logarithmic Depth" *Proceedings of the 20th STOC*, pp. 539-550, 1988.

[**L**] L. Lovasz, "Determinants, Matchings and Random Algorithms", in: *Proceedings of FCT '89*, (ed. L. Budach), Akademie-Verlag, pp. 565-574, 1979.

[**R1**] A. A. Razborov, "Lower Bounds for the Monotone Complexity of some Boolean Functions", *Dokl. Ak. Nauk. SSSR*, Vol 281, pp. 798-801, 1985 (in Russian). English translation in *Sov. Math. Dokl.* Vol 31, pp. 354-357, 1985.

[**R2**] A. A. Razborov, "Lower Bounds on the Monotone Network Complexity of the Logical Permanent", *Mat. Zametki*, Vol 37, pp. 887-900, 1985 (in Russian). English translation in : *Math. Notes of the Academy of Sciences of USSR*, Vol 37, pp. 485-493, 1985.

[R3] A. A. Razborov, "On the Distributional Complexity of Disjointness", ICALP 1990.

[RW] R. Raz and A. Wigderson, "Probabilistic Communication Complexity of Boolean Relations", *Proc. of the 30th FOCS*, to appear, 1989.

[T] E. Tardos, "The Gap between Monotone and Non-monotone Circuit Complexity is Exponential", *Combinatorica*, Vol 8, pp. 141-142, 1988.

[W] I. Wegner, *The Complexity of Boolean Functions* John Wiley, 1988.

[Y] A. C.-C. Yao, "Some Complexity Questions Related to Distributive Computing", *Proceedings of* 11^{th} *STOC*, pp. 209-213 (1979).