A Weight–Size Trade–Off for Circuits with MOD m Gates

Vince Grolmusz

Max Planck Institute and Eötvös University

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 $\log(wM) = \Omega(n)$, 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 have got a trade–off between the numbers of the MOD m gates and the AND gates. By our knowledge, this is the first trade–off result involving hard–to–handle MOD m gates.

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.

1. INTRODUCTION

1.1 MOD p vs. MOD m gates

After the famous lower–bound result of *Yao* [Y5] and *Håstad* [H] for Boolean circuits with AND, OR, and NOT gates, the following question emerged [Ba]: What happens if MOD ℓ gates are also allowed in the circuit ? Here ℓ is a positive integer, and a MOD ℓ gate outputs 1 if the sum of its input–bits is divisible by ℓ, and 0 otherwise.

Address: Department of Computer Science, Eötvös University, Múzeum krt. 6-8; H-1088 Budapest, Hungary; email: grolmusz@cs.elte.hu. Supported by grant OTKA 4271, and a grant from the "Magyar Tudományért" Foundation.

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. No lower bound was known even for depth–2 circuits with MOD 6 gates only.

The depth–2 case was settled by *Krause* and *Waack* [KrW]. They proved that any circuit with a MOD m gate at the top and arbitrary symmetric gates at the bottom needs exponential size to compute the $ID(x,y)$ function, where ID is defined as

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

Beigel and *Tarui* [BT] proved that every function computed by polynomial size, constant depth circuits of AND, OR, NOT and MOD m gates, can also be computed by a depth–2 circuit with a symmetric gate at the top, and $\exp(\log^{O(1)} n)$ AND-gates at the bottom. *Allender* and *Gore* [AG] proved that any *uniform* sequence of circuits of AND, OR, NOT, and MOD m gates needs exponential size to compute the *permanent* function. Using the uniformity assumption is *essential* here, since without it, it is unknown whether there exists any language in **NP**, or, even in **NEXP**, which cannot be computed with polynomial–size, bounded–depth circuits of AND, OR, NOT, and MOD m gates, where m is a non–prime–power positive integer.

Several results show that the computational properties of the MOD m and MOD p gates differ [BBR], [KM], [G], 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 [G] that depth-3 circuits with fan–in k MOD m gates on the bottom, arbitrary symmetric gates at the next, and threshold gates at the top need exponential size to compute the k-wise inner product function of [BNS], for any odd m which satisfies $m \equiv k \pmod{2m}$. In particular, this result yields a lower bound to the case when the lower and the middle level contain MOD m gates, and a threshold gate is at the top.

By a result of *Goldmann* and *Håstad* [GH], if the bottom fan–in is bounded by $k-1$, then arbitrary gates can be allowed on the bottom. This shows that the bound on the bottom fan–in is a strong assumption.

1.2 Our Results

A *weighted threshold function* $y = y_{\mathbf{w},b}$ is a Boolean function $y : \{0,1\}^t \to \{0,1\}$, defined in the following way:

$$y(x_1, x_2, ..., x_t) = \begin{cases} 1, & \text{if } \sum_{i=1}^t x_i w_i > b \\ 0 & \text{otherwise.} \end{cases}$$

Integers $w_1, w_2, ..., w_t$ are the *weights*, integer b is the *threshold.* A Boolean gate Y is a *weighted threshold gate* if it computes a weighted threshold function.

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

Theorem 1. *Let m and n be two positive integers, 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 input level, 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

$$\log(wM) = \Omega(n).$$

The size of the circuit is defined to be the number of the wires in it. Since M is an obvious lower bound to the size, Theorem 1 is also a size–weight trade–off. Another interpretation of Theorem 1 is the following:

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

$$\log(KM) = \Omega(n).$$

This result yields a trade–off between the fan–ins on the top and on the second level; or, in other words, between the numbers of the MOD m gates and the AND gates in the circuit.

Proof. Use Theorem 1 with $w = K$. ∎

One can also prove Theorem 1 for EXACT_m gates at the bottom (these gates outputs 1 exactly when the sum of their input bits is m), instead of MOD_m ones. Or, for a more general class:

Definition 3. *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*

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

Example. *MOD m gates compute a pc–simple function:*

$$u_I = -\sum_{i\in I} x_i \bmod m, \quad v_I = \sum_{i\in\{1,2,...,\ell\}-I} x_i \bmod m.$$

Or, $EXACT_m$ gates also compute a pc–simple function:

$$u_I = m - \sum_{i\in I} x_i, \quad v_I = \sum_{i\in\{1,2,...,\ell\}-I} x_i.$$

So we can state

Theorem 4. *Let m and n two positive integers, 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, 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

$$\log(wM) = \Omega(n).$$

1.3 Comparison with previous work

Krause and *Waack* [KrW] proved that computing $ID(x, y)$ (the Boolean function which is 1 exactly if $x = y$) on a circuit with a MOD m gate at the top and symmetric gates at the bottom, needs exponential size. However, $ID(x, y)$ can easily be computed by a circuit C of our Theorem 1: n MOD 2 gates at the bottom and one AND gate at the second level suffices. On the other hand, the $IP(x)$ function, which is hard for our circuit, is easy for the circuit of *Krause* and *Waack:* n AND gates at the bottom and one MOD 2 gate at the top can compute it. So the powers of our circuit and the circuit of [KrW] are *incomparable.*

Our earlier result in [G] was a lower bound for depth–3 circuits with a threshold gate at the top, arbitrary symmetric gates at the middle, and MOD m gates of bounded fan–in on the bottom, for some m. The present lower bound of Theorem 1 does not need the restriction on m and the bound on the fan–in, but, on the second level, only AND gates are allowed. The proof of the present result uses an elegant 2–player probabilistic communication protocol, instead of the intricate deterministic multi–party protocol of [G].

In addition, by our knowledge, the present result is the first which gives a trade–off between the computational resources in a circuit with hard–to–handle MOD m gates.

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 $y \in \{0,1\}^n$, and both of them has unlimited computational power (e.g. 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 bits to Bob, then Bob computes $f(x, y)$, and sends this bit to Alice.

The protocol above is optimal if $f = ID(x, y)$, (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 $0 < p \leq n^2$, 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 $x - y \neq 0$. A rough estimation of the probability of this event: $|x - y| \leq 2^n$, 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 Theorem 1.

3. PROOF OF THEOREM 1

First we prove (Lemma 5) 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 8) 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 9) which yields a lower bound to the probabilistic communication complexity of protocols, computing the outcome of C_i on a "big enough" portion of all inputs.

Lemma 5. *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 $(1 \leq i \leq t)$ such that either*

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

or

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

Proof. We need the following result of [HMPST]:

Lemma 6. ([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

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

Proof. See [HMPST]. ∎

Let us apply Lemma 6 to the circuit C of the statement of Lemma 5. With $A=IP^{-1}(1)$, $B=IP^{-1}(0)$, $w=w(C)$ we get that $\exists i:\ 1\le i\le t$,:

(1) $$|\Pr_A(C_i(x)=1)-\Pr_B(C_i(x)=1)| \ge \frac{1}{w}.$$

We also need:

Lemma 7.

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

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

Since $\Pr(A)+\Pr(B)=1$, Lemma 7 implies:

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

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

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):

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

From now on, as a shorthand, we write A instead of $x\in A$ and B instead of $x\in B$.

So

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

thus

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

$$\ge \frac{\Pr(A)}{w} \ge \frac{1}{3w}$$

for large enough n, using inequality (2).

By the triangle-inequality:

$$\frac{1}{3w} \le \left|\Pr(C_i(x)=1,A)-\frac{\Pr(A)}{\Pr(B)}\Pr(C_i(x)=1,B)\right| \le$$
$$\le |\Pr(C_i(x)=1,A)-\Pr(C_i(x)=1,B)|+$$
$$+\left|1-\frac{\Pr(A)}{\Pr(B)}\right|\Pr(C_i(x)=1,B) \le$$
$$\le |\Pr(C_i(x)=1,A)-\Pr(C_i(x)=1,B)|+\frac{1}{2^{\frac{n}{2}-2}}$$

using Lemma 7 and (3).

Consequently

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

Let us assume now that

$$\Pr(C_i(x)=1,A) > \Pr(C_i(x)=1,B).$$

So

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

and, since

$$\Pr(B)=\Pr(C_i(x)=1,B)+\Pr(C_i(x)=0,B),$$

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

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

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

because

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

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

(5) $$\frac{1}{2}+\frac{1}{3w}-\frac{1}{2^{\frac{n}{2}-3}} \le \Pr(\text{NOT}(C_i(x))=IP(x)),$$

and this completes the proof of Lemma 5. ∎

Lemma 8. *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*

$$\alpha \log N + \log\log m + O(1)$$

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 ℓ of T is corresponded to a MOD_m gate G_ℓ of circuit C_1:
– The first entry in row ℓ is the mod m sum of those inputs of gate G_ℓ, which are also elements of set U (i.e. known for Alice);
– the second entry in row ℓ is the mod m sum of those inputs of gate G_ℓ, 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_ℓ, then $1 - x_i$ is added up mod m.)

Let us observe that G_ℓ outputs 1 if and only if the mod m sum of row ℓ 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 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 $t'_{i2} = m - t_{i1} \mod m$, 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 congruent 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 $0 < |t - t'| \le m^N - 1$. 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 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 5, there exists an i such that

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

or

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

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

$$(6) \qquad \forall\, x \in D: \quad g(x) = IP(x).$$

By Lemma 8, there exists a probabilistic protocol, which computes $g(x)$, and its success probability is at least

$$(7) \quad 1 - \frac{\alpha \log N + \log\log m}{N^{\alpha-1}} = 1 - \frac{\alpha \log N + O(1)}{N^{\alpha-1}},$$

independently from x.
Because of (6), if Alice and Bob computes $g(x)$ with $O(\alpha \log n + O(1))$ communication (with a constant m), then they will get the value of $IP(x)$ with probability (7), if $x \in D$.
In other words, if Alice and Bob computes $g(x)$ by the protocol of Lemma 8, then they will get $IP(x)$ with average success probability

$$(8) \qquad \Pr(D)\Big(1-\frac{\alpha\log N+O(1)}{N^{\alpha-1}}\Big),$$

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

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

Theorem 9. *[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 ε and for fixed n — always $\gamma_\varepsilon(n)$ bits. Then

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

■

Case 1. If $N<\min(12w,2^{\frac{n}{2}-3})$, then we can give the following lower estimation for (8):

$$(9) \qquad \Big(\frac{1}{2}+\frac{1}{3w}-\frac{1}{2^{\frac{n}{2}-3}}\Big)\Big(1-\frac{\alpha\log N+O(1)}{N^{\alpha-1}}\Big)\geq$$

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

assuming, that $N^{\alpha-2}<2^{\frac{n}{2}-3}$, and $\alpha\geq 3$.
Let us set α such that

$$(10) \qquad 6w=\frac{1}{3}N^{\alpha-2},$$

where we use the obvious facts that $N\geq 2$, and $w>1$. If, with this α, $N^{\alpha-2}<2^{\frac{n}{2}-3}$ does not hold, then we have got a proper lower bound to w, and we are ready. Otherwise, we can use (9) and Theorem 9, with $\varepsilon=3N^{-\alpha+2}$:

$$(11) \qquad \gamma_\varepsilon(n)>n-3(\alpha-2)\log N-O(1).$$

Because of (10), and since $\alpha>3$, the protocol of Lemma 8 communicates at most

$$\Big(\frac{\alpha}{\alpha-2}\Big)\log w+O(1)\leq 3\log w+O(1)$$

bits, so (11) can be written:

$$(12) \qquad 6\log w>n-O(1).$$

Case 2. If $12w\leq\min(N,2^{\frac{n}{2}-3})$, then the lower estimation for (8) is:

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

$$\geq\frac{1}{2}+\frac{1}{6w}.$$

Let

$$6w=N^{\alpha-2},$$

where $2<\alpha<3$. Now, the protocol of Lemma 8 has communication of at most $3\log N+O(1)$ bits, so, from Theorem 9:

$$(13) \qquad 6\log N>n-O(1).$$

Now, unifying (12) and (13):

$$\log(Nw)\geq\max(\log N,\log w)\geq\frac{1}{6}n-O(1)=\Omega(n),$$

which completes the proof. ■

4. PROOF OF THEOREM 4.

(Sketch) The proof is the same as that of Theorem 1, except Lemma 8 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 8 can also be modified to this class of circuits with the same result. The further details are omitted here. ■

REFERENCES

[AG] E. Allender, V. Gore: A Uniform Circuit Lower Bound for the Permanent, preprint, 1992

[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

[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

[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: 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.

[H] J. Håstad: Almost optimal lower bounds for small depth circuits, Proc. 18th ACM STOC, 1986, pp. 6–20.

[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, (10) No. 1. pp. 17–22.

[KrW] M. Krause, S. Waack: Variation ranks of communication matrices and lower bounds for depth two circuits having symmetric gates with unbounded fan–in, Proc. 32nd IEEE FOCS, 1991, pp. 777-782.

[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

[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.

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

[Y5] A. C. Yao: Separating the polynomial–time hierarchy by oracles, Proc. 26th IEEE FOCS, 1985, pp. 1–10.