JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 34, 193-203 (2017)
DOI: 10.6688/JISE.2018.34.1.12

Representing Symmetric Boolean Functions with Polynomial over Composite Moduli*

SHI-CHUN TSAI AND MING-CHUAN YANG
Department of Computer Science
National Chiao Tung University
Hsinchu, 300 Taiwan
E-mail: sctsai@cs.nctu.edu.tw; mingchuan.cs96g@g2.nctu.edu.tw

Polynomial degree is an important measure for studying the computational complexity of Boolean function. A polynomial $P \in \mathbf{Z}_m[\boldsymbol{x}]$ is a *generalized representation* of f over $\mathbf{Z}_m$ if $\forall \boldsymbol{x}, \boldsymbol{y} \in \{0, 1\}^n$; $f(\boldsymbol{x}) \neq f(\boldsymbol{y}) \Rightarrow P(\boldsymbol{x}) \not\equiv P(\boldsymbol{y}) \pmod m$. Denote the minimum degree as $\deg_m^{ge}(f)$, and $\deg_m^{sym,ge}(f)$ if the minimum is taken from symmetric polynomials. In this paper we prove new lower bounds for the symmetric Boolean functions that depend on n variables. First, let m_1 and m_2 be relatively prime numbers and have s and t distinct prime factors respectively. Then we have

$$m_1 m_2 (\deg_{m_1}^{sym,ge}(f))^s (\deg_{m_2}^{sym,ge}(f))^t > n.$$

A polynomial $Q \in \mathbf{Z}_m[\boldsymbol{x}]$ is a *one-sided representation* of f over $\mathbf{Z}_m$ if $\forall \boldsymbol{x} \in \{0, 1\}^n$; $f(\boldsymbol{x})=0 \Leftrightarrow Q(\boldsymbol{x}) \equiv 0 \pmod m$. Denote the minimum degree among these Q as $\deg_m^{os}(f)$. Note that $Q(\boldsymbol{x})$ can be non-symmetric. Then with the same conditions as above, at least one of

$$m_1 m_2 (\deg_{m_1}^{sym,ge}(f))^s (\deg_{m_2}^{sym,ge}(f))^t > n$$

and

$$m_1 m_2 (\deg_{m_1}^{sym,ge}(f))^s (\deg_{m_2}^{sym,ge}(\neg f))^t > n$$

is true.

Keywords: degree lower bound, polynomial method, Boolean function complexity, $ACC^0[m]$ circuits, modulo degree complexity, multivariate polynomial, Möbius inversion, binomial coefficient

1. INTRODUCTION

Proving circuit lower bounds is a notoriously difficult task in theoretical computer science. Many computational open problems hinge on resolving this barrier [3]. The polynomial method [5] is one of the few known approaches to proving strong circuit lower bounds, where the polynomial degree lower bounds are used to derive the circuit sizes [17, 19]. By correlating a circuit with a low-degree or sparse polynomial, there are surprising applications of the polynomial method to the algorithm design [1, 22, 23]. Polynomial degrees also have tight connections with a long list of research problems, such as the quantum query complexity [2], the decision tree complexity [3, 15], the communication complexity [6, 8, 14], the pseudorandomness [7], and an explicit construction of Ramsey graph [12]. For instance, an exact quantum algorithm computing a Boolean function f needs at least $\deg(f)/2$ queries [2], where $\deg(f)$ is the degree of the

Received January 26, 2015; revised September 10, 2015; accepted September 11, 2015.
Communicated by Hee Kap Ahn.

multi-linear polynomial that exactly represents f. These connections motivate researchers to investigate the degree lower bounds under different polynomial representation models. The surveys of Beigel [5], Chattopadhyay [9] and Williams [22] respectively show classical works, challenges of representations over rings, and applications to the algorithm design. Despite of many efforts there are some unsolved fundamental problems in the non-exact representations. In fact, it is not clear how to obtain a tight degree bound of the OR function in the generalized representation model [4, 9, 13, 14]. This study is an attempt to gain more understanding for non-specific symmetric functions in the generalized and one-sided representation models over rings.

All Boolean circuits and functions can be represented as polynomials. The circuit class AC^0 consists of constant depth, unbounded fan-in and polynomial size (in terms of the number of input variables) circuits with AND, OR, NOT gates. AC^0 is a circuit class just like AC^0 but also with modular gates MOD_m, where a Boolean MOD_m gate outputs 1 if and only if the number of 1's in its input is not a multiple of the positive integer m. In particular, AC^0 functions can be modeled as polynomials over the field of real numbers $\mathbf{R}$, and $ACC^0[m]$ functions can be modeled as polynomials modulo m.

Definition 1: Let f: $\{0, 1\}^n \to \{0, 1\}$ be a Boolean function and $\mathbf{Z}_m$ be the ring over $\{0, \ldots, m-1\}$.

1. A polynomial $P \in \mathbf{R}[\boldsymbol{x}]$ is the *exact representation* of f over $\mathbf{R}$ if $\forall \boldsymbol{x} \in \{0, 1\}^n$, $f(\boldsymbol{x})=P(\mathbf{x})$. Denote the degree of P as $\deg_{\boldsymbol{R}}^{ex}(f)$.
2. A polynomial $P \in \mathbf{Z}_m[\boldsymbol{x}]$ is the *exact representation* of f over $\mathbf{Z}_m$ if $\forall \boldsymbol{x} \in \{0, 1\}^n$, $f(\boldsymbol{x})=P(\mathbf{x})$. Denote the degree of P as $\deg_m^{ge}(f)$.
3. A polynomial $P \in \mathbf{Z}_m[\boldsymbol{x}]$ is a *one-sided representation* of f over $\mathbf{Z}_m$ if $\forall \boldsymbol{x} \in \{0, 1\}^n$; $f(\boldsymbol{x})=0 \Leftrightarrow P(\mathbf{x}) \equiv 0 \pmod m$. With this representation, denote the smallest degree for f as $\deg_m^{os}(f)$.
4. A polynomial $P \in \mathbf{Z}_m[\boldsymbol{x}]$ is a *generalized representation* of f over $\mathbf{Z}_m$ if $\forall \boldsymbol{x}, \boldsymbol{y} \in \{0, 1\}^n$, $f(\boldsymbol{x}) \neq f(\boldsymbol{y}) \Rightarrow P(\boldsymbol{x}) \not\equiv P(\boldsymbol{y}) \pmod m$. With this representation, denote the smallest degree for f as $\deg_m^{ge}(f)$.

Equivalently, for a generalized representation polynomial $P \in \mathbf{Z}_m[\boldsymbol{x}]$ of f, there exist two disjoint sets $B_m^0 \subset \mathbf{Z}_m$ and $B_m^1(f) \subset \mathbf{Z}_m$, s.t. $f(\boldsymbol{x})=0 \Rightarrow P(\boldsymbol{x}) \pmod m \in \mathrm{B}_m^0$ and $f(\boldsymbol{x})=1 \Rightarrow P(\boldsymbol{x}) \pmod m \in B_m^1$.

Note that there is only one polynomial that exactly represents a given Boolean function [3, 13, 15], but this is not true in the one-sided model and the generalized model. Furthermore, for a given n-variable Boolean function f, it is clear that $n \geq \deg_m^{ex}(f) \geq \deg_m^{os}(f) \geq \min\{\deg_m^{os}(f), \deg_m^{os}(\neg f)\} \geq \deg_m^{ge}(f) = \deg_m^{ge}(\neg f)$. If the representing polynomials are restricted as symmetric ones [6, 14], we denote the degree as $\deg_m^{sym,os}(f)$ or $\deg_m^{sym,ge}(f)$ to prevent confusion. Observe that a symmetric polynomial can only represent a symmetric Boolean function while non-symmetric polynomials can represent not only non-symmetric but also symmetric Boolean functions.

Razborov [17] first proved that any function computed by $ACC^0[p]$ can be approximated well by some low degree polynomial modulo p and then argued that any low degree polynomial over $\mathbf{Z}_p$ can only match a limited fraction of inputs of MOD_q. This can be further proven that the MOD_q function cannot be calculated by any circuits in $ACC^0[p]$ with sub-exponential size if q and p are distinct primes. Smolensky [19] soon extended

the result from $\mathbf{Z}_p$ to $GP(p^k)$. This argument now is called Razborov-Smolensky method or Razborov's method of approximations [17, 18]. Then over a ring $\mathbf{Z}_m$ (where m has r distinct prime factors), degree lower bounds for several specific functions in non-exact representation models were found [4, 6, 14, 20, 21]. It is important to note there is a gap of degree bounds for the OR function between $O(n^{1/r})$ [4, 21] and $\Omega((\log n)^{1/(r-1)})$ [20].

The degree lower bounds for non-specific functions in the exact models are well-studied. For any n-variable Boolean function f it is well known $\deg_{\mathbf{R}}^{ex}(f) \geq \log_2 n - O(\log \log n)$ [15]. Gopalan *et al*. [13] proved that for polynomials over distinct finite fields $\lceil \log_2 p \rceil \cdot p^{2\deg_p^{ex}(f)} \cdot \deg_q^{ex}(f) \geq n$ holds. This implies that in the exact model, a Boolean function can have an extremely low degree (say $o(\log n)$) polynomial in at most one finite field. In non-exact models, degree lower bounds for general Boolean functions are known only for symmetric ones represented by univariate polynomials [10, 11, 16] as shown in Table 1.

Table 1. Lower bounds for symmetric Boolean functions.

Model	Lower Bounds	Ref.
Exact, over $\mathbf{R}$	Univariate P: $\{0, \ldots, n\} \to \{0,1\}$ $\deg_{\mathbf{R}}^{sym,ex}(f) \geq n - n^{0.525}$	[11]
Approximation, over $\mathbf{R}$	Univariate P: $\{0, \ldots, n\} \to \mathbf{R}$ $\deg_{1/3}^{sym,ex}(f) \geq [n(n-\Gamma_f)]^{1/2}$	[16]
Arbitrary, over $\mathbf{Z}_m$	Univariate P: $\{0, \ldots, n\} \to Z_m$; $m < n$ Either $\deg(f) \geq n - \Theta(n/\lg \lg n)$ or $n \leq 1$	[10]
Generalized, over $\mathbf{Z}_{m_1}$&$\mathbf{Z}_{m_2}$	Multivariate symmetric polynomials $m_1 m_2 (\deg_{m_1}^{sym,ge}(f))^s (\deg_{m_2}^{sym,ge}(f))^t > n$	This paper, Thm 4
Non-exact, over $\mathbf{Z}_{m_1}$&$\mathbf{Z}_{m_2}$	Multivariate symmetric polynomials $m_1 m_2 (\deg_{m_1}^{sym,ge}(f))^s (\deg_{m_2}^{sym,ge}(f))^t > n$	This paper, Thm 9

In the second row of Table 1, $\deg_{1/3}^{sym,ap}(f)$ is the minimum degree among symmetric polynomials $P \in \mathbf{R}[t]$ satisfying $\forall \boldsymbol{x} \in \{0, 1\}^n$; $|f(\boldsymbol{x}) - P(t)| \leq 1/3$ where $t := |\boldsymbol{x}|$. $\Gamma_f := \min\{|2t - n + 1| : f(t) \neq f(t+1), 0 \leq t \leq n-1\}$. In the third row, the result is not for any specific model. In the fifth row, $d_{m_2}^{os}(f, \neg f) := \max\{\deg_{m_2}^{os}(f), \deg_{m_2}^{os}(\neg f)\}$, *i.e.* the larger of the minimum degrees of non-symmetric representing polynomials of $\neg f$ and f.

The rest of the paper is organized as follows. We define some notations and review two useful tools in Section 2. In Section 3, we prove the main results for symmetric Boolean functions in the generalized and one-sided representation. Then we conclude with some remarks.

2. PRELIMINARIES

Let f: $\{0, 1\}^n \to \{0, 1\}$ be a Boolean function that depends on all n variables. Through this paper, an n-variable function f means f is not a constant function or k-junta for any $k < n$. Denote the set $\{1, 2, ..., n\}$ as $[n]$. Let $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \{0, 1\}^n$ be a Boolean valued vector. As a convention, denote the Hamming weight of a Boolean vector $\boldsymbol{x}$ as $|\boldsymbol{x}|$ while $|D|$ means the cardinality of the set D. If the value of a Boolean function

depends only on $|\boldsymbol{x}|$, then this function is symmetric. Additionally, $m_1 \perp m_2$ means m_1 and m_2 are relatively prime positive integers.

For $A \subseteq [n]$, we define $f(A)$ as $f(x_1, x_2, ..., x_n)$ where $x_i = 1$ if $i \in A$ and $x_i = 0$ if $i \notin A$. A multilinear polynomial of total degree d can be written as $P(\boldsymbol{x}) = \sum_{D\subseteq[n];|D|\le d} c_D X_D$, where $X_D := \prod_{i\in D} x_i$. Hence $P(A) = \sum_{D\subseteq A;|D|\le d} c_D$. A set $D \subseteq [n]$ is called a k-set if $|D| = k$; $D \subseteq A$ is a k-subset of A if $|D| = k$. If $P(\boldsymbol{x})$ is symmetric then all coefficients of k-sets are the same, *i.e.* $\forall D$ with $|D| = k$ we have $c_D = c_k$; in short $P(A) = \sum_{k=0}^{d} c_k \binom{|A|}{k}$.

We review some handy tools as follows.

Lemma 2: [21] Let $P(\boldsymbol{x})$ be a representing polynomial of some Boolean function with degree d. If $A \subseteq [n]$ and $|A| > d$, then

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

The above Möbius inversion formula holds in all representation models with the input domain $\{0, 1\}^n$. The representing polynomial $P(\boldsymbol{x})$ is multilinear since the domain of f is $\{0, 1\}^n$. Observe that if $P(D) = 0$ for all $D \subseteq [n]$ with $|D| \le d$ then $P(A) = 0$ for any $|A| > d$. Consequently, based on this lemma we know that if a nonconstant Boolean function f satisfies $f(\varnothing) = 0$ then the minimal cardinality of $D \subseteq [n]$ with $f(D) = 1$ must be at most the degree of the representing polynomial in the one-sided model.

Lemma 3: [21] Let k and $m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be arbitrary positive integers, where 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 $\binom{i}{k} \pmod m$ has the cycle length $\Pi_{i=1}^{r} p_r^{a_r}$.

For convenience, we abbreviate $a \equiv b \pmod m$ as $a \equiv_m b$. This periodic property means $\binom{j+cL_{(m,k)}}{k} \equiv_m \binom{j}{k}$ where $L_{(m,k)} = \prod_{i=1}^{r} p_i^{a_i + \lfloor \log_{p_i} k \rfloor}$ and c is an integer. Besides, for a fixed m if $k < l$ then $L_{(m,l)}$ is a multiple of $L_{(m,k)}$, *i.e.* $L_{(m,k)} | L_{(m,l)}$. Although the statement of this lemma is only for the case $k > 0$, in fact we have $\binom{j+cL_{(m,k)}}{l} \equiv_m \binom{j}{l}$ for $l \ge 0$ because $\binom{n}{0} = 1 = \binom{n'}{0}$, $\forall n, n' \in \mathbf{Z}^+ \cup \{0\}$. Also note that $L_{(m,k)} = \prod_{i=1}^{r} p_i^{a_i + \lfloor \log_{p_i} k \rfloor} \le mk^r$. The periodic property does not imply all Boolean functions are periodic, since the least common multiple of $\binom{|A|}{0}$'s can be larger than the number of variables n.

3. LOWER BOUNDS FOR SYMMETRIC FUNCTIONS

Note that a Boolean function represented by a symmetric polynomial in $\mathbf{Z}_m$ must be symmetric.

Theorem 4: Let f be an n-variable symmetric Boolean function. Let $m_1 \perp m_2$ and have s and t distinct prime factors respectively. Then

$$m_1 m_2 (\deg_{m_1}^{sym,ge}(f))^s (\deg_{m_2}^{sym,ge}(f))^t > n.$$

Proof: Since $\deg_{m_i}^{sym,ge}(f) = \deg_{m_i}^{sym,ge}(\neg f)$, for $i = 1, 2$, it suffices to prove the case of $f(\varnothing) = 0$. Define $\tau = \min\{|D|: f(D) = 1\}$. Assume $m_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ and $m_2 = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}$.

Let $P(\boldsymbol{x}) \in \mathbf{Z}_{m_1}[x]$ with $\deg(P(\boldsymbol{x})) = \deg_{m_1}^{sym,ge}(f)$, *i.e.* P is a symmetric polynomial and is a generalized representation of f with the smallest degree. For convenience, denote $\deg(P(x)) = d_1$. Assume $L_{m_1} = m_1 \cdot \prod_{i=1}^{s} p_i^{\lfloor \log_{p_i} d_1 \rfloor}$, $B_{m_1}^0 = \{P(\boldsymbol{x}) (\mathrm{mod}\, m_1) : f(\boldsymbol{x}) = 0\}$ and $B_{m_1}^0 = \{P(\boldsymbol{x}) (\mathrm{mod}\, m_1): f(\boldsymbol{x}) = 1\}$. The symmetry of $P(\boldsymbol{x})$ implies for any $A \subseteq [n]$, $P(A) = \sum_{D \subset A; |D| \le d} c_D^P = \sum_{k=0}^{d} c_k^P \binom{|A|}{k}$, where $c_k^P := c_{D_k}^P$ for any k-subset D_k of $[n]$. Hence, if $|A| \equiv_{L_{m_1}} \tau$ then

$$P(A) \equiv_{m_1} \sum_{k=0}^{d_1} c_k^P \binom{\tau}{k} = P(A')$$

for any τ-subset A' of $[n]$. Note that $|A'| = \tau \Rightarrow f(A') = 1$, hence $P(A) (\mathrm{mod}\, m_1) \in B_{m_1}^1$.

Similarly, let $Q(\boldsymbol{x}) \in \mathbf{Z}_{m_2}[\boldsymbol{x}]$ be a generalized representing symmetric polynomials of f with $\deg(Q(\boldsymbol{x})) = \deg_{m_2}^{sym,ge}(f) = d_2$. Let $L_{m_2} = m_2 \cdot \prod_{i=1}^{t} q_i^{\lfloor \log_{q_i} d_1 \rfloor}$, $B_{m_2}^0 = \{Q(\boldsymbol{x}) (\mathrm{mod}\, m_2) : f(\boldsymbol{x}) = 0\}$, $B_{m_2}^1 = \{Q(\boldsymbol{x}) (\mathrm{mod}\, m_2): f(\boldsymbol{x}) = 1\}$. Then for $A \subseteq [n]$, $|A| \equiv_{L_{m_2}} 0$,

$$Q(A) \equiv_{m_2} \sum_{k=0}^{d_2} c_k^Q \binom{|A|}{k} \equiv_{m_2} \sum_{k=0}^{d_2} c_k^Q \binom{0}{k} = c_\phi^Q \equiv_{m_2} Q(\phi).$$

This means $Q(A) (\mathrm{mod}\, m_2) \in B_{m_2}^0$ if $|A| \equiv_{L_{m_2}} 0$.

Observe that a positive integer a satisfying $a \equiv \tau (\mathrm{mod}\, L_{m1})$ and $a \equiv 0 (\mathrm{mod}\, L_{m2})$ can be calculated by the Chinese remainder theorem,

$$a \equiv \tau \cdot L_{m1} \cdot [(L_{m2})^{-1} (\mathrm{mod}\, L_{m1})] + 0 \cdot L_{m1} \cdot [(L_{m1})^{-1} (\mathrm{mod}\, L_{m2})] (\mathrm{mod}\, L_{m1} L_{m2}).$$

We can take the smallest possible $a \le L_{m1} L_{m2}$. Furthermore, the above implies if $A \subseteq [n]$ satisfies $|A| = a$ we have $f(A) = 1$ since $P(A) (\mathrm{mod}\, m_1) \in B_{m_1}^1$ and $f(A) = 0$ since $Q(A) (\mathrm{mod}\, m_2) \in B_{m_2}^0$. This leads to a contradiction unless $n < a$. Hence,

$$n < a \le L_{m1} L_{m2} \le m_1 m_2 (d_1)^s (d_2)^t.$$

This completes the proof. ❑

Taking m_1 and m_2 as two prime numbers, we immediately obtain the following result:

Corollary 5: Let f be an n-variable symmetric Boolean function, and p and q are distinct primes. Then

$$\deg_m^{sym,os}(f) \deg_q^{sym,os}(f) > pq \deg_p^{sym,ge}(f) \deg_q^{sym,ge}(f) > n.$$

This implies that for any symmetric Boolean function f: $\{0, 1\}^n \to \{0, 1\}$ that depends on all n variables, there is at most one finite field $\mathbf{Z}_p$ such that $\deg_p^{sym,os}(f) = o(n^{1/2})$ (and further $\deg_p^{sym,ge}(f) = o(n^{1/2})$. Note $\deg_q^{os}(\mathrm{MOD}_q) = \deg_q^{ge}(\mathrm{MOD}_q) = 1$ because $\sum_{i=1}^{n} x_i (\mathrm{mod}\, q)$ is an one-sided (and hence generalized) representing polynomial of MOD_q. On the other hand $\deg_q^{os}(\mathrm{MOD}_q) = \Omega(n)$. It shows that this bound is tight for some functions.

Next we show a simple combinatorial fact, which is useful to prove some degree lower bounds.

Fact 6: Let d, τ and c be fixed integers. Assume $m = \prod_{j=1}^{s} p_j^{\alpha_j}$ is an integer and $L_{(m,\tau)} = m \cdot \prod_{i=1}^{s} p_i^{\lfloor \log_{p_i} \tau \rfloor}$. Let F: $\{D \subset [n]\} \to \{0, \ldots, m-1\}$ be a function of subsets. If $A \subseteq [n]$, $|A| = cL_{(m,\tau)} + \tau$ and $\tau > d$, then

$$\sum_{D \subset A; |D| \le d} F(D) \equiv \sum_{E \subset A; |E| = \tau} \left\{ \sum_{D \subset E; |D| \le d} F(D) \right\} (\mathrm{mod}\, m).$$

***Proof*:** Observe that

$$\sum_{E \subset A; |E| = \tau} \left\{ \sum_{D \subset E; |D| \le d} F(D) \right\} = \sum_{D \subset A; |D| \le d} \binom{|A| - |D|}{\tau - |D|} F(D).$$

By the assumptions and Lemma 3 (periodic property), we have

$$\binom{|A| - |D|}{\tau - |D|} = \binom{cL_{(m,\tau)} + \tau - |D|}{\tau - |D|} \equiv \binom{\tau - |D|}{\tau - |D|} (\mathrm{mod}\, m).$$

Note that $|D| \le d < \tau$ and $\binom{\tau - |D|}{\tau - |D|} = 1$, so

$$\sum_{D \subset A; |D| \le d} \binom{|A| - |D|}{|E| - |D|} F(D) \equiv_m \sum_{D \subset A; |D| \le d} F(D).$$

In particular, set $F(D) = (-1)^{d-|D|} \binom{|A|-|D|}{d-|D|} p(D)$ where $D \subset A \subseteq [n]$ and $P(\boldsymbol{x}) \in \mathbf{Z}_m[\boldsymbol{x}]$ is a representing polynomial with $d = \deg(P)$, then

$$\sum_{D \subset A; |D| \le d} (-1)^{d-|D|} \binom{|A| - |D| - 1}{d - |D|} P(D) \equiv_m \sum_{E \subset A; |E| = \tau} \left\{ \sum_{D \subset E; |D| \le d} (-1)^{d-|D|} \binom{|E| - |D| - 1}{d - |D|} P(D) \right\}.$$

Theorem 7: Let f be an n-variable symmetric Boolean function. Let $m_1 \perp m_2$ and m_1, m_2 have s and t distinct prime factors respectively.

(1) Assume $f(\varnothing) = 1$. Let $\tau_0 = \min\{\tau \in [n] : f(D_\tau) = 0\}$. Then either $\tau_0 > \deg_{m_2}^{os}(f) \wedge \deg_{m1}^{sym,ge}(f) > (\frac{n}{m_1 m_2 \tau_0'})^{1/s}$ or $\deg_{m_2}^{os}(f) \ge \tau_0$.

(2) Assume $f(\varnothing) = 0$. Let $\tau_1' = \min\{\tau \in [n] : f(D_\tau) = 1\}$ and $\tau_0' \in \{\tau_1' + 1, \ldots, n\}$ with $f(D_{\tau_0'}) = 0$. Then either $\tau_0 > \deg_{m_2}^{os}(f) \wedge \deg_{m1}^{sym,ge}(f) > (\frac{n}{m_1 m_2 \tau_0'})^{1/s}$ or $\deg_{m_2}^{os}(f) \ge \tau_0$.

***Proof*:** (1) It suffices to prove the case $\tau_0 > \deg_{m_2}^{os}(f)$. Let $P(\boldsymbol{x}) \in \mathbf{Z}_{m_1}[\boldsymbol{x}]$ be the minimum degree symmetric polynomial that is a generalized representation of f, *i.e.*, $\deg(P(\boldsymbol{x})) = \deg_{m_1}^{sym,ge}(f)$. Denote $\deg(P(\boldsymbol{x})) = d_P$. Let $L_{m_1} = m_1 \cdot \prod_{i=1}^{s} p_i^{\lfloor \log p_i d_P \rfloor}$, and $B_{m_1}^0 = \{P(\boldsymbol{x}) (\mathrm{mod}\, m_1) : f(\boldsymbol{x}) = 1\}$. The symmetry of $P(\boldsymbol{x})$ implies for any $A \subseteq [n]$, $P(A) = \sum_{D \subset A; |D| \le d_P} c_D^P = \sum_{k=0}^{d_P} c_k^P \binom{|A|}{k}$, where $c_k^P := c_{D_k}^P$ for any k-subset D_k of $[n]$.

Similarly, let $Q(\boldsymbol{x}) \in \mathbf{Z}_{m_2}[\boldsymbol{x}]$ be a one-sided representing polynomial of f with $\deg(Q(\boldsymbol{x})) = \deg_{m_2}^{os}(f) = d_Q$. Note that $Q(\boldsymbol{x})$ is not necessarily symmetric. Let $L_{m_2} = m \cdot \prod_{i=1}^{s} q_i^{\lfloor \log q_i \tau_0 \rfloor}$.

Solving a satisfying $a \equiv 0 \pmod{L_{m1}}$ and $a \equiv 0 \pmod{L_{m2}}$ by the Chinese remainder theorem, we have

$$a \equiv 0 \cdot L_{m_2} \cdot [(L_{m_2})^{-1} (\mathrm{mod}\ L_{m_1})] + \tau_0 \cdot L_{m_{11}} \cdot [(L_{m_1})^{-1} (\mathrm{mod}\ L_{m_2})]\ (\mathrm{mod}\ L_{m_1} L_{m_2})$$

We can take the smallest possible a with $a \le L_{m_1} L_{m_2}$.

Assume there is an $A \subseteq [n]$, s.t. $|A| = a$, then $|A| = a \equiv_{L_{m_1}} 0$ implies,

$$P(A) = \sum_{k=0}^{d_P} c_k^P \binom{|A|}{k} \equiv_{m_1} \sum_{k=0}^{d_P} c_k^P \binom{0}{k} = c_0^P = P(\varnothing) \in B_{m_2}^1 \Leftrightarrow f(A) = 1.$$

On the other hand, $|A| = a \equiv_{L_{m_1}} 0$, and recall that by assumption $\tau_0 > \deg_{m_2}^{os}(f) = d_Q$ (so $|A|$ satisfies the conditions in Lemma 2),

$$\begin{aligned}
Q(A) &= \sum_{D \subset A; |D| \le d_Q} (-1)^{d_Q - |D|} \binom{|A| - |D| - 1}{d_Q - |D|} Q(D) \\
&\equiv_{m_2} \sum_{D \subset A; |D| \le d_Q} (-1)^{d_Q - |D|} \binom{\tau_0 - |D| - 1}{d_Q - |D|} Q(D) \\
&\equiv_{m_2} \sum_{E \subset A; |E| = \tau_0} \left\{ \sum_{D \subset E; |D| \le d_Q} (-1)^{d_Q - |D|} \binom{\tau_0 - |D| - 1}{d_Q - |D|} Q(D) \right\}, \text{(by Fact 6)} \\
&\equiv_{m_2} \sum_{E \subset A; |E| = \tau_0} Q(E), \qquad \text{(by Lemma 2)} \\
&\equiv_{m_2} \sum_{E \subset A; |E| = \tau_0} 0 (\text{because } f(E) = f(D_{\tau_0}) = 0) \\
&\equiv_{m_2} 0 \Leftrightarrow f(A) = 0
\end{aligned}$$

This leads to a contradiction unless $n < a$. Hence,

$$n < a \le L_{m_1} L_{m_2} \le m_1 m_2 (d_P)^s (\tau_0)^t \Rightarrow \left\lceil \frac{n}{(m_1 m_2 \tau_p^t)} \right\rceil^{\frac{1}{s}} < d_P.$$

(2) Consider the case $\tau_0' > \deg_{m_2}^{os}(f)$. Recall that $\deg_{m_2}^{os}(f) \ge \tau_1'$ holds for all f, hence the condition requires $\tau_0' > \tau_1'$. Set m_1, m_2, $P(\boldsymbol{x}) \in \mathbf{Z}_{m_1}[\boldsymbol{x}]$, $Q(\boldsymbol{x}) \in \mathbf{Z}_{m_2}[\boldsymbol{x}]$, and $L_{m1} = L_{(m1, d_P)}$ in the same way as in part (1) while set $L_{m2} = m_2 \cdot \prod_{i=1}^{t} q_i^{\lceil \log_{q_i} \tau_0' \rceil}$. Then select $A \subseteq [n]$ that satisfies $|A| = \tau_1' (\mathrm{mod}\ L_{m1})$ and $|A| = \tau_0' (\mathrm{mod}\ L_{m2})$. These force $P(A) \equiv_{m1} P(D_{\tau_1'}) \Leftrightarrow f(A) = 1$ and $Q(A) \equiv_{m2} 0 \Leftrightarrow f(A) = 0$. The corresponding result can be obtained similarly.

In Fact 6, the condition $|A| = cL_{(m,\tau)} + \tau$ with $\tau > d$ is considered. Now we consider the case $\tau > d$.

Fact 8: Let c and d be positive integers, $\theta \in \{0, 1, \ldots, d\}$, and $d < |A| = c \cdot L_{(m,d)} + \theta$. Then for $A \subseteq [n]$ and $\deg(P(\boldsymbol{x})) = d$,

$$P(A) \equiv \sum_{D \subset A; \theta \le |D| \le d} \binom{d - \theta}{d - |D|} P(D).$$

Particularly, if $|A| \equiv_m d$ then $P(A) \equiv_m \sum_{D \subset; A; |D| = d} P(D)$.

***Proof*:** The condition $d < |A|$ implies $P(A) = \sum_{D\subset A;|D|\le d}(-1)^{d-|D|}\binom{|A|-|D|-1}{d-|D|}P(D)$ by Lemma 2. Observe that $|A| = c \cdot L_{(m,d)} + \theta$ makes $(-1)^{d-|D|}\binom{|A|-|D|-1}{d-|D|} \equiv_m (-1)^{d-|D|}\binom{\theta-|D|-1}{d-|D|}$ by Newton's generalized binomial theorem $\binom{a}{b} = [a(a-1)\ldots(a-b+1)]/(b!)$, we can simplify $(-1)^{d-|D|}\binom{|A|-|D|-1}{d-|D|}$ as either 0 (if $0 \le |D| \le \theta - 1$) or $\binom{d-\theta}{|D|-\theta}$ (if $\theta \le |D| \le d$). Hence we obtain $P(A) \equiv \sum_{D\subset A;\theta\le|D|\le d}\binom{d-\theta}{d-|D|}P(D)$. Take θ as d *i.e.* $|A| \equiv_m d$ and note that $\binom{0}{0} = 1$ then $P(A) \equiv_m \sum_{D\subset A;|D|=d} P(D)$. ❑

Theorem 9: Let f be an n-variable symmetric Boolean function. Let m_1, m_2 be two positive integers with $m_1 \perp m_2$, and have s and t distinct prime factors respectively. Then at least one of the following statements is true:

$$m_1m_2(\deg^{sym,ge}_{m_1}(f))^s(\deg^{os}_{m_2}(f))^t > n,$$

and

$$m_1m_2(\deg^{sym,ge}_{m_1}(f))^s(\deg^{os}_{m_2}(\neg f))^t > n.$$

Proof: Let $Q(\boldsymbol{x})\in\mathbf{Z}_{m_2}[\boldsymbol{x}]$ be the minimum degree one-sided representing polynomial of f with $\deg(Q(\boldsymbol{x})) = \deg^{os}_{m_2}(f) = d_Q$, and $\tilde{Q}(\boldsymbol{x})\in\mathbf{Z}_{m_2}[\boldsymbol{x}]$ be the minimum degree one-sided representing polynomial of $\neg f$ with $\deg(\tilde{Q}(\boldsymbol{x})) = \deg^{os}_{m_2}(\neg f) = d_{\tilde{Q}}$. $P(\boldsymbol{x})\in\mathbf{Z}_{m_1}[\boldsymbol{x}]$ be the symmetric generalized representation of f with $\deg(P(x) = \deg^{sym,ge}_{m_1}(f) = \deg^{sym,ge}_{m_1}(\neg f)$. Let $d_P = \deg(P(\boldsymbol{x}))$. Although this $P(\boldsymbol{x})$ can be the minimum degree symmetric generalized representation of both $f(\boldsymbol{x})$ and $\neg f(\boldsymbol{x})$ by definition, it must be true that $P(\boldsymbol{x}) \pmod{m_1}\in B^1_{m_1}(f) \Leftrightarrow P(\boldsymbol{x}) \pmod{m_1}\in B^0_{m_1}(\neg f)$; moreover, $B^1_{m_1}(f) \cup B^0_{m_1}(f) = \varnothing$. In other words, if $(D_{d_P}) = 0$ (and hence $\neg f(D_{d_P}) = 1$).

Claim: (a) If $\neg f(D_{d_{\tilde{Q}}}) = 0$ then $m_1m_2(d_P)^s(d_{\tilde{Q}})^t > n$.
(b) If $f(D_{d_Q}) = 0$ then $m_1m_2(d_P)^s(d_Q)^t > n$.
(c) If $\neg f(D_{d_{\tilde{Q}}}) = 1$ and $f(D_{d_Q}) = 1$ then
either $d_Q > d_{\tilde{Q}} \wedge m_1m_2(d_P)^s(d_{\tilde{Q}})^t > n$ or $d_{\tilde{Q}} > d_Q \wedge m_1m_2(d_P)^s(d_Q)^t > n$.

Any n-variable symmetric function f must satisfy at least one of the above cases (where cases (a) and (b) may hold simultaneously). Thus, we can conclude at least one of $m_1m_2(d_P)^s(d_{\tilde{Q}})^t > n$ and $m_1m_2(d_P)^s(d_Q)^t > n$ is true. Also note that in case (c) each lower bound holds for the smaller of d_Q and $d_{\tilde{Q}}$, which implies a stronger result: $m_1m_2(\min\{d_Q, d_{\tilde{Q}}\})^t > n$.

***Proof*:** (a): Since $\neg f$ is a non-constant symmetric function and $\neg f(D_{d_{\tilde{Q}}}) = 0$, so there exists an integer $\tau \neq d_{\tilde{Q}}$ s.t. $\neg f(D_\tau) = 1$. Assume there is $A\subseteq[n]$ satisfying $|A| = a$ s.t. $a \equiv \tau \pmod{L_{m_1}}$ where $L_{m_1} = L_{(m_1,d_P)}$, and $a = c \cdot L_{m_2} + d_{\tilde{Q}}$, where $L_{m_2} = L_{(m_2,d_{\tilde{Q}})}$ and $c \ge 1$. A similar argument as in previous Theorems yields $P(A) \equiv_{m_1} P(D_\tau)\in B^1_{m_1}(\neg f) \Leftrightarrow \neg f(A) = 1$.

On the other hand by Lemma 2 and $\neg f(D_{d_{\tilde{Q}}}) = 0 \Leftrightarrow \tilde{Q}(D_{d_{\tilde{Q}}}) \equiv_{m_2} 0$,

$$\tilde{Q}(A) = \sum_{D\subset A;|D|\le d_{\tilde{Q}}}(-1)^{d_{\tilde{Q}}-|D|}\binom{|A|-|D|-1}{d_{\tilde{Q}}-|D|}\tilde{Q}(D)$$

$$\equiv_{m_2} \sum_{D\subset A;|D|\le d_{\tilde{Q}}} \tilde{Q}(D) \quad \text{(by Fact 8)}$$

$$\equiv_{m_2} \sum_{D\subset A;|D|\le d_{\tilde{Q}}} 0 \equiv_{m_2} 0 \Leftrightarrow \neg f(A) = 0.$$

Similar to the prior proofs, this implies $n < a \le L_{m_1} L_{m_2} \le m_1 m_2 (d_P)^s (d_{\tilde{Q}})^t$.
(b): Define g as $\neg f$ and repeat the same argument of part (a) for g (and its one-sided representation $Q(\boldsymbol{x}) \in \mathbf{Z}_{m_2}[\boldsymbol{x}]$), then the inequality follows.

(c): Observe that $\neg f(D_{d_{\tilde{Q}}}) = 1 \wedge \neg f(D_{d_Q}) = 1$ implies $f(D_{d_{\tilde{Q}}}) = 0 \wedge \neg f(D_{d_Q}) = 1$ and equivalently $\neg f(D_{d_{\tilde{Q}}}) = 1 \wedge \neg f(D_{d_Q}) = 0$. It is clear $d_{\tilde{Q}} \ne d_Q$. If $d_{\tilde{Q}} > d_Q$ then choose A such that $|A| \equiv d_{\tilde{Q}} (\text{mod } L_{(m_1,d_P)}) \wedge |A| \equiv d_Q (\text{mod } L_{(m_2,d_{\tilde{Q}})}$ which forces $P(A) \equiv_{m_1} P(D_{d_Q}) \Leftrightarrow f(A) = 1$ and (by Fact 6) $Q(A) \equiv_{m_2} 0 \Leftrightarrow f(A) = 0$. If $d_{\tilde{Q}} < d_Q$ then $\neg f(D_{d_{\tilde{Q}}}) = 1 \wedge \neg f(D_{d_Q}) = 0$ means that by choosing A such that $|A| \equiv d_{\tilde{Q}} (\text{mod } L_{(m_1,d_P)}) \wedge |A| \equiv d_Q (\text{mod } L_{(m_2,d_{\tilde{Q}})}$ forces $P(A) \equiv_{m_1} P(D_{d_{\tilde{Q}}})$ $\Leftrightarrow f(A) = 1$ and (by Fact 6) $Q(A) \equiv_{m_2} 0 \Leftrightarrow \neg f(A) = 0$. It leads to a contradiction as in the proof of Theorem 7.

Therefore, we show the claim of the theorem accordingly. ❑

All of the above lower bounds imply that any n-variable symmetric Boolean function that depends on n variables can only have very low degree one-sided or generalized representation in at most one finite field.

4. CONCLUSION

We prove some new degree lower bounds for symmetric Boolean functions under the one-sided and generalized representation models. By using the periodic property of binomial coefficients, we give elementary proofs on the degree lower bounds over different composite moduli for symmetric functions that depend on all of its variables. We only prove lower bounds for symmetric Boolean function. It would be interesting to know whether our approach can be extended to finding related lower bounds for general Boolean functions.

REFERENCES

1. A. Abboud, R. William, and H. Yu, "More application of the polynomial method to algorithm design," in *Proceedings of the 26th ACM-SIAM Symposium on Discrete Algorithms*, 2015, pp. 218-230.
2. A. Ambainis, "Polynomial degree vs. quantum query complexity," *Journal of Computer and System Sciences*, Vol. 72, 2006, pp. 220-238.
3. S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press, 2009.
4. D. A. M. Barrington, R. Beigel, and S. Rudich, "Representing Boolean functions as polynomials modulo composite numbers," *Computational Complexity*, Vol. 4, 1994, pp. 367-382.

5. R. Beigel, "The polynomial method in circuit complexity," in *Proceedings of the 8th Conference on Structure in Complexity Theory*, 1993, pp. 82-95.
6. N. Bhatnagar, P. Gopalan, and R. J. Lipton, "Symmetric polynomials over Z_n and simultaneous communication protocols," *Journal of Computer and System Sciences*, Vol. 72, 2006, pp. 252-285.
7. M. Braverman, "Poly-logarithmic independence fools bounded-depth Boolean circuits," *Communications of the ACM*, Vol. 54, 2011, pp. 108-115.
8. H. Buhrman and R. de Wolf, "Communication complexity lower bounds by polynomials," in *Proceedings of the 16th IEEE Conference on Computational Complexity*, 2001, pp. 120-130.
9. A. Chattopadhyay, "Multilinear polynomials modulo composites," *Bulletin of the EATCS*, Vol. 100, 2010, pp. 52-77.
10. G. Cohen, A. Shpilka, and A. Tal, "On the degree of univariate polynomials over the integers," in *Proceedings of the 3rd Innovations in Theoretical Computer Science*, 2012, pp. 409-427.
11. J. von zur Gathen and J. R. Roche, "Polynomials with two values," *Combinatorica*, Vol. 17, 1997, pp. 345-362.
12. P. Gopalan, "Constructing ramsey graph from Boolean function representations," in *Proceedings of the 21st IEEE Conference on Computational Complexity*, 2006, pp. 115-128.
13. P. Gopalan, S. Lovett, and A. Shpilka, "The complexity of Boolean functions in different characteristics," *Computational Complexity*, Vol. 19, 2010, pp. 235-263.
14. K. A. Hansen, "On modular counting with polynomials," in *Proceedings of the 21st IEEE Conference on Computational Complexity*, 2006, pp. 202-212.
15. N. Nisan and M. Szegedy, "On the degree of Boolean functions as real polynomials," *Computational Complexity*, 1994, pp. 301-313.
16. R. Paturi, "On the degree of polynomials that approximate symmetric Boolean functions," in *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, 1992, pp. 468-474.
17. A. Razborov, "Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$," *Mathematical Notes of the Academy of Science of the USSR*, Vol. 41, 1987, pp. 333-338.
18. J. Simon and S. C. Tsai, "On the bottleneck counting method," *Theoretical Computer Science*, Vol. 237, 2000, pp. 429-437.
19. R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity," in *Proceedings of the 19th Annual ACM Symposium on Theory of Computing*, 1987, pp. 77-82.
20. G. Tardos and D. A. M. Barrington, "A lower bound on the mod 6 degree of the OR function," *Computational Complexity*, Vol. 7, 1998, pp. 99-108.
21. S. C. Tasi, "Lower bounds on representing Boolean functions as polynomials in Z_m," *SIAM Journal on Discrete Mathematics*, Vol. 9, 1996, pp. 55-62.
22. R. Williams, "The polynomial method in circuit complexity applied to algorithm design," in *Proceedings of the 34th Foundations of Software Technology and Theoretical Computer Science Conference*, 2014, pp. 47-60.
23. R. Williams, "Faster all-pairs shortest paths via circuit complexity," in *Proceedings of the 46th ACM Symposium on Theory of Computing*, 2014, pp. 664-673.

Shi-Chun Tsai (蔡錫鈞) was born in Chiayi, Taiwan. He received the B.S. and M.S. degrees from National Taiwan University, Taipei, Taiwan, in 1984 and 1988, respectively, and the Ph.D. degree from the University of Chicago, Chicago, IL, in 1996, all in computer science. He is currently a Professor in the Computer Science Department, National Chiao Tung University, Hsinchu, Taiwan. His research interests include computational complexity, algorithms, cryptography, randomized computation and discrete mathematics. Dr. Tsai is a member of ACM, IEEE and SIAM.

Ming-Chuan Yang (楊名全) was born in Taipei, Taiwan. He received the B.S. and M.S. degrees from National Tsing Hua University, Hsinchu, Taiwan, in 1999 and 2002, respectively, both in mathematics. He taught math for junior high school before he enrolled a doctoral program. He is currently a Ph.D. student in the Computer Science Department, National Chiao Tung University, Hsinchu, Taiwan. His research interests include computational complexity, algorithms, and discrete mathematics.