# MAX-PLANCK-INSTITUT FÜR INFORMATIK

## Mod $m$ Gates do not Help on the Ground Floor

Technical Report No. MPII–1993–142

Vince Grolmusz
Max Planck Institute for Computer Science
and Eötvös University

October 11, 1993

MPI INFORMATIK

Im Stadtwald
66123 Saarbrücken
Germany

# Mod $m$ Gates do not Help on the Ground Floor

Technical Report No. MPII–1993–142

Vince Grolmusz
Max Planck Institute for Computer Science
and Eötvös University

October 11, 1993

# MOD m Gates do not Help on the Ground Floor

Technical Report No. MPII–1993–142

Vince Grolmusz

Max Planck Institute and Eötvös University

Keywords: communication complexity, random protocols, lower bounds, parallel computation

**ABSTRACT:**

We prove that any depth–3 circuit with MOD $m$ gates of unbounded fan-in on the lowest level, AND gates on the second, and a weighted threshold gate on the top needs either exponential size or exponential weights to compute the *inner product* of two vectors of length $n$ over GF(2). More exactly we prove that $\Omega(n \log n) \leq \log w \log M$, where $w$ is the sum of the absolute values of the weights, and $M$ is the maximum fan–in of the AND gates on level 2. Setting all weights to 1, we got a trade–off between the logarithms of the top–fan–in and the maximum fan–in on level 2.
In contrast, with $n$ AND gates at the bottom and *a single* MOD 2 gate at the top one can compute the *inner product* function.
The lower–bound proof does not use any monotonicity or uniformity assumptions, and all of our gates have unbounded fan–in. The key step in the proof is a *random* evaluation protocol of a circuit with MOD $m$ gates.

---

Address: Max Planck Institute for Computer Science, Im Stadtwald, D-66123 Saarbruecken, GERMANY; email: grolmusz@mpi-sb.mpg.de

## 1. INTRODUCTION

### 1.1 Class ACC

The class **ACC** consists of those languages which are accepted by sequences of bounded–depth, polynomial circuits of AND, OR, NOT and MOD $m$ gates, where a MOD $m$ gate outputs 1 if the sum of its inputs is divisible by $m$, and 0 otherwise. This class was first defined by *Barrington* [Ba].

Considerable efforts were done to prove that some restricted versions of **ACC** do not contain several "natural" languages.

*Razborov* [R1] proved that the MAJORITY function needs exponential size if it is computed by bounded–depth circuits with AND, OR, NOT and MOD 2 gates.

*Smolensky* [Sm] generalized this result to circuits with MOD $p$ gates instead of MOD 2 ones, where $p$ is a prime or prime–power. The case, where $p$ is a non-prime–power composite number, remained widely open.

*Yao* [Y3] showed that any language in ACC is accepted by a depth–3 threshold circuit of size $\exp(\log^{O(1)} n)$.

*Beigel* and *Tarui* [BT] proved that **ACC** can be recognized by a depth–2 circuit of size $\exp(\log^{O(1)} n)$ with a SYMMETRIC gate at the top, and AND gates on the bottom.

*Allender* and *Gore* [AG] proved that any *uniform* sequence of **ACC**–circuits needs exponential size to compute the *permanent* function. Using the uniformity assumption is *essential* here, since it is not known whether there is any language in **NP**, or, even in **NEXP**, which is not an element of *non–uniform* ACC.

Several results show that the computational properties of the MOD $m$ and MOD $p$ gates differ [BBR], [KM], [G3], i.e. the MOD $m$ gates, for non–prime–power $m$, are "stronger" in some sense than the MOD $p$ gates.

On the other hand, we have proved in [G3] that some depth-3 circuits with fan–in $k$ MOD $m$ gates on the bottom need exponential size to compute the $k$-wise inner product function of [BNS], for any odd $m$, for which $m \equiv k \pmod{2m}$. The $k$-wise inner product function of [BNS] can be computed by a *linear-sized* circuit of fan–in $k$ AND gates on the bottom, but, if we allow arbitrary gates at the bottom, but restrict the fan–in to at most $k-1$, then exponential size is needed to compute the $k$-wise inner product function [GH]. So restricting the lower fan–in severely affect the computing power of these circuits.

Without uniformity conditions or fan–in restrictions, we give here a weight—fan-in trade–off for depth–3 circuits with MOD $m$ gates of unbounded fan-in on the bottom:

**Theorem 1.** *Let $m$ and $n$ two positive integers, satisfying $m \le 2^{n^2}$, and let $C$ be a depth–3 circuit with $2n$ input variables $x = (x_1, x_2, ..., x_{2n}) \in \{0,1\}^{2n}$ and their negations on the bottom, unbounded fan–in MOD $m$ gates on the first, unbounded fan–in AND gates on the second and a weighted threshold gate $Y$ with weights $w_1, w_2, ..., w_t$ on the top. Let $M$ denote the maximum fan–in of the AND gates on the second level, and let*

$$w = w(C) = \sum_{i=1}^{t} |w_i|.$$

*If $C$ computes the inner product*

$$IP(x) = \sum_{i=1}^{n} x_{2i-1}x_{2i} \bmod 2$$

*for all $x \in \{0,1\}^{2n}$, then*

$$\frac{1}{5}n\log n - O(\log n) \le \log w \log M$$

**Corollary 2.** *Suppose that in threshold gate $Y$ every weight is equal to 1. Let $K$ denote the fan–in of gate $Y$. Then*

$$\frac{1}{5}n\log n - O(\log n) \le \log K \log M.$$

**Proof.** Use Theorem 1 with $w = K$. ∎

### 1.2 Communication Complexity

The notion of *communication complexity* was introduced by *Yao* [Ya1]. In this model two players, Alice and Bob intend to compute the value of a Boolean function $f(x,y) : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, where Alice knows $x \in \{0,1\}^n$, Bob knows $y \in \{0,1\}^n$, both of them has unlimited computational power (i.e. Alice would compute $f(x,y)$ at once if she also knew $y$). The players communicate through a 2–way channel, and function $f$ is computed, if one of them announces the (correct) value of $f(x,y)$. The cost of the computation is the number of bits communicated.

It is clear that every function can be computed using $n+1$ bits of communication: Alice sends her $n$ bit to Bob, then Bob computes $f(x,y)$, and sends this bit to Alice. The protocol above is optimal if $f = ID$, where $ID$ is defined as

$$ID(x,y) = \begin{cases} 1, & \text{if } x = y, \\ 0 & \text{otherwise} \end{cases}$$

(c.f. [Ya1]).
However, if Alice and Bob are allowed to use probabilistic bits (coin–flips) in their protocol, they can do better: with communicating only $O(\log n)$ bits, they can compute $ID(x)$ with high probability, as it was shown by several authors [Y4], [MS], [JPS], [Ra]:

(i) Alice chooses a random prime $0 < p \le n^2$, and transmits the $(p, x \bmod p)$ pair to Bob.
(ii) Bob outputs "not equal" if $x \not\equiv y \pmod p$ and "equal" otherwise.

The "not equal" answer is always correct. The "equal" may be not. It is incorrect if and only if $p$ divides $x - y \ne 0$. A rough estimation of the probability of this event: $|x-y| \le 2^n$, so $x - y$ has at most $n$ different prime divisors. By the Great Prime Number Theorem, there are $\Omega(n^2/\log n)$ primes $p$ under $n^2$ for Alice to choose from, so the probability that it happens to divide $x - y$ is

$$O\left(\frac{\log n}{n}\right).$$

A version of this random protocol will play a key role in the proof of our Theorem 1.

For a more detailed introduction to communication complexity see [BFS] or [L].

## 2. PROOF OF THEOREM 1

First we prove (Lemma 3) that a depth–2 subcircuit $C_i$ of $C$ correctly computes $IP(x)$ on a "big enough" portion of all inputs. After that we show a probabilistic 2–player protocol in our Main Lemma (Lemma 6) which computes the outcome of circuit $C_i$ with high probability. The proof then concludes with the application of a lower bound result of *Chor* and *Goldreich* [CG] (Theorem 7) which yields also a lower bound to the probabilistic communication complexity of protocols, computing the outcome of $C_i$, and, consequently, for the size and the weight of circuit $C$.

**Lemma 3.** *Let $C_1, C_2, ..., C_t$ denote the depth–2 subcircuits of C, each with an AND gate at the top, and unbounded–fan–in MOD m gates at the bottom. Let Pr denote the probability measure associated with the uniform distribution on $\{0,1\}^{2n}$. Then there exists an i $(1 \geq i \geq t)$ such that either*

$$\frac{1}{2} + \frac{1}{3w} - \frac{1}{2^{\frac{n}{2}-3}} \leq \Pr(C_i(x) = IP(x))$$

or

$$\frac{1}{2} + \frac{1}{3w} - \frac{1}{2^{\frac{n}{2}-3}} \leq \Pr(NOT(C_i(x)) = IP(x)).$$

**Proof.**

**Lemma 4.** ([HMPST], Lemma 3.3)
*Let C be a circuit with 2n inputs, with a threshold gate T with weights $w_1, w_2, ..., w_t$ at the top, $w = \sum_{i=1}^{t} |w_i|$, and suppose that the in–coming wires of gate T are connected to subcircuits $C_1, C_2, ..., C_t$. Let $A, B \subset \{0,1\}^{2n}$ be disjoint sets, such that circuit C accepts the elements of A and rejects those in B. Let $\Pr_A$ (respectively, $\Pr_B$) denote the uniform probability distribution on A (respectively, on B). Then*

$$\max_{1 \leq i \leq t} |\Pr_A(C_i(x) = 1) - \Pr_B(C_i(x) = 1)| \geq \frac{1}{w}.$$

**Proof.** See [HMPST]. ∎

Let us apply Lemma 4 to the circuit $C$ of the statement of Lemma 3. With $A = IP^{-1}(1)$, $B = IP^{-1}(0)$, $w = w(C)$ we get:

$$\text{(1)} \qquad \exists i : 1 \leq i \leq t, \quad |\Pr_A(C_i(x) = 1) - \Pr_B(C_i(x) = 1)| \geq \frac{1}{w}.$$

Then

**Lemma 5.**

$$|\Pr(A) - \Pr(B)| \le \frac{1}{2^{n/2}}.$$

**Proof.** See [HMPST] Lemma 3.4. or [CG]. ∎

Since $\Pr(A) + \Pr(B) = 1$, Lemma 5 implies:

$$\frac{1}{2} - \frac{1}{2^{\frac{n}{2}+1}} \le \Pr(A) \le \frac{1}{2} + \frac{1}{2^{\frac{n}{2}+1}} \tag{2}$$

$$\frac{1}{2} - \frac{1}{2^{\frac{n}{2}+1}} \le \Pr(B) \le \frac{1}{2} + \frac{1}{2^{\frac{n}{2}+1}} \tag{3}$$

It is easy to see that $\Pr_A(C_i(x) = 1) = \Pr(C_i(x) = 1 | x \in A)$, and $\Pr_B(C_i(x) = 1) = \Pr(C_i(x) = 1 | x \in B)$, where $\Pr(X|Y)$ denotes the conditional probability:

$$\Pr(X|Y) = \frac{\Pr(X \text{ AND } Y)}{\Pr(Y)}.$$

So, from (1)

$$\left|\Pr(C_i(x) = 1 | x \in A) - \Pr(C_i(x) = 1 | x \in B)\right| \ge \frac{1}{w}$$

or

$$\left|\frac{\Pr(C_i(x) = 1, x \in A)}{\Pr(x \in A)} - \frac{\Pr(C_i(x) = 1, x \in B)}{\Pr(x \in B)}\right| \ge \frac{1}{w}$$

thus

$$\left|\Pr(C_i(x) = 1, x \in A) - \frac{\Pr(x \in A)}{\Pr(x \in B)}\Pr(C_i(x) = 1, x \in B)\right| \ge \frac{\Pr(x \in A)}{w} \ge \frac{1}{3w}$$

using inequality (2).

By the triangle-inequality:

$$\frac{1}{3w} \le \left|\Pr(C_i(x) = 1, x \in A) - \frac{\Pr(x \in A)}{\Pr(x \in B)}\Pr(C_i(x) = 1, x \in B)\right|$$

$$\le |\Pr(C_i(x) = 1, x \in A) - \Pr(C_i(x) = 1, x \in B)| + \left|1 - \frac{\Pr(x \in A)}{\Pr(x \in B)}\right|\Pr(C_i(x) = 1, x \in B)$$

$$\le |\Pr(C_i(x) = 1, x \in A) - \Pr(C_i(x) = 1, x \in B)| + \frac{1}{2^{\frac{n}{2}-2}}$$

using Lemma 5 and (3).

Consequently

$$(4) \qquad \frac{1}{3w} - \frac{1}{2^{\frac{n}{2}-2}} \leq |\Pr(C_i(x) = 1, x \in A) - \Pr(C_i(x) = 1, x \in B)|.$$

Let us assume now that $\Pr(C_i(x) = 1, x \in A) > \Pr(C_i(x) = 1, x \in B)$.

So

$$\frac{1}{3w} - \frac{1}{2^{\frac{n}{2}-2}} \leq \Pr(C_i(x) = 1, x \in A) - \Pr(C_i(x) = 1, x \in B),$$

and, since $\Pr(x \in B) = \Pr(C_i(x) = 1, x \in B) + \Pr(C_i(x) = 0, x \in B)$:

$$\frac{1}{3w} - \frac{1}{2^{\frac{n}{2}-2}} \leq \Pr(C_i(x) = 1, x \in A) + \Pr(C_i(x) = 0, x \in B) - \Pr(x \in B).$$

From here, using the lower bound in inequality (3):

$$(5) \qquad \frac{1}{2} + \frac{1}{3w} - \frac{1}{2^{\frac{n}{2}-3}} \leq \Pr(C_i(x) = IP(x)),$$

because $\Pr(C_i(x) = IP(x)) = \Pr(C_i(x) = 1, x \in A) + \Pr(C_i(x) = 0, x \in B)$.

Similarly, if $\Pr(C_i(x) = 1, x \in A) < \Pr(C_i(x) = 1, x \in B)$ holds, then – exchanging the roles of $A$ and $B$ – we shall get:

$$(6) \qquad \frac{1}{2} + \frac{1}{3w} - \frac{1}{2^{\frac{n}{2}-3}} \leq \Pr(NOT(C_i(x)) = IP(x)).$$

■

**Lemma 6.** *Let $g(x) = g(x_1, x_2, ..., x_{2n}) : \{0,1\}^{2n} \to \{0,1\}$ such that $g(x)$ is computed by a depth–2 circuit $C_1$ with an AND gate at the top and $N$ $MOD_m$ gates at the bottom. Let $I \subset \{1, 2, ..., 2n\}$, and suppose that Alice knows the values of the variables $U = \{x_i : i \in I\}$, and Bob knows the values of the variables $V = \{x_j : j \in \{1, 2, ..., 2n\} - I\}$. Let $\alpha > 2$. Then there exists a probabilistic protocol which communicates*

$$O(\alpha \log N + \log\log m)$$

*bits, and for each $x \in \{0,1\}^{2n}$, it computes $g(x)$ with success probability at least*

$$1 - \frac{\alpha \log N + \log\log m}{N^{\alpha-1}}.$$

**Proof.** One can suppose that both Alice and Bob know the circuit $C_1$ and index-set $I$.

First, they prepare a matrix $T$ with 2 columns and $N$ rows in the following way: Row $\ell$ of $T$ is corresponded to a $\text{MOD}_m$ gate $G_\ell$ of circuit $C_1$:

– The first entry in row $\ell$ is the mod $m$ sum of those inputs of gate $G_\ell$, which are also elements of set $U$ (i.e. known for Alice);
– the second entry in row $\ell$ is the mod $m$ sum of those inputs of gate $G_\ell$, which are also elements of set $V$ (i.e. known for Bob),
for $\ell = 1, 2, ..., N$. (If $\bar{x}_i$ is an input to $G_\ell$, then $1 - x_i$ is added up mod $m$.)

Let us observe that $G_\ell$ outputs 1 if and only if the mod $m$ sum of row $\ell$ of $T$ is 0. Circuit $C_1$ outputs 1, if and only if the mod $m$ sum of *each* row of $T$ is 0.

Since the first column of $T$ consists of sums of variables from $U$, this column is known for Alice. Similarly, the second column of $T$ is known for Bob.
Alice knows the first column of $T$, and that also, that the circuit outputs 1 if and only if every row has a mod $m$ sum 0. Consequently, Alice knows that the only case when the circuit outputs 1 is when the second column of $T$ is

$$t' = (t'_{12}, t'_{22}, ..., t'_{N2})$$

where $t'_{i2} = m - t_{i1} \bmod m$, where $t_{i1}$ is the $i^{th}$ entry in the first column of $T$, $i = 1, 2, ..., N$.

$t'$ can be thought of as an $m$-ary representation of an integer $0 \le t' \le m^N - 1$.

Now we can use a version of the randomized protocol described in Section 1.2:

(i) Alice chooses a random prime $p$:

$$2 \le p \le N^\alpha \log m$$

and transmits the $(p, t' \bmod p)$ pair to Bob with $O(\alpha \log N + \log\log m)$ bits of communication.

(ii) Bob outputs "Yes" if the second column of $T$, interpreted as an $m$–ary number, $t$, is equal to $t' \mod p$, and "No" otherwise.

Again, the "No" answer is always correct. The "Yes" answer is incorrect exactly when $p$ is a divisor of $|t - t'| \le m^N - 1$. By a rough estimation, $t - t'$ has at most $N \log m$ different prime–divisors, but Alice have had

$$\frac{N^\alpha \log m}{\alpha \log N + \log\log m}$$

possibilities to choose from (using the Great Prime Number Theorem), so the failure probability is at most:

$$\frac{\alpha \log N + \log\log m}{N^{\alpha-1}}.$$

∎

Now we are ready to prove our Theorem 1.
Suppose that circuit $C$ computes $IP(x)$. For $i = 1, 2, ..., N$ let $D_i$ be defined as

$$D_i = \{x \in \{0,1\}^{2n} : C_i(x) = IP(x)\}.$$

By Lemma 3, there exists an $i$ such that

$$\frac{1}{2}+\frac{1}{3w}-\frac{1}{2^{\frac{n}{2}-3}} \leq \Pr(D_i)$$

or

$$\frac{1}{2}+\frac{1}{3w}-\frac{1}{2^{\frac{n}{2}-3}} \leq \Pr(\{0,1\}^{2n}-D_i).$$

Without restricting the generality we can assume that the first inequality holds. Let $D = D_i$. Let $g(x)$ be the function, computed by circuit $C_i$. Then

$$\forall\, x \in D: \quad g(x) = IP(x). \tag{7}$$

By Lemma 6, there exists a protocol, which computes $g(x)$, and its success probability is

$$1-\frac{\alpha \log N + \log\log m}{N^{\alpha-1}}, \tag{8}$$

independently from $x$.
Because of (7), if Alice and Bob computes $g(x)$ with $O(\alpha \log n + \log\log m)$ communication, then they will get the value of $IP(x)$ with probability (8), if $x \in D$.
In other words, if Alice and Bob computes $g(x)$ by the protocol of Lemma 6, then they will get $IP(x)$ with average success probability

$$\Pr(D)\Big(1-\frac{\alpha \log N + \log\log m}{N^{\alpha-1}}\Big), \tag{9}$$

where the "average" is computed over all $x \in \{0,1\}^{2n}$.

We can apply here the lower bound result of *Chor* and *Goldreich* [CG]:

**Theorem 7.** *[CG] Suppose that probabilistic protocol $P$, computing $IP(x)$, has an average success probability at least*

$$\frac{1}{2}+\varepsilon \text{ for some } \varepsilon > \frac{1}{2^{\frac{n}{2}}-2},$$

*and the protocol communicates — for fixed $\varepsilon$ and for fixed $n$ — always $\gamma_\varepsilon(n)$ bits. Then*

$$\gamma_\varepsilon(n) > n-3-3\log\frac{1}{\varepsilon}.$$

■

We can give a lower estimation for the average success probability (9):

$$\Big(\frac{1}{2}+\frac{1}{3w}-\frac{1}{2^{\frac{n}{2}-3}}\Big)\Big(1-\frac{\alpha \log N + \log\log m}{N^{\alpha-1}}\Big) \geq$$

$$\geq \frac{1}{2} + \frac{1}{3w} - \frac{1}{N^{\alpha-2}} \tag{10}$$

if $N^{\alpha-2}$ is not too large.
Let us set $\alpha$ such that

$$6w = N^{\alpha-2}. \tag{11}$$

Then, from (10), and from Theorem 7, with $\varepsilon = N^{-\alpha+2}$:

$$\gamma_\varepsilon(n) > n - 3(\alpha - 2)\log N - O(1). \tag{12}$$

Because of (11), the protocol of Lemma 6 has communication at most $2\log w$, so (12) can be written:

$$2\log w > n - 3(\alpha - 2)\log N - O(1)$$

or

$$n - O(1) < 2\log w + 3\frac{\log w}{\log N}\log N \leq 2\log w + 3\frac{\log w}{\log n}\log N$$

using (11) and the obvious fact that $N \geq n$.
From this

$$n\log n - O(\log n) \leq 2\log w \log n + 3\log w \log N \leq 5\log w \log N$$

or

$$\frac{1}{5}n\log n - O(\log n) \leq \log w \log N \leq \log w \log M$$

which completes the proof. ∎

## 3. A GENERALIZATION

It is not difficult to see that a little modification of the proof of Theorem 1 facilitates giving a lower bound for circuits with EXACT gates at the bottom, instead of MOD $m$ ones. Exploring this idea, we shall define a class of functions, for which our results can be generalized:

**Definition 8.** *Boolean function $f : \{0,1\}^\ell \to \{0,1\}$ is called* **pc–simple** *with parameter $m$ (stays for probabilistic-communication-simple), if for all $I \subset \{1,2,...,\ell\}$ there exist functions $u_I, v_I : \{0,1\}^\ell \to \{1,2,...,m\}$ such that*

- *$u_I$ depends only on variables $\{x_i : i \in I\}$,*
- *$v_I$ depends only on variables $\{x_i : i \in \{1,2,...,\ell\} - I\}$, and*

$$f(x) = 1 \iff u_I(x) = v_I(x).$$

Now we can state

**Theorem 9.** *Let $m$ and $n$ two positive integers, satisfying $m \leq 2^{n^2}$, and let $C$ be a depth–3 circuit with $n$ input variables $x = (x_1, x_2, ..., x_{2n}) \in \{0,1\}^{2n}$ and their negations on the bottom, gates, which computes pc–simple functions with parameter $m$ on the first, unbounded fan–in AND gates on the second and a weighted threshold gate $Y$ with weights $w_1, w_2, ..., w_t$ on the top. Let $M$ denote the maximum fan–in of the AND gates on the second level, and let*

$$w = w(C) = \sum_{i=1}^{t} |w_i|.$$

*If $C$ computes $IP(x)$ for all $x \in \{0,1\}^{2n}$, then*

$$\frac{1}{5} n \log n - O(\log n) \leq \log w \log M$$

**Proof.** (Sketch) The proof is the same as that of Theorem 1, except Lemma 6 should be stated for a depth–2 circuit $C_1$ with an AND gate at the top and gates, computing pc–simple functions with parameter $m$, at the bottom. The probabilistic protocol of Lemma 6 can also be applied to this class of circuits with the same result. The further details are omitted here. ∎

**REFERENCES**

[A] E. Allender: A note on the power of threshold circuits, Proc. 30th IEEE FOCS, 1989, pp. 580-584

[ABFR] J. Aspnes, R. Beigel, M. Furst, S. Rudich: The expressive power of voting polynomials, Proc. 23rd ACM STOC, 1991, pp. 402-409

[Ba] D. A. Barrington: Bounded-width polynomial size branching programs recognize exactly those languages in $NC^1$, Proc. 18th ACM STOC, 1986, 1-5

[BBR] D. A. Barrington, R. Beigel, S. Rudich: Representing Boolean functions as polynomials modulo composite numbers, Proc. 24th ACM STOC, 1992, pp. 455-461

[Be] R. Beigel: When do extra MAJORITY gates help?, Proc. 24th ACM STOC, 1992, pp. 450-454

[BFS] L. Babai, P. Frankl, J. Simon: Complexity classes in communication complexity theory, Proc. 27th IEEE FOCS, 1986, pp. 337-347.

[BG] C.G. Bennet, J. Gill: Relative to a random oracle A, $P^A \neq NP^A \neq co - NP^A$ with probability 1. SIAM J. on Computing, 10, (1981) pp. 96–113.

[BRS] R. Beigel, N. Reingold, D. Spielman: The perceptron strikes back, Proc. 6th Annual Conference on Structure in Complexity Theory, IEEE Comp. Soc. Press, 1991

[BNS] L. Babai, N. Nisan, M. Szegedy: Multiparty Protocols and Pseudorandom Sequences, Proc. 21st ACM STOC, 1989, pp. 1-11.

[BT] R. Beigel, J. Tarui: On ACC, Proc. 32nd IEEE FOCS, 1991, pp. 783-792

[CFL] A. K. Chandra, M. L. Furst, R. J. Lipton: Multi-party Protocols, Proc. 15th ACM STOC, 1983, pp. 94–99.

[CG] B. Chor, O. Goldreich: Unbiased bits from sources of weak randomness and probabilistic communication complexity, Proc. 26th IEEE FOCS, 1985, pp. 429-442

[G] V. Grolmusz: The BNS Lower Bound for Multi–Party Protocols is Nearly Optimal, to appear in "Information and Computation".

[G2] V. Grolmusz: Circuits and Multi–Party Protocols, Technical Report No. MPII-1992-104, Max Planck Institute for Computer Science, Saarbruecken, Germany, 1992,

[G3] V. Grolmusz: Separating the communication complexities of MOD m and MOD p circuits, Proc. 33rd IEEE FOCS, 1992, pp. 278-287

[GH] M. Goldmann, J. Håstad: On the Power of Small–Depth Threshold Circuits, 31st IEEE FOCS, 1990, pp. 610–618.

[HMPST] A. Hajnal, W. Maass, P. Pudlak, M. Szegedy, G. Turán: Threshold Circuits of Bounded Depth, Proc. 28th IEEE FOCS, 1987, pp. 99–110.

[JPS] J. JaJa, V.K. Prasanna Kumar, J. Simon: Information transfer under different sets of protocols, SIAM J. on Computing, 13 (1984) pp. 840-849

[KM] J. Kahn, R. Meshulam: On mod $p$ Transversals, Combinatorica, 1991, (11) No. 1. pp. 17–22.

[KS] B. Kalyanosundaram, G. Snitger: The Probabilistic Communication Complexity of Set Intersection, Proc. Structure in Complexity Theory, 1987, pp. 41–49.

[KW] M. Karchmer, A. Wigderson: Monotone Circuits for Connectivity Require Super–Logarithmic Depth, Proc. 20th ACM STOC, 1988, pp. 539–550

[L] L. Lovász: Communication Complexity: A Survey, Technical Report, CS–TR–204–89, Princeton University, 1989.

[MS] Mehlhorn, K., Schmidt, E. M.: Las Vegas is better than determinism in VLSI and distributive computing, Proc. 14th ACM STOC, 1982, pp. 330-337

[Ra] Rabin, M. unpublished

[R1] A. A. Razborov: Lower Bounds on the Size of Bounded Depth Networks Over a Complete Basis with Logical Addition, (in Russian), Mat. Zametki, 41 (1987), 598–607

[RW1] R. Raz, A. Wigderson: Probabilistic Communication Complexity of Boolean Relations. Proc. 30th IEEE FOCS, 1989, pp.

[RW2] R. Raz, A. Wigderson: Monotone Circuits for Matching Require Linear Depth. 22nd ACM STOC, pp. 287–292.

[S] M. Szegedy: Functions with Bounded Symmetric Communication Complexity and Circuits with MOD m Gates, Proc. 22nd ACM STOC, pp. 278–286.

[Sm] R. Smolensky, Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity, Proc. 19th ACM STOC, pp. 77-82, (1987).

[Ya1] A.C. Yao: Some Complexity Questions Related to Distributive Computing, Proc. 11th ACM STOC, 1979, pp. 209–213.

[Y2] A.C. Yao: Circuits and Local Computation, Proc. 21st ACM STOC, 1989, pp. 186–196

[Y3] A. C. Yao: On ACC and Threshold Circuits, 31st IEEE FOCS, 1990, pp. 619–627.

[Y4] A. C. Yao: Lower bounds by probabilistic arguments, Proc. 24th IEEE FOCS, 1983, pp. 420-428.