Uniqueness of Optimal Mod 3 Circuits for Parity

Frederic Green and Amitabha Roy

Abstract. In this paper, we prove that the quadratic polynomials modulo 3 with the largest correlation with parity are unique up to permutation of variables and constant factors. As a consequence of our result, we completely characterize the smallest MAJ $\circ$ $\mathrm{MOD}_3 \circ \mathrm{AND}_2$ circuits that compute parity, where a MAJ $\circ$ $\mathrm{MOD}_3 \circ \mathrm{AND}_2$ circuit is one that has a majority gate as output, a middle layer of MOD_3 gates and a bottom layer of AND gates of fan-in 2. We also prove that the sub-optimal circuits exhibit a stepped behavior: any sub-optimal circuits of this class that compute parity must have size at least a factor of $\frac{2}{\sqrt{3}}$ times the optimal size. This verifies, for the special case of $m = 3$, two conjectures made in [**5**] for general MAJ $\circ$ $\mathrm{MOD}_m \circ \mathrm{AND}_2$ circuits for any odd m. The correlation and circuit bounds are obtained by studying the associated exponential sums, based on some of the techniques developed in [**7**].

1. Introduction

In this paper, we investigate the correlation between parity (MOD_2) and functions computed by polynomial-size $\mathrm{MOD}_m \circ \mathrm{AND}_{f(n)}$-circuits: these are depth 2 circuits with a MOD_m gate at the top (output) layer followed by a layer of AND-gates with fan-in $f(n)$ connected to the n Boolean inputs (our specific focus is on $m = 3, f(n) = 2$). Note that the functions computed by $\mathrm{MOD}_3 \circ \mathrm{AND}_2$ circuits correspond in a natural manner to multilinear quadratic polynomials in $\mathbb{Z}_m[x_1, x_2, \ldots, x_n]$. The correlation of two functions $f, g : \{0,1\}^n \to \{0,1\}$, defined as

$$C(f,g) = 2^{-n} \sum_{(x_1,\ldots,x_n \in \{0,1\}^n} (-1)^{f(x_1,x_2,\ldots,x_n)+g(x_1,x_2,\ldots,x_n)},$$

is a measure of the statistical closeness of two functions over the input domain (note $C(f,g) < 1$). In circuit complexity, bounds on the correlation enable us to prove restrictions on the computational power of threshold circuits. In particular, let f, g be Boolean functions as above and suppose $C(f,g) < \epsilon$. Then any circuit with a threshold gate as output requires $1/\epsilon$ input g-circuits to compute f (this is the ϵ-discriminator lemma of Hajnal *et al.* [**9**]). Indeed, Green [**7**] proved that the correlation between parity and $\mathrm{MOD}_3 \circ \mathrm{AND}_2$ circuits is at most $(\sqrt{3}/2)^{\lceil n/2 \rceil}$, thereby proving an exponential lower bound on the size of the corresponding threshold circuits. The proof of [**7**] used a technique of Cai, Green and Thierauf [**3**], in which the correlation is expressed as the

Dagstuhl Seminar Proceedings 07411
Algebraic Methods in Computational Complexity
http://drops.dagstuhl.de/opus/volltexte/2008/1305

exponential sum,

$$S_m(t,k,n) = \frac{1}{2^n} \sum_{\substack{x_i \in \{1,-1\} \\ 1 \le i \le n}} \left(\prod_{i=1}^{n} x_i \right) \ \omega^{t(x_1,x_2,\ldots,x_n)+k(x_1,x_2,\ldots,x_n)}$$

where $\omega = e^{2\pi i/m}$ is the primitive m-th root of unity for odd m, and $t = t(x_1, \ldots, x_n)$ and $k = k(x_1, \ldots, x_n)$ denote quadratic and linear forms respectively in $\mathbb{Z}_m[x_1, \ldots, x_n]$. The goal is then to prove an exponentially small upper bound on the norm of $S_m(t, k, n)$. In this equivalent formulation, Green's result is

$$|S_3(t,k,n)| \le (\sqrt{3}/2)^{\lceil n/2 \rceil} \tag{1}$$

This upper bound is also shown to be tight, since the maximum norm is achieved by polynomials $\pm x_1x_2 \pm x_3x_4 \pm \cdots \pm x_{n-1}x_n$ if n is even and by $\pm x_1 \pm x_2x_3 \pm x_4x_5 \pm \cdots \pm x_{n-1}x_n$ if n is odd. (These polynomials correspond in a natural way to the $\mathrm{MOD}_3 \circ \mathrm{AND}_2$ circuits that best compute parity, i.e., agree with parity on the most inputs). The result given in [**7**] was subsequently generalized dramatically to polynomials with degree $O(\lg n)$ and arbitrary odd moduli m, by Bourgain [**2**] and further by Green, Roy and Straubing [**8**], who proved a similar exponentially decreasing bound on the norm of the associated sums. These bounds have been improved in subsequent work by Viola and Wigderson [**12**] and Chattopadhyay [**4**]. In [**6**], Gál and Trifonov prove exponentially decreasing upper bounds for special classes of polynomials modulo m.

Bourgain's technique [**2**], essentially a sophisticated adaptation of Weyl differencing (see e.g. [**11**]) to multidimensional sums, leads to bounds that are far from tight (as do the techniques of Chattopadhyay [**4**] and Viola and Widgerson [**12**]). Furthermore, these techniques do not seem to apply to polynomials of significantly higher degree. In fact, it is believed that one can still obtain exponentially small upper bounds on the exponential sum even for polynomials of degree $O(\lg^k n)$ for any k. Some evidence supporting this comes from the fact that such a bound exists for $O(\lg^k n)$ degree *symmetric* polynomials [**3**]. Furthermore, the bounds obtained by Gál and Trifonov [**6**] apply to polynomials of very high degree (although they again do not hold for general polynomials).

In the interest of finding techniques for tighter bounds, we revisit the quadratic case. It is our hope that a complete understanding of this case will point the way to sharper bounds for higher degrees. Indeed, even for quadratic $t(x)$ there are still numerous unsettled questions. Prior to [**7**], Alon and Biegel [**1**] considered the quadratic polynomials and general odd m. Using a Ramsey theoretic argument, they first reduced the question to the symmetric quadratic case (which was studied in [**3**]) thereby getting a $2^{-n^{(\lg n)^{\Omega(1)}}}$ bound, which is again not tight. In a subsequent paper, the quadratic case for arbitrary moduli was analyzed by Dueñez *et al.* [**5**]. Specifically, they conjectured that if t was quadratic, then

$$|S_m(t,k,n)| \le \left(\cos\left(\frac{\pi}{2m} \right) \right)^{\lceil n/2 \rceil}$$

(this upper bound reduces to the upper bound of [**7**] when $m = 3$). Note that if the conjecture is true, then this upper bound is also tight: there are polynomials that achieve this bound, namely

$$c(\sum_{i=1}^{n/2} \pm x_{2i-1}x_{2i}) \text{ if } n \text{ is even and } \pm cx_1 + \sum_{i=1}^{(n-1)/2} \pm cx_{2i+1}x_{2i} \text{ if } n \text{ is odd}$$

where $c = \lfloor (m+1)/4 \rfloor$. Dueñez *et al.* further conjectured that these were the *unique* polynomials that gave the maximum norm (up to permutations of variables or constant terms). They verified this conjecture for up to $n = 10$ variables for arbitrary odd m and showed that, for all n, the bound holds for a special class of quadratic polynomials in $\mathbb{Z}_m$ (when the undirected graph corresponding to the quadratic form is "nearly" a tree). In the course of their verification, they noticed that $S_m(t,k,n)$ exhibited a "stepped" behavior when it is close to the maximum norm. Thus they conjectured that if t,k were such that $S(t,k,n)$ was submaximal, then $S_m(t,k,n) \leq \cos(\frac{\pi}{2m}) \cdot B_{m,n}$ where $B_{m,n} = (\cos(\frac{\pi}{2m}))^{\lceil n/2 \rceil}$ is the maximum possible norm. These conjectures, "uniqueness" and "gap," were key elements of Dueñez *et al.*'s argument. Thus they provide a framework for an (as yet undiscovered) inductive proof for arbitrary odd m, since they could possibly be used as a part of a stronger inductive hypothesis.

In this paper, we prove this conjecture of Dueñez *et al.* for the special case when $m = 3$. The proof is quite nontrivial, even in this special case, and even given the basic tools as set down in [**7**].

To summarize, the main contribution of our paper is:

Theorem: *Let $n \geq 1$. Then $|S_3(t,k,n)| = B_{3,n} = (\sqrt{3}/2)^{\lceil n/2 \rceil}$ iff*

$$t(x) + k(x) = \begin{cases} \alpha + \sum_{i=1}^{n/2} \pm x_{\pi(2i-1)}\, x_{\pi(2i)} & \text{if } n \text{ is even} \\ \alpha \pm x_{\pi(1)} + \sum_{i=1}^{(n-1)/2} \pm x_{\pi(2i+1)}\, x_{\pi(2i)} & \text{if } n \text{ is odd} \end{cases} \tag{2}$$

where $\alpha \in \mathbb{Z}_3$ and π is some permutation of the variables.
Furthermore, if $|S(t,k,n)| < B_{3,n}$, then $|S(t,k,n)| \leq \frac{\sqrt{3}}{2}\, B_{3,n}$.

For a permutation π of variables, we define the $\mathrm{MOD}_3 \circ \mathrm{AND}$ circuit $C_\pi^\alpha(x)$ to be the circuit that naturally corresponds to the polynomial $t(x)+k(x)$ in Equation (2) (where each monomial $x_i x_j$ is computed by an AND gate connected to inputs x_i and x_j). Using the ϵ-discriminator Lemma ([**9**]), we get the following corollary:

Corollary: *The smallest (i.e., optimal)* $\mathrm{MAJ} \circ \mathrm{MOD}_3 \circ \mathrm{AND}_2$ *circuits that compute parity consist of a majority gate connected to* $\left(\frac{2}{\sqrt{3}}\right)^{\lceil n/2 \rceil}$ $\mathrm{MOD}_3 \circ \mathrm{AND}$*-circuits* $C_{\pi_i}^\alpha(x)$ *for permutations $\{\pi_i\}_{i \in I}$, constants $\{\alpha_i\}_{i \in I}$. Every non-optimal* $\mathrm{MAJ} \circ \mathrm{MOD}_3 \circ \mathrm{AND}_2$ *circuit that computes parity has size at least $\frac{2}{\sqrt{3}}$ the size of the optimal circuit.*

Remark: We regard this result as being of intrinsic interest, since we are not aware of any other non-trivial language in the circuit complexity literature for which one obtains such a complete characterization of optimal circuits for Boolean functions or where one observes a similar step-like behavior for non-optimal circuits. Further note that while the theorem speaks to the optimal polynomials, the translation back into circuits in the corollary introduces extra constants that are needed as inputs to the circuits (for example, when we change basis from inputs over $\{1,-1\}$ to $\{0,1\}$), which may be realized in different ways. But these are irrelevant to the main idea behind the characterization.

For reasons of clarity and ease of exposition, we have broken up the above theorem into two statements (Theorem 3.2 and Theorem 4.1) in Section 3 and Section 4.

2. Preliminaries and Notations

In the rest of the paper, we only consider $S_3(t,k,n)$ which we now refer to as $S(t,k,n)$ without any confusion. We similarly write B_n in place of $B_{3,n}$. For the rest of the paper, we let $\omega = e^{2\pi i/3}$ denote the primitive 3-rd root of unity, and note that $\omega^{-1} = \bar{\omega}$. The proof in [**7**] of the upper bound in Equation (1) relies on identities involving ω that we make use of in our theorems. We use several of these identities in our proofs and for completeness, we include derivations of the relevant identities in this section. As in [**7**], we let $\chi : \mathbb{Z}_3 \mapsto \mathbb{C}$ denote the quadratic character of $\mathbb{Z}_3$ (i.e. $\chi(1) = 1, \chi(-1) = -1, \chi(0) = 0$, so that $\chi(-x) = -\chi(x)$).

Lemma 2.1. [**7**] *Let $a, b \in \mathbb{Z}_3$. Then*
- (i) $\omega^a + \omega^{-a} = \omega^{-a^2} + \omega^{-a^2}$.
- (ii) $\omega^a - \omega^{-a} = (\omega - \bar{\omega})\chi(a)$.
- (iii) $\chi(1+a)\omega^b + \chi(1-a)\omega^{-b} = \omega^{(a-b)^2} + \omega^{-(a+b)^2}$.
- (iv) $\omega^{a^2} = \frac{1+\omega^{a-1}+\omega^{-a-1}}{\bar{\omega}-\omega}$.

The preceding lemma can be proved by enumerating over all possible choices of a and b in $\mathbb{Z}_3$ and verifying that the identities hold.

Remark: One possible avenue of generalization of our results to arbitrary odd moduli and to a resolution of the conjectured upper bound of Dueñez *et al.* is to generalize the identities in Lemma 2.1. While one can generalize identities (i) and (ii) to any m with minor modifications, the generalization of (iii) to arbitrary m eludes us. We discuss some possible approaches to this problem in Section 5.

Notation: To simplify notation, we let x denote the tuple $(x_1, x_2, \ldots, x_n)$ and $x^{\lfloor 2}$ denote $(x_2, \ldots, x_n)$. To simplify $S(t,k,n)$ we often expand by x_1 and look at the resulting sums. We use the following notation, uniformly throughout the paper. We set $t(x) = x_1 \cdot r(x^{\lfloor 2}) + t_2(x^{\lfloor 2})$ and $k(x) = a_1 x_1 + l(x^{\lfloor 2})$ where $a_1 \in \{0, 1, -1\}$, t_2 is a quadratic form in $\mathbb{Z}_3[x_2, \ldots, x_n]$, and both l and r are linear forms in $\mathbb{Z}_3[x_2, \ldots, x_n]$. If $a_1 \neq 0$, then without loss of generality, we may assume that $a_1 = 1$: if not, then we can flip x_1, i.e. change the variable $x_1 \mapsto -x_1$, which does not affect the absolute value of $S(t,k,n)$. We state equalities in $\mathbb{Z}_3$ in the form "$a = b$" rather than "$a \equiv b \pmod 3$." The context (usually equalities between polynomials) will make the meaning clear.

We frequently make the change of variables $x_i \mapsto -x_i$ for $1 \leq i \leq n$. This induces the maps $\prod x_i \mapsto (-1)^n \prod x_i, t(x) \mapsto t(x), k(x) \mapsto -k(x)$. Thus we have $S(t,k,n) = (-1)^n S(t,-k,n)$. Using Lemma 2.1 (i)–(iii), one can prove the following identities:

Corollary 2.2. [**7**] *Let $t(x) = t_2(x^{\lfloor 2}) + x_1 \cdot r(x^{\lfloor 2})$.*
- (i) *If n is even, then $S(t,0,n) = S(t_2, r, n-1)$. Furthermore,*

$$S(t,k,n) = \frac{1}{2^{n+1}} \sum_x \left(\prod_{i=1}^n x_i \right) \omega^{t(x)} (\omega^{k(x)^2} + \omega^{-k(x)^2})$$

(ii) *If n is odd, then $S(t,0,n)=0$. If $k(x)\neq 0$, let $k(x)=x_1+l(x^{\lfloor 2})$. Then,*

$$S(t,k,n)=\frac{1}{2^n}\,\frac{\omega-\omega^{-1}}{2}\sum_{x^{\lfloor 2}}\left(\prod_{i=2}^{n}x_i\right)\ \omega^{t_2(x)}\left(\omega^{(l-r)^2}+\omega^{-(l+r)^2}\right)$$

Green [**7**] derived an upper bound on $S(t,k,n)$ using the identities in Corollary 2.2. We now review the main idea of his inductive proof. If n is odd, on applying the triangle inequality in part (ii) of the Lemma we have:

$$|S(t,k,n)|\leq\frac{|\omega-\bar{\omega}|}{2}\cdot\left|S(t',k',n-1)\right|$$

for some t' and k'. If n is even, then $|S(t,k,n)|\leq S(t',k',n-1)$ for some t' and k'. Thus we pick up a factor of $|\omega-\bar{\omega}|$ when we go from n odd to $n-1$ even and pick up no new factors from n even to $n-1$ odd. This gives a bound of $(|\omega-\bar{\omega}|/2)^{\lceil n/2\rceil}$.

Remark: A reformulation of the Dueñez *et al.* conjecture [**5**] is the following conjecture for arbitrary odd m: in the step from odd n to even $n-1$, one picks up a factor of $\max_{i\in\mathbb{Z}_m}\frac{\left|\omega^i-\omega^{-i}\right|}{2}=\cos(\pi/2m)$. It is easy to prove that as is the $m=3$ case, no factors are picked up in the step from even n to odd $n-1$. This leads to the conjectured upper bound of $(\cos(\pi/2m))^{\lceil n/2\rceil}$. The obstacle is getting the right generalization of Lemma 2.1 (iii) to apply in the crucial moment of the proof of Corollary 2.2, where we are able to pull out a factor of $\omega-\bar{\omega}$. We do not see how to pull out this requisite factor of $\max_{i\in\mathbb{Z}_m}\left|\omega^i-\omega^{-i}\right|$ for arbitrary odd m.

3. Uniqueness

In this section, we prove that the polynomials $t+k$ such that $S(t,k,n)$ has maximal norm are unique up to permutations of variables and constant coefficients.

Notation: We let $\bar{v}_m$ denote the ordered tuple $(v_1,v_2,\ldots,v_m)$, and when m is obvious from the context we write $\bar{v}$. Let π be a permutation on n variables $x_1,x_2,\ldots,x_n$. Let $n>0$ be even and suppose $\bar{c}\in\{1,-1\}^{n/2}$ and $\alpha\in\mathbb{Z}_3$. Define

$$Q_\sigma^{\bar{c}}(x_1,x_2,\ldots,x_n)=\sum_{i=1}^{n/2}c_i\,x_{\sigma(2i-1)}\,x_{\sigma(2i)}$$

When n is odd, we similarly define

$$Q_\sigma^{\bar{c}}(x_1,x_2,\ldots,x_n)=\sum_{i=1}^{(n-1)/2}c_i\,x_{\sigma(2i-1)}\,x_{\sigma(2i)}+c_{\frac{n+1}{2}}x_{\sigma(n)}$$

where $\bar{c}\in\{1,-1\}^{(n+1)/2}$. We denote $Q_\sigma^{\bar{c},\alpha}(x)=Q_\sigma^{\bar{c}}(x)+\alpha$, where $\alpha\in\mathbb{Z}_3$ (when $\alpha=0$, we simply write $Q_\sigma^{\bar{c}}(x)$).

The *parity* of $\bar{c}\in\{1,-1\}^{\lceil n/2\rceil}$ is

$$\mathrm{parity}(\bar{c})=|\{i|\ c_i=-1\}|\bmod 2$$

The *support* of a linear form l, denoted by $\mathrm{supp}(l)$, is the set of variables that appear in l with non-zero coefficient.

Given a polynomial q with quadratic part $\sum_{i<j} a_{i,j}x_ix_j$, we associate with it an undirected labelled graph $G(q)$. The vertices of the graph are $\{x_1, x_2, \ldots, x_n\}$ and edges $\{\{x_i, x_j\}|\ a_{i,j} \neq 0\}$. Edge $\{x_i, x_j\}$ has label $a_{i,j} \in \{1, -1\}$. We refer to vertices, cycles and triangles in q, when we really mean in $G(q)$. The following lemma is used throughout our paper.

LEMMA 3.1. *Let $q(x)$ be a quadratic form, and suppose $a(x), b(x)$ are linear forms in $\mathbb{Z}_3[x]$ where $x = (x_1, \ldots, x_n)$. If $q + a^2 = Q_\sigma^{\bar{c},\alpha}(x)$ and $q - b^2 = Q_\tau^{\bar{d},\beta}(x)$ then either*

(i) $a = b = 0$ *and* $q = Q_\sigma^{\bar{c},\alpha}(x) = Q_\tau^{\bar{d},\beta}(x)$ *or*
(ii) $\mathrm{parity}(\bar{c}) \neq \mathrm{parity}(\bar{d})$ *or*
(iii) $\alpha \neq \beta \bmod 3$.

In particular, if either a or b is non-zero, then

$$\left|\mathrm{parity}(\bar{c})\, \omega^\alpha + \mathrm{parity}(\bar{d})\, \omega^\beta\right| \leq |\omega - \bar{\omega}| = \sqrt{3}$$

PROOF. Note that if $|\mathrm{supp}(a)| + |\mathrm{supp}(b)| \neq 0 \bmod 3$, then $a^2 + b^2$ has a non-zero constant term mod 3 ($a^2 + b^2$ is a polynomial of degree at most 2). Since $Q_\sigma^{\bar{c},\alpha}(x) - Q_\tau^{\bar{d},\beta}(x) = a^2 + b^2$, we conclude that $\alpha - \beta \neq 0 \bmod 3$. So in what follows, we only consider the situation when $|\mathrm{supp}(a)| + |\mathrm{supp}(b)| = 0 \bmod 3$.

Observation: if $Q_\sigma^{\bar{c}}(x) - Q_\tau^{\bar{d}}(x) = \pm x_i x_j$ for distinct variables x_i, x_j, then $\bar{c}$ and $\bar{d}$ have differing parity. Further note that $Q_\sigma^{\bar{c},\alpha}(x) - Q_\tau^{\bar{d},\beta}(x)$ cannot contain a triangle.

We argue by cases depending on whether a and b are linear forms over the same set of variables.

Case 1: supp(a) = supp(b):

Without loss of generality (wlog), assume $a = \sum_{i\in S} x_i$ and $b = \sum_{i\in U} x_i - \sum_{i\in S\setminus U} x_i$ for sets $S \subseteq \{1, 2, \ldots, n\}$ and $U \subseteq S$. If $|U| \geq 3$, then $a^2 + b^2$ will contain a triangle, whereas $Q_\sigma^{\bar{c},\alpha}(x) - Q_\tau^{\bar{d},\beta}(x)$ cannot contain a triangle. Thus $|U| \leq 2$ and $|S \setminus U| \leq 2$ and so $|S| \leq 4$. We argue each possible case below:

(i) $|S| = 0$**:** Then $a = b = 0$ and so $q = Q_\sigma^{\bar{c},\alpha}(x) = Q_\tau^{\bar{d},\beta}(x)$.

(ii) $|S| = 1$ **or** $|S| = 2$ **or** $|S| = 4$**:** In each of these cases, $|\mathrm{supp}(a)| + |\mathrm{supp}(b)| \neq 0 \bmod 3$, thus $\alpha \neq \beta \bmod 3$.

(iii) $|S| = 3$**:** Wlog, $a = x_1 + x_2 + x_3$. Then a^2 has a triangle whereas $a^2 + b^2$ does not. So one of the edges in a^2 has to be cancelled by an edge in b^2. Wlog, $b = \pm(x_1 + x_2 - x_3)$ since $|U|, |S \setminus U| \leq 2$. Thus, $a^2 + b^2 = x_1x_2 = Q_\sigma^{\bar{c},\alpha}(x) - Q_\tau^{\bar{d},\beta}(x)$ and so $\bar{c}, \bar{d}$ have opposite parity.

Case 2: supp$(a) \triangle$ supp$(b) \neq \emptyset$:

Wlog, $x_1 \in \mathrm{supp}(a) \setminus \mathrm{supp}(b)$ and assume $a = x_1 + \sum_{i\in S} x_i$. Note that $|S| \leq 2$ otherwise x_1 appears with degree ≥ 3 in $a^2 + b^2$ (since $x_1 \notin \mathrm{supp}(b)$). We argue by cases:

- **(i)** $|S| = 0$**:** Then, $a = x_1$ and $|\mathrm{supp}(b)| \leq 2$ (otherwise b^2 and hence $a^2 + b^2$ has a triangle). Since $|\mathrm{supp}(a)| + |\mathrm{supp}(b)| = 0 \bmod 3$, we may assume that $a = x_1$ and $b = x_2 + x_3$, in which case $a^2 + b^2 = -x_2x_3$. This implies that $\mathrm{parity}(\bar{c}) \neq \mathrm{parity}(\bar{d})$.
- **(ii)** $|S| = 1$**:** Then wlog, $a = x_1 + x_2$. Note that this implies $|\mathrm{supp}(b)| \leq 2$, since otherwise there are variables x_3, x_4 (say) in $\mathrm{supp}(b)$ which form a triangle with either x_2 or some other variable in $\mathrm{supp}(b)$. Avoiding $|\mathrm{supp}(a)| + |\mathrm{supp}(b)| \neq 0 \bmod 3$, we are left with $|\mathrm{supp}(b)| = 1$ so wlog, $b = x_3$ or x_2. In which case $a^2 + b^2$ has a single edge and $\mathrm{parity}(\bar{c}) \neq \mathrm{parity}(\bar{d})$.
- **(iii)** $|S| = 2$**:** Then $a = x_1+x_2+x_3$. Then a^2 has a triangle, one of whose edges has to cancel with a term from b^2. Since $x_1 \notin \mathrm{supp}(b)$, this edge has to be $\{x_2, x_3\}$. So wlog $b = \pm(x_2 - x_3 \pm \sum_{i\in T} x_i)$. If $|T| \geq 2$, assume that $x_4, x_5 \in \mathrm{supp}(b)$ (hence $x_4, x_5 \in \mathrm{supp}(b)\setminus\mathrm{supp}(a)$). This implies that b^2 has a triangle x_4, x_5, x_2, a contradiction. Thus $|T| \leq 1$. If $|T| = 0$, then $|\mathrm{supp}(a)| + |\mathrm{supp}(b)| \neq 0 \bmod 3$. Thus $|T| = 1$ so wlog, $b = \pm(x_2 - x_3 + x_4)$. But then $a^2 + b^2 = -x_1x_2 - x_1x_3 - x_2x_4 + x_3x_4$. Thus there are two possibilities, either

$$Q^{\bar{c}}_{\sigma}(x) = -x_1x_2 + x_3x_4 + Q_{\sigma'}(x_5, \ldots, x_n) \text{ and}$$
$$Q^{\bar{d}}_{\tau}(x) = -x_1x_3 - x_2x_4 + Q_{\sigma'}(x_5, \ldots, x_n)$$

or

$$Q^{\bar{c}}_{\sigma}(x) = -x_1x_3 + x_2x_4 + Q_{\sigma'}(x_5, \ldots, x_n) \text{ and}$$
$$Q^{\bar{d}}_{\tau}(x) = -x_1x_2 - x_3x_4 + Q_{\sigma'}(x_5, \ldots, x_n)$$

In either case, $\bar{c}$ and $\bar{d}$ have different parities.

□

The following theorem establishes uniqueness; it is also used in Section 4.

THEOREM 3.2. *Let $n \geq 1$. Then $|S(t,k,n)| = B_n$ iff $t(x) + k(x) = Q^{\bar{c},\alpha}_{\sigma}(x)$ for some permutation σ of variables, $\bar{c} \in \{1,-1\}^{\lceil n/2\rceil}$ and $\alpha \in \mathbb{Z}_3$.*

PROOF. If $t(x) + k(x) = Q^{\bar{c},\alpha}_{\sigma}(x)$ then a simple calculation shows that the bound holds. The proof in the other direction is by induction on n. Our base case consists of $n = 1$. Note that

$$S(0, ax, 1) = \omega^a - \omega^{-a}$$

so $|S(0, ax, 1)| = B_1$ iff $a \in \{1, -1\}$. Thus the optimal polynomial is of the required form.

Assume $n \geq 2$. First consider the case when n is odd. Assume that $|S(t, k, n)| = B_n$. This implies that there is at least one x_i such that $x_i \in \mathrm{supp}(k)$ (since otherwise $S(t, 0, n) = 0$). Without loss of generality, assume that $k = x_1 + l(x^{\lfloor 2})$. Write $t(x) = t_2(x^{\lfloor 2}) + x_1 \cdot r(x^{\lfloor 2})$, where wlog, we may assume that l and r do not have any constant terms. If $r = 0$, then expand by x_1 to obtain:

$$S(t, k, n) = \frac{(\omega - \bar{\omega})}{2}\, S(t_2, l, n-1)$$

If $S(t,k,n)$ is optimal, then $S(t_2,l,n-1)$ has to be optimal and so by induction, $t_2 = Q_\sigma^{\bar{c},\alpha}(x^{\lfloor 2})$ and $l=0$ for some π. Then $t+k = Q_\sigma^{\bar{c},\alpha}(x^{\lfloor 2}) + x_1$, as required.

We now prove that if $r \neq 0$, then $S(t,k,n)$ is suboptimal, a contradiction. Corollary 2.2 (ii) implies that

$$S(t,k,n) = \frac{\omega - \overline{\omega}}{2} \cdot \frac{1}{2} \cdot (S_{n-1}^{+} + S_{n-1}^{-})$$

where

$$S_{n-1}^{+} = S(t_2 + (l-r)^2, 0, n-1) \text{ and } S_{n-1}^{-} = S(t_2 - (l+r)^2, 0, n-1)$$

If $S(t,k,n)$ has maximum norm, then so do S_{n-1}^{+} and S_{n-1}^{-}: if not, then the triangle inequality implies that $|S(t,k,n)| < \sqrt{3}/2 \cdot B_{n-1} < B_n$ which violates maximality of $|S(t,k,n)|$. By induction, there exist permutations π, σ, coefficients $\bar{c}, \bar{d} \in \{1,-1\}^{(n-1)/2}$ and constants $\alpha, \beta \in \mathbb{Z}_3$ such that

$$t_2 + (l-r)^2 = Q_\sigma^{\bar{c},\alpha}(x)$$
$$t_2 - (l+r)^2 = Q_\tau^{\bar{d},\beta}(x)$$

Since $r \neq 0$, either $l-r$ or $l+r$ has to be non-trivial. Lemma 3.1 implies that either the parities of $\bar{c}$ and $\bar{d}$ are different or $\alpha \neq \beta \bmod 3$ (condition (i) of the Lemma does not apply since $l-r$ or $l+r$ is non-trivial). Since S^+ and S^- have the same norm,

$$S(t,k,n) = \frac{\omega - \overline{\omega}}{2} \cdot \frac{\text{parity}(\bar{c})\,\omega^\alpha + \text{parity}(\bar{d})\,\omega^\beta}{2} \cdot i^{(n-1)/2}\, B_{n-1}$$

where note that this is an equality of expressions, not simply of their norms. If $\alpha - \beta \neq 0 \bmod 3$, then $\left|\frac{\pm\omega^\alpha \pm \omega^\beta}{2}\right| < 1$ and so $|S(t,k,n)| < B_n$, a contradiction. If instead $\alpha = \beta \bmod 3$, then $S^+ = -S^-$ (S^- is the conjugate of S^+, and since the sums are over disjoint pairs of variables, we have $S^- = -S^+$) and so $S(t,k,n) = 0$, a contradiction. This concludes the proof for n odd.

Now suppose n is even and $|S(t,k,n)| = B_n$. Corollary 2.2 (i) implies that

$$S(t,k,n) = \frac{1}{2}(S(t^+,0,n) + S(t^-,0,n))$$

where $t^\pm = t \pm k(x)^2$. If $S(t,k,n)$ has maximum norm, so do $S(t^\pm,0,n)$. Write, as usual, $t^+(x) = t_2(x^{\lfloor 2}) + x_1 \cdot r(x^{\lfloor 2}) + \gamma$ (where $\gamma \in \mathbb{Z}_3$ is non-zero if $|\text{supp}(k)| \neq 0 \bmod 3$). By Corollary 2.2, we have

$$S(t^+,0,n) = \omega^\gamma\ S(t_2(x^{\lfloor 2}), r(x^{\lfloor 2}), n-1)$$

Since $S(t^+,0,n)$ has maximum norm, $S(t_2,r,n-1)$ must have maximum norm. By induction, we have wlog,

$$t_2 = Q_\sigma^{\bar{c},\alpha+\gamma}(x_3,\ldots,x_n) \text{ and } r = x_2$$

for some choice of parameters. This implies that

$$t^+ = x_1x_2 + Q_\sigma^{\bar{c},\alpha+\gamma}(x_3,\ldots,x_n)$$

Similarly, we have wlog,

$$t^- = x_1x_3 + Q_\tau^{\bar{d},\beta+\delta}(x_2,x_4,\ldots,x_n)$$

for a (possibly) different choice of parameters $\bar{d}, \tau, \beta, \delta$.

This implies that for some choice of parameters $\sigma', \tau', \bar{c'}, \bar{d'}$,

$$\begin{aligned} t + k^2 = & \quad Q_{\sigma'}^{\bar{c'},\alpha'}(x) \\ t - k^2 = & \quad Q_{\tau'}^{\bar{d'},\beta'}(x) \end{aligned}$$

Thus

$$|S(t,k,n)| = \frac{1}{2}\left|\text{parity}(\bar{c})\,\omega^{\alpha'} + \text{parity}(\bar{d})\,\omega^{\beta'}\right| \cdot B_n$$

Lemma 3.1 now implies that if k was non-zero then $|S(t,k,n)| \leq (\sqrt{3}/2) \cdot B_n < B_n$, a contradiction. Thus $k = 0$ and t has the desired form. $\square$

4. The Gap Theorem

THEOREM 4.1. *Let $n \geq 1$. If $|S(t,k,n)| < B_n$, then $|S(t,k,n)| \leq \frac{\sqrt{3}}{2} \cdot B_n$.*

The proof is by induction on n. The base case is $n = 1$ for which a simple calculation shows that the statement is true: the norm has two possible values, $|(\omega - \bar{\omega})/2|$ or 0.

Let $n > 1$ be odd and suppose that $|S(t,k,n)| < B_n$. As before, we write $t(x) = t_2(x^{\lfloor 2}) + x_1 \cdot r(x^{\lfloor 2})$ and $k(x) = x_1 + l(x^{\lfloor 2})$. Without loss of generality, we may assume that $k \neq 0$ since otherwise $S(t,k,n) = 0$ and the statement to be proved is clearly true. Now recall from Corollary 2.2 that

$$S(t,k,n) = \frac{1}{2}.\frac{\omega - \bar{\omega}}{2}(S_{n-1}^{+} + S_{n-1}^{-}) \tag{3}$$

where $S_{n-1}^{+} = S(t_2 + (l-r)^2, 0, n-1)$ and $S_{n-1}^{-} = S(t_2 - (l+r)^2, 0, n-1)$.

A number of easy cases are taken care of in the following. The proof is in Appendix A.

LEMMA 4.2. *If $r = 0$, $l = 0$, or if both S_{n-1}^{+} and S_{n-1}^{-} are either optimal or suboptimal, then $|S(t,k,n)| \leq (\sqrt{3}/2)B_n$.*

Thus we need only consider the case when exactly one of S_{n-1}^{+} and S_{n-1}^{-} is optimal. Wlog, assume that S_{n-1}^{+} is optimal and S_{n-1}^{-} is suboptimal. This implies, wlog, that

$$t_2 + (l-r)^2 = \sum x_2 x_3 \tag{4}$$

where $\sum x_2 x_3$ is shorthand for $\sum_{i=1}^{(n-1)/2} x_{2i+1}x_{2i}$.

If $l = r$ then, by definition of $S(t,k,n)$ and summing over x_1,

$$\begin{aligned} S(t,k,n) &= \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} \prod x \; \omega^{t_2 + x_1.r + x_1 + r} \\ &= \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} \prod x \; (\omega^{t_2 + 1 + 2r} - \omega^{t_2 - 1}) \\ &= \frac{1}{2}(\omega \; S_1 - \bar{\omega} \; S_2) \end{aligned}$$

where $S_1 = S(t_2, -r, n-1)$ and $S_2 = S(t_2, 0, n-1)$. Since $t_2 = \sum x_2 x_3$, $|S_2| = B_{n-1}$. To evaluate S_1, we need the following lemma, which a simple calculation can verify.

Lemma 4.3. *If $a \neq 0$ or $b \neq 0$,*

$$|S(x_1x_2, ax_1 + bx_2, 2)| \leq \frac{\sqrt{3}}{4}$$

Since $r \neq 0$, one of the blocks $\{x_i, x_{i+1}\}$ in t_2 must be associated with a linear part $ax_i + bx_{i+1}$ where either $a \neq 0$ or $b \neq 0$. Since S_1 factors into sums over the blocks,

$$|S_1| \leq \left(\frac{\sqrt{3}}{4}\right) \cdot B_{n-3} = \frac{B_{n-1}}{2}$$

Thus the triangle inequality implies that

$$|S| \leq \frac{1}{2}\left[\frac{B_{n-1}}{2} + B_{n-1}\right] = \frac{3}{4}B_{n-1} = \frac{\sqrt{3}}{2}\ B_n,$$

as desired. Similarly, if $l = -r$, we get the desired bound. So now assume that $l \neq \pm r$, $l \neq 0$ and $r \neq 0$. In particular, $l, r, l+r, l-r$ are all non-zero. Collecting terms and simplifying we get, using Equations (3) and (4):

$$S(t,k,n) = \frac{\omega - \bar{\omega}}{2}\ \frac{1}{2^n} \sum_{x^{\lfloor 2}} \left(\prod_{i=2}^{n} x_i\right)\ \omega^{\sum x_2x_3}\,(1 + \omega^{l^2+r^2}) \tag{5}$$

Lemma 2.1 (iv) implies that:

$$1 + \omega^{l^2+r^2} = \frac{2}{3} - \frac{1}{3}\,\bar{\omega}\ (\omega^l + \omega^r + \omega^{-l} + \omega^{-r}) - \frac{1}{3}\,\omega\ (\omega^{l+r} + \omega^{-l-r} + \omega^{l-r} + \omega^{r-l})$$

Substituting this expression for $1 + \omega^{l^2+r^2}$ into Equation (5), we get

$$S(t,k,n) \quad = \quad \frac{\omega - \bar{\omega}}{2} \cdot \frac{1}{2} \cdot \left[\frac{2}{3}\ S\left(\sum x_2x_3, 0, n-1\right) - \frac{1}{3}\bar{\omega}\,T_1(l,r) - \frac{1}{3}\omega\,T_2(l,r)\right]$$

where

$$\begin{aligned} T_1(a,b) = S\left(\sum x_2x_3, a, n-1\right) + S\left(\sum x_2x_3, -a, n-1\right) + \\ S\left(\sum x_2x_3, b, n-1\right) + S\left(\sum x_2z_3, -b, n-1\right) \end{aligned}$$

and $T_2(a,b) = T_1(a+b, a-b)$.

We say that a linear form l is incident on a block $\{x_i, x_{i+1}\}$ of $\sum x_2x_3$ if $\{x_i, x_{i+1}\} \cap \mathrm{supp}(l) \neq \emptyset$. The following Lemma has an easy proof, given in Appendix B.

Lemma 4.4. *If any two of the forms $l, r, l+r, l-r$ are incident on two distinct blocks of $\sum x_2x_3$, then*

$$|S(t,k,n)| \leq \frac{\sqrt{3}}{2}\ B_n$$

Note that wlog we may assume that both l and r are incident on at most one block (since $l, r \neq 0$, this implies that they are incident on exactly one block). If one of them is incident on one block and the other on 2 blocks, then one of $l+r$ or $l-r$ is incident on 2 blocks and Lemma 4.4 applies. Also wlog, we may assume that l and r are both incident on block $\{x_2, x_3\}$. This means that we can *factor* out of $S(t, k, n)$ the sum over variables $x_4, x_5 \ldots, x_n$. Thus

$$S(t,k,n) \quad = \quad \frac{(\omega - \bar{\omega})}{2} \cdot \frac{1}{2} \cdot S\left(\sum x_4 x_5, 0, n-1\right) \cdot S' \tag{6}$$

where

$$S' = \left[\frac{2}{3}S_2(x_2x_3) - \frac{1}{3}\bar{\omega}T_1(l_2x_2 + l_3x_3, r_2x_2 + r_3x_3) - \frac{1}{3}\omega T_2(l_2x_2 + l_3x_3, r_2x_2 + r_3x_3)\right]$$

We can find out the maximum norm of S' under the assumption that $l \neq \pm r$, $l \neq 0$, $r \neq 0$ by simple enumeration. Under this restriction, we see that the maximum norm of S' is $\sqrt{3}/2$ (the other higher values correspond to the invalid choices of l and r).

Thus from Equation 6, we get

$$|S(t,k,n)| \leq \frac{\sqrt{3}}{2} \cdot \frac{1}{2} \cdot \left(\frac{\sqrt{3}}{2}\right)^{(n-3)/2} \cdot \frac{\sqrt{3}}{2} = \frac{1}{\sqrt{3}} \cdot \frac{\sqrt{3}}{2} B_n \leq \frac{\sqrt{3}}{2} B_n$$

as required. This concludes the inductive step for odd n.

The case for even n is similar, although somewhat simpler. The argument is given in Appendix C, which concludes the proof of Theorem 4.1.

5. Conclusion and Future Work

In this paper, we proved two conjectures made by Dueñez *et al.* [**5**] for quadratic polynomials defined over $\mathbb{Z}_3$. The conjecture is still open for arbitrary odd moduli (even for $m = 5$), despite large experimental evidence supporting it (along with the verification by [**5**] for all odd moduli and up to 10 variables). Here are two directions to pursue, and some of the difficulties they present.

Perhaps the most obvious route to a complete understanding of the quadratic case would be to isolate precisely what elements of the $n \leq 10$ technique of [**5**] can be used to obtain an induction that works for all n. Our results here are a step in that direction, since the uniqueness and gap properties were instrumental in the argument given in [**5**], and at least we now know for sure that they hold when $m = 3$. What properties are sufficient to obtain a full inductive proof for all odd m?

Another possible way to overcome these obstacles is to generalize Lemma 2.1 to arbitrary odd moduli m. In fact, one can readily prove analogues for identities (i) and (ii) as below when m is prime (here $\mathbb{Z}_m^*$ denotes non-zero elements of the ring $\mathbb{Z}_m$):

Lemma 5.1. *(see e.g., [**10**]) Let p be prime, $a, b \in \mathbb{Z}_p$ and $\chi : \mathbb{Z}_p \mapsto \mathbb{C}$ be a non-trivial multiplicative character of $\mathbb{Z}_p$. Then*

(i) $\sum_{x \in \mathbb{Z}_p^*} \omega^{x\,a} = \sum_{x \in \mathbb{Z}_p^*} \omega^{x\,a^2}$

(ii) $\sum_{x \in \mathbb{Z}_p^*} \chi(x)\omega^{ax} = (\sum_{x \in \mathbb{Z}_p^*} \chi(x)\omega^{x})\chi(a)$

One would expect that if p is any odd prime (not just 3), then the presence of the finite field would enable us to get tight upper bounds. It is, however, not obvious how to generalize Lemma 2.1 (iii). Even if this generalization was possible, use of the above lemma would require "completion" of the sum (i.e., to express it in terms of a sum over all non-zero field elements rather than just 1 and -1). We have explored a number of schemes for completion of the sum, but none have as yet yielded any insight. For such complete sums, the main technique that is often used in finite field sums for quadratics is to diagonalize the quadratic form t in $S(t,k,n)$. Unfortunately this technique does not work in this instance because $\chi(\prod_{i=1}^n x_i)$ does not transform nicely under linear transformations of the x_i (and also because we restrict our variables to $\{1,-1\}$). Finally, if indeed bounds can be obtained for odd primes p (or odd prime powers, e.g., via a suitable generalization of Lemma 2.1 (iii)), would it then be possible to reduce the problem of estimating the maximum norm of $S_m(t,k,n)$ when m is composite, to when m is a prime power?

References

[1] N. Alon and R. Beigel. Lower bounds for approximations by low degree polynomials over Z_m. In *IEEE Conference on Computational Complexity*, pages 184–187, 2001.

[2] J. Bourgain. Estimation of certain exponential sums arising in complexity theory. *C. R. Math. Acad. Sci. Paris*, 340(9):627–631, 2005.

[3] J. Cai, F. Green, and T. Thierauf. On the correlation of symmetric functions. *Math. Systems Theory*, 29(3):245–258, 1996.

[4] Arkadev Chattopadhyay. Discrepancy and the power of bottom fan-in in depth-three circuits. In *Proceedings of 48th Annual Symposium on Foundations of Computer Science (FOCS 2007)*, 2007.

[5] E. Dueñez, S. J. Miller, A. Roy, and H. Straubing. Incomplete quadratic exponential sums in several variables. *J. Number Theory*, 116(1):168–199, 2006.

[6] A. Gál and V. Trifonov. On the correlation between parity and modular polynomials. *MFCS 2006, Lecture Notes in Computer Science 4162*, pages 387–398, 2006.

[7] F. Green. The correlation between parity and quadratic polynomials mod 3. *J. Comput. System Sci.*, 69(1):28–44, 2004.

[8] F. Green, A. Roy, and H. Straubing. Bounds on an exponential sum arising in Boolean circuit complexity. *C. R. Math. Acad. Sci. Paris*, 341(5):279–282, 2005.

[9] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, and G. Turán. Threshold circuits of bounded depth. *J. Comput. System Sci.*, 46(2):129–154, 1993.

[10] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[11] H. Iwaniec and E. Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[12] E. Viola and A. Wigderson. Norms, xor lemmas, and lower bounds for gf(2) polynomials and multiparty protocols. *Proceedings of the 22th IEEE Conference on Computational Complexity (CCC).*, 2007.

Appendix

A. Proof of Lemma 4.2

Suppose $r=0$, then

$$S(t,k,n) = \frac{\omega-\bar{\omega}}{2}\ S(t_2,l,n-1)$$

Thus if $|S(t,k,n)|$ is suboptimal, so is $S(t_2,l,n-1)$. By induction we have $|S(t_2,l,n-1)| \leq (\sqrt{3}/2)B_{n-1}$ and so $|S(t,k,n)| \leq (\sqrt{3}/2)^2 B_{n-1} = (\sqrt{3}/2)\ B_n$ as desired.

If $l = 0$, then

$$\begin{aligned}
S(t,k,n) &= \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} \prod x_i \; \omega^{t_2 + x_1 . r + x_1} \\
&= \frac{1}{2^n} \sum_{x\lfloor 2} \prod_{i \geq 2} x_i \; (\omega^{t_2+1+r} - \omega^{t_2-1-r}) \text{ (expanding } x_1) \\
&= \frac{1}{2^n} \sum_{x\lfloor 2} \prod x_i \; \omega^{t_2} (\omega^{r+1} - \omega^{-r-1}) \\
&= \frac{1}{2^n} \left(\sum_{x\lfloor 2} \prod x_i \; \omega^{t_2} \omega^{r+1} - \sum_{x\lfloor 2} \prod x \; \omega^{t_2} \omega^{-r-1} \right) \\
&= \frac{1}{2^n} \sum_{x\lfloor 2} \prod x_i \; \omega^{t_2} (\omega^{r+1} - \omega^{r-1}) \text{ (flipping all variables in second sum)} \\
&= \frac{\omega - \bar{\omega}}{2} \; \frac{1}{2^{n-1}} \sum_{x\lfloor 2} \prod x_i \; \omega^{t_2 + r} = \frac{\omega - \bar{\omega}}{2} \; S(t_2, r, n-1)
\end{aligned}$$

If $S(t,k,n)$ is suboptimal, so is $S(t_2, r, n-1)$. Thus following a similar argument for $r = 0$, we conclude that

$$|S(t,k,n)| \leq (\sqrt{3}/2) \; B_n$$

Now assume that both l and r are non-zero. Adopting the notation of Equation 3, if both S^+_{n-1} and S^-_{n-1} are optimal, then by Theorem 3.2,

$$t_2 + (l-r)^2 = Q^{\bar{c},\alpha}_{\sigma}(x) \text{ and } t_2 - (l+r)^2 = Q^{\bar{d},\beta}_{\tau}(x)$$

where σ, τ are permutations on $x_2, \ldots, x_n$. But then,

$$S(t,k,n) = \frac{\omega - \bar{\omega}}{2} \cdot \frac{\text{parity}(\bar{c})\,\omega^{\alpha} + \text{parity}(\bar{d})\,\omega^{\beta}}{2} \cdot i^{(n-1)/2} B_{n-1}$$

Lemma 3.1 implies that either $\text{parity}(\bar{c}) \neq \text{parity}(\bar{d})$ or $\alpha \neq \beta \bmod 3$ (case (i) of Lemma 3.1 cannot arise since both l and r are non-zero). In either case,

$$\left| \frac{\text{parity}(\bar{c})\,\omega^{\alpha} + \text{parity}(\bar{d})\,\omega^{\beta}}{2} \right| \leq \left| \frac{\omega^{\alpha} - \omega^{\beta}}{2} \right| \leq \frac{\sqrt{3}}{2}$$

and so

$$|S(t,k,n)| = \left(\frac{\sqrt{3}}{2} \right)^2 B_{n-1} = \frac{\sqrt{3}}{2} \; B_n$$

as required. Similarly, if both S^+_{n-1} and S^-_{n-1} are suboptimal, induction implies that $\left|S^+_{n-1}\right| \leq (\sqrt{3}/2) \; B_{n-1}$ and $\left|S^-_{n-1}\right| \leq (\sqrt{3}/2) \; B_{n-1}$. Now Equation (3) and the triangle inequality imply as before:

$$|S(t,k,n)| \leq (\sqrt{3}/2)^2 \; B_{n-1} \leq (\sqrt{3}/2) \; B_n$$

as required. □

B. Proof of Lemma 4.4

We start with,

Lemma B.1. *If a linear form* $l = \sum_{i=2}^{n} l_2 x_2$ *is incident on at least* k *blocks of* $\sum x_2 x_3$*, then*

$$|S\left(\sum x_2 x_3, l, n-1\right)| \leq \frac{1}{2^k}\ B_{n-1}$$

Proof. A straightforward computation and Lemma 4.3 imply that

$$\left|\frac{1}{4} \cdot \sum_{x,y} xy\ \omega^{axy+bx+cy}\right| = \frac{\sqrt{3}}{2} \text{ if } b = c = 0 \text{ and } a \neq 0$$

and otherwise it has norm $\leq \frac{\sqrt{3}}{4}$ when $a \neq 0$. Thus

$$|S\left(\sum x_2 x_3, l, n-1\right)| \leq \left(\frac{\sqrt{3}}{4}\right)^k \left(\frac{\sqrt{3}}{2}\right)^{\frac{n-1-2k}{2}}$$

(on removing the at most $2k$ variables in the k blocks, we are left with an optimal form on at most $n-2k-1$ variables). The result now follows. $\square$

Proof of Lemma 4.4: The hypothesis implies that 4 of the forms $l, r, -l, -r, l+r, -l-r, l-r, -l+r$ are incident on two distinct blocks of $\sum x_2 x_3$. Also note that each of the other 4 forms have non-zero support so are incident on at least one block (since $l \neq \pm r, l \neq 0, r \neq 0$). So by Lemma B.1, 4 of the corresponding $S(t,k,n)$ terms have norm at most $(1/4)B_{n-1}$ each and the other 4 have norm at most $(1/2)B_{n-1}$.

Applying the triangle inequality and Lemma B.1,

$$\begin{aligned}
|S(t,k,n)| &\leq \frac{\sqrt{3}}{2} \cdot \frac{1}{2} \cdot \left[\frac{2}{3}B_{n-1} + \frac{1}{3}(4 \cdot \frac{B_{n-1}}{4} + 4 \cdot \frac{B_{n-1}}{2})\right] \\
&= \frac{5}{6} \cdot \frac{\sqrt{3}}{2} \cdot B_{n-1} = \frac{5}{6} \cdot B_n \leq \frac{\sqrt{3}}{2} B_n
\end{aligned}$$

$\square$

C. The Even n Case for Theorem 4.1

Let n be even. First consider the situation when we have a quadratic form (i.e., $k = 0$). Then, by Corollary 2.2(i),

$$S(t,0,n) = S(t_2(x^{\lfloor 2}), r(x^{\lfloor 2}), n-1)$$

If $S(t,0,n)$ is suboptimal, so is $S(t_2(x^{\lfloor 2}), r(x^{\lfloor 2}), n-1)$ and so

$$|S(t,0,n)| = \left|S(t_2(x^{\lfloor 2}), r(x^{\lfloor 2}), n-1)\right| \leq \frac{\sqrt{3}}{2}\ B_{n-1} = \frac{\sqrt{3}}{2}\ B_n,$$

as desired. Now suppose that $k \neq 0$. Then, by Corollary 2.2(i),

$$|S(t,k,n)| \leq \frac{1}{2}(\left|S(t^+,0,n)\right| + \left|S(t^-,0,n)\right|)$$

where $t^{\pm} = t \pm k(x)^2$. If both $S(t^+, 0, n)$ and $S(t^-, 0, n)$ are optimal (in which case $|S(t, k, n)|$ is also maximal), Theorem 3.2 implies that

$$t + k^2 = Q_\tau^{\bar{d},\beta}(x),\ t - k^2 = Q_\sigma^{\bar{c},\alpha}(x)$$

This implies that $k^2 = Q_\sigma^{\bar{c},\alpha}(x) - Q_\tau^{\bar{d},\beta}(x)$ and hence $|\mathrm{supp}(k)| \leq 2$ (otherwise, k^2 would have a triangle). If $|\mathrm{supp}(k)| = 1$, then $Q_\tau^{\bar{d},\beta}(x) - Q_\sigma^{\bar{c},\alpha}(x)$ is a constant so $\sigma = \tau$, and wlog $t + k = \sum x_1 x_2 + x_1$. Thus $S(t, k, n)$ factors into sums over the connected components of t, and the component that contains x_1 gives a factor of $\sqrt{3}/4$ (Lemma 4.3). Thus

$$|S(t, k, n)| \leq \frac{\sqrt{3}}{4} \cdot B_{n-2} \leq \frac{\sqrt{3}}{2} B_n$$

Similarly, we get the desired factor for $|\mathrm{supp}(k)| = 2$.

Department of Mathematics and Computer Science, Clark University, Worcester, MA 01610.
E-mail address: fgreen@black.clarku.edu

Computer Science Department, Boston College, Chestnut Hill, MA 02467.
E-mail address: aroy@cs.bc.edu