Electronic Colloquium on Computational Complexity - Reports Series 1997 - available via:
ECCC
TR97-002
FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

Upper and Lower Bounds for Some Depth-3 Circuit Classes

Richard Beigel*
Yale University and University of Maryland

Alexis Maciel†
University of Maryland

January 27, 1997

Abstract

We investigate the complexity of depth-3 threshold circuits with majority gates at the output, possibly negated AND gates at level two, and MOD_m gates at level one. We show that the fan-in of the AND gates can be reduced to $O(\log n)$ in the case where m is unbounded, and to a constant in the case where m is constant. We then use these upper bounds to derive exponential lower bounds for this class of circuits. In the unbounded m case, this yields a new proof of a lower bound of Grolmusz; in the constant m case, our result sharpens his lower bound. In addition, we prove an exponential lower bound if OR gates are also permitted on level two and m is a constant prime power.

1 Introduction

About ten years ago, Furst, Saxe and Sipser [FSS] and Ajtai [Aj] showed that polynomial-size AC^0 circuits could not compute the parity function. It was hoped that this seminal result would be the first in a series of lower bounds for increasingly larger classes of circuits and that this would lead to the development of new and powerful techniques for proving lower bounds. At the time, this was seen as the most promising approach towards a proof that $\mathrm{P} \neq \mathrm{NP}$.

*On sabbatical from the Yale University Department of Computer Science. Address: Department of Computer Science and UMIACS, A.V. Williams Building, University of Maryland, College Park, MD 20742, U.S.A. Email: beigel@cs.umd.edu. Supported in part by the National Science Foundation under grants CCR–8958528 and CCR–9415410. Also affiliated with the Human–Computer Interaction Laboratory and supported in part by NASA under grant NAG 52895.

†Address: Department of Computer Science and UMIACS, A.V. Williams Building, University of Maryland, College Park, MD 20742, U.S.A. Email: alexis@cs.umd.edu. Supported in part by the National Science Foundation under grant CCR–9522084.

Several other lower bound results did follow in the next few years. Yao [Ya1] and Håstad [Hås] showed that the AC^0 lower bound for parity was in fact exponential. Razborov showed that $ACC^0[2]$ circuits require exponential size to compute the majority function [Ra]. Smolensky later sharpened and generalized the result to $MOD_q \notin ACC^0[p^k]$ if k is fixed and p and q are distinct primes [Sm].

As for circuits with MOD_m gates for m not a prime power and circuits with majority gates, exponential lower bounds are known for TC^0_2 [Haj] and for $MOD_m \circ SYM$ [KW], where SYM is the class of functions computed by polynomial-size circuits consisting of a single level of symmetric gates. Exponential lower bounds are also known for $TC^0_2 \circ AND_{\frac{1}{3}\log n}$ [HG] and a quasipolynomial lower bound is known for $TC^0_2 \circ AC^0_1$ [RW]. However, to this day, no superpolynomial lower bound is known for general depth-3 TC^0 circuits.

In fact, until recently, no superpolynomial lower bound was known for depth-3 TC^0 circuits unless some restriction was put on the fan-in of some of the gates or unless the class was simply $TC^0_2 \circ AC^0_1$. And no exponential lower bound was known without fan-in restrictions, unless the class was simply $TC^0_1 \circ AC^0_2$ [Gre]. The situation changed however when Grolmusz proved an exponential lower bound on the size of $TC^0_1 \circ AND \circ MOD_m$ circuits computing the inner product mod 2 function [Gro]. Note that only AND gates are allowed on level two of these circuits but there is no restriction on the fan-in of the gates and the lower bound holds even if m is any function of n.

In this paper, we give a new proof of this lower bound, one that better explains the computational limitations of this class of circuits. By developing a new proof technique based on random linear combinations, we show that $TC^0_1 \circ AND \circ MOD_m$ is in fact contained in $TC^0_1 \circ AND_{O(\log n)} \circ MOD_m$. We then show that this class is contained in quasipolynomial-size TC^0_2; the lower bound now follows directly from the exponential TC^0_2 lower bound.

Then, in the case where m is constant, we sharpen the lower bound by showing that $TC^0_1 \circ AND \circ MOD_m$ circuits require exponential size to compute MOD_q if q is divisible by a prime that does not divide m. This is done by using random linear combinations in a different way to show that $TC^0_1 \circ AND \circ MOD_m$ is contained in $TC^0_1 \circ AND_{O(1)} \circ MOD_m$. The lower bound then follows from a lower bound of Krause and Pudlák [KP].

Finally, we consider allowing OR gates on the second level of the circuits. We first point out that the union over all $m \in n^{O(1)}$ of the classes $TC^0_1 \circ OR \circ MOD_m$ contains $TC^0_1 \circ AC^0_1 \circ TC^0_1$, a class for which no lower bounds are known. Then we show that a lower bound can be proved in the case where the inputs to the OR gates are only MOD_{p^k} gates for some constant prime power p^k. More precisely, we show an exponential lower bound for $TC^0_1 \circ AC^0_1 \circ CC^0[p^k]$, for k fixed and p prime.

2 Definitions and background

We first define the circuit classes that will occur in this article. Note that the size of a circuit is the number of edges it contains. In addition, unless otherwise indicated, all

circuit classes allow gates of unbounded fan-in and input gates can be labeled by input variables, their negations and the constants 0 and 1. AC^0 is the class of constant-depth polynomial-size circuits consisting of AND, OR and NOT gates. $ACC^0[m]$ is similar but MOD_m gates are also allowed. MOD_m gates are defined by $MOD_m(x_1, \ldots, x_n) = 1$ if and only if $\sum_{i=1}^{n} x_i \equiv 0 \pmod{m}$. $CC^0[m]$ is the subclass of $ACC^0[m]$ that allows only AND-OR gates of constant fan-in. As usual, $ACC^0 = \bigcup_m ACC^0[m]$ and similarly for CC^0. TC^0 is the class of constant-depth polynomial-size circuits consisting of AND, OR, NOT and majority gates. For all of these classes, a subscript denotes the subclass of circuits with depth exactly d.

SYM denotes the class of polynomial-size circuits consisting of a single level of symmetric gates. MAJ denotes the class of polynomial-size circuits consisting of a single level of majority gates, but with no negations allowed at the input. In other words, every output of a MAJ circuit is the majority of some subset of the inputs. The classes AND, OR and MOD_m are defined similarly. Note that in the case of MOD_m circuits, allowing negated inputs yields exactly the same class. In the case of MAJ, however, we get TC^0_1. A subscript used with AND and OR denotes the restriction to gates of fan-in k.

Classes of circuits whose levels consist of various types of gates can be conveniently described as the composition of various classes of functions [Ma, MT]. If Γ and Λ are classes of Boolean functions (not necessarily circuit classes), then $\Gamma \circ \Lambda$ denotes the class of functions f of the form $f(x) = g(h(x))$, where $g \in \Gamma$, $h \in \Lambda$ and h has monotone increasing output length. For example, $TC^0_1 \circ AND \circ MOD_m$ is the class of functions computed by depth-3 polynomial-size circuits with majority gates at the output, possibly negated AND gates at level two, and MOD_m gates at level one. In the case where Γ and Λ are both circuit classes, then we will refer to the corresponding circuits as $\Gamma \circ \Lambda$ circuits. Note that the condition on the output length of h guarantees that the complexity of g, which is measured relative to the output length of h, is related to the input length of f. This is important in some contexts but of no consequence for the circuit classes considered in this article.

We will make frequent use of the following basic fact which is an easy corollary of a result in [Haj]:

Proposition 1 $TC^0_1 \circ SYM = TC^0_2$.

Proof Any symmetric gate with m inputs can be expressed as the sum of $2m+2$ majority gates [Haj]. The sums can then be combined with the majority gate at the output by feeding their terms directly into the gate. □

The following functions have played a central role in the study of small-depth TC^0 circuits:

Definition 2

a) The inner product mod 2 function, denoted IP_2, is defined by

$$\mathrm{IP}_2(x,y) = \left(\sum_{i=1}^{n} x_i y_i\right) \bmod 2,$$

where $x = x_1, \ldots, x_n$ and $y = y_1, \ldots, y_n$.

b) More generally, for any prime p, the function IP_p is defined by

$$\mathrm{IP}_p(x,y) = 1 \quad \text{iff} \quad \sum_{i=1}^{n} x_i y_i \not\equiv 0 \pmod{p},$$

where $x = x_1, \ldots, x_n$, $y = y_1, \ldots, y_n$ and the x_i and y_i are elements of $\mathbf{Z}_p$ represented in binary. Thus IP_p is a function of $2\lceil \log p \rceil n$ Boolean variables.

c) Finally, for any function k of n, the function $\mathrm{GIP}_{2,k}$ is defined by

$$\mathrm{GIP}_{2,k}(x_1, \ldots, x_k) = \left(\sum_{j=1}^{n} x_{1j} \cdots x_{kj}\right) \bmod 2,$$

where $x_i = x_{i1}, \ldots, x_{in}$ and $x_{ij} \in \{0,1\}$.

Table 1 summarizes our new lower bound results together with some other relevant lower bounds. Table 2, on the other hand, summarizes our new upper bounds and other related results.

An exponential lower bound for TC^0_2 was first established by Hajnal *et al.* who showed that TC^0_2 circuits computing IP_2 have size $2^{\Omega(n)}$ [Haj]. Krause and Waack then generalized this result to IP_p, for any prime p.

Fact 3 ([KW]) *For any prime p, TC^0_2 circuits computing IP_p have size $2^{\Omega(n)}$.*

Since the value of each term $x_i y_i$ in the definition of IP_p depends on only $2\lceil \log p \rceil$ input variables, a constant number, it is easy to see that IP_p belongs to $\mathrm{MOD}_p \circ \mathrm{AND}_{2\lceil \log p \rceil (p-1)}$ and thus to $\mathrm{MOD}_m \circ \mathrm{AND}_{2\lceil \log p \rceil (p-1)}$ for any multiple m of p. Therefore, Fact 3 implies that $\mathrm{MOD}_m \circ \mathrm{AND}_{O(1)} \not\subseteq \mathrm{TC}^0_2$ for any constant m. In particular, $\mathrm{MOD}_2 \circ \mathrm{AND}_2 \not\subseteq \mathrm{TC}^0_2$ which implies that $\mathrm{TC}^0_2 \circ \mathrm{AND}_2 \not\subseteq \mathrm{TC}^0_2$.

Now consider $\mathrm{TC}^0_1 \circ \mathrm{MOD}_m$ circuits for m constant. Since $\mathrm{TC}^0_1 \circ \mathrm{MOD}_m \subseteq \mathrm{TC}^0_2$, we have that for every prime p, $\mathrm{TC}^0_1 \circ \mathrm{MOD}_m$ circuits computing IP_p have size $2^{\Omega(n)}$. However, Goldmann has established the following sharper result: if q is divisible by a prime p that does not divide m, then $\mathrm{TC}^0_1 \circ \mathrm{MOD}_m$ circuits computing MOD_q have size $2^{\Omega(n)}$ [Go]. Since then, this lower bound has been generalized by Krause and Pudlák:

Fact 4 ([KP]) *If q is divisible by a prime p that does not divide m, then $\mathrm{TC}^0_1 \circ \mathrm{AND}_{O(1)} \circ \mathrm{MOD}_m$ circuits computing MOD_q have size $2^{\Omega(n)}$.*

Circuit class	Previously Known			In This Paper	
	Function	*L. b.*	*Ref.*	*Function*	*L. b.*
TC^0_2	IP_p	$2^{\Omega(n)}$	[KW]		
$\mathrm{TC}^0_2 \circ \mathrm{AND}_{\frac{1}{3}\log n}$	$\mathrm{GIP}_{2,\frac{1}{3}\log n+1}$	$2^{\Omega(n)}$	[HG]		
$\mathrm{TC}^0_2 \circ \mathrm{AC}^0_1$	$\mathrm{GIP}_{2,\log n}$ of MOD_2's	$n^{\Omega(\log n)}$	[RW]		
$\mathrm{TC}^0_1 \circ \mathrm{AC}^0$	MOD_2	$2^{n^{\Omega(1)}}$	[Gre]		
$\mathrm{TC}^0_1 \circ \mathrm{CC}^0[p^k]$	MOD_q	$2^{\Omega(n)}$			
$\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$				MOD_q	$2^{\Omega(n)}$
$\mathrm{TC}^0_1 \circ \mathrm{AND}_{O(1)} \circ \mathrm{MOD}_m$	MOD_q, $q \not\mid m$	$2^{\Omega(n)}$	[KP]		
$\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$	IP_2	$2^{\Omega(n)}$	[Gro]	MOD_q, $q \not\mid m$	$2^{\Omega(n)}$
$\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$, m unbounded	IP_2	$2^{\Omega(n)}$	[Gro]	IP_p	$2^{\Omega(\sqrt{n})}$

Table 1: Summary of lower bound results. Unless otherwise indicated, p and q are distinct prime constants, and k and m are constant.

Note that Fact 4 is only a special case of one of the results in [KP].

The TC^0_2 lower bound (Fact 3) has been extended by Håstad and Goldmann to depth-3 TC^0 circuits in which the level-one gates have fan-in bounded by $\frac{1}{3}\log n$.

Fact 5 ([HG]) *If* $2 \leq k \leq \frac{1}{3}\log n$, *then* $\mathrm{TC}^0_2 \circ \mathrm{AND}_{k-1}$ *circuits computing* $\mathrm{GIP}_{2,k}$ *have size* $2^{\Omega(n)}$.

Since $\mathrm{GIP}_{2,k}$ is easily seen to be computable in $\mathrm{MOD}_2 \circ \mathrm{AND}_k$, Fact 5 implies that $\mathrm{MOD}_2 \circ \mathrm{AND}_k \not\subseteq \mathrm{TC}^0_2 \circ \mathrm{AND}_{k-1}$ and therefore that $\mathrm{TC}^0_2 \circ \mathrm{AND}_k \not\subseteq \mathrm{TC}^0_2 \circ \mathrm{AND}_{k-1}$.

We will later make use of the following version of the Chernoff bound:

Fact 6 (Chernoff bound) *If* $X_1, \ldots, X_N$ *are mutually independent 0-1 random variables such that* $\mathrm{Prob}[X_i = 1] = p$, *then*

$$\mathrm{Prob}\left[\left|\sum_{i=1}^{N} X_i - pN\right| \geq \alpha pN\right] \leq 2e^{-\alpha^2 pN/3}.$$

In other words, the probability that $\sum_{i=1}^{N} X_i$ is far from its expected value, pN, decreases exponentially with N.

Circuit class	*Contains*	*Using size*	*Ref.*
$\mathrm{TC}^0_1 \circ \mathrm{AND}_{O(1)} \circ \mathrm{MOD}_m$	$\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$	$n^{O(1)}$	This paper
$\mathrm{TC}^0_1 \circ \mathrm{AND}_{O(\log n)} \circ \mathrm{MOD}_m$, m unbounded	$\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$, m unbounded	$n^{O(1)}$	This paper
TC^0_2	$\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$, m unbounded	$n^{O(\log n)}$	This paper
$\mathrm{TC}^0_1 \circ \mathrm{MOD}_p \circ \mathrm{AND}_{O(1)}$	$\mathrm{TC}^0_1 \circ \mathrm{CC}^0[p^k]$	$n^{O(1)}$	Folklore
	$\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$	$n^{O(1)}$	This paper
$\mathrm{TC}^0_1 \circ \mathrm{MOD}_p \circ \mathrm{AND}_{(\log n)^{O(1)}}$	$\mathrm{TC}^0_1 \circ \mathrm{ACC}^0[p^k]$	$n^{(\log n)^{O(1)}}$	By [Al]
$\mathrm{TC}^0_2 \circ \mathrm{AND}_{(\log n)^{O(1)}}$	$\mathrm{TC}^0_1 \circ \mathrm{ACC}^0$	$n^{(\log n)^{O(1)}}$	[Ya2]

Table 2: Summary of upper bound results. Unless otherwise indicated, p is a prime constant, and k and m are constant.

3 $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits: the unbounded m case

In this section, we show that for any $m \in n^{O(1)}$, $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits require size $2^{\Omega(\sqrt{n})}$ to compute IP_p, for any prime p. This will be done by proving two upper bound results. First, we will show that the fan-in of the AND gates in $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits can be reduced to $O(\log n)$. Second, we will show that TC^0_2 circuits of size $n^{O(\log n)}$ can simulate any $\mathrm{TC}^0_1 \circ \mathrm{AND}_{O(\log n)} \circ \mathrm{MOD}_m$ circuit.

We begin by showing that $\mathrm{AND} \circ \mathrm{MOD}_m$ subcircuits can be well approximated by probabilistic MOD_m gates.

Lemma 7 *For every* $\mathrm{AND} \circ \mathrm{MOD}_m$ *circuit* C*, there is a probabilistic* MOD_m *gate* G *such that*

$$\begin{aligned} C(x) = 0 &\Rightarrow \mathrm{Prob}[G(x) = 1] \leq 1/2 \\ C(x) = 1 &\Rightarrow \mathrm{Prob}[G(x) = 1] = 1 \end{aligned}$$

Proof Suppose that $G_1, \ldots, G_s$ are the MOD_m gates of C and that G_i tests whether $\sum_{j=1}^n a_{ij}x_j + a_{i0} \equiv 0 \pmod m$. Let $R_i = \sum_{j=1}^n a_{ij}x_j + a_{i0}$. Now let $R = b_1R_1 + \cdots + b_sR_s$ where $b_1, \ldots, b_s$ are chosen randomly and independently in $\{0, 1\}$.

Let x be arbitrary. If $C(x) = 1$, then for every i, $R_i \equiv 0 \pmod m$ so that $R \equiv 0 \pmod m$ for every possible value of $b_1, \ldots, b_s$.

If $C(x) = 0$, then there is j such that $R_j \equiv c \pmod m$ for some $c \not\equiv 0$. For every possible value of $b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_s$, we have either $R = \sum_{i \neq j} b_iR_i$ or $R =$

$\sum_{i \neq j} b_i R_i + c$. Since $c \not\equiv 0$, these two values cannot be both congruent to 0. Therefore, $R \equiv 0 \pmod{m}$ with probability no greater than $1/2$.

Now take the MOD_m gate G corresponding to R. This probabilistic gate satisfies the conditions in the statement of the lemma. □

Theorem 8 *For every* $m \in n^{O(1)}$,

$$\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m = \mathrm{TC}^0_1 \circ \mathrm{AND}_{O(\log n)} \circ \mathrm{MOD}_m.$$

Proof Suppose that C is of the form $\mathrm{MAJ}(D_1, \ldots, D_s)$ where each D_i is equal to C_i or $\mathrm{NOT}(C_i)$, for some C_i in $\mathrm{AND} \circ \mathrm{MOD}_m$. Without loss of generality, we assume that s is even. Let $G_1, \ldots, G_s$ be the probabilistic MOD_m gates given by the lemma. Let G'_i be the AND of $\lceil \log 1/\alpha \rceil$ independent copies of G_i. The appropriate value of α will be determined later; for the moment, let α be an arbitrary number less than 1. For every i, we have

$$\begin{aligned} C_i(x) = 0 &\Rightarrow \mathrm{Prob}[G'_i(x) = 1] \leq \alpha \\ C_i(x) = 1 &\Rightarrow \mathrm{Prob}[G'_i(x) = 1] = 1 \end{aligned}$$

If $D_i = C_i$, then let $H_i = G'_i$. If $D_i = \mathrm{NOT}(C_i)$, then let $H_i = \mathrm{NOT}(G'_i)$. Then, for every i,

$$\begin{aligned} D_i(x) = 0 &\Rightarrow \mathrm{Prob}[H_i(x) = 1] \leq \alpha \\ D_i(x) = 1 &\Rightarrow \mathrm{Prob}[H_i(x) = 1] \geq 1 - \alpha \end{aligned}$$

Let $H_{i1}, \ldots, H_{iN}$ be N independent copies of H_i. The appropriate value of N will also be determined later. If $D_i(x) = 0$, then $\mathrm{E}(\sum_j H_{ij}) \leq \alpha N$. If $D_i(x) = 1$, then $\mathrm{E}(\sum_j H_{ij}) \geq N - \alpha N$.

Now take an arbitrary x. Two cases are possible:

1) For every i, $|\sum_j H_{ij} - \mathrm{E}(\sum_j H_{ij})| < \alpha N$.

2) There is an i such that $|\sum_j H_{ij} - \mathrm{E}(\sum_j H_{ij})| \geq \alpha N$.

Consider the first case. If $C(x) = \mathrm{MAJ}(D_1(x), \ldots, D_s(x)) = 0$, then

$$\sum_{i,j} H_{ij} \quad < \quad \frac{s}{2}(2\alpha N) + \left(\frac{s}{2} - 1\right) N \tag{1}$$

On the other hand, if $C(x) = 1$, then

$$\sum_{i,j} H_{ij} \quad > \quad \frac{s}{2}(N - 2\alpha N) \tag{2}$$

A straightforward calculation shows that the number in (1) is less than the number in (2) if $1/\alpha \geq 2s$. In that case,

$$C(x) = 1 \quad \Leftrightarrow \quad \sum_{i,j} H_{ij} \geq t$$

where t is the number in (2). Notice that an appropriate value for α can be chosen with $1/\alpha \in O(s)$. This also implies that $\lceil \log 1/\alpha \rceil \in O(\log s)$.

Consider now the second case. By using the Chernoff bound (Fact 6), we will show that this case is not very likely. First, for every i, if $\mathrm{E}(\sum_j H_{ij}) = pN$, then

$$\mathrm{Prob}\left[\left|\sum_j H_{ij} - \mathrm{E}\left(\sum_j H_{ij}\right)\right| \geq \alpha N\right] \leq 2e^{-(\alpha/p)^2 pN/3} \leq 2e^{-\alpha^2 N/3},$$

since $p \leq 1$. Therefore,

$$\mathrm{Prob}\left[\exists i \left(\left|\sum_j H_{ij} - \mathrm{E}\left(\sum_j H_{ij}\right)\right| \geq \alpha N\right)\right] \leq 2se^{-\alpha^2 N/3}.$$

It is easy to verify that $N \in O(ns^2) \subseteq n^{O(1)}$ can be chosen so that this probability is less than 2^{-n}.

Therefore, the probability that there is a value of x for which Case 2 occurs is less than $\sum_x 2^{-n} = 1$. This implies that there is a sequence of H_{ij} such that Case 1 occurs for every x. For this particular sequence of H_{ij}, $C(x) = 1$ if and only if $\sum_{i,j} H_{ij} \geq t$. Notice that the H_{ij} can each be computed in $\mathrm{AND}_{O(\log s)} \circ \mathrm{MOD}_m$ or in $\mathrm{NOT} \circ \mathrm{AND}_{O(\log s)} \circ \mathrm{MOD}_m$. This implies that C can be computed in $\mathrm{TC}^0_1 \circ \mathrm{AND}_{O(\log n)} \circ \mathrm{MOD}_m$. □

Corollary 9

a) For every $m \in n^{O(1)}$, any $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuit can be simulated by a size-$n^{O(\log n)}$ TC^0_2 circuit.

b) For every prime p and for every $m \in n^{O(1)}$, $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits computing IP_p have size $2^{\Omega(\sqrt{n})}$.

c) For every constant q, $\mathrm{MOD}_q \circ \mathrm{AND}_{O(1)} \not\subseteq \mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$.

Proof For part (a), first use the theorem to get an equivalent $\mathrm{TC}^0_1 \circ \mathrm{AND}_{O(\log n)} \circ \mathrm{MOD}_m$ circuit. By using a simple technique, each of the $\mathrm{AND}_{O(\log n)} \circ \mathrm{MOD}_m$ subcircuits can be simulated by a single symmetric gate of fan-in $n^{O(\log n)}$ (see, for example, [HHK], [Be] or [Ma].) This yields a $\mathrm{TC}^0_1 \circ \mathrm{SYM}$ circuit of size $n^{O(\log n)}$. The result follows by Proposition 1.

For part (b), first notice from part (a) and the proofs of the lemma and theorem, that any $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuit of size s can be simulated by a TC^0_2 circuit of size $s^{O(\log s)}$. The lower bound then follows from the Krause and Waack lower bound (Fact 3).

Part (c) follows from the fact that IP_p is in $\mathrm{MOD}_q \circ \mathrm{AND}_{O(1)}$ for any multiple q of p. □

Note that Part (b) of the corollary extends the exponential lower bound of Grolmusz [Gro] from IP_2 to IP_p for any prime p. In addition, Theorem 8 implies that restricting the level-two gates in a $\mathrm{TC}^0_2 \circ \mathrm{MOD}_m$ circuit to be only AND gates is in fact equivalent to restricting the fan-in of those gates to be $O(\log n)$.

4 $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits: the constant m case

In this section, we show that for any constant m, $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits require size $2^{\Omega(n)}$ to compute MOD_q if q is divisible by a prime p that does not divide m. As in the previous section, this lower bound will be obtained by first establishing an upper bound: we will show that the fan-in of the AND gates in $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits can be reduced to a constant.

We again begin by showing that $\mathrm{AND} \circ \mathrm{MOD}_m$ subcircuits can be well approximated by probabilistic MOD_m gates.

Lemma 10 *For every* $\mathrm{AND} \circ \mathrm{MOD}_m$ *circuit* C*, there is a probabilistic* MOD_m *gate* G *and a finite set of probabilities* Π*, depending only on* m*, such that* $1 \notin \Pi$ *and*

$$\begin{aligned} C(x) = 0 &\Rightarrow \mathrm{Prob}[G(x) = 1] \in \Pi \\ C(x) = 1 &\Rightarrow \mathrm{Prob}[G(x) = 1] = 1 \end{aligned}$$

Proof Suppose that $G_1, \ldots, G_s$ are the MOD_m gates of C and that G_i tests whether $\sum_{j=1}^n a_{ij}x_j + a_{i0} \equiv 0 \pmod m$. Let $R_i = \sum_{j=1}^n a_{ij}x_j + a_{i0}$. Now let $R = b_1R_1 + \cdots + b_sR_s$ where $b_1, \ldots, b_s$ are chosen randomly and independently in $\mathbf{Z}_m$.

Let x be arbitrary. If $C(x) = 1$, then for every i, $R_i \equiv 0 \pmod m$ so that $R \equiv 0 \pmod m$ for every possible value of $b_1, \ldots, b_s$.

Now suppose that $C(x) = 0$, i.e., that not all the R_i are divisible by m. We will consider several cases. For concreteness, suppose for the moment that $m = pq$, the product of two distinct primes. (1) If one of the R_i is not divisible by either p or q, then $\mathrm{Prob}[R \equiv 0] = 1/m$ since R_i has an inverse in $\mathbf{Z}_m$. (2) If all the R_i are divisible by p but not by q, then R is a random multiple of p since all the R_i/p have inverses in $\mathbf{Z}_m$. This implies that $\mathrm{Prob}[R \equiv 0] = 1/q$. (3) If all the R_i are divisible by q but not by p, then, similarly, $\mathrm{Prob}[R \equiv 0] = 1/p$. Finally, (4) if some R_i are divisible by p but not by q, and some R_i are divisible by q but not by p, then $R = ap + bq$ where a and b are random elements of $\mathbf{Z}_m$. This implies that $\mathrm{Prob}[R \equiv 0] = (1/p)(1/q) = 1/m$. Therefore, by combining all the cases, if $C(x) = 0$, then $\mathrm{Prob}[R \equiv 0] \in \{1/p, 1/q, 1/m\}$.

In general, up to $(\log m)^{2 \log m}$ cases have to be considered. Notice that this is a constant. In each case, depending on which divisors of m occur as $\gcd(m, R_i)$ for some R_i, R will be congruent to 0 modulo m with some fixed probability less than 1.

Now take the MOD_m gate G corresponding to R. This probabilistic gate satisfies the conditions in the statement of the lemma. □

Theorem 11 *For every constant* m*,*

$$\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m = \mathrm{TC}^0_1 \circ \mathrm{AND}_{O(1)} \circ \mathrm{MOD}_m.$$

Proof Suppose that C is of the form $\mathrm{MAJ}(D_1, \ldots, D_s)$ where each D_i is equal to C_i or $\mathrm{NOT}(C_i)$, for some C_i in $\mathrm{AND} \circ \mathrm{MOD}_m$. Without loss of generality, we assume that s

is even. Let $G_1, \ldots, G_s$ and $\Pi = \{p_1, \ldots, p_k\}$ be given by the lemma. Let $G_{i1}, \ldots, G_{iN}$ be N independent copies of G_i. The appropriate value of N will be determined later; for the moment, let N be an arbitrary number. We have that

$$\begin{aligned} C_i(x) = 0 &\Rightarrow \mathrm{E}(\textstyle\sum_j G_{ij}) \in \{p_1 N, \ldots, p_k N\} \\ C_i(x) = 1 &\Rightarrow \mathrm{E}(\textstyle\sum_j G_{ij}) = N \end{aligned}$$

Let N_i be the value of $p_i N$ rounded to the nearest integer. Let $P(X)$ be the degree k polynomial $(X - N_1) \cdots (X - N_k)$. Then, for every i, $P(N_i) = 0$ while $P(N) = (N - N_1) \cdots (N - N_k)$. Let M denote that last number. It is easy to verify that for sufficiently small α and for sufficiently large N, if $|B - p_i N| < \alpha N$, then $|P(B)| \leq 2\alpha N^k$, and if $|B - N| < \alpha N$, then $|P(B) - M| \leq \alpha k N^k$. Therefore, if $|\sum_j G_{ij} - \mathrm{E}(\sum_j G_{ij})| < \alpha N$, then

$$\begin{aligned} C_i(x) = 0 &\Rightarrow |P(\textstyle\sum_j G_{ij})| \leq 2\alpha k N^k \\ C_i(x) = 1 &\Rightarrow |P(\textstyle\sum_j G_{ij}) - M| \leq 2\alpha k N^k \end{aligned}$$

If $D_i = C_i$, then let $R_i = P(\sum_j G_{ij})$. If $D_i = \mathrm{NOT}(C_i)$, then let $R_i = M - P(\sum_j G_{ij})$. Then, for every i, if $|\sum_j G_{ij} - \mathrm{E}(\sum_j G_{ij})| < \alpha N$,

$$\begin{aligned} D_i(x) = 0 &\Rightarrow |R_i| \leq 2\alpha k N^k \\ D_i(x) = 1 &\Rightarrow |R_i - M| \leq 2\alpha k N^k \end{aligned}$$

Now take an arbitrary x. Two cases are possible:

1) For every i, $|\sum_j G_{ij} - \mathrm{E}(\sum_j G_{ij})| < \alpha N$.

2) There is an i such that $|\sum_j G_{ij} - \mathrm{E}(\sum_j G_{ij})| \geq \alpha N$.

The appropriate value of $\alpha < 1$ will be determined later.

Consider the first case. If $C(x) = \mathrm{MAJ}(D_1(x), \ldots, D_s(x)) = 0$, then

$$\sum_i R_i \;<\; s(2\alpha k N^k) + \left(\frac{s}{2} - 1\right) M \tag{3}$$

On the other hand, if $C(x) = 1$, then

$$\sum_i R_i \;>\; s(-2\alpha k N^k) + \frac{s}{2} M \tag{4}$$

A straightforward calculation shows that the number in (3) is less than the number in (4) if $1/\alpha \geq 4ksN^k/M$. In that case,

$$C(x) = 1 \quad \Leftrightarrow \quad \sum_{i,j} R_i \geq t$$

where t is the number in (4). For sufficiently large N, we have that $N^k/M \leq 2^k/((1-p_1)\cdots(1-p_k))$, a constant. Therefore, an appropriate value for α can be chosen with $1/\alpha \in O(s)$.

Consider now the second case. By using the Chernoff bound (Fact 6), as was done in the proof of Theorem 8, we can show that this case is not very likely. In fact,

$$\text{Prob}\left[\exists i \left(\left|\sum_j G_{ij} - \text{E}\left(\sum_j G_{ij}\right)\right| \geq \alpha N\right)\right] \leq 2se^{-\alpha^2 N/3}.$$

It is again easy to verify that $N \in O(ns^2) \subseteq n^{O(1)}$ can be chosen so that this probability is less than 2^{-n}.

Therefore, there is a sequence of MOD_m gates G_{ij} such that Case 1 occurs for every x. For this particular sequence, $C(x) = 1$ if and only if $\sum_i R_i \geq t$. Now $\sum_i R_i$ is a degree k polynomial in the G_{ij}. Write this polynomial in standard form, i.e., as a linear combination of monomials. It is easy to verify that the coefficients are bounded in $O(N^k) \subseteq n^{O(1)}$. Therefore, the test $\sum_i R_i \geq t$ can be carried out by a $\text{TC}^0_1 \circ \text{AND}_k$ whose inputs are the G_{ij}: the monomials are computed by AND gates of fan-in k and the possibly negative coefficients are handled by using standard techniques. This implies that C can be computed in $\text{TC}^0_1 \circ \text{AND}_{O(1)} \circ \text{MOD}_m$. □

We can now apply the lower bound result of Krause and Pudlák (Fact 4):

Corollary 12 *For every pair of numbers q and m, if q is divisible by a prime p that does not divide m, then $\text{TC}^0_1 \circ \text{AND} \circ \text{MOD}_m$ circuits computing MOD_q have size $2^{\Omega(n)}$.*

Note that this result sharpens the lower bound of the previous section (Corollary 9, Part (b)) and that of Grolmusz [Gro], in the case of constant m, by showing that exponential size is required to compute not only IP_p but also MOD_p, if p is a prime that does not divide m. Corollary 12 also extends the lower bound of Krause and Pudlák [KP] (Fact 4) from $\text{TC}^0_1 \circ \text{AND}_{O(1)} \circ \text{MOD}_m$ to $\text{TC}^0_1 \circ \text{AND} \circ \text{MOD}_m$ circuits. In fact, Theorem 11 implies that in the case of constant m, restricting the level-two gates in a $\text{TC}^0_2 \circ \text{MOD}_m$ circuit to be only AND gates is equivalent to restricting the fan-in of those gates to be constant.

5 Allowing OR gates on level two

The fact that only AND gates are allowed on level two in $\text{TC}^0_1 \circ \text{AND} \circ \text{MOD}_m$ circuits plays an essential role in the results of the previous section. The same is true for the results of Grolmusz [Gro]: his technique does not seem to work if OR gates are allowed on level two. In fact, we can show that the union over all $m \in n^{O(1)}$ of the classes $\text{TC}^0_1 \circ \text{OR} \circ \text{MOD}_m$ contains $\text{TC}^0_1 \circ \text{AC}^0_1 \circ \text{TC}^0_1$, a class for which no lower bounds are known.

Proposition 13 $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{TC}^0_1 \subseteq \bigcup_{m \in n^{O(1)}} \mathrm{TC}^0_1 \circ \mathrm{OR} \circ \mathrm{MOD}_m$.

Proof Let C be a $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{TC}^0_1$ circuit. By using standard techniques, C can be transformed into a $\mathrm{TC}^0_1 \circ \mathrm{OR} \circ \mathrm{TC}^0_1$ circuit. The result now follows from the fact that any symmetric gate can be expressed as an OR of MOD_m gates if m is larger than the size of the original circuit. (See the proof of Corollary 9, part (a).) □

However, in the case where $m = p^k$, a constant prime power, it is possible to allow OR gates and prove a lower bound for $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{MOD}_{p^k}$. In fact,

Theorem 14 *For every prime p and every constant k,*

$$\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k] = \mathrm{TC}^0_1 \circ \mathrm{MOD}_p \circ \mathrm{AND}_{O(1)}.$$

Proof It is well-known that OR gates can be well approximated by probabilistic constant-degree polynomials over $\mathbf{Z}_p$. (See [Al], for example.) Let $y_1, \ldots, y_s$ be the inputs to an OR gate and let $R = b_1 y_1 + \cdots + b_s y_s$ where the b_i are chosen randomly and independently in $\mathbf{Z}_p$. If $C(y) = 0$ then $R \equiv 0 \pmod p$ for every possible value of the b_i. If $C(y) = 1$ then $R \equiv 0 \pmod p$ with probability $1/p$. Therefore, by Fermat's Little Theorem, R^{p-1} satisfies

$$\begin{aligned} C(y) = 0 &\Rightarrow \mathrm{Prob}[R^{p-1}(y) \equiv 1] = 0 \\ C(y) = 1 &\Rightarrow \mathrm{Prob}[R^{p-1}(y) \equiv 1] = 1 - (1/p) \end{aligned}$$

It is also well-known that any $\mathrm{CC}^0[p^k]$ circuit can be expressed as a constant-degree polynomial over $\mathbf{Z}_p$. (See [BT], for example.) Therefore, for every circuit C in $\mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$, there is a probabilistic $\mathrm{MOD}_m \circ \mathrm{AND}_{O(1)}$ circuit D such that

$$\begin{aligned} C(x) = 0 &\Rightarrow \mathrm{Prob}[D(x) = 1] = q_0 \\ C(x) = 1 &\Rightarrow \mathrm{Prob}[D(x) = 1] = q_1 \end{aligned}$$

with $q_1 - q_0 = 1 - \frac{1}{p}$.

Now suppose that C is a $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$ circuit of the form $\mathrm{MAJ}(C_1, \ldots, C_s)$. Replace each C_i by an approximating probabilistic $\mathrm{MOD}_m \circ \mathrm{AND}_{O(1)}$ circuit. The resulting probabilistic circuit can then be transformed into a deterministic one by a special case of the argument used in the proof of Theorem 8. □

Corollary 15 *If p is prime, k is constant and r is not bounded by a constant, then $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$ circuits computing $\mathrm{GIP}_{2,r}$ have size $2^{\Omega(n)}$.*

Proof From the proof of the theorem, we get that any $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$ circuit of size s can be simulated by a $\mathrm{TC}^0_1 \circ \mathrm{MOD}_p \circ \mathrm{AND}_{O(1)}$ circuit of size polynomial in s. This circuit can in turn be simulated by a $\mathrm{TC}^0_2 \circ \mathrm{AND}_{O(1)}$ circuit of size $s^{O(1)}$, by Proposition 1. The lower bound then follows from the lower bound of Håstad and Goldmann (Fact 5). □

This result extends a special case of our lower bound of the previous section (Corollary 12) from $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_{p^k}$ circuits to $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$ circuits, for p prime and k constant. Note however that the lower bound in this section is for $\mathrm{GIP}_{2,r}$, r not bounded by a constant, instead of MOD_q, q a prime different from p.

6 Conclusions and open problems

As researchers investigate the computational complexity of small-depth Boolean circuits, a lot of effort is naturally devoted to proving negative results, i.e., lower bounds. For example, the conjectures $\mathrm{NP} \not\subseteq \mathrm{TC}^0_3$ and $\mathrm{ACC}^0 \subset \mathrm{TC}^0 \subset \mathrm{NC}^1$ have attracted a great deal of attention.

But a lot of effort is also devoted to proving positive results, i.e., upper bounds. Showing how resources can be used effectively to solve computational problems has always been a defining goal of theoretical computer science. Positive results, whether in the form of problems belonging to a particular complexity class, or in the form of containments between complexity classes, help us to fully understand the complexity of computation. Positive results also help reduce the proliferation of complexity classes, such as the variety of restricted versions of TC^0_3 circuits. Finally, positive results also help to prove lower bounds.

In this article, we proved two positive results concerning the complexity of $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits. First, in the case where m is unbounded, we showed that the fan-in of the AND gates on level two can be reduced to $O(\log n)$. This led to the proof that $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits are no more powerful than TC^0_2 circuits of size $n^{O(\log n)}$. In particular, $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits require exponential size to compute IP_p.

Then, in the case where m is constant, we showed that the fan-in of the AND gates can be reduced to a constant. By the same argument that was used in the proof of Corollary 9, Part (a), this implies that $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits are no more powerful than TC^0_2 circuits (of polynomial size). But our upper bound actually leads to a better lower bound than in the unbounded m case: if q is divisible by a prime that does not divide m, then $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{MOD}_m$ circuits require exponential size to compute MOD_q.

A natural continuation of this work would be to investigate the complexity of $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{MOD}_m$ circuits where both AND and OR gates are allowed on level two. As we pointed out earlier, a general lower bound for this class, i.e., for $m \in n^{O(1)}$, would imply a new lower bound for the class $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{TC}^0_1$. In this article, we obtained a partial result, once again by first proving an upper bound. We showed that $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$ circuits are no more powerful than $\mathrm{TC}^0_1 \circ \mathrm{MOD}_p \circ \mathrm{AND}_{O(1)}$ circuits, if p^k is a constant prime power. This implies that these circuits require exponential size to compute $\mathrm{GIP}_{2,r}$ if r is not bounded by a constant. It would be interesting to extend the lower bounds for $\mathrm{TC}^0_1 \circ \mathrm{MOD}_m$ circuits [Go] to $\mathrm{TC}^0_1 \circ \mathrm{MOD}_m \circ \mathrm{AND}_{O(1)}$ circuits, even in the special case of a prime power. Together with our upper bound, such a lower bound might imply sharper lower bounds for $\mathrm{TC}^0_1 \circ \mathrm{AC}^0_1 \circ \mathrm{CC}^0[p^k]$.

More generally, as a first step towards lower bounds for $\mathrm{TC}^0_2 \circ \mathrm{AND}_{(\log n)^{O(1)}}$ circuits, a lower bound for $\mathrm{TC}^0_1 \circ \mathrm{MOD}_p \circ \mathrm{AND}_{(\log n)^{O(1)}}$, for p prime, would generate a lot of excitement. By the positive results of Allender [Al] (see also [AH]) this would imply a lower bound for $\mathrm{TC}^0_1 \circ \mathrm{ACC}^0[p]$.

Finally, note that the exact definition used for the MOD_m gates plays a crucial role in the results presented in this article. Generalized MOD_m gates, denoted GMOD_m, are defined by $\mathrm{MOD}^S_m(x_1, \ldots, x_n) = 1$ if and only if $(\sum_{i=1}^n x_i) \bmod m \in S$, for any subset S of $\mathbf{Z}_m$. Our results still hold even if $\mathrm{MOD}^{\{c\}}_m$ gates are used in the circuits, for any $c \in \mathbf{Z}_m$. If instead $\mathrm{MOD}^{\mathbf{Z}_m - \{c\}}_m$ gates are used, then we get lower bounds for circuits with OR gates instead of AND gates on level two. But if arbitrary GMOD_m gates are used, then our techniques no longer work. More precisely, we do not know how to prove Lemmas 7 and 10 in this case. In fact, no lower bounds are known for $\mathrm{TC}^0_1 \circ \mathrm{AND} \circ \mathrm{GMOD}_m$ circuits. Note that the definition of MOD_m gates also plays an essential role in the proofs of Grolmusz [Gro] and in the lower bounds for the class $\mathrm{MOD}_m \circ \mathrm{MOD}_m$ (see [KW], [BST] and [Ca]). In particular, no lower bounds are known for $\mathrm{GMOD}_m \circ \mathrm{GMOD}_m$ circuits. (See also [BBR] for related work.)

References

[Aj] M. Ajtai, Σ^1_1 formulae on finite structures, *Ann. Pure Appl. Logic* **24** (1983) 1–48.

[Al] E. Allender, A Note on the power of threshold circuits, in *Proc. 30th IEEE Symp. on Foundations of Computer Science*, 1989, 580–584.

[AH] E. Allender and U. Hertrampf, Depth reduction for circuits of unbounded fan-in, *Inform. and Comput.* **108** (1994) 217–238.

[BBR] D.A. Mix Barrington, R. Beigel and S. Rudich, Representing Boolean Functions as Polynomials Modulo Composite Integers, in *Proc. 24th ACM Symp. on Theory of Computing*, 1992, 455–461.

[BST] D.A. Mix Barrington, H. Straubing and D. Thérien, Non uniform automata over groups, *Inform. and Comput.* **89** (1990) 109–132.

[Be] R. Beigel, When do extra majority gates help? polylog(n) majority gates are equivalent to one, *Comput. Complexity* **4** (1994) 314–324.

[BT] R. Beigel and J. Tarui, On ACC, *Comput. Complexity* **4** (1994) 350–366.

[Ca] H. Caussinus, A note on a theorem of Barrington, Straubing and Thérien, *Inform. Process. Lett.* **58** (1996).

[FSS] M. Furst, J.B. Saxe and M. Sipser, Parity, circuits, and the polynomial-time hierarchy, *Math. Systems Theory* **17** (1984) 13–27.

[Go] M. Goldmann, A Note on the Power of Majority Gates and Modular Gates, *Inform. Process. Lett.* **53** (1995) 321–327.

[Gre] F. Green, An oracle separating $\oplus$P from $\mathrm{PP}^{\mathrm{PH}}$, *Inform. Process. Lett.* **37** (1991) 149–153.

[Gro] V. Grolmusz, A Weight–Size Trade–Off for Circuits with MOD m Gates, in *Proc. 26th ACM Symp. on Theory of Computing*, 1994, 68–74.

[Haj] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy and G. Turán, Threshold circuits of bounded depth, *J. Comput. System Sci.* **46** (1993) 129–154.

[Hås] J. Håstad, *Computational Limitations of Small Depth Circuits*, MIT Press, Cambridge, MA, U.S.A., 1986.

[HG] J. Håstad and M. Goldmann, On the power of small-depth threshold circuits, *Comput. Complexity* **1** (1991) 113-129.

[HHK] T. Hofmeister, W. Hohberg and S. Köhling, Some notes on threshold circuits, and multiplication in depth 4, *Inform. Process. Lett.* **39** (1991) 219–225.

[KP] M. Krause and P. Pudlák, On the Computational Power of Depth 2 Circuits with Threshold and Modulo Gates, in *Proc. 26th ACM Symp. on Theory of Computing*, 1994, 48–57.

[KW] M. Krause and S. Waack, Variation ranks of communication matrices and lower bounds for depth two circuits having symmetric gates with unbounded fan-in, in *Proc. 32nd IEEE Symp. on Foundations of Computer Science*, 1991, 777–782.

[Ma] A. Maciel, Threshold Circuits of Small Majority-Depth, Ph.D. Thesis, School of Computer Science, McGill University, Montréal, Québec, Canada, 1995.

[MT] A. Maciel and D. Thérien, Threshold Circuits of Small Majority-Depth, *Information and Computation*, to appear. Preliminary version: Technical Report SOCS–95.5, School of Computer Science, McGill University, Montréal, Québec, Canada, 1995.

[Ra] A.A. Razborov, Lower bounds on the size of bounded-depth networks over a complete basis with logical addition, *Mathematical Notes of the Academy of Sciences of the USSR* **41:4** (1987) 333–338.

[RW] A.A. Razborov and A. Wigderson, $n^{\Omega(\log n)}$ lower bounds on the size of depth 3 threshold circuits with AND gates at the bottom, *Inform. Process. Let.* **45** (1993) 303–307.

[Sm] R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity, in *Proc. 19th ACM Symp. on Theory of Computing*, 1987, 77–82.

[Ya1] A.C.-C. Yao, Separating the polynomial-time hierarchy by oracles, in *Proc. 26th IEEE Symp. on Foundations of Computer Science*, 1985, 1–10.

[Ya2] A.C.-C. Yao, On ACC and threshold circuits, in *Proc. 31st IEEE Symp. on Foundations of Computer Science*, 1990, 619–627.