On the Degree of Boolean Functions as Polynomials over $\mathbb{Z}_m$

Xiaoming Sun$^1$, Yuan Sun$^1$, Jiaheng Wang$^2$, Kewen Wu$^2$, Zhiyu Xia$^1$, and Yufan Zheng$^1$

$^1$Institute of Computing Technology, Chinese Academy of Sciences, China
$^2$School of Electronics Engineering and Computer Science, Peking University, China

Abstract

Polynomial representations of Boolean functions over various rings such as $\mathbb{Z}$ and $\mathbb{Z}_m$ have been studied since Minsky and Papert (1969). From then on, they have been employed in a large variety of fields including communication complexity, circuit complexity, learning theory, coding theory and so on. For any integer $m \geq 2$, each Boolean function has a unique multilinear polynomial representation over ring $\mathbb{Z}_m$. The degree of such polynomial is called modulo-$m$ degree, denoted as $\text{deg}_m(\cdot)$.

In this paper, we discuss the lower bound of modulo-$m$ degree of Boolean functions. When $m = p^k$ ($k \geq 1$) for some prime $p$, we give a tight lower bound that $\text{deg}_m(f) \geq k(p-1)$ for any non-degenerated function $f : \{0,1\}^n \to \{0,1\}$, provided that $n$ is sufficient large. When $m$ contains two different prime factors $p$ and $q$, we give a nearly optimal lower bound for any symmetric function $f : \{0,1\}^n \to \{0,1\}$ that $\text{deg}_m(f) \geq \frac{n}{\frac{1}{p-1} + \frac{1}{q-1}}$.

The idea of the proof is as follows. First we investigate properties of polynomial representation of $\text{MOD}$ function, then use it to span symmetric Boolean functions to prove the lower bound for symmetric functions, when $m$ is a prime power. Afterwards, Ramsey Theory is applied in order to extend the bound from symmetric functions to non-degenerated ones. Finally, by showing that $\text{deg}_p(f)$ and $\text{deg}_q(f)$ cannot be small simultaneously, the lower bound for symmetric functions can be obtained when $m$ is a composite but not prime power.

1 Introduction

Given a Boolean function $f : \{0,1\}^n \to \{0,1\}$, the degree (resp., modulo-$m$ degree), denoted as $\text{deg}(f)$ (resp., $\text{deg}_m(f)$), is the degree of the unique multilinear polynomial representation over $\mathbb{R}$ (resp., $\mathbb{Z}_m$). These complexity measures and related notions have been well studied since the work of Minsky and Papert [21]. The polynomial representation of a Boolean function has found numerous applications in the study of query complexity (see e.g. [5]), communication complexity [1, 9, 22, 26, 29], learning theory [15, 16, 19, 23], explicit combinatorial constructions [6, 10, 12, 13], circuit lower bounds [11, 12, 25, 31] and coding theory [14, 20, 33, 34].

In this paper, we focus on modulo-$m$ degree of Boolean functions. One of the complexity theoretic motivations of studying $\text{deg}_m(f)$ is to understand the power of modular counting. The famous Razborov–Smolensky polynomial method [25, 31] reduces the task of proving size lower bounds for $\mathcal{AC}^0[p]$ circuits to proving the lower bound of approximate modulo-$p$ degree of the target Boolean function. However, their idea only works when $p$ is a prime. Nevertheless, it is still important to understand the computational power of polynomials over $\mathbb{Z}_m$ for general $m$.

1 The existence and uniqueness are guaranteed by the Möbius inversion, see e.g. [11].

2 It is a folklore that $\mathcal{AC}^0[m] = \mathcal{AC}^0[\text{rad}(m)]$, where $\text{rad}(m)$ is the square-free part of $m$. Therefore in fact we are able to handle $\mathcal{AC}^0[q]$ circuits for any prime power $q$. 
Towards the complexity measure $\deg_m(f)$ itself, the case when $m$ is a prime has been studied a lot in previous works. For example, one natural question is whether $\deg_m(f)$ is polynomially related to $\deg(f)$ for general $m$, as other complexity measures like decision tree complexity $D(f)$ do? The answer is a NO according to the parity function $\text{PARITY}(x) := \bigoplus_{i=1}^n x_i$. That is, $\deg_2(\text{PARITY}) = 1$ but $\deg(\text{PARITY}) = n$. Though this function works as a counterexample for the relationship between $\deg_2(f)$ and $\deg(f)$, it is still inspiring because its modulo-3 degree seems to be large. After some careful calculation, one can get $\deg_3(\text{PARITY}) = \Theta(n)$. Actually, Gopalan et al. [11] give the following relationship between the polynomial degrees modulo two different primes $p$ and $q$:

$$\deg_q(f) \geq \frac{n}{\log_2 p} \deg_p(f) p^{2\deg_p(f)}.$$ 

Daunting at the first glance, the inequality implies an essential fact that, as long as $\deg_p(f) = o(\log n)$, a lower bound of $\Omega(n^{1-o(1)})$ for $\deg_q(f)$ follows. Moreover, if $m$ has at least two different prime factors $p$ and $q$, then $\deg_m(f) \geq \max \{\deg_p(f), \deg_q(f)\} = \Omega(\log n)$.

Having negated the possibility for the case of prime $m$, it is natural to study the case of composite modulo. The systematic study of this case was initiated by Barrington et al. [3]. Alas, whether $\deg_m(f)$ is polynomially related to $\deg(f)$ is still a widely open problem. Though the answer for the case $m$ being prime power is proved to be a NO in Gopalan’s thesis [9], we are unable to find better separation between $\deg_m(f)$ and $\deg(f)$, for $m = pq$ with $p$ and $q$ being two distinct primes, than the quadratic one given by Li and Sun [18]. This leads to the following conjecture:

**Conjecture 1.** Let $f$ be a Boolean function. If $m$ has at least two distinct prime factors, then, $\deg(f) = O(\text{poly}(\deg_m(f))).$

Towards this conjecture, the first step is to deal with symmetric Boolean functions. Lee et al. [17] proves that $2\deg_p(f)\deg_q(f) > n$ for any distinct primes $p, q$ and non-trivial symmetric Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, implying the correctness of Conjecture 1 in symmetric cases. Li and Sun [18] improved their bound to $p\deg_p(f) + q\deg_q(f) > n$, which implies $\deg_{pq}(f) > \frac{n}{p+q}$. This is far from being tight; actually, as we will present later, $p$ and $q$ can be eliminated from the denominator.

On the tight lower bound of $\deg(f)$, Nisan and Szegedy [24] give the bound $\deg(f) \geq \log_2 n - O(\log \log n)$ as long as $f$ is non-degenerated. Note that this bound is tight up to the $O(\log \log n)$ term by the address function on $n = k + 2^k$ input bits. Gathen and Roche [32] show that $\deg(f) \geq \deg_{p(n)}(f) \geq p(n) - 1$ for any non-trivial symmetric Boolean function, where $p(n)$ is the largest prime below $n + 2$. (Notice that for symmetric functions, module degree can give a lower bound of degree.) Using currently best result on prime gaps [2], this gives an $n - O(n^{0.525})$ lower bound. On the other side, Gathen and Roche give a polynomial family with $\deg(f) = n - 3$, and they propose Conjecture 2 below with a probabilistic heuristic argument:

**Conjecture 2.** For any non-trivial symmetric Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $\deg(f) \geq n - O(1)$.

**Our Results.** In this paper, we extend many previous works by giving better lower bounds for $\deg_m(f)$. To be concrete, we focus on general Boolean functions over $\mathbb{Z}_{p^k}$, and symmetric Boolean functions over $\mathbb{Z}_m$ where $m$ has at least two distinct prime factors. As we have already mentioned it, the gap between $\deg(f)$ and $\deg_{p^k}(f)$ can be arbitrarily large. Nevertheless, we claim that $\deg_{p^k}(f)$ cannot be too small either. This begins with symmetric functions:
Theorem 1. For any prime $p$, positive integer $k$, and non-trivial symmetric function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ with $n \geq (k-1)\varphi(p^\mu) + p^\mu - 1 = O(p^2 k^2)$ where $\mu = \lceil \log_p ((p-1)k-1) \rceil$, $\deg_{pk}(f) \geq (p-1) \cdot k$. The lower bound is tight.

In addition, Theorem 1 can be extended to general non-degenerated Boolean functions. We achieve this using an embedding technique from hypergraph Ramsey theory.

Theorem 2. For any prime $p$, positive integer $k$, and non-degenerated function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ with sufficient large $n$, $\deg_{pk}(f) \geq (p-1) \cdot k$. The lower bound is tight.

For any non-prime-power composite $m$, the following lower bound on modulo-$m$ degree of symmetric functions can be obtained:

Theorem 3. For any composite number $m$ with at least two different prime factors $p, q$ and any non-trivial symmetric Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, $\deg_m(f) \geq \frac{1}{2 + \frac{1}{p-1} + \frac{1}{q-1}} \cdot n$.

Note that this bound approaches $n/2$ when $p$ and $q$ are also growing with $n$. It improves the $n/(p + q)$ bound in [18]. On the other hand, the next theorem shows that the lower bound in Theorem 3 cannot be larger than $(\frac{1}{2} + o(1))n$:

Theorem 4. For any two different prime numbers $p$ and $q$, there exists symmetric $f : \{0, 1\}^n \rightarrow \{0, 1\}$ with arbitrarily large $n$, such that $\deg_{pq}(f) \leq \left(\frac{1}{2} + O\left(\frac{\log p \log q}{\log n}\right)\right) n$.

2 Preliminaries

2.1 Boolean Functions and Polynomial Representation

An $n$-bit Boolean function is a mapping from $\{0, 1\}^n$ to $\{0, 1\}$. We say a Boolean function is non-trivial if it is not a constant function. A Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ is non-degenerated, if there does not exist any $j \in [n]$ that satisfies, for all $x \in \{0, 1\}^n$, $f(x[j\leftarrow 0]) = f(x[j\leftarrow 1])$. Here $x[j\leftarrow a]$ means we fix the $j$th bit of $x$ to be $a$.

We say a polynomial $q \in R[x_1, \ldots, x_n]$ represents a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ over ring $R$ if $f(x) = q(x)$ for all $x \in \{0, 1\}^n$. Actually, the representation over $\mathbb{Z}$ is unique, owing to the following fact.

Fact 1. For any Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$, the unique polynomial

$$\sum_{a \in \{0, 1\}^n} f(a) \prod_{i=1}^n ((2a_i - 1)x_i + 1 - a_i) =: \sum_{S \subseteq [n]} \alpha_S \prod_{i \in S} x_i$$

represents $f$ over $\mathbb{Z}$.

Analogously, the representation of $f$ over $\mathbb{Z}_m$ is unique too: $\sum_{S \subseteq [n]} (\alpha_S \mod m) \prod_{i \in S} x_i$ is its representation. These facts allow the degree, as well as the modulo-$m$ degree, to be well-defined.

Definition 1. The degree (resp., modulo-$m$ degree) of a Boolean function $f$, denoted by $\deg(f)$ (resp., $\deg_m(f)$), is the degree of the polynomial representing $f$ over $\mathbb{Z}$ (resp., $\mathbb{Z}_m$).

The following facts are useful for analysis.

Fact 2. For any Boolean function $f$ and integer $m_1, m_2$,
• if \( \gcd(m_1, m_2) = 1 \), then \( \deg_{m_1, m_2}(f) = \max\{\deg_{m_1}(f), \deg_{m_2}(f)\} \)\(^3\)

• if \( m_1 \mid m_2 \), then \( \deg_{m_1}(f) \leq \deg_{m_2}(f) \);

• furthermore, we have \( \deg(f) \geq \deg_{m_1}(f) \).

A Boolean function \( f \) is symmetric if \( f(x) = f(y) \) for any \( x, y \) satisfying \( |x| = |y| \). Here \( |x| \) is the number of \( 1 \)'s in \( x \). A symmetric \( f \) can be written as a Mahler expansion of \( |x| \), i.e.,

\[
f(x) = r(|x|) = \sum_j a_j \binom{|x|}{j}, \quad \text{where} \quad a_j \in R.
\]

Note that on any commutative ring \( R \), if the domain of \( r \) is \( \{0, 1, \ldots, n\} \), then \( (a_j)_{0 \leq j \leq n} \) is uniquely determined. This can be shown by observing that (i) the multilinear representation of \( f \) is unique due to the Möbius inversion presented above and (ii) there is a one-to-one correspondence between the multilinear representation and the univariate representation of a symmetric function.

We call \( r \) the univariate representation of \( f \). To ease the notation, we sometimes still write \( f(x) \) when we refer to \( r(|x|) \) in the rest of the paper. In such case the ambiguity can be eliminated by the range of \( x \) (a binary string or an integer).

**Definition 2** (Based period of symmetric Boolean functions). For a symmetric \( f : \{0, 1\}^n \to \{0, 1\} \) with the univariate representation \( r \), we say \( f \) is \( \ell \)-periodic if for all \( a, b \in \{0, \ldots, n\} \), \( \ell \mid |a - b| \) implies \( r(a) = r(b) \). Define \( \pi_m(f) \), the periodic of \( f \) on base \( m \), as the minimal integer \( \ell \) such that \( \ell \) is a power of \( m \) and \( f \) is \( \ell \)-periodic. (Note that it may be larger than \( n \).)

We give several examples to help reader understand this definition.

• \( \pi_3(\text{AND}_3) = 3 \) and \( \pi_3(\text{AND}_4) = 9 \).

• \( \pi_3(f) = 1 \) where \( f \) is any constant function.

• \( \pi_3(g) = 3 \) where \( g(x) = 1 \) if and only if \( |x| \equiv 0 \pmod{3} \).

### 2.2 MOD and Its Mahler Expansion Representation over \( \mathbb{Z}_{p^k} \)

We look into a class of extended parity functions, weight modular functions, which is an indicator of whether the weight of the input is congruent to \( c \) modulo \( m \).

**Definition 3** (Weight modular functions). For positive integer \( n, m \) and \( c \in \mathbb{Z}_m \), define a weight modular function \( \text{MOD}^{c, m}_n : \{0, 1\}^n \to \{0, 1\} \) as

\[
\text{MOD}^{c, m}_n(x) = \begin{cases} 
1 & \text{if } |x| \equiv c \pmod{m}, \\
0 & \text{otherwise.}
\end{cases}
\]

As a prior work, Wilson researched the univariate representation of \( \text{MOD} \) and showed the following result.

**Theorem 5** (Wilson, [33]). Given prime \( p \), positive integer \( t, k \), let \( d := (k - 1) \cdot \varphi(p^t) + p^t - 1 \).

• For \( p^t \)-periodic symmetric \( f : \{0, 1\}^n \to \{0, 1\} \), \( \deg_{p^d}(f) \leq d \).

\(^3\)It follows from Chinese Remainder Theorem.
• For $p^t$-periodic symmetric $f: \{0,1\}^n \rightarrow \{0,1\}$ with Mahler expansion $\sum_{i \geq 0} \alpha_i \cdot (\frac{|x|}{t})$, $p^j \mid \alpha_{\ell}$ holds for all $\ell \geq j \cdot \varphi(p^t) + p^t$.

• For all $n \geq d$, $\deg_{p^k}(\text{MOD}_{n, p^t}^i) = d$.

For all $a \in \mathbb{Z}_{p^t}$, let $\sum_{i=0}^{d} \alpha_i \cdot (\frac{|x|}{i})$ be the Mahler expansion of $\text{MOD}_{n, p^t}^i(x)$. Obviously, it can also be represented by “shifted” Mahler expansion with coefficients of $\text{MOD}_{n, p^t}^i(x)$ as $\sum_{i=0}^{d} \alpha_i \cdot (|x| - a)$. Thus, we get $\alpha_i^{(a)} = \sum_{i=0}^{d} \alpha_i \cdot (|x| - a)$ by Vandermonde convolution, which implies $\alpha_i^{(a)} = \alpha_i^{(a)}$ for all $a \in \mathbb{Z}_{p^t}$ and leads to the following corollary.

**Corollary 1.** Given prime $p$, positive integer $t, k$, let $d := (k - 1) \cdot \varphi(p^t) + p^t - 1$. For all $n \geq d$ and $a \in \mathbb{Z}_{p^t}$, $\deg_{p^k}(\text{MOD}_{n, p^t}^i) = d$.

Consider a special case over $\mathbb{F}_p$. Assume $n = p^t - 1$ without loss of generality. Let $A_{p^t} \in \mathbb{F}_p^{p^t \times p^t}$ be the Mahler expansion coefficient matrix of MODs satisfying the condition that, for $i \in \mathbb{Z}_{p^t}$ and $x \in \{0,1\}^n$,

$$\text{MOD}_{n, p^t}^i(x) = \sum_{j=0}^{p^t - 1} (A_{p^t})_{j,i} \left(\frac{|x|}{j}\right).$$

Note that such $A_{p^t}$ always exists since $\deg_{p^k}(\text{MOD}_{n, p^t}^i) = p^t - 1$ holds for all $j \in \mathbb{Z}_{p^t}$. It is feasible to set $(A_{p^t})_{i,j} = \binom{p^t - 1 - j}{p^t - 1 - i}$ for all $i, j \in \mathbb{Z}_{p^t}$ since

$$\sum_{j=0}^{p^t - 1} \binom{p^t - 1 - i}{p^t - 1 - j} \left(\frac{|x|}{j}\right) = \begin{cases} p^t - 1 - i + |x| & \text{if } |x| \equiv i \pmod{p^t}, \\ 0 & \text{otherwise}. \end{cases}$$

The selection of $A_{p^t}$ is unique due to the uniqueness of Mahler expansion. According to Lucas’s Theorem, $A_{p^t} = A_{p^{st}}$ since

$$\binom{p^t - 1 - i}{p^t - 1 - j} = \binom{\sum_{\ell=0}^{t-1} (p^t - 1 - j) \cdot p^\ell}{p^t - 1 - i} \equiv \prod_{\ell=0}^{t-1} \left(p^t - 1 - j\right)^{i \cdot p^\ell} \equiv \prod_{\ell=0}^{t-1} (A_{p^t})_{i,j} \pmod{p},$$

where $i = \sum_{\ell=0}^{t-1} i \cdot p^\ell$ and $j = \sum_{\ell=0}^{t-1} j \cdot p^\ell$. As we have already mentioned, for any $p^t$-periodic Boolean function $f$, $A_{p^t}$ is a conversion matrix between $\{\text{MOD}_{n, p^t}^i\}$ and $\{\binom{|x|}{i}\}$, i.e., $\alpha = A_{p^t} \cdot v$ where $\alpha$ is the Mahler expansion coefficient vector of $f$ and $v$ is the univariate representation such that $f(x) = v_{|x| \mod p^t}$ for all $x \in \{0,1\}^n$.

### 3. Lower Bound of $\deg_{p^k}(f)$

By identifying the degree of $\text{MOD}_{n, p^t}^i$ over $\mathbb{Z}_{p^k}$, we show that the degree of all $p^t$-periodic functions is constantly small since they can be spanned by $\{\text{MOD}_{n, p^t}^i\}_{i=0}^{p^t-1}$. In [Section 3.1.](#) we prove that the degree of any $p^t$-periodic (but not $p^t-1$-periodic) function will not decrease too much from $(k - 1) \cdot \varphi(p^t) + p^t - 1$ during the spanning, despite the cancellation of the high-order coefficients. By a Ramsey-type argument in [Section 3.2.](#) we further extend our lower bound to all non-degenerated Boolean function with sufficiently many input bits.
3.1 Symmetric Functions

First, we give a \((k - 1) \cdot p\) lower bound for \(p\)-periodic functions. Note that all \(p\)-periodic functions also have a \((k - 1) \cdot p\) upper bound of \(\deg_{p,k}(f)\), and therefore our lower bound is tight.

**Lemma 1.** For all non-trivial \(p\)-periodic symmetric Boolean function \(f : \{0,1\}^n \rightarrow \{0,1\}\) with \(n \geq (p-1) \cdot k\), \(\deg_{p,k}(f) = (p-1) \cdot k\).

*Proof.* Span \(f\) by \(\{\text{MOD}^{i,p}_n\}_{i=0}^{p-1}\) with \(v\), i.e., \(f = \sum_{i=0}^{p-1} v_i \cdot \text{MOD}^{i,p}_n\). Since \(f\) is non-trivial, \(0 < |v| < n\). The highest-order coefficients \(\alpha_{(p-1)k}^{(i)}\) for all \(i \in \mathbb{Z}_p\) are the same, and moreover, the degree of the sum will not decrease because \(p^k | |v| \cdot \alpha_{(p-1)k}\) according to Theorem 5 \(\square\).

Second, for functions with large \(p\)-period, i.e., \(\pi_p(f) > p\), \(\deg_{p,k}(f) \geq (p-1) \cdot k\) also holds.

**Lemma 2.** For all non-trivial symmetric Boolean function \(f : \{0,1\}^n \rightarrow \{0,1\}\) with \(\pi_p(f) = p^t\), \(t \geq 1\) and \(n \geq (k-1) \cdot \varphi(p^t) + p^t - 1\), \(\deg_{p,k}(f) \geq (k-2) \cdot \varphi(p^t) + p^t\) holds.

*Proof.* Set \(m = \varphi(p^t)\) and \(d = (k - 1) \cdot m + p^t - 1\). Since \(f\) is \(p^t\)-periodic, \(f\) is spanned by \(\{\text{MOD}^{i,p}_n\}_{i=0}^{p^t - 1}\) with coefficient vector \(w\), or spanned by \(\big(\binom{i}{p}\big)_{i=0}^{p^t - 1}\) with coefficient vector \(\alpha\). Let \(\alpha_i^{(j)}\) be the \(i\)-th Mahler expansion coefficient of \(\text{MOD}^{i,p}_n\). According to Theorem 5, \(p^k | \alpha_i^{(j)}\) for all \(i \in \mathbb{Z}_p\) and \(j \in [d - m + 1, d]\). So, we define reduced Mahler expansion coefficient \(\tilde{\alpha}_{d}^{(i)} : = (\alpha_i^{(a)} / p^{k-1}) \mod p\) for all \(i \in [d - m + 1, d]\) and \(a \in \mathbb{Z}_p\). Let \(A \in \mathbb{F}_p^{m \times p^t}\) be the matrix gathering the highest \(m\) reduced coefficients of each \(\text{MOD}\) where \(A_{i,j} = \tilde{\alpha}_{d_i}^{(j)}\) for \(i \in [0, m - 1]\) and \(j \in [p^t]\). Note that

\[
\begin{bmatrix}
\tilde{\alpha}_d^{(m-1)} & \ldots & \tilde{\alpha}_d^{(0)} \\
\vdots & \ddots & \vdots \\
\tilde{\alpha}_d^{(0)} & \ldots & \tilde{\alpha}_d^{(m-1)}
\end{bmatrix}
= \begin{bmatrix}
(1-m) & \ldots & (1-m) \\
\vdots & \ddots & \vdots \\
0 & \ldots & (m-1)
\end{bmatrix}
\cdot
\begin{bmatrix}
\tilde{\alpha}_d^{(0)} & \ldots & \tilde{\alpha}_d^{(0)} \\
\vdots & \ddots & \vdots \\
0 & \ldots & \tilde{\alpha}_d^{(0)}
\end{bmatrix}
\]

is full-rank over \(\mathbb{F}_p\). Consequently, \(A\) is full-rank and the dimension of the null space is \(p^t - 1\). Define \(w^{(0)}, \ldots, w^{(p^t - 1)} \in \{0,1\}^{p^t}\) such that \(\text{MOD}^{i,p}_n^{p^t - 1} = \sum_{j=0}^{p^t - 1} w_j^{(i)} \cdot \text{MOD}^{j,p}_n\). Since \(\deg_{p,k}(\text{MOD}^{i,p}_n^{p^t - 1}) \leq d - m\), \(A \cdot w^{(j)} = \mathbf{0}\) over \(\mathbb{F}_p\) for all \(j \in \mathbb{Z}_p^{p^t - 1}\). So, \(W := \text{span}(w^{(0)}, \ldots, w^{(p^t - 1)})\) is the null space of \(A\). Note that \(f\) is not \(p^t - 1\)-periodic and \(f\) cannot be spanned by \(\{\text{MOD}^{i,p}_n^{p^t - 1}\}_{i=0}^{p^t - 1}\), i.e., \(w \notin W\), which implies \(A \cdot w \neq \mathbf{0}\) and \(\deg_{p,k}(f) \geq (k-2) \cdot \varphi(p^t) + p^t\). \(\square\)

Finally, when the \(p\)-period of \(f\) is so large that \((k - 1) \cdot \varphi(p^t) + p^t - 1\) is larger than \(n\), the fact that \(f\) is not \(p^t - 1\)-periodic implies a lower bound due to the counter-proposition of the following lemma.

**Lemma 3.** Boolean function \(f : \{0,1\}^n \rightarrow \{0,1\}\) is \(p^t\)-periodic if \(\deg_{p,k}(f) \leq p^t - 1\).

*Proof.* Let \(d = p^t - 1\) and \(\sum_{j=0}^{d} \alpha_j^{(x)}\) be the Mahler expansion over \(\mathbb{Z}_p^{k}\). Note that the value is zero or one. So, \(\sum_{j=0}^{d} \alpha_j^{(x)} \mod p^k = \sum_{j=0}^{d} \alpha_j^{(x)} \mod p\) for all \(x \in \{0,1\}^n\). Meanwhile, for any \(a, b \in \mathbb{N}\) where \(a \equiv b \pmod {p^t}\), \((a) \equiv (b) \pmod {p^t}\) for all \(j \leq p^t - 1\) due to Lucas’s Theorem, which means \(f\) is \(p^t\)-periodic. \(\square\)

We are ready to prove Theorem 1.
Proof of [Theorem 1]. Assume towards contradiction there exists \( f : \{0,1\}^n \to \{0,1\} \) such that \( \text{deg}_{p^k}(f) < (p-1) \cdot k \). According to Lemma 3, \( f \) is \( p^{t'} \)-periodic where \( t' = \lceil \log_p((p-1)k-1) \rceil \). Being non-trivial, \( f \) is not \( p^0 \)-periodic. Thus, there exists \( t \in [t'] \) such that \( f \) is \( p^t \)-periodic but not \( p^{t-1} \)-periodic. If \( t \geq 2 \), \( \text{deg}_{p^k}(f) \geq (k-2) \cdot \varphi(p^t) + p^t \geq (p-1) \cdot k \) due to Lemma 2. Otherwise, \( t = 1 \) and \( \text{deg}_{p^k}(f) \geq (p-1) \cdot k \) due to Lemma 1.

3.2 Non-Degenerated Functions

With the help of Ramsey theory on hypergraphs, the bound for symmetric functions can be applied to a wider class of Boolean functions — the non-degenerated functions.

Theorem 6 (Erdős and Rado, [7]).

\[
\text{r}_k(s, t) \leq 2^\left( r_{k-1}(s-1, t-1) \right),
\]

where \( \text{r}_k(\cdot, \cdot) \) is Ramsey number on \( k \)-uniform hypergraphs.

The theorem indicates the following property: any 2-edge-colored \( k \)-uniform hypergraph on \( n \) vertices has a monochromatic clique of size \( \Omega(\log^k(n)) \) where all hyperedges within have the same color. This property allows us to embed an \( \omega(1) \)-size symmetric function into any non-degenerated function \( f : \{0,1\}^n \to \{0,1\} \), provided \( n \) sufficiently large. Before continuing, we need to introduce the sensitivity of a Boolean function.

Definition 4. Given a Boolean function \( f : \{0,1\}^n \to \{0,1\} \) and an input \( x \), we say a bit \( i \) is sensitive if \( f(x) \neq f(x \oplus i) \). Here \( x \oplus i \) is the string which differs from \( x \) on the \( i \)th bit. The sensitivity of \( f \) on input \( x \) is \( s(f, x) := |\{ i : i \in [n], f(x) \neq f(x \oplus i) \}| \). The sensitivity of \( f \) is then defined as \( s(f) := \max_x s(f, x) \).

Simon [30] proved that for any non-degenerated function \( f : \{0,1\}^n \to \{0,1\} \), \( s(f) = \Omega(\log n) \). In addition, we also find the following notation useful.

Definition 5. Given positive integer \( n \), \( x \in \{0,1\}^n \) and \( S \subseteq [n] \) where \( x_i = 1 \) for all \( i \in S \), define

\[
\text{DOWN}(S, x, k) := \{ x \oplus T | T \subseteq S, |T| = k \}.
\]

Here, \( x \oplus T \) is the string which only differs from \( x \) on all the \( i \)th \((i \in T)\) bits.

Lemma 4. For any non-degenerated function \( f : \{0,1\}^n \to \{0,1\} \) with sufficient large \( n \), there exists \( S \subseteq [n], |S| = \omega(1) \) and \( \sigma : [n] \setminus S \to \{0,1\} \) such that \( f|_\sigma \) is a non-trivial symmetric function.

Proof. Pick \( \tilde{x} \in \{0,1\}^n \) such that \( s(f, \tilde{x}) = \Omega(\log n) \). Define \( S_0 := \{ i \in [n] | f(\tilde{x}) \neq f(\tilde{x}_{i \leftarrow 1}) \} \). W.l.o.g, assume \( |S_0| = \Omega(\log n) \). Define \( S_t \) recursively as the maximum set such that \( S_t \subseteq S_{t-1} \) and satisfies all \( y \in \text{DOWN}(S_t, \tilde{x}, t) \) has the same \( f(y) \) value. Next, we show the size of \( S_t \) cannot be too small.

Claim 1. \( |S_t| = \Omega(\log^{\omega(t-1)}(|S_{t-1}|)) \).

\[4\log^k(n) := \log \cdot \log \cdot \log \cdots \log n . \log^*(n) := \min \{ k : \log^k(n) \leq 1 \} \]
Note that the inputs in $\text{DOWN}(S_t, \bar{x}, t)$ have the same $f$ value, since it corresponds to a monochromatic clique.

By applying Claim 1 inductively, $|S_t| = \Omega \left( \log^\omega(t-1)(|S_{t-1}|) \right)$. For any $n \geq 4$, let $t' = t'(n) = \lfloor \log^* (n) - 2 \rfloor$. Therefore, $t'$ satisfies $(t' - 1)t'/2 + 1 < \log^* (n)$, and thus $|S_{t'}| = \omega(1)$. Furthermore, $r(n) := \min \left\{ \log^\omega(t'-1)/2+1(n), t'(n) \right\} = \omega(1)$.

Pick arbitrary $r(n)$-size subset $T$ of $S_{r(n)}$. We fix the function on the input $\bar{x}$ for all bits in $[n] \setminus T$, i.e., let $g := f\big|_{[n] \setminus T \leftarrow \bar{x}}$ as an $r(n)$-variable Boolean function. Recall the definition of $S_0, \ldots, S_{r(n)}$. For any $x, y \in \{0, 1\}^{r(n)}$ where $|x| = |y|$, let $x' = x|_{[n] \setminus T \leftarrow \bar{x}}$ and $y' = y|_{[n] \setminus T \leftarrow \bar{x}}$.

Note that $x', y' \in \text{DOWN}(S_{r(n)}, \bar{x}, |x|) \subseteq \text{DOWN}(S_{[x]} \bar{x}, |x|)$.

Thus, $g(x) = f(x') = f(y') = g(y)$, namely, $g$ is symmetric. Let $z = 0$ and $w$ be any input with weight 1. Then denote $z' = z|_{[n] \setminus T \leftarrow \bar{x}}$ and $w' = w|_{[n] \setminus T \leftarrow \bar{x}}$.

If $i \in T \subseteq S_0$ is a sensitive bit then $z' = \bar{x}$ and $w' = x \oplus e_i$. Hence, $g$ is non-trivial because $g(z) = f(z') \neq f(w') = g(w)$.

Consequently, an $r(n)$-size symmetric function can be embedded into any non-degenerated function. It immediately leads to that, for any non-degenerated function $f : \{0, 1\}^n \to \{0, 1\}$ with $n \geq r^{-1}((k-1) \cdot \varphi(p^k) + p^k - 1)$ where $\mu$ is defined in Theorem 1, $\deg_{pq}(f) \geq (p - 1)k$.

4 Lower Bounds of $\deg_{pq}(f)$ for Symmetric Functions

4.1 Proof of Theorem 3

Suppose $m$ contains at least two different prime factors $p$ and $q$. To prove Theorem 3, the simple fact that $\deg_{pq}(f) = \max\{\deg_p(f), \deg_q(f)\}$ will become crucial. To be concrete, $\deg_p(f)$ and $\deg_q(f)$ cannot be small simultaneously, due to the following two lemmas.

Lemma 5 (Periodicity Lemma, [8]). Let $g$ be an $a$-periodic and $b$-periodic function on domain $\{0, 1, \ldots, n\}$ with $\gcd(a, b) = 1$ and $n \geq a + b - 2$. Then $g$ is a constant function.

Lemma 6. Let $p$ be a prime. For any non-trivial symmetric $f : \{0, 1\}^n \to \{0, 1\}$, $\deg_p(f) \geq \min\{n/2, (1 - 1/p)\pi_p(f)\}$. 
For any non-trivial symmetric Boolean function $f : \{0, 1\}^n \to \{0, 1\}$ and two different primes $p$ and $q$, if $\max\{\deg_p(f), \deg_q(f)\} \geq \frac{n}{2}$, then the theorem is self-evident; otherwise, by Lemma 6, we have

$$\deg_{pq}(f) = \max\{\deg_q(f), \deg_q(f)\} \geq \max \left\{ \left( 1 - \frac{1}{p} \right) \pi_p(f), \left( 1 - \frac{1}{q} \right) \pi_q(f) \right\}.$$  

On the other hand, since $f$ is not a constant function, by Lemma 5, we have $\pi_p(f) + \pi_q(f) > n + 2$. Combining the results above we get $\deg_{p}(f) \geq \deg_{pq}(f) \geq \frac{1}{2 + \frac{1}{p - 1} + \frac{1}{q - 1}} \cdot n$.

The only thing left here is why Lemma 6 holds. Before continuing, we need the following two lemmas.

**Lemma 7.** For any prime $p$, integers $j, k$ with $j + k < p$ and distinct $a_0, \ldots, a_k \in \mathbb{F}_p$ satisfying $a_0, \ldots, a_k \geq j$, the following matrix is non-singular over $\mathbb{F}_p$,

$$
\begin{bmatrix}
\binom{a_0}{j} & \binom{a_1}{j+1} & \cdots & \binom{a_k}{j+k} \\
\binom{a_0}{j+1} & \binom{a_1}{j+2} & \cdots & \binom{a_k}{j+k+1} \\
\vdots & \vdots & \ddots & \vdots \\
\binom{a_0}{j+k} & \binom{a_1}{j+k+1} & \cdots & \binom{a_k}{j+2k} \\
\end{bmatrix}.
$$

Proof. It is easy to see that

$$\text{diag} \left( \binom{j+0)0}{j}, \ldots, \binom{j+k)k}{j} \right) \cdot S \cdot \begin{bmatrix}
\binom{a_0}{j} & \cdots & \binom{a_k}{j+k} \\
\vdots & \ddots & \vdots \\
\binom{a_0}{j+k} & \cdots & \binom{a_k}{j+k} \\
\end{bmatrix} = \begin{bmatrix}
(a_0 - j)^0 & \cdots & (a_k - j)^0 \\
\vdots & \ddots & \vdots \\
(a_0 - j)^k & \cdots & (a_k - j)^k \\
\end{bmatrix},$$

where $S$ is the second Stirling number matrix, i.e., $S_{ij} = \text{Stirling}_2(i, j)$, and the notation $x^k$ stands for $x(x-1) \cdots (x-y+1)$. The Vandermonde matrix on the RHS is also non-singular since $a_0, \ldots, a_k$ are distinct. \[\square\]

**Lemma 8.** For all prime $p$, positive integer $n < p - 1$ and $v \in \{0, 1\}^p$, there exists $\ell \in [\lceil n/2 \rceil + 1, n]$ such that $(A_p \cdot v)_\ell \neq 0$ if there are $i, j \leq n$ satisfying $v_i \neq v_j$.

Proof. Assume that there exists $v \in \{0, 1\}^p$ where the first $n + 1$ entries are not all-zero or all-one, such that $(A_p \cdot v)_\ell = 0$ for all $\ell \in [\lceil n/2 \rceil + 1, n]$, i.e., the following equality holds,

$$B \cdot \bar{v} = 0,
B = \begin{bmatrix}
(A_p)_{n/2}+1,0 & (A_p)_{n/2}+1,1 & \cdots & (A_p)_{n/2}+1,n \\
\vdots & \ddots & \vdots & \vdots \\
(A_p)_{n,0} & (A_p)_{n,1} & \cdots & (A_p)_{n,n} \\
\end{bmatrix},$$

where $\bar{v} := (v_0, \ldots, v_n)^T$. Recall that $(A_p)_{i,j} = \binom{p-1-j}{p-1-i}$. According to Lemma 7, any submatrix of $B$ is non-singular. Since $B \cdot 1 = 0$, we assume the number of 1s in $\bar{v}$ is no more than $\lceil (n + 1)/2 \rceil$ without loss of generality. This means there are at most $n - \lfloor n/2 \rfloor$ columns of $B$ with the summation of zero, which is a contradiction. \[\square\]

The lemma implies a lower bound of $\deg_p(f)$ for the following special case.

**Corollary 2.** For all non-trivial symmetric $f : \{0, 1\}^n \to \{0, 1\}$, $\deg_p(f) \geq \lceil n/2 \rceil + 1$ if $n < p - 1$.  


Now we prove Lemma 6. Let $\pi_p(f) = p^j$. Let $v \in \{0, 1\}^{p^j}$, $\alpha \in \mathbb{F}_p^{p^j}$ be the coefficient vectors over bases $\{\text{MOD}_n^i \cdot p^j(x)\}_{i=0}^{p^j-1}$ and $\{\langle x \rangle \}_{i=0}^{p^j-1}$ respectively with a conversion matrix $A_{p^j}$ satisfying $\alpha = A_{p^j} \cdot v$. Divide $v$ and $\alpha$ into $p^{j-1}$-length blocks as $v = (v(0), \ldots, v(p^{j-1}))^\top$ and $\alpha = (\alpha(0), \ldots, \alpha(p^{j-1}))^\top$ where $v(i) \in \{0, 1\}^{p^{j-1}}$, $\alpha(i) \in \mathbb{F}_p^{p^{j-1}}$. Thus, for all $i \in \mathbb{F}_p$, we have

$$\alpha(i) = A_{p^{j-1}} \sum_{j=0}^{p-1} (A_{p^j})_{ij} \cdot v(i).$$

If $\pi_p(f) < n$ holds, assume $\alpha(p^{j-1}) = 0$. Since $A_{p^{j-1}}$ is full-rank and $(A_{p^{j}})_{p^{j-1}, j} = 1$ for all $j$, $\sum_{j=0}^{p^{j-1}} v(j) = 0$ should hold, which implies $v(0) = \ldots = v(p^{j-1})$. Thus, $f$ is $p^{j-1}$-periodic, which contradicts $\pi_p(f) = p^j$. So, $\alpha(p^{j-1}) \neq 0$ and $\deg_p(f) \geq \frac{p^{j-1} - 1}{p} \cdot \pi_p(f)$.

If $\pi_p(f) \geq n$, we extend $f$ into a mapping $\tilde{f} : \{0, 1\}^{p^{j-1}} \rightarrow \{0, 1\}$:

$$\tilde{f}(x) = \begin{cases} f(x) & \text{if } |x| \leq n, \\ 0 & \text{otherwise}, \end{cases}$$

and vectors $v, \alpha$ are constructed for $\tilde{f}$. It easy to see that $\deg_p(f) = \deg_p(\tilde{f}) = \max \{i \in [0, n] \mid \alpha_i \neq 0\}$. Perform the conversion as following:

$$(A_{p^{j-1}})^{-1} \otimes I_p \cdot A_{p^{j-1}} \otimes A_p \cdot v = (A_{p^{j-1}})^{-1} \otimes I_p \cdot \alpha, \quad \text{and} \quad I_p \otimes A_{p^{j}}^\top \cdot v = \begin{bmatrix} (A_{p^{j-1}})^{-1} \cdot \alpha(0) \\ \vdots \\ (A_{p^{j-1}})^{-1} \cdot \alpha(p^{j-1}) \end{bmatrix}.$$}

Furthermore, for all $j \in \mathbb{Z}^{p^{j-1}}$, $\ell \in \mathbb{F}_p$, define $\beta(\ell) := (A_{p^{j-1}})^{-1} \cdot \alpha(\ell)$,

$$\tilde{\beta}(j) := \begin{bmatrix} ((A_{p^{j-1}})^{-1} \cdot \alpha(0))_j \\ \vdots \\ ((A_{p^{j-1}})^{-1} \cdot \alpha(p^{j-1}))_j \end{bmatrix} \quad \text{and} \quad \tilde{v}(j) := \begin{bmatrix} v(j(0)) \\ \vdots \\ v(j(p^{j-1})) \end{bmatrix}.$$}

Then, $A_p \cdot \tilde{v}(j) = \tilde{\beta}(j)$ holds for all $j \in \mathbb{Z}^{p^{j-1}}$. Recall $\pi_p(f) = p^j$. Let $n' = [(n + 1)/p^{j-1}] - 1$, $n'' = [(n + 1)/p^{j-1}] - 1$ and $m' = n \mod p^{j-1}$. Consider the following two cases:

**Case I.** In the first case, there exists $\ell \leq m'$ and $i, j \in [0, n'']$ such that $\tilde{v}(i) \neq \tilde{v}(j)$. Note the first $n'' + 1$ entries of $\tilde{v}(\ell)$ are not all-zero or all-one in this case. According to Lemma 8, there exists $i' \in [(n''/2) + 1, n'']$ such that $\tilde{\beta}(i') = \tilde{\beta}(i') \neq 0$. Then $\alpha(\ell) = A_{p^j} \cdot \beta(i')$.

- If $i' < n'$, $\beta(i') \neq 0$ implies $\deg_p(f) \geq (\lfloor n''/2 \rfloor + 1) \cdot p^{j-1} \geq n'/2$.
- If $i' = n'$, assume $\ell$ is minimal such that $\beta(i') \neq 0$ without loss of the generality. Thus,

$$\alpha(i') = \sum_{j=0}^{\ell} (A_{p^{j-1}})_{\ell,j} \beta_j(i') = (A_{p^{j-1}})_{\ell,i} \beta(i') \neq 0,$$

which implies $\deg_p(f) \geq n' \cdot p^{j-1} \geq n'/2$ since $\ell \leq m'$. 

10
Case II. Otherwise, there exists $\ell \in [m' + 1, p^{t-1} - 1]$ and $i, j \in [0, n']$ such that $\tilde{v}_i^{(\ell)} \neq \tilde{v}_j^{(\ell)}$. Assume $\ell$ is the minimal one. Due to the same argument, there exists $\ell' \in [\lceil n'/2 \rceil + 1, n']$ such that $\beta_{\ell'}^{(v)} \neq 0$. Besides, for all $\ell' < \ell$, $\tilde{v}_0^{(\ell')} = \ldots = \tilde{v}_{n'}^{(\ell')}$ implies that

$$\beta_{\ell'}^{(v)} = \tilde{\beta}_{\ell'}^{(v)} = \sum_{j=0}^{p-1} (A_p)_{\ell',j} \tilde{v}_j^{(\ell')} = v_0^{(\ell')} \cdot \sum_{j=0}^{\ell'} (A_p)_{\ell',j} = 0.$$  

Recall that $\alpha^{(v)} = A_p \cdot \beta^{(v)}$. Thus, in the same way, it can be shown that $\alpha_{\ell'}^{(v)} \neq 0$, which implies $\deg_p(f) \geq \lceil n'/2 \rceil \cdot p^{t-1} + m' + 1 \geq n/2$.

4.2 Proof of Theorem 4

In this subsection, we prove Theorem 4, showing that it is impossible to improve the constant coefficient in Theorem 3 to be greater than 1/2.

Lemma 9. For two different prime numbers $p, q$, there exist integers $u$ and $v$, which can be both arbitrarily large, such that

$$\frac{p^v}{q^u} = 1 \pm O\left(\frac{\log q}{v}\right) = 1 \pm O\left(\frac{\log p}{u}\right).$$

Proof. Let $\alpha = \frac{\log p}{\log q}$. Note that $\alpha$ is irrational because otherwise we will have $p^s = q^t$ for some integers $s$ and $t$, which is impossible. By writing $\alpha$ as a continued fraction, we obtain infinite integer pairs $(u, v)$ such that $|\alpha - \frac{u}{v}| \leq \frac{1}{v^2}$, which implies $|v \log p - u \log q| \leq \frac{\log q}{v}$ and thus $\frac{p^v}{q^u} = 1 \pm O\left(\frac{\log q}{v}\right)$. \hfill \square

Now we prove Theorem 4

Proof of Theorem 4. For each pair $(u, v)$ in Lemma 9 we construct a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. W.l.o.g., assume $p^v > q^u$ (otherwise we swap $p$ and $q$ below). Let $n = 2q^u - 3$ and define $f$ as follows: $f(x) = 1$ if and only if $|x| = q^u - 1$. $f$ is a non-trivial symmetric function and clearly it is both $p^v$-periodic and $q^u$-periodic. By Theorem 5 we get that $\deg_p(f) \leq p^v - 1$ and $\deg_q(f) \leq q^u - 1$. Thus $\deg_{pq}(f) = \max\{\deg_p(f), \deg_q(f)\} \leq p^v - 1$. Finally,

$$\frac{\deg_{pq}(f)}{n} \leq \frac{p^v - 1}{2q^u - 3} \leq \frac{1}{2} + O\left(\frac{\log p}{u}\right) = \frac{1}{2} + O\left(\frac{\log p \log q}{\log n}\right).$$

\hfill \square

5 Conclusion

In this paper, we discuss the modulo degree of Boolean functions, especially for symmetric functions. We give a complete characterization of the modulo degree when the modulo number is a prime or prime power. When the modulo base is a composite number with at least two different prime factors, we give a nearly tight lower bound for symmetric functions. We believe that our work and technique may give a better characterization of polynomial representation of Boolean functions.

Nonetheless, there is space for further discussion. First, we conjecture that the constant coefficient in Theorem 3 can be improved to 1/2, which would be tight due to Theorem 4. Aside from this, both Conjecture 1 and Conjecture 2 still remain open.

See also Theorem 5 in https://en.wikipedia.org/wiki/Continued_fraction
Acknowledgements

We want to thank Noga Alon for pointing us to [1], and Xiaoxu Guo for pointing us to [8].

References

[1] Noga Alon and Richard Beigel. Lower bounds for approximations by low degree polynomials over $\mathbb{Z}_m$. In Proceedings 16th Annual IEEE Conference on Computational Complexity, pages 184–187. IEEE, 2001.

[2] Roger C Baker, Glyn Harman, and János Pintz. The difference between consecutive primes, ii. Proceedings of the London Mathematical Society, 83(3):532–562, 2001.

[3] David A. Mix Barrington, Richard Beigel, and Steven Rudich. Representing boolean functions as polynomials modulo composite numbers. Computational Complexity, 4:367–382, 1994. URL: https://doi.org/10.1007/BF01263424, doi:10.1007/BF01263424.

[4] Harry Buhrman and Ronald de Wolf. Communication complexity lower bounds by polynomials. In Proceedings 16th Annual IEEE Conference on Computational Complexity, pages 120–130. IEEE, 2001.

[5] Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. Theor. Comput. Sci., 288(1):21–43, 2002. URL: https://doi.org/10.1016/S0304-3975(01)00144-X, doi:10.1016/S0304-3975(01)00144-X.

[6] Klim Efremenko. 3-query locally decodable codes of subexponential length. SIAM Journal on Computing, 41(6):1694–1703, 2012.

[7] P. Erdős and R. Rado. Combinatorial theorems on classifications of subsets of a given set. Proceedings of the London Mathematical Society, s3-2(1):417–439, 1952.

[8] Nathan J Fine and Herbert S Wilf. Uniqueness theorems for periodic functions. Proceedings of the American Mathematical Society, 16(1):109–114, 1965.

[9] Parikshit Gopalan. Computing with polynomials over composites. PhD thesis, Georgia Institute of Technology, 2006.

[10] Parikshit Gopalan. Constructing ramsey graphs from boolean function representations. In 21st Annual IEEE Conference on Computational Complexity (CCC’06), pages 14–pp. IEEE, 2006.

[11] Parikshit Gopalan, Shachar Lovett, and Amir Shpilka. On the complexity of boolean functions in different characteristics. Conference on Computational Complexity, 19(2):173–183, 2009.

[12] Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit ramsey graphs. Combinatorica, 20(1):71–86, 2000.

[13] Vince Grolmusz. Constructing set systems with prescribed intersection sizes. Journal of Algorithms, 44(2):321–337, 2002.

[14] Daniel J Katz. $p$-adic valuation of weights in abelian codes over $\mathbb{Z}_{p^d}$. IEEE transactions on information theory, 51(1):281–305, 2005.
[15] Adam R Klivans and Rocco A Servedio. Learning DNF in time $2^{\tilde{O}(n^{1/3})}$. \textit{Journal of Computer and System Sciences}, 68(2):303–318, 2004.

[16] Eyal Kushilevitz and Yishay Mansour. Learning decision trees using the fourier spectrum. \textit{SIAM Journal on Computing}, 22(6):1331–1348, 1993.

[17] Chia Jung Lee, Satyanarayana V. Lokam, Shi Chun Tsai, and Ming Chuan Yang. Restrictions of nondegenerate boolean functions and degree lower bounds over different rings. In \textit{IEEE International Symposium on Information Theory}, 2015.

[18] Qian Li and Xiaoming Sun. On the modulo degree complexity of boolean functions. In \textit{Computing and Combinatorics: 23rd International Conference, COCOON 2017, Hong Kong, China, August 3-5, 2017, Proceedings}, volume 10392, page 384. Springer, 2017.

[19] Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, fourier transform, and learnability. In \textit{30th Annual Symposium on Foundations of Computer Science}, pages 574–579. IEEE, 1989.

[20] Xiaoyu Liu. An equivalence of wards bound and its application. \textit{Designs, Codes and Cryptography}, 58(1):1–9, 2011.

[21] Marvin Minsky and Seymour Papert. An introduction to computational geometry. \textit{Cambridge tiass., HIT}, 1969.

[22] Ashley Montanaro and Tobias Osborne. On the communication complexity of xor functions. \textit{arXiv preprint arXiv:0909.3392}, 2009.

[23] Elchanan Mossel, Ryan O’Donnell, and Rocco P Servedio. Learning juntas. In \textit{Proceedings of the thirty-fifth annual ACM symposium on Theory of computing}, pages 206–212. ACM, 2003.

[24] Noam Nisan and Mario Szegedy. On the degree of boolean functions as real polynomials. \textit{Computational Complexity}, 4:301–313, 1994. URL: \url{https://doi.org/10.1007/BF01263419}, \url{doi:10.1007/BF01263419}.

[25] Alexander A Razborov. Lower bounds for the size of circuits of bounded depth with basis \{$\wedge, \oplus$\}. \textit{Math. notes of the Academy of Sciences of the USSR}, 41(4):333–338, 1987.

[26] Alexander A Razborov. Quantum communication complexity of symmetric predicates. \textit{Izvestiya: Mathematics}, 67(1):145, 2003.

[27] Alexander A Sherstov. Communication lower bounds using dual polynomials. \textit{arXiv preprint arXiv:0805.2135}, 2008.

[28] Alexander A Sherstov. Strong direct product theorems for quantum communication and query complexity. \textit{SIAM Journal on Computing}, 41(5):1122–1165, 2012.

[29] Yaoyun Shi and Yufan Zhu. Quantum communication complexity of block-composed functions. \textit{arXiv preprint arXiv:0710.0095}, 2007.

[30] Hans-Ulrich Simon. A tight $\Omega(\log \log n)$-bound on the time for parallel Ram’s to compute non-degenerated boolean functions. In \textit{International Conference on Fundamentals of Computation Theory}, pages 439–444. Springer, 1983.
[31] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In Proceedings of the nineteenth annual ACM symposium on Theory of computing, pages 77–82. ACM, 1987.

[32] Joachim von Zur Gathen and James R Roche. Polynomials with two values. Combinatorica, 17(3):345–362, 1997.

[33] Richard M. Wilson. A lemma on polynomials modulo $p^m$ and applications to coding theory. Discrete Mathematics, 306(23):3154–3165, 2006. URL: https://doi.org/10.1016/j.disc.2004.10.030, doi:10.1016/j.disc.2004.10.030

[34] Bahattin Yildiz. Weights modulo $p^e$ of linear codes over rings. Designs, Codes and Cryptography, 43(2-3):147–165, 2007.