On the Modulo Degree Complexity of Boolean Functions

Qian Li[1,2(✉)] and Xiaoming Sun[1,2]

[1] CAS Key Lab of Network Data Science and Technology, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China
{liqian,sunxiaoming}@ict.ac.cn
[2] University of Chinese Academy of Sciences, Beijing 100049, China

Abstract. For each integer $m \geq 2$, every Boolean function f can be expressed as a unique multilinear polynomial modulo m, and the degree of this multilinear polynomial is called its *modulo m degree*. In this paper we investigate the modulo degree complexity of total Boolean functions initiated by Parikshit Gopalan et al. [8], in which they asked the following question: whether the degree complexity of a Boolean function is polynomially related with its modulo m degree. For m be a power of primes, it is already known that the module m degree can be arbitrarily smaller compare to the degree complexity (see Sect. 2 for details). When m has at least two distinct prime factors, the question remains open. Towards this question, our results include: (1) we obtain some nontrivial equivalent forms of this question; (2) we affirm this question for some special classes of functions; (3) we prove a no-go theorem, explaining why this problem is difficult to attack from the computational complexity point of view; (4) we show a super-linear separation between the degree complexity and the modulo m degree.

1 Introduction

The polynomial representation of Boolean functions in different characteristics is a powerful tool in extensive areas of computer science, such as machine learning [12,13,16,18], computational complexity [1–3,19–21,23,25], explicit combinatorial constructions [5,7,9,10]. In this paper, we investigate the polynomial degree of a function.

The *modulo m degree* of a Boolean function f, denoted by $\deg_m(f)$, is the degree of the unique multilinear polynomial representing f over $\mathbb{Z}/m\mathbb{Z}$. In addition, we denote $\deg_0(f)$ (where the underlie ring is $\mathbb{Z}$) simply by $\deg(f)$. A central topic here is to investigate the relationship between module m degrees for different m. From the definition it is clear that for any f, $\deg_m(f) \geq \deg_{m'}(f)$ if m' is a factor of m, particularly, $\deg(f) \geq \deg_m(f)$. This is because the

This work was supported in part by the National Natural Science Foundation of China Grant 61433014, 61502449, 61602440, the 973 Program of China Grants No. 2016YFB1000201 and the China National Program for support of Top-notch Young Professionals.

Y. Cao and J. Chen (Eds.): COCOON 2017, LNCS 10392, pp. 384–395, 2017.
DOI: 10.1007/978-3-319-62389-4_32

polynomial representing f over $\mathbb{Z}/m\mathbb{Z}$ can be obtained from the representation over $\mathbb{Z}$ by taking each coefficient modulo m. The gap between $\deg(f)$ and $\deg_m(f)$ can be arbitrarily large when m is a prime: consider the function $f(x) = (x_1 + \cdots + x_n)^{m-1} \mod m$, it is easy to see f is Boolean due to Fermat's little theorem, $\deg_m(f) \leq m - 1$, and $\deg(f) = \Omega(n)$. Actually, the gap can be arbitrarily large even when m is a prime power [6].

In the seminal paper, Gopalan et al. [8] showed a general principle: low degree polynomials modulo p are hard to compute by polynomials in other characteristics. More precisely, let f be a Boolean function which depends on n variables, p and q be distinct primes, then

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

Moreover, they also showed that it's still hard even to approximate, which implies most known lower bounds for $AC_0[q]$ circuits.

In this work, we focus on the relation between $\deg(f)$ and $\deg_m(f)$. As mentioned above, $\deg(f) \geq \deg_m(f)$, and the equality can be achieved by AND function. For the other direction, the gap can be arbitrarily large for prime powers [6]. The situation becomes different when m has at least two distinct prime factors p and q: according to the result in [8] as mentioned above, we have $\deg_m(f) \geq \max\{\deg_p(f), \deg_q(f)\} = \Omega(\log n) = \Omega(\log \deg(f))$. Gopalan et al. [8] asked what is the largest possible separation between $\deg(f)$ and $\deg_m(f)$. Here we conjecture these quantities are polynomially related:

Conjecture 1. Let f be a boolean function and m be an integer which has at least two distinct prime factors, then

$$\deg(f) \leq \mathrm{poly}(\deg_m(f)).$$

Our Results. Towards Conjecture 1, we first give some equivalent conjectures that might easier to solve. More precisely, we can replace the degree complexity on the left side by some other complexity measures that could be exponentially smaller than $\deg(f)$, such as the minimum certificate complexity etc.

We also confirm the conjecture for some special classes of functions, such as k-uniform hypergraph properties and functions with small alternating numbers.

Theorem 1. *For any non-trivial k-uniform hypergraph property f on n vertices and any integer m with at least two distinct prime factors, we have*

$$\deg(f) = O(\deg_m(f)^k).$$

Theorem 2. *Let f be a boolean function, then for any $m \geq 2$,*

$$\deg(f) = O(\mathrm{alt}(f) \cdot \deg_m(f)^2),$$

where $\mathrm{alt}(f)$ is the alternating number of f.

Note that $\deg_6(f) = \max\{\deg_2(f), \deg_3(f)\}$ according to the Chinese Remainder Theorem, thus Conjecture 1 for the case $m = 6$ is equivalent to conjecture that the module 3 degree of any polynomial P_2 over $\mathbb{F}_2$ with low degree must be large if the degree of the function represented by P_2 is large. The following no-go theorem somehow explains why this problem is hard to solve even for this simplest case from the computational complexity point of view.

Theorem 3. *Given a polynomial $P_2(x_1, x_2, \ldots, x_n)$ over $\mathbb{F}_2$ with $\mathrm{poly}(n)$ monomials, it's impossible to decide whether $\deg_3(P_2) = n$ or not in polynomial time, unless $NP = RP$.*

Finally, in the direction to disprove this conjecture, we provide a quadratic separation. As we will see in Sect. 2, Conjecture 1 doesn't lose generality only focusing on the case $m = p_1 p_2$, where p_1 and p_2 are two distinct primes.

Theorem 4. *For any two distinct primes p_1 and p_2, there exists a sequence of boolean functions f, s.t:*

$$\deg_{p_1 p_2}(f) = O(\deg(f)^{1/2}).$$

We wonder whether this is the largest separation between $\deg_{p_1 p_2}(f)$ and $\deg(f)$.

Organization. We present some preliminaries in Sect. 2, and give other equivalent conjectures in Sect. 3. We confirm this conjecture for k-uniform hypergraph properties and functions with small alternating number in Sect. 4 and present a no-go theorem and a super-linear separation in Sect. 5. Finally, we conclude this paper in Sect. 6.

2 Preliminaries

Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and R be a commutative ring containing $\{0,1\}$ with characteristic m, we say a multilinear polynomial $P(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$ represents f if $P(x) = f(x)$ for any $x \in \{0,1\}^n$. From the Mobius inversion formula, such a polynomial always exists and is unique. Moreover, the degree of P only depends on the characteristic of R[6], thus we can denote the degree of P by $\deg_m(f)$. In the paper we will only consider the case where $R = \mathbb{Z}/m\mathbb{Z}$ and denote such polynomials by $P_m(x)$.

We list some basic facts in the following, proofs of which can be found in [6].

Fact 1. *Suppose the polynomial representation of f is $\sum_{S\subseteq[n]} C_S \prod_{i\in S} x_i$, then the representation over $\mathbb{Z}/m\mathbb{Z}$ should be $\sum_{S\subseteq[n]} (C_S \bmod m) \prod_{i\in s} x_i$.*

For example, let f be the parity function, i.e., $x_1 \oplus \cdots \oplus x_n$. The polynomial representing f over $\mathbb{Z}$ is $\sum_{\emptyset\neq S\subseteq[n]} (-2)^{|S|} \prod_{i\in S} x_i$ with $\deg(f) = n$ from the Mobius inverse formula, the representation over $\mathbb{F}_2$ is $\sum_i x_i$ with $\deg_2(f) = 1$ by taking each coefficient modulo 2, and similarly the representation over $\mathbb{F}_3$ is $\sum_{\emptyset\neq S\subseteq[n]} \prod_{i\in S} x_i$ with $\deg_3(f) = n$. Indeed, it is not hard to see that $\deg_p(f) = n$ for every prime $p \neq 2$.

Fact 2. *For any Boolean function f, we have* $\deg(f) \geq \deg_m(f)$ *for all* m. *Similarly* $\deg_m(f) \geq \deg_{m'}(f)$ *if* $m'|m$.

The above fact implies $\deg_m(f) \leq \deg_{m^k}(f)$. The following fact shows that they are always within a factor $2k-1$ of each other.

Fact 3. *For any Boolean function f, and any integers $m \geq 2$, $k \geq 1$, we have*

$$\deg_m(f) \leq \deg_{m^k}(f) \leq (2k-1)\deg_m(f).$$

Now recall the function $f(x) = (x_1 + \cdots + x_n)^{m-1} \mod m$ with $\deg_m(f) \leq m-1$ and $\deg(f) = \Omega(n)$ for prime m, as mentioned in the introduction. Indeed, such functions also exist for power of primes.

Fact 4. *For any prime power m, there exists a sequence of functions f such that* $\deg_m(f) = O(1)$ *and* $\deg(f) = \Omega(n)$.

The following fact is a consequence of the Chinese Remainder Theorem,

Fact 5. *For any Boolean function f and any m and m' with* $\gcd(m, m') = 1$, *we have*

$$\deg_{m'm}(f) = \max\{\deg_{m'}(f), \deg_m(f)\}.$$

Due to Facts 2 and 5, we get an equivalent form of Conjecture 1 straightforwardly:

Conjecture 2. Let f be a boolean function, p and q be two distinct primes, then

$$\deg(f) \leq \mathrm{poly}(\deg_p(f), \deg_q(f)).$$

Next, we give the definitions of some other complexity measures which will be used in this paper. For an input $x \in \{0,1\}^n$ and a subset B, x^B denotes the input obtained by flipping all the bit x_j such that $j \in B$.

Definition 1. *The sensitivity complexity of f on input x is defined as* $s(f,x) := |\{i : f(x) \neq f(x^i)\}|$. *The sensitivity complexity of the function f is defined as* $s(f) := max_x s(f,x)$.

It has been shown that $s(f) = O(\deg(f)^2)$[19], but whether $\deg(f)$ can be polynomially bounded in terms of $s(f)$ is still open today, actually it is what the famous *sensitivity conjecture* asks [11].

Definition 2. *The block sensitivity $bs(f,x)$ of f on input x is the maximum number of disjoint subsets $B_1, B_2, \cdots, B_r$ of $[n]$ such that for all j, $f(x) \neq f(x^{B_j})$. The block sensitivity of f is defined as $bs(f) = max_x bs(f,x)$, and the minimum block sensitivity of f is defined as $bs_{min}(f) = min_x bs(f)$.*

Definition 3. *Let C be an assignment $C : S \to \{0,1\}$ of values to some subsets $S \subseteq [n]$. We say C is consistent with $x \in \{0,1\}^n$ if $x_i = C(i)$ for all $i \in S$.*

For $b \in \{0,1\}$, a $b-$certificate for f is an assignment C such that $f(x) = b$ whenever x is consistent with C. The size of C is $|S|$.

The certificate complexity $C(f,x)$ of f on input x is the size of a smallest $f(x)$-certificate that is consistent with x. The certificate complexity of f is $C(f) = \max_x C(f,x)$. The minimum certificate complexity of f is $C_{min}(f) = \min_x C(f,x)$.

Definition 4. *Let $m \geq 2$ be an integer, the mod-m rank of a boolean function f, denoted by* $\mathrm{rank}_m(f)$*, is the minimum integer r s.t. f can be expressed as*

$$f = x_{i_1} f_1 + \cdots + x_{i_r} f_r + f_0 \qquad (\mathrm{mod}\ m),$$

where $\deg_m(f_i) < \deg_m(f)$ *for all* $0 \leq i \leq r$*. Equivalently,* $\mathrm{rank}_m(f)$ *is the minimum number of variables to hit all largest monomials in $P_m(x)$. Here we say a monomial is largest if it has maximal degree.*

Since we have to fix at least $\mathrm{rank}_m(f)$ variables to make all the largest monomials in $P_m(x)$ vanish, thus $\mathrm{rank}_m(f) \leq C_{min}(f)$ for any m. $C_{min}(f)$, $bs_{min}(f)$ and $\mathrm{rank}_m(f)$ are all polynomially bounded by $\deg(f)$, since $\{bs_{min}(f), \mathrm{rank}_m(f)\} \leq C_{min}(f) \leq C(f) = O(\deg(f)^3)$[17], and sometimes they can be very small: $\mathrm{rank}_m(AND_n) = bs_{min}(AND_n) = C_{min}(AND_n) = 1 \ll n = \deg(AND_n)$.

Definition 5. *For a Boolean function $f : \{0,1\}^n \to \{0,1\}$, we define the alternating number* $\mathrm{alt}(f)$ *of f to be the largest k such that there exist a list $\{x^{(1)}, x^{(2)}, \cdots, x^{(k+1)}\}$ with $x^{(i)} \preceq x^{(i+1)}$ and $f(x^{(i)}) \neq f(x^{(i+1)})$ for any $i \in [k]$. Here we say $x \preceq y$ if $x_i \leq y_i$ for all i.*

Definition 6. *A Boolean function f is symmetric if for every input $x = x_1, \cdots, x_n$ and every permutation $\sigma \in S_n$,*

$$f(x_1, \cdots, x_n) = f(x_{\sigma(1)}, \cdots, x_{\sigma(n)}).$$

A Boolean string can represent a graph in the following manner: $x_{(i,j)} = 1$ means there is an edge connecting vertex i and vertex j, and $x_{(i,j)} = 0$ means there is no such edge. Graph properties are functions which are independent with the labeling of vertices, i.e. two isomorphic graphs have the same function value.

Definition 7. *A Boolean function $f : \{0,1\}^{\binom{n}{2}} \to \{0,1\}$ is called a graph property if for every input $x = (x_{(1,2)}, \cdots, x_{(n-1,n)})$ and every permutation $\sigma \in S_n$,*

$$f(x_{(1,2)}, \cdots, x_{(n-1,n)}) = f(x_{(\sigma(1),\sigma(2))}, \cdots, x_{(\sigma(n-1),\sigma(n))}).$$

Similarly, we define k-uniform hypergraph properties.

Definition 8. *A Boolean function $f : \{0,1\}^{\binom{n}{k}} \to \{0,1\}$ is called a k-uniform hypergraph property if for every input $x = (x_{(1,2,\ldots,k)}, \cdots, x_{(n-k+1,\ldots,n-1,n)})$ and every permutation $\sigma \in S_n$,*

$$f(x_{(1,2,\ldots,k)}, \cdots, x_{(n-k+1,\ldots,n-1,n)}) = f(x_{(\sigma(1),\sigma(2),\ldots,\sigma(k))}, \cdots, x_{(\sigma(n-k+1),\ldots,\sigma(n-1),\sigma(n))}).$$

It is easy to see graph property is 2-uniform hypergraph property.

3 Equivalent Conjectures

Observe that the $\deg(f)$ on the left side in Conjectures 1 and 2 can be replaced by any other complexity measures which are polynomially related with $\deg(f)$, such as $D(f)$, $bs(f)$ etc. [4], to get equivalent conjectures. Surprisingly, we find that we can also replace it with some smaller complexity measures, such as $\mathrm{rank}_p(f)$, $C_{min}(f)$, $bs_{min}(f)$ and $s(f)$. In the following, we prove them one by one.

Conjecture 3. Let f be a boolean function, p and q be two distinct primes, then

$$\mathrm{rank}_p(f) \leq \mathrm{poly}(\deg_p(f), \deg_q(f)).$$

Theorem 5. *Conjecture 3* $\Longleftrightarrow$ *Conjecture 2.*

Proof. $\Longleftarrow$: Trivial, since $\mathrm{rank}_p(f) = O(\deg(f)^3)$, as mentioned above.

$\Longrightarrow$: We design an algorithm to query f, which contains at most $\deg_p(f)$ rounds and each round reduces $\deg_p$ by at least one. Denote the function at round t by $f^{(t)}$. Note that $f^{(t)}$ is a subfunction of f, hence $\deg_p(f^{(t)}) \leq \deg_p(f)$ and $\deg_q(f^{(t)}) \leq \deg_q(f)$. For each round, we can query $\mathrm{rank}_p(f^{(t)})$ variables to make the largest monomials in $P_p(x)$ vanish, which means $\deg_p(f^{(t)})$ is reduced by at least one. Therefore assuming Conjecture 3, we have $\mathrm{rank}_p(f^{(t)}) \leq \mathrm{poly}(\deg_p(f^{(t)}), \deg_q(f^{(t)})) \leq \mathrm{poly}(\deg_p(f), \deg_q(f))$, which implies $\deg(f) \leq D(f) \leq \mathrm{poly}(\deg_p(f), \deg_q(f))$.

Recall that $\mathrm{rank}_p(f) \leq C_{min}(f) = O(\deg(f)^3)$, we get another equivalent conjecture.

Conjecture 4. Let f be a boolean function, p and q be two distinct primes, then

$$C_{min}(f) \leq \mathrm{poly}(\deg_p(f), \deg_q(f)).$$

Now, we show $\deg(f)$ in Conjecture 2 can be replaced with $bs_{min}(f)$:

Conjecture 5. Let f be a boolean function, p and q be two distinct primes, then

$$bs_{min}(f) \leq \mathrm{poly}(\deg_p(f), \deg_q(f)).$$

Theorem 6. *Conjecture 5* $\Longleftrightarrow$ *Conjecture 2.*

Proof. $\Longleftarrow$: Directly follows from $bs_{min}(f) \leq bs(f) = O(\deg(f)^2)$ [19].

$\Longrightarrow$: We call monomial M maximal in $P_p(x)$ if no other monomials contains it. Observe that for any input x and any maximal monomial M, there exist a block $B \subseteq \mathrm{supp}(M)$ such that $f(x) \neq f(x^B)$, because for any restriction S: $[n] \backslash M \to \{0, 1\}$ monomial M can't be cancelled, which implies $f|_S$ is a non-constant function. In addition, according to the definition of $\mathrm{rank}_p(f)$, there exists at least $\mathrm{rank}_p(f)/\deg_p(f)$ disjoint largest monomials in $P_p(x)$. Therefore we get $bs_{min}(f) \geq \mathrm{rank}_p(f)/\deg_p(f)$, which implies Conjecture 3 assuming Conjecture 5.

Finally, we show $\deg(f)$ in Conjecture 2 can be replaced with $s(f)$. The key technique is called *"replacing"*: just replace the occurrences of x_i with x_j, i.e., the new function is $f(\cdots, x_i, \cdots, x_i, \cdots)$. Note that x_i in the corresponding $P_m(x)$ are also replaced with x_j, thus $\deg_m(f)$ cannot increase, and the new function is still boolean.

For example, let $P_2(x) = x_1x_2 + x_1x_3 + x_2x_3$ and the corresponding $P_3(x)$ is $x_1x_2 + x_1x_3 + x_2x_3 + x_1x_2x_3$. If we replace x_2 with x_1, the new $P_2(x)$ is $x_1x_1 + x_1x_3 + x_1x_3 = x_1$ and the new $P_3(x)$ is $x_1x_1 + x_1x_3 + x_1x_3 + x_1x_1x_3 = x_1$.

Conjecture 6. Let f be a boolean function, p and q be two distinct primes, then

$$s(f) \leq \mathrm{poly}(\deg_p(f), \deg_q(f)).$$

Theorem 7. *Conjecture 2* $\iff$ *Conjecture 6.*

The following simplified proof is observed by Shachar Lovett.

Proof. $\Longrightarrow$: Recall $s(f) = O(\deg(f)^2)$ [19], thus Conjecture 3 $\Rightarrow$ Conjecture 2 $\Rightarrow$ Conjecture 6.

$\Longleftarrow$: W.L.O.G, assume $bs(f, \mathbf{0}) = bs(f) = r$, thus there exist r disjoint blocks $B_1, \cdots, B_r \subseteq [n]$ such that for all i, $f(\mathbf{0}) \neq f(\mathbf{0}^{B_i})$. Further, we assume that $i \in B_i$. Now, we "replace" all variables in B_i with x_i to get a new function f'. It is easy to see that $f'(\mathbf{0}) = f(\mathbf{0}) \neq f(\mathbf{0}^{B_i}) = f'(\mathbf{0}^i)$, thus

$$bs(f) = s(f') \leq \mathrm{poly}(\deg_p(f'), \deg_q(f')) \leq \mathrm{poly}(\deg_p(f), \deg_q(f)),$$

Now we get the conclusion immediately by noting that $bs(f)$ and $\deg(f)$ are polynomially related [4].

4 Special Classes of Functions

In this section, we confirm Conjecture 1 for some special classes of functions.

4.1 Symmetric Functions

Chia-Jung Lee et al. [14] already confirmed the case of symmetric functions by showing that $2\deg_{p_1}(f)\deg_{p_2}(f) > n$. Here, we give another proof with better parameters.

Theorem 8. *Let* $f : \{0,1\}^n \to \{0,1\}$ *be symmetric and nonconstant, and* p_1, p_2 *are two distinct primes. Then*

$$\deg(f) \leq n < p_1 \deg_{p_1}(f) + p_2 \deg_{p_2}(f).$$

Proof. For the sake of the presentation, let $d_i = \deg_{p_i}(f)$ and $L_i = p_i^{1+\lfloor \log_{p_i} d_i \rfloor}$. Since f is symmetric, each $P_{p_i}(x)$ can be written as $\sum_{k=0}^{d_i} c_{i,k}\binom{|x|}{k}$. Then according to Lucas formula, for any nonnegative integers s, j and $k \leq d_i$, we have

$$\binom{sL_i + j}{k} \equiv_{p_i} \binom{j}{k}.$$

Define $g(|x|) = f(x)$, the above equality says $g(k + L_i) = g(k)$. Next, we want to show $n < L_1 + L_2$, which implies $n < p_1 d_1 + p_2 d_2$. Note that $L_1 \neq L_2$, w.l.o.g., assume $L_1 < L_2$.

Suppose $n \geq L_1 + L_2$, we claim that $\forall k \leq L_2$, $g(k) = g(k + L_1 \mod L_2)$, this is because if $k + L_1 \leq L_2$, it's trivial, otherwise, $g(k) = g(k + L_1) = g(k + L_1 - L_2) = g(k + L_1 \mod L_2)$. Moreover, $\gcd(L_1, L_2) = 1$, hence $\forall l \leq L_2$, there exists a integer t such that $l - k \equiv_{L_2} tL_1$, i.e. $g(k) = g(k + tL_1 \mod L_2) = g(l)$, which means f is constant, a contradiction.

Corollary 1. *Let $f : \{0,1\}^n \to \{0,1\}$ be symmetric and nonconstant, $p_1 < p_2 < \cdots p_r$ be distinct primes, and r and e_i's be positive integers. Let $m = \Pi_{i=1}^r p_i^{e_i}$. Then*

$$\deg(f) \leq n < \deg_m(f)(p_1 + p_2).$$

Proof. First we have $\deg_m(f) \geq \deg_{p_1 p_2}(f) = \max\{\deg_{p_1}(f), \deg_{p_2}(f)\}$. Then according to the above theorem, $(p_1 + p_2)\deg_{p_1 p_2}(f) \geq p_1 deg_{p_1}(f) + p_2 deg_{p_2}(f) > n$, as expected.

4.2 Uniform Hypergraph Properties

Using Theorem 8, we can confirm Conjecture 2 for all k-uniform hypergraph properties, where k is a constant. For the reader's convenience, we restate Theorem 1 here.

Theorem 1. *For any non-trivial k-uniform hypergraph property f on n vertices and any integer m with distinct prime factors p_1 and p_2, we have*

$$\frac{1}{p_1 + p_2 + k} n \leq \deg_m(f),$$

which implies

$$\deg(f) \leq \binom{n}{k} = O(\deg_m(f)^k).$$

Proof. (The proof is similar with Lemma 8 in [22].) W.l.o.g., we assume that for the empty graph $\overline{K_n}$, $f(\overline{K}_n) = 0$. Since f is non-trivial, there must exist a graph G such that $f(G) = 1$. Let's consider graphs in $f^{-1}(1) = \{G : f(G) = 1\}$ with the minimum number of edges. Define $m = \min\{|E(G)| : f(G) = 1\}$.

We claim that if $m \geq \frac{1}{p_1+p_2+k} n$, then $\deg_m(f) \geq \frac{1}{p_1+p_2+k} n$. Let G be a graph in $f^{-1}(1)$ and $|E(G)| = m$. Consider the subfunction f' where $\forall e \notin E(G)$, x_e

is restricted to 0, since G has the the minimum number of edges, deleting any edges from G will change the values of $f(G)$, therefore, f' is a AND function. Thus, $\deg_m(f) \geq \deg_m(f') = m \geq \frac{1}{p_1+p_2+k}n$.

In the following we assume $m < \frac{1}{p_1+p_2+k}n$. Again let G be a graph in $f^{-1}(1)$ with $|E(G)| = m$. Let us consider the isolated vertices set I, as

$$\sum_{v\in V} deg(v) = k|E(G)| < \frac{k}{p_1+p_2+k}n.$$

We have

$$|I| \geq n - \sum_{v\in V} deg(v) > \frac{p_1+p_2}{p_1+p_2+k}n.$$

Suppose $\deg_m(f) < \frac{1}{p_1+p_2+k}n$, we will deduce that there exists another graph with fewer edges and the same value, against the assumption that G has the minimum number of edges in $f^{-1}(1)$, which ends the whole proof.

Pick a vertex u with $deg(u) = d > 0$. Suppose in the graph G vertex u is adjacent to $(k-1)$-edges $\{e_1^{(k-1)}, e_2^{(k-1)}, \cdots, e_d^{(k-1)}\}$ and $I = \{u_1, u_2, \cdots, u_t\}$, where $t = |I|$.

Consider the t-variable Boolean function g_1: $\{0,1\}^t \to \{0,1\}$, where

$$g_1(x_1, \cdots, x_t) = f(G + x_1(e_1^{(k-1)}, u_1) + \cdots + x_t(e_1^{(k-1)}, u_t)).$$

It is easy to see that g_1 is a symmetric function. We claim that g_1 is a constant function: if not, we have $\deg_m(g_1) \geq \frac{1}{p_1+p_2}t$ according to Corollary 1, which implies $\deg_m(f) \geq \frac{1}{p_1+p_2+k}n$ since g_1 is a restriction of f. In particular, $g_1(1, \cdots, 1) = g_1(0, \cdots, 0)$, i.e. $f(G_1) = f(G)$, where $G_1 = G + \sum_{i=1}^{t}(e_1^{(k-1)}, u_i)$.

Define $G_i = G_{i-1} + \sum_{j=1}^{t}(e_i^{(k-1)}, u_j)$ $(i = 2, \cdots, d)$. Similarly, we can show that

$$f(G) = f(G_1) = \cdots = f(G_d).$$

Next we will delete all the edges between $\{u, u_1, \cdots, u_t\}$ and $\{e_1^{(k-1)}, e_2^{(k-1)}, \cdots, e_d^{(k-1)}\}$ from G_d by reversing the adding edge procedure of $G \to G_1 \to \cdots \to G_d$. More precisely, define $H_1 = G_d$; for $i = 2, \cdots, d$, define

$$H_i = H_{i-1} - (e_i^{(k-1)}, u) - (e_i^{(k-1)}, u_1) - \cdots - (e_i^{(k-1)}, u_t),$$

and

$$h_i(y_0, y_1, \cdots, y_t) = f(H_i + y_0(e_i^{(k-1)}, u) + y_1(e_i^{(k-1)}, u_1) + \cdots + y_t(e_i^{(k-1)}, u_t)).$$

Similarly, by the fact $\deg_m(f) < \frac{1}{p_1+p_2+k}n$ we can show that all the functions $h_2, \cdots, h_d$ are constant, which implies $f(H_1) = f(H_2) = \cdots = f(H_d)$. So we find another graph H_d with fewer edges than G and $f(H_d) = 1$.

4.3 Functions with Small Alternating Numbers

We can also confirm the functions with small alternating numbers.

Theorem 2. *Let f be a boolean function, then for any $m \geq 2$,*

$$D(f) = O(\mathrm{alt}(f) \cdot \deg_m(f)^2),$$

which implies

$$\deg(f) = O(\mathrm{alt}(f) \cdot \deg_m(f)^2).$$

Recall that $\deg_m(f) = \Omega(\log n)$ when m has two distinct prime factors [8], thus the above theorem confirms Conjecture 1 for non-degenerate functions with $\mathrm{alt}(f) = \mathrm{poly}\log(n)$.

Lin and Zhang [15] have shown the case $m = 2$, and their argument applies to general m as well. We omit the proof here.

5 A No-Go Theorem and a Super-Linear Separation

The following theorem somehow explains why it's hard to solve Conjecture 2, even for the simplest case where $p = 2$ and $q = 3$.

Theorem 3. *Given a polynomial $P_2(x_1, x_2, \ldots, x_n)$ over $\mathbb{F}_2$ with $\mathrm{poly}(n)$ monomials, it's impossible to decide whether $\deg_3(P_2) = n$ or not in polynomial time, unless $NP = RP$.*

Proof. It's sufficient to give a reduction to Unique-3CNF, since Unique-3CNF can't be solved in polynomial time unless $NP = RP$ [24].

Given a Unique-3CNF formula $\phi(x_1, \cdots, x_n)$ with m clauses, we first remove negated literals to make the formula monotone: for any variable x_i replace the occurrences of its negation by a new variable $x_i^\star$. Also introduce new variables x_i' and x_i'' and conjoin ϕ with the clauses $(x_i \vee x_i^\star) \wedge (x_i \vee x_i') \wedge (x_i^\star \vee x_i'') \wedge (x_i' \vee x_i'')$. Denote the new formula by ϕ' with n' variables and m' clauses. It is easy to see that $\sharp\phi \equiv -\sharp\phi' \mod 3$. Here $\sharp\phi$ is the number of solutions of ϕ, i.e., $\sharp\phi = \sharp\{x : \phi(x) = 1\}$.

Then we construct a polynomial P_2 over $\mathbb{F}_2$ from ϕ': There are m' variables $y_1, y_2, \cdots, y_{m'}$ and n' monomials $t_1, t_2, \cdots, t_{n'}$ in P_2, and t_i contains y_j if the jth clause contains x_i in ϕ'.

Note that the corresponding polynomial over $\mathbb{F}_3$ is

$$P_3 = \frac{1}{2}[1 - \prod_{i=1}^{m'}(1 - 2t_i)] = \prod_{i=1}^{m'}(1 + t_i) - 1,$$

According to the fact that $y_i^l = y_i$ for any integer $l \geq 1$ and any $y_i \in \{0, 1\}$, it is not hard to see the coefficient of $\prod_{i=1}^{m'} y_i$ is $\sharp\phi' \mod 3$. Note that ϕ has at most one solution, then ϕ is satisfiable if and only if $\sharp\phi \equiv -\sharp\phi' \equiv 1 \mod 3$, which means $\deg_3(P_2) = n$.

In the direction to disprove Conjecture 1, we give a quadratic separation.

Theorem 4. *For any two distinct prime p_1 and p_2, there exists a sequence of boolean functions f, s.t:*

$$\deg_{p_1p_2}(f) = O(\deg(f)^{1/2}).$$

Proof. Let $f=\mathtt{Mod}_3(\mathtt{Mod}_2(x_1,\cdots,x_{\sqrt{n}}),\cdots,\mathtt{Mod}_2(x_{n-\sqrt{n}+1},\cdots,x_n))$. Here, $\mathtt{Mod}_{p_i}(\cdot) = 0$, if the sum of inputs can be divided by p_i, otherwise $\mathtt{Mod}_{p_i}(\cdot) = 1$. On one hand, since $\mathtt{Mod}_{p_i}(\cdot)$ is symmetric, it is easy to see $\deg(f) = \Omega(n)$. On the other hand, it is also not hard to see that $\deg_{p_i}(f) = O(\sqrt{n})$ for each i, which implies $\deg_{p_1p_2}(f) = O(\sqrt{n})$.

6 Conclusion

In this work, we investigate the relationship between $\deg(f)$ and $\deg_m(f)$, more specifically, we focus on an open problem proposed by Gopalan et al. in [8], which asks whether $\deg(f)$ and $\deg_m(f)$ are polynomially related, when m has at least two distinct prime factors. First we present some nontrivial equivalent forms of this problem, then we affirm it for some special classes of functions. Finally we show a no-go theorem by which try to explain why this problem is hard, as well as a super-linear separation. Most of the problems remain open, here we list some of them:

1. Can we prove Conjecture 1 for cyclically invariant functions first?
2. Given a polynomial P_2 over $\mathbb{F}_2$ with poly(n) size, we have shown that there's no efficient algorithms to compute its modulo 3 degree exactly unless $NP = RP$. Is it still hard to approximate that?

Acknowledgments. We thank the anonymous reviewer for pointing out the better construction in Theorem 4, and Shachar Lovett for providing us the simple proof of Theorem 7.

References

1. Aspnes, J., Beigel, R., Furst, M.L., Rudich, S.: The expressive power of voting polynomials. Combinatorica **14**(2), 135–148 (1994)
2. Beigel, R., Reingold, N., Spielman, D.A.: The perceptron strikes back. In: Proceedings of the Sixth Annual Structure in Complexity Theory Conference, pp. 286–291 (1991)
3. Bhatnagar, N., Gopalan, P., Lipton, R.J.: Symmetric polynomials over z_m and simultaneous communication protocols. J. Comput. Syst. Sci. **72**(2), 252–285 (2006)
4. Buhrman, H., De Wolf, R.: Complexity measures and decision tree complexity: a survey. Theor. Comput. Sci. **288**(1), 21–43 (2002)
5. Efremenko, K.: 3-query locally decodable codes of subexponential length. SIAM J. Comput. **41**(6), 1694–1703 (2012)

6. Gopalan, P.: Computing with Polynomials over Composites. Ph.D. thesis (2006)
7. Gopalan, P.: Constructing ramsey graphs from boolean function representations. Combinatorica **34**(2), 173–206 (2014)
8. Gopalan, P., Shpilka, A., Lovett, S.: The complexity of boolean functions in different characteristics. Comput. Complex. **19**(2), 235–263 (2010)
9. Grolmusz, V.: Superpolynomial size set-systems with restricted intersections mod 6 and explicit ramsey graphs. Combinatorica **20**(1), 71–86 (2000)
10. Grolmusz, V.: Constructing set systems with prescribed intersection sizes. J. Algorithms **44**(2), 321–337 (2002)
11. Hatami, P., Kulkarni, R., Pankratov, D.: Variations on the sensitivity conjecture. Theor. Comput. Grad. Surv. **4**, 1–27 (2011)
12. Klivans, A.R., Servedio, R.A.: Learning DNF in time $2^{\tilde{o}(n^{1/3})}$. J. Comput. Syst. Sci. **68**(2), 303–318 (2004)
13. Kushilevitz, E., Mansour, Y.: Learning decision trees using the fourier spectrum. SIAM J. Comput. **22**(6), 1331–1348 (1993)
14. Lee, C.J., Lokam, S.V., Tsai, S.C., Yang, M.C.: Restrictions of nondegenerate boolean functions and degree lower bounds over different rings. In: Proceedings of IEEE International Symposium on Information Theory, pp. 501–505 (2015)
15. Lin, C., Zhang, S.: Sensitivity conjecture and log-rank conjecture for functions with small alternating numbers. CoRR, abs/1602.06627 (2016)
16. Linial, N., Mansour, Y., Nisan, N.: Constant depth circuits, fourier transform, and learnability. J. ACM **40**(3), 607–620 (1993)
17. Midrijanis, G.: Exact quantum query complexity for total boolean functions. arXiv preprint quant-ph/0403168 (2004)
18. Mossel, E., O'Donnell, R., Servedio, R.A.: Learning juntas. In: Proceedings of the 35th Annual ACM Symposium on Theory of Computing, pp. 206–212 (2003)
19. Nisan, N., Szegedy, M.: On the degree of boolean functions as real polynomials. Comput. Complex. **4**, 301–313 (1994)
20. Razborov, A.A.: Lower bounds for the size of circuits of bounded depth with basis $\{\wedge, \oplus\}$. Math. Notes Acad. Sci. USSR **41**, 333–338 (1987)
21. Smolensky, R.: Algebraic methods in the theory of lower bounds for boolean circuit complexity. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing, pp. 77–82 (1987)
22. Sun, X.: An improved lower bound on the sensitivity complexity of graph properties. Theor. Comput. Sci. **412**(29), 3524–3529 (2011)
23. Tsang, H.Y., Wong, C.H., Xie, N., Zhang, S.: Fourier sparsity, spectral norm, and the log-rank conjecture. In: Proceedings of 54th Annual IEEE Symposium on Foundations of Computer Science, pp. 658–667 (2013)
24. Valiant, L.G., Vazirani, V.V.: NP is as easy as detecting unique solutions. Theor. Comput. Sci. **47**, 85–93 (1986)
25. Viola, E.: The sum of D small-bias generators fools polynomials of degree D. Comput. Complex. **18**(2), 209–217 (2009)