LOWER BOUNDS ON REPRESENTING BOOLEAN FUNCTIONS AS POLYNOMIALS IN Z_m

SHI-CHUN TSAI †‡

Abstract. Define the MOD_m-degree of a boolean function F to be the smallest degree of any polynomial P, over the ring of integers modulo m, such that for all 0-1 assignments $\vec{x}$, $F(\vec{x}) = 0$ iff $P(\vec{x}) = 0$. By exploring the periodic property of the binomial coefficients modulo m, two new lower bounds on the MOD_m-degree of the MOD_l and $\neg MOD_m$ functions are proved, where m is any composite integer and l has a prime factor not dividing m. Both bounds improve from sub-linear to $\Omega(n)$. With the periodic property, a simple proof of a lower bound on the MOD_m-degree with symmetric multilinear polynomial of the OR function is given. It is also proved that the majority function has a lower bound $\frac{n}{2}$ and the MidBit function has a lower bound $\sqrt{n}$.

Key words. boolean function complexity, circuit complexity, computational complexity

AMS subject classifications. 68Q05, 68Q15, 68Q25, 94C10

1. Introduction. Proving lower bounds on explicitly given boolean functions is a notoriously difficult task. While the problem of proving nonlinear size lower bounds for general boolean functions is still not in sight, very powerful results are available for restricted classes, such as monotone circuits, or circuits of unbounded fan-in gates with small depth [5, 17]. One of the major tools in obtaining these lower bounds, was the use of algebraic techniques [11, 12, 13]. As a result, several researchers started the study of polynomials that in some sense represent boolean functions. In particular, one wishes to find lower bounds on the degree of such polynomials: in some situations this enables us to prove a lower bound on circuit size [12]. In any case, the degree of the representing polynomial is a natural characteristic of the boolean function, and it is interesting to try to find bounds on it.

In this paper we prove lower bounds on the MOD_m-degree of some functions for composite m. These bounds substantially improve previous results [2], use elementary methods, and we hope shed some more light on the power of the MOD_m function for composite m. Recall that the Smolensky-Razborov technique seems not applicable in this situation, and Szegedy's dissertation [13] also shows that such gates are surprisingly powerful. Thus any lower bound for these gates is of interest.

We briefly review the main previous results. There are many possible representations of boolean functions as polynomials over some ring or field. Nisan and Szegedy [9] studied the degree of real polynomials that represent boolean functions. Paturi [10] studied the degree of real polynomials that approximate symmetric boolean functions. In [14, 15] Tarui proved some results on the degree complexity of boolean functions over rings and he applied these results to prove the separations of certain relativized classes. In [2] Barrington, Beigel and Rudich studied representing boolean functions as polynomials modulo m. Our work is an extension of the results in [2].

The techniques of Razborov and Smolensky [11, 12] that show that polynomial size constant depth circuits with MOD_p gates cannot compute the MOD_q function (the boolean function $MOD_m(x_1, ..., x_n)$ is defined to be 0 if $\sum_{i=0}^{n} x_i$ is a multiple of m and 1 otherwise) when p and q are distinct primes, suggest the following definition

† Department of Computer Science, University of Chicago, 1100 E. 58th Street, Chicago, Illinois 60637 (tsai@cs.uchicago.edu).

‡ A preliminary version of this paper appeared in the Proceedings of the 8th Annual Structure in Complexity Theory Conference, San Diego, CA, 1993, pp. 96–101.

[1]. A polynomial P over Z_m represents a boolean function F if for all 0-1 valued assignments $\vec{x}$, $F(\vec{x}) = 0$ iff $P(\vec{x}) = 0$. The MOD_m-degree of F, denoted $\delta(F, m)$, is the degree of the lowest degree polynomial which represents it. This is an interesting complexity measure on its own, and, in the case of prime moduli, yields lower bounds for circuit size.

For moduli m that are prime, or prime power, the situation is well understood [12, 3]. It is known that for the OR function of n variables $\delta(OR, p) = \lceil \frac{n}{p-1} \rceil$ [12, 16]. It is also known that $\delta(MOD_l, p) = \Omega(n)$ when l is not a power of p. These results depend crucially on the fact that Z_p is a finite field.

For composite moduli, when Z_m is a ring, and not a field, many of the lemmas simply fall apart. Barrington, Beigel and Rudich [2] proved the first few lower bounds for the OR and MOD functions for composite m. They proved that if the representing polynomial is symmetric $\delta(OR, m) = \Theta(n^{1/r})$, where r is the number of distinct prime factors of m. They also proved that for any non-square-free composite integer m, $\delta(MOD_l, m) = n^{\Omega(1)}$ and $\delta(\neg MOD_l, m) = n^{\Omega(1)}$, where l has a prime factor that is not a divisor of m and $\delta(\neg MOD_m, m) = n^{\Omega(1)}$. If m is square-free they have $\delta(MOD_l, m) = n^{\Omega(1)}$, $\delta(\neg MOD_l, m) = \Omega(n)$ and $\delta(\neg MOD_m, m) = \Omega(n)$.

Our paper improves these results. First, we give a new simple proof for the lower bound for the OR function, that does not depend on m being square-free. We prove that the MOD_m-degree of the majority function is at least $\frac{n}{2}$. We also show a lower bound, $\sqrt{n}$, for the MidBit function. (The MidBit function, defined in [4], is the boolean function that takes $x_1, ..., x_n$ as input and outputs the value of the $\lfloor \frac{\log n}{2} \rfloor$-th bit in the binary representation of the number $\sum_{i=1}^{n} x_i$.)

Finally, we prove that $\delta(MOD_l, m) = \Omega(n)$ and $\delta(\neg MOD_l, m) = \Omega(n)$ when l has a prime that is not a factor of m, and that $\delta(\neg MOD_m, m) = \Omega(n)$. These improve the bounds in [1] for the case m is not square-free. Our proofs rely on a periodic property of the binomial coefficients. They are simpler and more straightforward than the previous proofs of weaker statements.

2. Notations. As a convention, $[n]$ denotes the set $\{1, 2, \cdots, n\}$. Let A and B be sets. We write $A \subseteq B$ if every member of A also belongs to B, i.e. A is a subset of B. We write $A \subset B$ to indicate that A is a proper subset of B. Boolean functions on n variables will be represented as polynomials in the ring $Z_m[x_1, \cdots, x_n]$. Since we will consider the domain $\{0,1\}^n$ only, we are interested in the multilinear polynomials. For $A \subseteq [n]$, we define $X_A = \prod_{i \in A} x_i$. It is clear that $\{X_A | A \subseteq [n]\}$ forms a basis for the multilinear polynomials in $Z_m[x_1, \cdots, x_n]$. And $\{X_A | A \subseteq [n], |A| \leq d\}$ forms a basis for the multilinear polynomials of degree at most d in $Z_m[x_1, \cdots, x_n]$. Let $P(x_1, \cdots, x_n)$ be any n-variable function with domain $\{0,1\}^n$. We say that $P(A)$ has the value obtained with the assignment $x_i = 1$ if $i \in A$; 0 otherwise.

DEFINITION 2.1. *Define $\delta(F, m)$, the MOD_m-degree of a boolean function F to be the smallest degree of any polynomial P in Z_m such that for all 0-1 assignments $\vec{x}$, $F(\vec{x}) = 0$ iff $P(\vec{x}) = 0$.*

DEFINITION 2.2. *Let m, r and n be positive integers, where $0 \leq r \leq m-1$. The $MOD_{(m,r)}$ function of n variables is defined as:*

$$MOD_{(m,r)}(x_1, \cdots, x_n) = \begin{cases} 0 & \text{if } \sum_i x_i \equiv r \pmod{m} \\ 1 & \text{otherwise.} \end{cases}$$

We use MOD_m to indicate $MOD_{(m,0)}$.

DEFINITION 2.3. *Let k and n be any positive integers and $k \leq n$. The threshold function TH_k^n of n variables is defined as:*

$$TH_k^n(x_1, \cdots, x_n) = \begin{cases} 1 & \text{if } \sum_i x_i \geq k \\ 0 & \text{otherwise.} \end{cases}$$

DEFINITION 2.4. *Let n be a positive integer. The MidBit function of n variables is defined as $MidBit(x_1, \cdots, x_n) = \lfloor \frac{\log n}{2} \rfloor$-th bit in the binary representation of $\sum_{i=1}^n x_i$.*

3. Main lemmas. Let j be a non-negative integer, and let k and m be any positive integers. Fix k and m, then the integer function $f(j) = \binom{j}{k} \bmod m$ is a cyclic function of j. As H. Kwong pointed out, this property has been proved by several other authors by using different methods [6, 7, 18]. For completeness we show the proof in the following.

LEMMA 3.1. *Let p be any prime number, and let a and k be any positive integers. Then $\binom{j}{k} \bmod p^a$ has the cycle length p^{a+e}, where $e = \lfloor \log_p k \rfloor$.*

Proof.

Define $L_k = p^{a+\lfloor \log_p k \rfloor}$. We want to prove $\binom{sL_k+j}{k} \equiv \binom{j}{k} \pmod{p^a}$ for any non-negative integer s and any positive integer k by induction on j. For the base case $j = 0$, since $\binom{sL_k}{k} = \frac{sL_k}{sL_k-k}\binom{sL_k-1}{k}$ is an integer and the largest power of p that divides sL_k-k is at most $p^{\lfloor \log_p k \rfloor}$, we know $\binom{sL_k}{k}$ is divisible by p^a. Thus $\binom{sL_k}{k} \equiv 0 \pmod{p^a}$ for all non-negative integer s and any positive integer k. Suppose $\binom{sL_k+j}{k} \equiv \binom{j}{k} \pmod{p^a}$ for any non-negative integer s and any positive integer k, for $0 \leq j \leq i$. Now consider the case when $j = i+1$.

$$\begin{aligned} \binom{sL_k+i+1}{k} &= \binom{sL_k+i}{k} + \binom{sL_k+i}{k-1} \\ &\equiv \binom{i}{k} + \binom{i}{k-1} \pmod{p^a}, \quad \text{because } L_{k-1} | L_k. \\ &\equiv \binom{i+1}{k} \pmod{p^a}. \end{aligned}$$

Next we need to prove that L_k is the smallest cycle. To show L_k is the smallest cycle of $\binom{j}{k} \bmod p^a$, we prove that there exists an i, $0 \leq i < k$, such that $\binom{\frac{L_k}{p}+i}{k} \not\equiv \binom{i}{k} \equiv 0 \pmod{p^a}$. WLOG let $k = p^l + i$, where l is any positive integer and $0 \leq i < p^{l+1} - p^l$. With this assumption we have $\lfloor \log_p k \rfloor = l$. By induction on i, we will prove $p^a \not| \binom{p^{l+a-1}+i}{p^l+i}$. This is clear for the base case $i = 0$. Suppose it holds for the case up to i, i.e. $p^a \not| \binom{p^{l+a-1}+m}{p^l+m}$, where $0 \leq m \leq i \leq p^{l+1} - p^l - 1$. Consider the case $m = i+1$. We are interested in the case when $i+1 < p^{l+1} - p^l$. Then $\binom{p^{l+a-1}+i+1}{p^l+i+1} = \frac{p^{l+a-1}+i+1}{p^l+i+1}\binom{p^{l+a-1}+i}{p^l+i}$. We know $\frac{p^{l+a-1}+i+1}{p^l+i+1}$ is not divisible by p. By the induction hypothesis we have $p^a \not| \binom{p^{l+a-1}+i+1}{p^l+i+1}$. This completes the proof. $\square$

By applying the Chinese Remainder Theorem we can generalize the above lemma as follows.

LEMMA 3.2. *Let m_1 and m_2 be any two relatively prime positive integers. If $\binom{j}{k} \bmod m_1$ and $\binom{j}{k} \bmod m_2$ has the cycle length l_1 and l_2, respectively, then $\binom{j}{k} \bmod m_1 m_2$ has the cycle length $l_1 l_2$.*

THEOREM 3.3. *Let $m = p_1^{a_1} \cdots p_r^{a_r}$ be an arbitrary positive integer, where the p_i's are distinct prime numbers and the a_i's are positive integers. Let $e_i = \lfloor \log_{p_i} k \rfloor$ for $1 \le i \le r$, then $\binom{j}{k}$ mod m has the cycle length $\prod_{i=1}^{r} p_i^{a_i+e_i}$.*

Proof. By Lemmas 3.1 and 3.2. $\square$

Let $P(x_1, \cdots, x_n) \in Z_m[x_1, \cdots, x_n]$ be a polynomial representing a Boolean function $f(x_1, \cdots, x_n)$. If the degree of P is d, then we can write $P(x_1, \cdots, x_n) = \sum_{A \subseteq [n]; |A| \le d} c_A X_A$. Recall that we define $f(A) = f(a_1, \cdots, a_n)$, where $a_i = 1$ if $i \in A$; 0 otherwise. $P(A)$ is defined similarly. For convenience, for each $A \subseteq [n]$ we use b_A to denote $P(A)$. Since P represents f, it is clear that if $f(A) = 0$ then $b_A = 0$ and if $f(A) = 1$ then b_A can be any non-zero integer in Z_m. If there are M different assignments in $\{0,1\}^n$ satisfying f then by a simple counting argument there are $(m-1)^M$ multilinear polynomials in Z_m representing f. For any $A \subseteq [n]$ it is clear that $X_D(A) = 0$ if $D \not\subseteq A$ and $X_D(A) = 1$ if $D \subseteq A$. Thus $b_A = P(A) = \sum_{D \subseteq A; |D| \le d} c_D$. There are 2^n possible inputs. With the given boolean function we can choose a set of b_A's such that $b_A = 0$ if $f(A) = 0$ and $b_A \ne 0$ if $f(A) = 1$. Then we can set up a system of linear equations with $\sum_{i=0}^{d} \binom{n}{i}$ variables if the representing polynomial has degree d. By solving the linear equations, we prove some useful relations among b_D's and c_A's over any ring Z_m. Actually, Lemma 3.4.1 is a special case of the well known Möbius inversion theorem [8].

LEMMA 3.4.

1. *If $A \subset [n]$ and $|A| \le d$ then*

$$c_A = \sum_{D \subseteq A} (-1)^{|A|-|D|} b_D.$$

2. *If $A \subseteq [n]$ and $|A| > d$ then*

$$b_A = \sum_{D \subset A; |D| \le d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} b_D.$$

Proof.

1. By induction on the size of A. It is clear for the case of $|A| = 0$ and 1. Suppose it is true for all $|A| \le k$. Consider the case of $d \ge |A| = k+1$. Then

$$\begin{aligned} P(A) &= b_A \\ &= c_A + \sum_{S \subset A} c_S \\ &= c_A + \sum_{S \subset A} (b_S + \sum_{D \subset S} (-1)^{|S|-|D|} b_D). \end{aligned}$$

The third equality is by induction hypothesis. Then

$$c_A = b_A - \sum_{S \subset A} (b_S + \sum_{D \subset S} (-1)^{|S|-|D|} b_D).$$

Let D_l be any subset of A with size $l < |A|$. We want to figure out the common coefficient of b_{D_l}'s for a fixed l. It can be found as follows

$$-(\sum_{D_l \subset A} b_{D_l} + \sum_{S \subset A} \sum_{D_l \subset S} (-1)^{|S|-l} b_{D_l})$$

$$
\begin{aligned}
&= -(\sum_{D_l \subset A} b_{D_l} + \sum_{D_l \subset A} \sum_{i=1}^{|A|-l-1} (-1)^i \binom{|A|-l}{i} b_{D_l}) \\
&= -\sum_{D_l \subset A} \sum_{i=0}^{|A|-l-1} (-1)^i \binom{|A|-l}{i} b_{D_l} \\
&= -\sum_{D_l \subset A} (-1)^{|A|-l-1} b_{D_l} \\
&= \sum_{D_l \subset A} (-1)^{|A|-l} b_{D_l}.
\end{aligned}
$$

This proves the first claim.

2.

$$
\begin{aligned}
b_A &= \sum_{D \subset A; |D| \leq d} c_D \\
&= \sum_{D \subset A; |D| \leq d} (\sum_{T \subseteq D} (-1)^{|D|-|T|} b_T) \\
&= \sum_{T \subset A; |T| \leq d} \sum_{i=0}^{d-|T|} (-1)^i \binom{|A|-|T|}{i} b_T \\
&= \sum_{T \subset A; |T| \leq d} (-1)^{d-|T|} \binom{|A|-|T|-1}{d-|T|} b_T \\
&= \sum_{D \subset A; |D| \leq d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} b_D
\end{aligned}
$$

In the second to the last equation we use the fact $\sum_{i=0}^{l} (-1)^i \binom{m}{i} = (-1)^l \binom{m-1}{l}$. ∎

From the above lemma we know the first $(\sum_{i=0}^{d} \binom{n}{i})$ b_A's will determine the coefficients of the polynomial P and the rest of the b_A's. With the above lemmas we can prove several lower bounds systematically. The key of the proof relies on the periodic property of the binomial coefficients modulo m.

4. Lower bounds. From Lemma 3.4 we have an immediate lower bound for the threshold function.

THEOREM 4.1. *$\delta(TH_k^n, m) \geq k$, where m is any positive integer.*

Proof. Let P be a polynomial over Z_m, which represents TH_k^n and has degree less than k. By the definition of the threshold function, we know $b_A = 0$ for all $A \subset [n]$ with $|A| < k$, and by Lemma 3.4.1 we have $c_A = 0$ for all $A \in [n]$ with $|A| < k$. By Lemma 3.4.2 $b_A = 0$ for all $A \subseteq [n]$ with $|A| \geq k$, which is a contradiction to the definition of the threshold function. Thus the degree must be at least k. ∎

Let's look at the majority function. We define the majority function on n variables as $MAJ(x_1, \cdots, x_n) = 1$ if there are at least $\frac{n}{2}$ 1's in the input; 0 otherwise. Clearly, it is a special case of the threshold function. Thus we have the following immediate corollaries.

COROLLARY 4.2. *Let m be any positive integer.*

1. $\delta(MAJ, m) \geq \frac{n}{2}$.
2. $\delta(AND, m) = n$.
3. $\delta(MidBit, m) = \Omega(\sqrt{n})$.

It is clear that part 2 is trivial and part 3 follows from the proof of Theorem 4.1. Next we're going to prove the lower bound for the OR function. With the previous lemmas we prove it without distinguishing between the cases of square-free and non-square-free m.

THEOREM 4.3. *Let m be any non-prime-power composite number. If the OR function of n variables is represented by a symmetric polynomial modulo m, then the degree is $\Omega(n^{1/r})$, where r is the number of distinct primes dividing m.*

Proof. Let P be a symmetric polynomial of degree d that represents the OR function over Z_m. Say $m = \prod_{i=1}^{r} p_i^{a_i}$. Suppose $p_i^{e_i} \le d < p_i^{e_i+1}$ for $1 \le i \le r$. It is clear that $P(\emptyset) = b_\emptyset = 0$ and $P(A) = b_A \ne 0$ if $A \subseteq [n]$ and $A \ne \emptyset$. Since P is symmetric for any $A, B \subseteq [n]$, if $|A| = |B|$ then $b_A = b_B$ and so $c_A = c_B$. Thus we can use $c_{|A|}$ to indicate c_A and the others of the same cardinality. Consider the case $|A| > d$. It is easy to see $b_A = \sum_{i=1}^{d} \binom{|A|}{i} c_i$. By Theorem 3.3, we know $\binom{|A|}{d} \bmod m$ has the cycle length $\prod_{j=1}^{r} p_j^{e_j+a_j}$, when $|A|$ ranges over the non-negative integers. We denote the cycle length as L. If $i > j$ then the cycle length of $\binom{|A|}{i} \bmod m$ is a multiple of the cycle length of $\binom{|A|}{j} \bmod m$. Thus $\binom{0+L}{i} \equiv 0 \pmod m$, for $1 \le i \le d$, since $\binom{0}{i} \equiv 0 \pmod m$. We must have $n < L$ otherwise $b_A = 0$ for $|A| = L$, which contradicts the definition of the OR function. Hence, $n < L = \prod_{j=1}^{r} p_j^{e_j+a_j} \le md^r$, and therefore $d = \Omega(n^{1/r})$. □

It is still open to find an upper bound for the non-symmetric case. A very weak lower bound can be obtained by a Ramsey argument. Meanwhile in [1], Alon et al. proved a better lower bound than the one that follows from the Ramsey argument. To resolve the problem, we can either try to improve the lower bound or find a small upper bound for the non-symmetric representation of the OR function.

THEOREM 4.4. *Let m be a positive composite integer which is not a prime power then $\delta(\neg MOD_m, m) = \Omega(n)$.*

Proof. Let P be a representing polynomial of the $\neg MOD_m$ function of degree d. Choose p^l such that $p^l | m$ and $p^l \nmid c_\emptyset$, where p is a prime factor of m. Such p and l exist, since $c_\emptyset \not\equiv 0 \pmod m$. It is clear $b_\emptyset = c_\emptyset$. WLOG, let $n = p^{k+l} + p^k - 1$, where k is an arbitrary integer. From Lemma 3.4.2, we have $b_A = \sum_{D \subset A; |D| \le d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} b_D$, for $|A| > d$. We are interested in the sets $A \subset [n]$ with $|A| = p^{k+l}$ and the sum of the corresponding b_A's.

$$\begin{aligned}
\sum_{A \subset [n]} b_A &= \sum_{A \subset [n]} \sum_{D \subset A; |D| \le d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} b_D \\
&= \sum_{D \subset [n]; |D| \le d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} \binom{n-|D|}{|A|-|D|} b_D \\
&= \sum_{D \subset [n]; |D| \le d} (-1)^{d-|D|} \binom{|A|-|D|-1}{d-|D|} \binom{n-|D|}{n-|A|} b_D.
\end{aligned}$$

It's clear $n - |A| = p^k - 1$ and $b_A \equiv 0 \pmod m$, since $m \nmid |A|$ and by the definition of the $\neg MOD_m$ function. If $0 < |D| < p^k$ then $n - |D| = p^{k+l} + (p^k - |D| - 1)$. And so $\binom{n-|D|}{n-|A|} = \binom{n-|D|}{p^k-1} \equiv \binom{p^k-|D|-1}{p^k-1} \equiv 0 \pmod{p^l}$, since by Lemma 3.1, $\binom{j}{p^k-1} \bmod p^l$ has the cycle length p^{k+l-1}. Therefore, we have

$$0 \equiv (-1)^d \binom{|A|-1}{d} \binom{n}{n-|A|} b_\emptyset \pmod{p^l}$$

$$\equiv \quad (-1)^d \binom{|A|-1}{d} b_\emptyset \pmod{p^l}.$$

If we let $d < p^k$, then $\binom{j}{d} \pmod{p^l}$ has the cycle length at most p^{k+l-1}. Thus,

$$\begin{aligned} 0 &\equiv (-1)^d \binom{|A|-1}{d} b_\emptyset \pmod{p^l} \\ &\equiv (-1)^d \binom{p^{l+\lfloor \log_p d \rfloor}-1}{d} b_\emptyset \pmod{p^l} \\ &\equiv b_\emptyset \sum_{i=0}^{d} (-1)^i \binom{p^{l+\lfloor \log_p d \rfloor}}{i} \pmod{p^l} \qquad (1) \\ &\equiv b_\emptyset \pmod{p^l}. \end{aligned}$$

The modular equality in (1) follows from the identity $\sum_{i=0}^{n}(-1)^i\binom{m}{i} = (-1)^n\binom{m-1}{n}$. It leads to a contradiction. Therefore , $d \geq p^k = \frac{n+1}{p^l+1}$. The theorem is clear now for the case of $n = p^{k+l} + p^k - 1$. For the case $p^{k+l} + p^k - 1 < n < p^{k+1+l} + p^{k+1} - 1$, the MOD_m-degree must be at least p^k, which is at least $\frac{n+1}{p^{l+1}+p}$. And the proof is completed. □

By following the above proof we have an immediate corollary.

COROLLARY 4.5. *Let p be a prime number which is not a factor of m, then* $\delta(\neg MOD_p, m) = \Omega(n)$.

It is a fact that for any positive integer l, $\delta(MOD_l, m) = \delta(MOD_{(l,1)}, m) + c$, where c is a constant. Thus following the lines in the proof of Theorem 4.4, we have the following theorem, which not only improves a previous sub-linear lower bound in [2] but also extends it to any composite integer m.

THEOREM 4.6. *Let m be a positive composite integer and q be a prime number which is not a factor of m, then $\delta(MOD_q, m) = \Omega(n)$.*

Proof. Instead of proving the lower bound for the MOD_q function we prove it for the $MOD_{(q,1)}$ function. As usual let P be a representing polynomial for the $MOD_{(q,1)}$ function. Choose p^l as we did in Theorem 4.4. WLOG, let $n = p^{(k+l)(q-1)} + p^{k(q-1)} - 1$, where k is an arbitrary integer. Then by following the proof in Theorem 4.4 and Fermat's Little Theorem we can prove the lower bound. □

Theorem 4.4 and 4.6 show that it is difficult to compute the functions MOD_p and $\neg MOD_p$ by polynomials over Z_m, when p is not a factor of m. By a simple counting argument, we know that almost every boolean function needs MOD_m-degree at least $\frac{n}{2} - o(\sqrt{n})$ for any positive integer m. It will be interesting to see whether $\frac{n}{2} - o(\sqrt{n})$ is enough for almost every boolean function when n is big enough.

Acknowledgments. I am grateful to Richard Beigel and Janos Simon for very useful comments on the earlier version of this paper. I would also like to thank Lance Fortnow, Katalin Friedl and Mario Szegedy for helpful discussion, Harris Kwong for telling me the papers about the periodic property of binomial coefficients modulo m and last but not least the anonymous referees for their useful comments.

REFERENCES

[1] N. ALON, D. KLEITMAN, R. LIPTON, R. MESHULAM, M. RABIN AND J. SPENCER, *Set systems with no union of cardinality 0 modulo m*, Graphs and Combinatorics, 7 (1991), pp. 97–99.

[2] D. A. M. Barrington, R. Beigel, and S. Rudich, *Representing boolean functions as polynomials modulo composite numbers*, in Proc. 24th Annual ACM Symposium on Theory of Computing, 1992, pp. 455-461.

[3] R. Beigel and J. Tarui, *On ACC*, in Proc. 32nd IEEE Symposium on Foundations of Computer Science, 1991, pp. 783–792.

[4] F. Green, J. Köbler and J. Torán, *The power of the middle bit*, in Proc. 7th Annual IEEE Conference on Structure in Complexity Theory, Boston, MA, 1992, pp. 111–117.

[5] J. Håstad, *Computational limitations of small-depth circuits*, MIT PRESS, Cambridge, MA, 1986.

[6] Y.H.H. Kwong, *Minimum periods of binomial coefficients modulo M*, Fibonacci Quarterly, 27 (1989), pp. 348–351.

[7] Y.H.H. Kwong, *Periodicities of a class of infinite integer sequences modulo M*, J. Number Theory, 31 (1989), pp. 64–79.

[8] L. Lovász, *Combinatorial Problems and Exercises*, 2nd ed., North-Holland, Amsterdam, 1993.

[9] N. Nisan and M. Szegedy, *On the degree of boolean functions as real polynomials*, in Proc. 24th Annual ACM Symposium on Theory of Computing, 1992, pp. 462–467.

[10] R. Paturi, *On the degree of polynomials that approximate symmetric boolean functions*, in Proc. 24th Annual ACM Symposium on Theory of Computing, 1992, pp. 467–474.

[11] A. A. Razborov, *Lower bounds for the size of circuits of bounded depth with basis* $\{\wedge, \oplus\}$, Math. notes of the Academy of Science of the USSR, 41-4, (1987), pp. 333–338.

[12] R. Smolensky, *Algebraic methods in the theory of lower bounds for boolean circuit complexity*, in Proc. 19th Annual ACM Symposium on Theory of Computing, 1987, pp. 77–82.

[13] M. Szegedy, *Algebraic methods in lower bounds for computational models with limited communication*, Ph.D. thesis, Department of Computer Science, University of Chicago, Chicago, IL, 1989.

[14] J. Tarui, *Randomized polynomials, threshold circuits, and the polynomial hierarchy*, in Proc. 8th Annual Symposium on Theoretical Aspects of Computer Science, 1991, pp. 238–250.

[15] J. Tarui, *Degree complexity of boolean functions and its applications to relativized separations*, in Proc. 6th Annual IEEE Conference on Structure in Complexity Theory, 1991, pp. 382–390.

[16] S. C. Tsai, *A simple proof of representing boolean functions as polynomials modulo p*, Technical Report CS 92-27, Department of Computer Science, University of Chicago, Chicago, IL, 1992.

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

[18] S. Zabek, *Sur la périodicité modulo m des suites de nombres* $\binom{n}{k}$, Ann. Univ. Mariae Curie-Sklodowska, A10 (1956), pp. 37–47.