Electronic Colloquium on Computational Complexity, Report No. 160 (2012)

Block-symmetric polynomials correlate with parity better than symmetric

Frederic Green* Daniel Kreymer† Emanuele Viola†

November 16, 2012

Abstract

We show that degree-d block-symmetric polynomials in n variables modulo any odd p correlate with parity exponentially better than degree-d symmetric polynomials, if $n \geq cd^2 \log d$ and $d \in [0.995 \cdot p^t - 1, p^t)$ for some $t \geq 1$. For these infinitely many degrees, our result solves an open problem raised by a number of researchers including Alon and Beigel in 2001 [AB01]. The only previous case for which this was known was $d = 2$ and $p = 3$ [Gre04].

The result is obtained through the development of a theory we call *spectral analysis of symmetric correlation*, which originated in works of Cai, Green, and Thierauf [CGT96, Gre99]. In particular, our result follows from a detailed analysis of the correlation of symmetric polynomials, which is determined up to an exponentially small relative error when $d = p^t - 1$.

We give a partial complement to our result by showing that for degree $d = p^t$, p prime, block-symmetric polynomials correlate exponentially worse than symmetric, assuming that the blocks are large enough which is the case above. Moreover we show the same holds for every d in the case of polynomials modulo $p = 2$ vs. the Mod_3 function. In this setting we present computational evidence that symmetric polynomials may in fact be optimal.

This work builds on a study of correlation using computer search by the authors which gave unexpected results. The latter are here explained analytically. We advocate further use of computer search in complexity theory.

*Email: fgreen@black.clarku.edu

†Supported by NSF grant CCF-0845003, REU supplements. Email: {dank,viola}@ccs.neu.edu

ISSN 1433-8092

1 Introduction

Among the dozens of simple-to-state, long-standing challenges in complexity lower bounds, one challenge arguably stands out. This is the challenge of exhibiting explicit functions that have small correlation (a.k.a. are very hard on average for) low-degree polynomials in n variables modulo p. As discussed in the survey [Vio09], it stands out for three reasons:

i) progress on correlation bounds is a prerequisite for basic progress on circuit complexity such as, say, establishing that NP does not have depth-4 majority circuits of size $n^{O(\log n)}$. (This follows from a boosting/min-max argument.) It is also sufficient for long-sought progress on AC^0 circuits with mod p gates and one majority gate [Raz87, Smo87, HMP$^+$93].

ii) so-called "barriers" [BGS75, RR97, AW08] are not known to apply.

iii) arguably more is known about this challenge than others. For example, consider the Mod q function which outputs 1 on input $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ if $q | \sum_i x_i$. Two different bounds are known on its correlation with degree-d polynomials in n variables modulo p, for co-prime p and q. First, $O(d/\sqrt{n})$ [Raz87, Smo87, Smo93]; second, $\exp(-\Omega(n/c^d))$ [BNS92, Bou05, GRS05] (cf. [Vio09] for Nisan's simple derivation of this from [BNS92]).

Motivated by the above three points, and especially by iii), in this work we consider the correlation with the Mod q functions. For concreteness let us define "correlation." Following previous work, we work with a complex sum; for completeness we review in §A the close relationship between this sum and other notions of correlation, such as the fraction of inputs in which the functions disagree.

Definition 1.1. *The "correlation" between a polynomial t in the n variables $x_1, \ldots, x_n$ modulo p and the Mod q function in the same variables is*

$$\gamma = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \zeta_q^{\sum_{i=1}^n x_i} \zeta_p^{t(x)}, \tag{1}$$

where $\zeta_u = e^{2\pi i/u}$ is the primitive complex u^{th} root of unity.

When we say that the correlation is maximized/bigger/etc., we refer to its norm $|\gamma|$.

It is natural to conjecture that $|\gamma|$ is exponentially small in n for every fixed, co-prime p and q, even for degree $d = n^{\Omega(1)}$. Alas, for all we know $|\gamma| \geq 1/n$ even for $d = \log_2 n$. Indeed, regarding point iii) above, the techniques of [Raz87, Smo87] are insufficient to prove $|\gamma| \leq 1/n$, while those of [BNS92, Bou05] do not yield interesting bounds when $d \geq \log_2 n$.

It thus seems natural to investigate which polynomials have (close to) maximum correlation. In this direction a specific question was asked by a number of researchers, including Alon and Beigel [AB01] over a decade ago:

Do symmetric polynomials have maximum correlation?

Recall that a polynomial is symmetric if it is invariant under permutation of the variables, and so its output depends only on the Hamming weight of the input. A positive solution to the above question would have dramatic consequences, as for symmetric polynomials very strong bounds are known [CGT96]. But until the present work it was only known that the answer is negative for polynomials of degree $d = 2$ modulo $p = 3$ vs. the Mod $q = 2$ function (a.k.a. parity) [Gre04]. By contrast, in other cases empirical results (reproduced in §6) had suggested that, for higher degrees $d > 2$, symmetric may actually maximize correlation.

1.1 Our results

We prove that, in fact, symmetric polynomials modulo p have correlation with parity that is exponentially worse than the maximum for infinitely many degrees d, and any odd p. We accomplish this by showing that *block-symmetric* polynomials, those polynomials whose variables are divided into blocks and are symmetric within each block but not overall, achieve exponentially better correlation than symmetric polynomials of the same degree.

Theorem 1.2 (Block-symmetric beats symmetric.)**.** *For every odd $p \geq 3$, every n, and every d that satisfies $p^t > d \geq 0.995p^t - 1$ for some $t \geq 1$, let $|\gamma_b|$ be the maximum correlation between degree-d block-symmetric polynomials in n variables modulo p and the parity function, and let $|\gamma_s|$ be the maximum for symmetric polynomials instead. Then,*

$$\frac{|\gamma_b|}{|\gamma_s|} \geq \frac{1.01^{\lfloor n/(cd^2 \lg d) \rfloor}}{pd},$$

where $c > 0$ depends only on p.

We note that the above theorem applies to "small" degrees such as $d = 8$ (for $p = 3$), and to a constant fraction of all the degrees up to p^t. The latter degrees can be as large as $n^{0.49}$, for large enough n. This regime of large degrees is the most interesting for applications.

The only case that was previously known is $d = 2$ and $p = 3$ [Gre04], corresponding to $t = 1$. In fact, [Gre04] shows that the optimal polynomials over $\{-1, 1\}$ are of the block-symmetric form $\pm x_1x_2 \pm x_3x_4 \pm \cdots \pm x_{n-1}x_n$ (if n is even; the case n odd has an extra degree-1 term). However, the natural generalization of these polynomials to higher degrees (e.g., $x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n$) does *not* beat symmetric, for any $d \geq 3$. We find it somewhat surprising that a different type of block-symmetric polynomials beats symmetric, as given by our above theorem.

In fact, we complement the above result with more settings where symmetric polynomials do beat block-symmetric, as long as the blocks are large enough. We note that the blocks in the above result are indeed large enough. First, we show this is the case when d is a power of p, indicating that the inequality $p^t > d$ in Theorem 1.2 must be strict.

Theorem 1.3 (Symmetric beats large-block-symmetric for $d = p^t$.)**.** *Fix any odd prime p and degree $d = p^t$. There is a constant c such that for $n \geq c$, any block-symmetric polynomial with block-size $\geq c$ correlates with parity worse than symmetric.*

Second, we consider the case of polynomials modulo $p = 2$ vs. the Mod 3 function. Before this paper, nothing suggested that different moduli yield different optimal polynomials. We can in fact show that symmetric beats block-symmetric, again with large enough blocks.

Theorem 1.4 (Symmetric mod 2 beats large-block-symmetric in computing Mod 3.)**.** *For any fixed degree d, block-symmetric polynomials modulo 2 with sufficiently large blocks have worse correlation with the Mod_3 function than symmetric.*

In fact, in the setting $p = 2$ of Theorem 1.4 we provide later computational evidence that symmetric may be optimal.

All the results discussed so far concern the relationship between block-symmetric and symmetric polynomials. We also introduce a new family of polynomials which we call *switch-symmetric*. These are polynomials of the form $x_1 f(x_2, \ldots, x_n) + f'(x_2, \ldots, x_n)$ where f, f' are symmetric polynomials in $n-1$ variables. We obtain various settings of the degree d and the modulus p such that switch-symmetric beats symmetric for infinitely many n. Specifically:

Theorem 1.5 (Switch-symmetric beats symmetric)**.** *Let $(d, p) \in \{(4, 3), (10, 3), (6, 5)\}$. For all sufficiently large, even n there exists a degree-d switch-symmetric polynomial mod p over n variables that correlates with parity better than degree-d symmetric polynomials.*

1.2 Techniques: Spectral analysis of symmetric correlation

Our main results are obtained by developing a theory we call *spectral analysis of symmetric correlation*, which originated in works of Cai, Green, and Thierauf [CGT96, Gre99]. Before describing it, we mention that we will use the terminology "symmetric polynomial of degree d" to refer to the $d+1$ choices of the coefficients for the polynomial, independently from the values of n. Thus, it makes sense to fix a certain symmetric polynomial and let n grow.

The aforementioned theory allows us to re-write the correlation γ in the format

$$\gamma = \frac{1}{D} \sum_{i \le D} \alpha_i^n \beta_i, \tag{2}$$

where $D \le pd$ is the smallest power of p larger than d, the α_i are real numbers independent from the polynomial and decreasing (i.e., $\alpha_1 > \alpha_2 > \ldots > \alpha_D > 0$); and the β_i are complex numbers that depend on the symmetric polynomial, but only on n modulo $O(D)$.

Hence, for any symmetric polynomial there exists a value β_1' such that the correlation is dominated asymptotically by the leading term $\alpha_1^n \beta_1'/D$ in the sum (2). All the results in this paper are obtained by analyzing this leading term β_1 only. Because of its importance, we refer to β_1 as β. In the rest of this informal discussion we ignore lower-order terms (corresponding to $i > 1$) and we think of the correlation of a symmetric polynomial as

$$\alpha_1^n \beta / D. \tag{3}$$

Note the analogy with spectral graph theory. Just as the latter rewrites a transition matrix in an eigenvector basis and typically proceeds by bounding the maximum (non-trivial) eigenvalue, spectral analysis of symmetric correlation rewrites correlation in the form of Equation (2) and proceeds by bounding the leading β_i.

To study the relationship between symmetric and block-symmetric, we start by making the following key observation. If we divide up the variables into n/b blocks of b variables each, and in each we use a symmetric polynomial with a specific β, the resulting correlation multiplies across blocks and becomes:

$$\left(\alpha_1^b \beta/D\right)^{n/b} = \alpha_1^n (\beta/D)^{n/b}. \tag{4}$$

Comparing Equations (3) and (4) we see that:

Block-symmetric beats symmetric if $|\beta|/D > 1$.

To obtain our main Theorem 1.2 that block symmetric beats symmetric we exhibit (for the parameters in the theorem) a polynomial such that $|\beta|/D > 1$. In fact, we show how to approach $2\sqrt{3}/\pi = 1.102\ldots$ and prove that this is the best possible. Along the way, these bounds determine the correlation up to a relative error $1+\epsilon$ where $|\epsilon| = 2^{-\Omega(n)}$, in the case $d = p^t - 1$ for some t.

Our proof that there exists a polynomial achieving $|\beta|/D > 1$ has multiple steps. First, we provide in Lemma 2.1 a refined spectral formulation which yields the following key expression for β in Equation (2):

$$\beta = 2 \sum_{k=0}^{D-1} (-1)^k \zeta_p^{r(k)} \cos(\pi(n-2k)/2D), \tag{5}$$

where $r(k)$ is the value of the polynomial on inputs of Hamming weight k.

The advantage of our above Expression (5) for β over the previous expressions in [CGT96, Gre99] is that ours depends only on the values of the symmetric polynomial at the first D Hamming weights. As we show in Lemma 3.4, this grants us complete freedom in the choice of the $r(k)$, in the case $d = p^t - 1 = D - 1$. In other words, for every set of values $r(k), 0 \le k \le D-1$, there exists a symmetric degree-d polynomial achieving those values. (The case of degree $d = p^t - \ell$ for $\ell > 1$ is reduced to the case $\ell = 1$.)

A minute's thought now suggests that in order to maximize $|\beta|$ we should pick $r(k)$ to agree with the sign of $(-1)^k \cos(\pi(n-2k)/2D)$ as much as possible. Specifically:

$$r(k) := \begin{cases} 0 & \text{if } (-1)^k \cos(\pi(n-2k)/2D) \ge 0, \\ (p-1)/2 & \text{if } (-1)^k \cos(\pi(n-2k)/2D) < 0. \end{cases}$$

And in fact we show this choice is best possible for $p = 3$ (Theorem 7.1).

At this point, a somewhat technical result in this paper (Theorem 3.1) shows that for the above choice of r the sum (5) may be rewritten as a simpler expression which does not involve cancelations and is thus easier to bound. Indeed, we then bound this simpler expression in Lemma 3.3 to show $|\beta|/D > 1$. This concludes the overview of the proof of our main Theorem 1.2.

Our complementary results, Theorems 1.3 and 1.4, are proved via a similar two-step approach. That is, we obtain suitable spectral formulations, and then we bound $|\beta|$, this time from above to establish that $|\beta|/D < 1$. (Here the disregard for lower-order terms corresponding to $i > 1$ in (2) yields the requirements that the blocks are large enough.)

For our results on switch-symmetric polynomials we prove that the maximum correlation, for a fixed even degree d, decreases "in steps" as a function of n. That is, it stays the same for $n-1$ and n variables, when n is also odd. Then we show that this is incompatible with (5) for select values of d, using computer search.

The role of computer search. All the main results in this paper, including Theorems 1.2, 1.3, and 1.4 are obtained analytically without any use of computer (a.k.a. brute-force) search. However, this work builds on a computer search by the authors. In this paragraph, we wish the elaborate on this to provide some perspective. First, the authors verified using computer search that symmetric polynomials modulo p have maximum correlation with the Mod q function for various small values of n, d, p, q, except precisely the case $q = 2$ and $d = 2$, cf. §6. This motivated the authors to investigate further the symmetric case. The authors then used computer search to compute a few maximum values for $|\beta|$ in Expression (2), cf. §6. To their surprise, the authors observed that in some cases $|\beta|/D > 1$, and realized that this in particular implies that block-symmetric beats symmetric; whence this paper.

Computer search is frequently used in cryptography and combinatorics, see e.g. [BK10, Rad09]. Despite a few exceptions, e.g. [VW08, Wil07], computer search seems underused in Theoretical Computer Science. We wish to reverse this trend. We believe that the apparent lack of progress on fundamental complexity lower bounds lends itself to computer search, and we see this paper as a step towards a broader use of computer search.

Organization. In §2 we obtain our spectral formulation which refines [CGT96, Gre99], providing in particular an expression for β. Various bounds on β are obtained in §3, establishing our main Theorem 1.2. For readability, some proofs from this section are postponed to §7. §4 contains our complementary results about symmetric beating block symmetric, proving Theorems 1.3 and 1.4. The step-wise behavior of optimal correlation, and switch-symmetric polynomials are discussed in §5, in particular proving Theorem 1.5. For completeness, we report in §6 the results of a computer search which also sparked the development of this paper. A number of open problems is discussed in §8.

2 A spectral formulation

In this section we state and prove our spectral formulation. First we fix some notation. When t is a symmetric polynomial, it can be expressed as a function $r : \mathbb{Z}_p \to \mathbb{Z}_p$, where $r(k) \equiv t(x) \pmod{p}$ exactly when $k = \sum_{i=1}^{n} x_i$. We say that t *is symmetric through* r. Denoting the degree of t by d, it turns out that the function r is periodic, with a period which depends on d, and which we denote by D; that is, for any k, $r(k + D) = r(k)$. When p is prime, we have $D = p^t$ where t is the least integer such that $d < p^t$.

Lemma 2.1 (Spectral expression for correlation)**.** *Let t be a degree-d polynomial modulo p that is symmetric through r. Let D be the smallest power of p greater than d. Then the correlation between t and parity on n variables is*

$$\gamma = \frac{1}{D} \sum_{\ell=1,3,5\ldots D-2} \alpha_\ell^n \beta_\ell, \tag{6}$$

where for every ℓ:

$$\alpha_\ell = \cos(\pi\ell/2D), \tag{7}$$

$$\beta_\ell = 2\sum_{k=0}^{D-1} (-1)^k \zeta_p^{r(k)} \cos(\pi\ell(n-2k)/2D). \tag{8}$$

For simplicity we use the notation β for β_1 throughout this paper.

Since $\max_\ell \alpha_\ell$ is clearly attained for $\ell = 1$, and $|\beta_\ell| \leq 2D$, it follows from Lemma 2.1 that the correlation of a symmetric polynomial is

$$|\gamma| \leq \frac{1}{D}\alpha_1^n \frac{D}{2} 2D \leq D\alpha_1^n. \tag{9}$$

The proof of Lemma 2.1 uses the following lemma from [Gre99]. For completeness, we remark that the latter is proved by first rewriting the correlation (cf. Definition 1.1) as

$$\gamma = \frac{1}{2^n}\sum_{j=0}^{n} \binom{n}{j} \zeta_q^j \zeta_p^{r(j)},$$

and then essentially rewriting $\binom{n}{j}$ as a sum of complex numbers via the binomial theorem.

Lemma 2.2 (Lemma 2.6 in [Gre99])**.** *Let t be polynomial modulo p that is symmetric through r, and let r have period D. Then*

$$\gamma = \frac{1}{2^n}\frac{1}{qD}\sum_{\ell=0}^{qD-1} (1+\zeta_{qD}^{-\ell})^n \sigma^{(\ell)}, \tag{10}$$

where

$$\sigma^{(\ell)} = \sum_{k=0}^{qD-1} \zeta_q^k \zeta_p^{r(k)} \zeta_{qD}^{k\ell}. \tag{11}$$

Moreover, $\sigma^{(\ell)} = 0$ if $\ell + D \not\equiv 0 \mod q$.

Proof of Lemma 2.1. We use the expression for γ in Lemma 2.2, in the setting $q = 2$, corresponding to parity. Because D is odd, from the lemma we know that in the sum for γ we can disregard the even values of ℓ. We may also disregard the value $\ell = D$, since $(1 + \zeta_{2D}^{-D}) = 0$.

Pairing off each term with $0 < \ell < D-1$ with $2D-\ell$, we therefore find,

$$\begin{aligned}
\gamma &= \frac{1}{2^n}\frac{1}{2D}\sum_{\ell=1,3,5\ldots D-2}\left[(1+\zeta_{2D}^{-\ell})^n\sigma^{(\ell)} + (1+\zeta_{2D}^{\ell})^n\sigma^{(2D-\ell)}\right] \\
&= \frac{1}{2^n}\frac{1}{2D}\sum_{\ell=1,3,5\ldots D-2}(\zeta_{4D}^{-\ell}+\zeta_{4D}^{\ell})^n(\zeta_{4D}^{-n\ell}\cdot\sigma^{(\ell)}) + (\zeta_{4D}^{-\ell}+\zeta_{4D}^{\ell})^n(\zeta_{4D}^{n\ell}\cdot\sigma^{(2D-\ell)}) \\
&\quad \text{(using } 1+z = (\sqrt{z^{-1}}+\sqrt{z})\sqrt{z}; \quad 1+z^{-1} = (\sqrt{z^{-1}}+\sqrt{z})\sqrt{z^{-1}}) \\
&= \frac{1}{2D}\sum_{\ell=1,3,5\ldots D-2}\cos(\pi\ell/2D)^n(\zeta_{4D}^{-n\ell}\cdot\sigma^{(\ell)} + \zeta_{4D}^{n\ell}\cdot\sigma^{(2D-\ell)}) \\
&= \frac{1}{2D}\sum_{\ell=1,3,5\ldots D-2}\cos(\pi\ell/2D)^n\sum_{k=0}^{2D-1}(-1)^k\zeta_p^{r(k)}\left(\zeta_{4D}^{-n\ell}\zeta_{2D}^{k\ell} + \zeta_{4D}^{n\ell}\zeta_{2D}^{k(2D-\ell)}\right) \\
&\quad \text{(using } \zeta_{4D}^{-n\ell}\zeta_{2D}^{k\ell} + \zeta_{4D}^{n\ell}\zeta_{2D}^{k(2D-\ell)} = \zeta_{4D}^{-n\ell+2k\ell} + \zeta_{4D}^{n\ell-2k\ell}) \\
&= \frac{1}{D}\sum_{\ell=1,3,5\ldots D-2}\cos(\pi\ell/2D)^n\sum_{k=0}^{2D-1}(-1)^k\zeta_p^{r(k)}\cos(\pi\ell(n-2k)/2D) \\
&= \frac{1}{D}\sum_{\ell=1,3,5\ldots D-2}\cos(\pi\ell/2D)^n 2\sum_{k=0}^{D-1}(-1)^k\zeta_p^{r(k)}\cos(\pi\ell(n-2k)/2D) \\
&= \frac{1}{D}\sum_{\ell=1,3,5\ldots D-2}\alpha_\ell^n\beta_\ell,
\end{aligned}$$

where in the second-to-last equality we use the following. First, $(-1)^{k+D} = -(-1)^k$ because k is odd. Second, $r(k) = r(k+D)$ because r has period D. Finally, $\cos(\pi\ell(n-2(k+D))/2D) = \cos(\pi\ell(n-2k)/2D - \pi\ell) = -\cos(\pi\ell(n-2k)/2D)$ because ℓ is odd. □

3 Block-symmetric beats symmetric

Here we establish that block symmetric polynomials beat symmetric. First we rewrite the expression for β when r is the specific function discussed in §1.2. We will make contact between this r and the r of period D that represents a symmetric polynomial t later. For now, it is not necessary to exploit the periodicity of r, so we take it to be any function $r : \mathbb{Z}_D \to \mathbb{Z}_p$.

Theorem 3.1. *Let p, c be any integers, and let D be any odd integer. Let $v = (D-1)/2 = \lfloor D/2 \rfloor$, $u_1 = \lfloor v/2 \rfloor$ and $u_2 = \lceil v/2 \rceil$. If n is even there exists an $r : \mathbb{Z}_D \to \mathbb{Z}_p$ such that,*

$$\beta = (-1)^{n/2}\frac{2}{\sin\left(\frac{\pi}{D}\right)}\left[\sin\left(\frac{2u_1+1}{D}\pi\right) - \zeta_p^c\sin\left(\frac{2u_2}{D}\pi\right)\right]. \tag{12}$$

If n is odd there exists an $r : \mathbb{Z}_D \to \mathbb{Z}_p$,

$$\beta = (-1)^{(n-1)/2}(1-\zeta_p^c)\frac{\sin\left(\frac{v\pi}{D}\right)}{\sin\left(\frac{\pi}{2D}\right)}. \tag{13}$$

The proof of the above theorem is in §7.

The special values for β given in Theorem 3.1 play an important role.

Definition 3.2 ($\beta^\star$)**.** *We denote by $\beta^\star = \beta^\star(n \mod 2, p, c, D)$ the value for β given in Theorem 3.1.*

Lemma 3.3 (Bounds on $\beta^\star$)**.** *Let $c := (p-1)/2$. Then:*
For any p, we have $\lim_{D\to\infty} |\beta^\star(D)/D| = 4\sin(\pi c/p)/\pi \geq 2\sqrt{3}/\pi > 1.102$.
For $p = D = 3$, we have $|\beta^\star| = 3$ for n even, and $|\beta^\star| = 2\sqrt{3}$ if n is odd.
Finally, for any $p \geq 3$ and $D \geq 5$, we $|\beta^\star|/D > 1.04$.

The proof of this lemma is in §7.

The following lemma shows that a symmetric polynomial of degree d can be designed to output any $d+1$ desired values on inputs of hamming weight $0, \ldots, d$. This also follows from a more general result by Bhatnagar, Gopalan, and Lipton [BGL06, Corollary 2.7]. The following proof of this case is more elementary because it avoids Lucas' theorem.

Lemma 3.4. *For every integers $d \geq 0$ and $n \geq d$, and any integers $a_0, a_1, \ldots, a_d$, there is a symmetric polynomial f_d of degree d in n variables and with integer coefficients such that for any input $x \in \{0,1\}^n$ of Hamming weight $|x| \leq d$, $f_d(x) = a_{|x|}$.*

Proof. By induction on d. Let $f_0 := a_0$. Given f_{d-1}, define $f_d(x) := f_{d-1}(x) + (a_d - f_{d-1}(w_d))\sum_{i_1,\ldots,i_d} x_{i_1}\cdots x_{i_d}$, where $w_d \in \{0,1\}^n$ is any input with Hamming weight d.

Note that f_d is symmetric and has degree d. On inputs $x \in \{0,1\}^n$ of Hamming weight $< d$, each monomial $x_{i_1}\cdots x_{i_d}$ will be 0 and so $f_d(x) = f_{d-1}(x) = a_{|x|}$. Finally, on any input x of Hamming weight d exactly one monomial $x_{i_1}\cdots x_{i_d}$ will be 1, and so $f_d(x) = f_{d-1}(x) + a_d - f_{d-1}(w_d) = a_d$. □

The next lemma summarizes the existence of symmetric polynomials whose β approaches $\beta^\star$.

Lemma 3.5. *For every n, odd p, and D a power of p, and for every $\ell \geq 0$, there exists a symmetric polynomial of degree $d = D-1-\ell$ in n variables with $|\beta| \geq |\beta^\star| - 2|\zeta_p^{(p-1)/2} - 1|\ell \geq |\beta^\star| - 4\ell$.*

Note the case $\ell = 0$ is of special interest; in this case we in fact achieve $\beta = \beta^\star$. It should be possible to optimize the constant 4 somewhat.

Proof. Let $r : \mathbb{Z}_D \to \mathbb{Z}_p$ be the function guaranteed by Theorem 3.1.

Obtain from Lemma 3.4 a symmetric polynomial f of degree $D-1-\ell$ that on inputs x of Hamming weight $|x| < D-\ell$ gives value $f(x) = r(|x|)$. Let $r'(|x|)$ denote the value of $f(x)$ on inputs x of Hamming weight $|x|$, for $|x| < D$. The value of $|\beta|$ for f is now

$$\begin{aligned}&\left|\beta^\star - 2\sum_{k=0}^{D-1}(-1)^k\left(\zeta_p^{r(k)} - \zeta_p^{r'(k)}\right)\cos\left(\frac{2k-n}{2D}\pi\right)\right|\\ =&\left|\beta^\star - 2\sum_{k:r'(k)\neq r(k)}(-1)^k\left(\zeta_p^{r(k)} - \zeta_p^{r'(k)}\right)\cos\left(\frac{2k-n}{2D}\pi\right)\right|\\ \geq& |\beta^\star| - 2|\zeta_p^{(p-1)/2} - 1|\ell,\end{aligned}$$

using $|\cos(x)| \leq 1$ and $\max_{a\neq b}|\zeta_p^a - \zeta_p^b| = |\zeta_p^{(p-1)/2} - 1|$. □

We now prove our main theorem.

Theorem 1.2 (Block-symmetric beats symmetric.)**.** *For every odd $p \geq 3$, every n, and every d that satisfies $p^t > d \geq 0.995p^t - 1$ for some $t \geq 1$, let $|\gamma_b|$ be the maximum correlation between degree-d block-symmetric polynomials in n variables modulo p and the parity function, and let $|\gamma_s|$ be the maximum for symmetric polynomials instead. Then,*

$$\frac{|\gamma_b|}{|\gamma_s|} \geq \frac{1.01^{\lfloor n/(cd^2\lg d)\rfloor}}{pd},$$

where $c > 0$ depends only on p.

Proof. First recall that from Lemma 2.1 the correlation of degree-d symmetric polynomials is in absolute value $\leq D\alpha_1^n \leq pd\alpha_1^n$, cf. Equation (9).

The rest of the proof constructs a block-symmetric polynomial of degree d with correlation $\geq \alpha_1^n(1+\epsilon)^{\lfloor n\epsilon/d^2\lg d\rfloor}$, from which the theorem follows. The construction proceeds by first exhibiting a symmetric polynomial with correlation $\geq \alpha_1^b(1+\epsilon)$, for any large enough b, and then boosting the correlation by dividing the n variables into blocks of size b.

Combining the above Lemma 3.5 with the last bound in Lemma 3.3, we obtain that there exists a symmetric polynomial in b variables with, say, $|\beta|/D > 1.02$ as long as the degree d satisfies $d = D-1-\ell$ for $1.04 - 4\ell/D > 1.02$. This is implied by $d \geq 0.995D - 1$. This is the desired polynomial. (In the case $p = 3$ and $d = 2$, which is also in [Gre04], we need to take b odd, which is sufficient for the proof.)

The rest of this proof shows that when b is sufficiently large, the lower-order terms lower $|\beta|/D$ to no more than 1.01.

Specifically, recall from Equation (6) that the correlation of this polynomial with parity on b variables is

$$\begin{aligned}\geq&\alpha_1^b\left(|\beta|/D - \frac{1}{2}\max_{\ell=3,5,\ldots,D-2}|\beta_\ell|(\alpha_\ell/\alpha_1)^b\right)\\ \geq&\alpha_1^b\left(|\beta|/D - D(\alpha_3/\alpha_1)^b\right),\end{aligned}$$

using that $|\beta_\ell| \leq 2D$ for any polynomial and ℓ, as is apparent from Equation (8), and that α_ℓ, for $\ell = 3, 5, \ldots, D-2$ has its maximum for $\ell = 3$, as is again apparent from Equation (7). Now, using the triple-angle formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ and the small-angle approximation $\cos^2\theta \leq 1 - \theta^2/3$ we bound α_3/α_1 as follows:

$$\alpha_3/\alpha_1 = 4\cos^2(\pi/2D) - 3 \leq 1 - \pi^2/D^2.$$

Hence, recalling $D \leq pd$, for any $b \geq cd^2 \lg d$ for a sufficiently large constant c depending only on p, we have $|\beta|/D - D(\alpha_3/\alpha_1)^b \geq 1.01$, and so the correlation $\geq 1.01\alpha_1^b$.

To obtain the desired block-symmetric polynomial, divide the n variables into $\lfloor n/(cd^2 \lg d)\rfloor$ blocks of $\geq cd^2 \lg d$ variables each.

Apply in each block the symmetric polynomial just constructed with correlation $\geq 1.01\alpha_1^b$. Correlation multiplies across blocks, as is evident from Equation (1). Hence we get the correlation

$$\geq \left(1.01\alpha_1^b\right)^{\lfloor n/(cd^2 \lg d)\rfloor} = 1.01^{\lfloor n/(cd^2 \lg d)\rfloor}\alpha_1^n,$$

concluding the proof. □

4 When symmetric beats large-block-symmetric

In this section we present two settings where symmetric polynomials beat block-symmetric with large blocks.

4.1 Degree $d = D/p$

We find, for odd prime p, that if the degree is D/p, symmetric polynomials beat block-symmetric. The following is the main technical lemma needed for the proof.

Lemma 4.1. *Let p be an odd prime, and $r(k)$ represent a symmetric polynomial of degree $d = p^{t-1}$, $t > 1$. Let $D = p^t$ denote the period of $r(k)$. Then $|\beta| < D$. Moreover, there is a polynomial with $|\beta| > 0$.*

Proof. Start with,

$$\beta = 2\sum_{k=0}^{D-1}(-1)^k \zeta_p^{r(k)} \cos\left(\frac{2k-n}{2D}\pi\right).$$

When $d = D/p$, wlog we may write $r(k) = c\binom{k}{D/p} + r'(k)$, where the degree of the polynomial for r' is at most $D/p-1$, and hence the period of $r'(k)$ is D/p. By Lucas' theorem, for each ℓ with $0 \leq \ell \leq p-1$, we have $\binom{k}{D/p} \equiv \ell \pmod p$ for $\ell D/p \leq k < (\ell+1)D/p$. Hence for the same choices of ℓ and $\ell D/p \leq k < (\ell+1)D/p$, $r(k) = r'(k) + \ell$. Therefore,

$$\beta \;=\; 2\sum_{\ell=0}^{p-1}\zeta_p^{c\ell}\sum_{k=\ell D/p}^{(\ell+1)D/p-1}(-1)^k \zeta_p^{r'(k)}\cos\left(\frac{2k-n}{2D}\pi\right).$$

Via the change of variable $k \mapsto k+\ell D/p$ in the inner sum, and using the facts that $(-1)^{\ell D/p} = (-1)^\ell$ (since D/p is odd) and $r'(k+\ell D/p) = r'(k)$, we find

$$\sum_{k=\ell D/p}^{(\ell+1)D/p-1} (-1)^k \zeta_p^{r'(k)} \cos\left(\frac{2k-n}{2D}\pi\right) = (-1)^\ell \sum_{k=0}^{D/p-1} (-1)^k \zeta_p^{r'(k)} \cos\left(\frac{2k-n}{2D}\pi + \ell\pi/p\right).$$

Let us now perform the outer sum (over ℓ) in β:

$$s_k = \sum_{\ell=0}^{p-1} (-1)^\ell \zeta_p^{c\ell} \cos\left(\theta + \ell\pi/p\right).$$

where we set $\theta = \frac{2k-n}{2D}\pi$. We now compute s_k.

$$\begin{aligned} s_k &= \frac{1}{2}\sum_{\ell=0}^{p-1}(-1)^\ell \zeta_p^{c\ell}(e^{i\theta+\ell i\pi/p} + e^{-i\theta-\ell i\pi/p}) \\ &= \frac{1}{2}e^{i\theta}\sum_{\ell=0}^{p-1}(-1)^\ell\zeta_p^{c\ell}\zeta_{2p}^{\ell} + \frac{1}{2}e^{-i\theta}\sum_{\ell=0}^{p-1}(-1)^\ell\zeta_p^{c\ell}\zeta_{2p}^{-\ell}. \end{aligned}$$

Now $(-1)^\ell = \zeta_{2p}^{p\ell}$, so

$$(-1)^\ell\zeta_p^{c\ell}\zeta_{2p}^{\ell} = \zeta_p^{c\ell}\zeta_{2p}^{(p+1)\ell} = \zeta_p^{c\ell}\zeta_p^{\ell(p+1)/2} = \zeta_p^{(c+(p+1)/2)\ell}.$$

Similarly, observe that $(-1)^\ell\zeta_p^{\ell}\zeta_{2p}^{-\ell} = \zeta_p^{(c+(p-1)/2)\ell}$. We are thus faced with the two sums,

$$\sum_{\ell=0}^{p-1}\zeta_p^{(c+(p+1)/2)\ell} \quad \text{and} \quad \sum_{\ell=0}^{p-1}\zeta_p^{(c+(p-1)/2)\ell}. \tag{14}$$

Taking $c = (p-1)/2$, we find that the first sum is p and the second is 0. If $c = (p+1)/2$, the first sum is 0 and the second is p. Both choices for c yield the same bound for β. Any other choice for c implies both sums in (14) are 0, which yields $\beta = 0$. (This includes $c = 0$, which implies that $|\beta| = 0$ when the period of r is $D/p - 1$.)

Thus take, for example, $c = (p-1)/2$. Then, since $\frac{p}{2}e^{i\theta} = \frac{p}{2}e^{i\frac{2k-n}{2D}\pi} = \frac{p}{2}\zeta_{4D}^{2k-n}$, it follows that,

$$\beta = p\sum_{k=0}^{D/p-1}(-1)^k\zeta_p^{r'(k)}\zeta_{4D}^{2k-n}. \tag{15}$$

Each of the terms in the sum is of unit norm, so $|\beta| \leq p \cdot D/p = D$.

We now show that this inequality is strict, i.e., $|\beta| < D$. For the only way we can have $|\beta| = D$ would be for all terms in Eq. (15) to be the same. Taking the first and the last, this would imply $\zeta_p^{r'(0)}\zeta_{4D}^{-n} = \zeta_p^{r'(D/p-1)}\zeta_{4D}^{2D/p-2-n}$, which implies $\zeta_p^{r'(0)-r'(D/p-1)}\zeta_{2p}^{-1} = \zeta_{2D}^{-1}$. But the latter implies $\zeta_{2D}^{2p} = \zeta_D^p = 1$, which is false since $D > p$.

To show the "moreover" part that there exists a polynomial for which $|\beta| > 0$, note that by Lemma 3.4 we are free to set the values of $r'(k)$ any way we please. Obviously, one can set them so that $|\beta| > 0$, because given any setting resulting in $|\beta| = 0$ we can change a single value to obtain $|\beta| > 0$. □

Theorem 1.3 (Symmetric beats large-block-symmetric for $d = p^t$.)**.** *Fix any odd prime p and degree $d = p^t$. There is a constant c such that for $n \geq c$, any block-symmetric polynomial with block-size $\geq c$ correlates with parity worse than symmetric.*

Proof. Let $D = p^{t+1}$. By Lemma 4.1, in any block of size $b \geq c$, the maximum correlation is $\alpha_1^b(|\beta|/D)(1+\epsilon)$, for some $|\beta|/D \in (0,1)$ and some real number ϵ that approaches 0 in absolute value as c increases.

If there are m blocks, the correlation of a block-symmetric polynomial is $\leq \alpha_1^n(|\beta|/D)^m(1+\epsilon)^m$. This is $< (|\beta|/D)\alpha_1^n(1+\epsilon)$ for any $m > 1$ and sufficiently large c. □

4.2 Other moduli

The next theorem shows that the leading terms in the expression for γ (see Eq. (10)) only pair up (as they do in the derivation of Eq. (6)) when $q = 2c$ for $c \in \{0, \dots, q-1\}$ such that $c \equiv -D$ modulo q. In particular, $q = 2$ is the only prime for which they pair up. Then we note that in the case of $q = 3$ and $p = 2$, when the terms do not pair up, the coefficient β of the leading term is small, i.e., $|\beta| < qD$. This implies that block-symmetric polynomials, with large enough blocks, correlate with the Mod$_3$ function exponentially worse than symmetric.

Theorem 4.2 (When things don't pair up)**.** *Let t be a polynomial of degree $d \geq 2$ modulo $p = 2$ that is symmetric through r. Let D be the smallest power of p greater than d. Then the correlation between t and the Mod$_q$ function, for $q = 3$ is*

$$\gamma = \frac{1}{qD}\sum_{\ell=0}^{qD-1} \cos(\pi\ell/(qD))^n \zeta_{2qD}^{-\ell n}\sigma^{(\ell)},$$

where σ is defined as in Lemma 2.2.

Moreover, there is exactly one value ℓ' of ℓ such that $\sigma^{(\ell)} \neq 0$ and $|\cos(\pi\ell/(qD))^n|$ is maximized. Furthermore, this value satisfies

$$0 < \max_t |\sigma^{(\ell')}| < qD.$$

Note that the restriction $d \geq 2$ is necessary, for there is no useful distinction between symmetric and block-symmetric polynomials for $d = 1$.

Proof. Beginning with Lemma 2.2, and using similar manipulations as before, we find,

$$\begin{aligned}\gamma =&\frac{1}{2^n}\frac{1}{qD}\sum_{\ell=0}^{qD-1}(\zeta_{2qD}^{\ell}+\zeta_{2qD}^{-\ell})^n\zeta_{2qD}^{-\ell n}\sigma^{(\ell)}\\ =&\frac{1}{qD}\sum_{\ell=0}^{qD-1}\cos(\pi\ell/(qD))^n\zeta_{2qD}^{-\ell n}\sigma^{(\ell)}.\end{aligned}$$

Now recall from the same lemma that $\sigma^{(\ell)}\neq 0 \Rightarrow \ell\equiv -D$ modulo q. The latter are the values $\ell=c+sq$ where $c\in\{1,\ldots,q-1\}$ satisfies $c\equiv -D$ modulo q, and $s\in\{0,1,\ldots,D-1\}$. By inspection, the corresponding values $|\cos(\pi\ell/(qD))|$ are maximized for $s=0$ or $s=D-1$. We now argue that these values of $|\cos(\pi\ell/(qD))|$ are different (in fact, all are). Indeed, they are equal exactly when

$$\frac{\pi c}{qD}=\pi-\left(\frac{\pi c}{qD}+\frac{\pi(D-1)}{D}\right)\Leftrightarrow 2c=q.$$

Hence, asymptotically, when q is odd, exactly one $\sigma^{(\ell)}$ coefficient matters. In the case $p=2,q=3$, the one that matters is given either by $\ell=1$ (for $D=2,8,32,\ldots$) or by $\ell=qD-1$ (for $D=4,16,64,\ldots$). In this proof we only use that these values of ℓ are odd.

Fix any odd ℓ. We proceed to bound $|\sigma^{(\ell)}|$ from below and above.

To bound from below for some polynomial t, it is convenient to rewrite, for any ℓ,

$$\begin{aligned}\sigma^{(\ell)}&=\sum_{k=0}^{qD-1}\zeta_q^k\zeta_p^{r(k)}\zeta_{qD}^{k\ell}\\ &=\sum_{k=0}^{qD-1}\zeta_p^{r(k)}\zeta_{qD}^{k(D+\ell)}\\ &=\sum_{k=0}^{qD-1}\zeta_p^{r(k)}\zeta_{D}^{ku}\\ &=q\sum_{k=0}^{D-1}\zeta_p^{r(k)}\zeta_{D}^{ku}\end{aligned}$$

where we used that $D+\ell=qu$ for some u as noted previously, that $r(k)$ has period D, and that $\zeta_D^{(k+jD)u}=\zeta_D^{ku}$ for any j. (Note that u may not be the same as s.)

Note that since D is even, ℓ is odd, and q is odd, we have from the above equation $D+\ell=qu$ that u is odd as well.

Recall that $d\geq D/2$. We consider symmetric polynomials t of degree $D/2$ which have the highest-degree terms. Such a t may be written as a polynomial t' of degree $<D/2$ plus the polynomial $\sum_{i_1,\ldots,i_{D/2}}x_{i_1}\cdots x_{i_{D/2}}$. We have that t and t' are symmetric respectively through r and r' which satisfy

$$r(k)=r'(k)+\binom{k}{D/2}.$$

Also note that r' has period $D/2$. Hence, by Lucas' theorem

$$r(k + D/2) = r(k) + 1,$$

for any $0 \leq k < D/2$. This allows us to rewrite:

$$\begin{aligned}\sigma^{(\ell)} &= q \sum_{k<D/2} \zeta_p^{r'(k)} \zeta_D^{ku} + q \sum_{k<D/2} \zeta_p^{r'(k)+1} \zeta_D^{ku} \zeta_D^{uD/2} \\ &= q \sum_{k<D/2} \zeta_p^{r'(k)} \zeta_D^{ku} (1 - (-1)^u) \\ &= 2q \sum_{k<D/2} \zeta_p^{r'(k)} \zeta_D^{ku}.\end{aligned}$$

At this point we can apply Lemma 3.4 to argue that for any choice of the $D/2$ values $r'(k)$ we can find a polynomial t' symmetric through the same r. Hence, for some t, $|\sigma^{(\ell)}| > 0$.

We now turn to bounding $|\sigma^{(\ell)}|$ from above, similarly to the proof of Lemma 4.1. Note $|\sigma^{(\ell)}| \leq qD$ trivially. Recall $\sigma^{(\ell)}$ is a sum of qD complex numbers of unit norm. Hence the only way in which $|\sigma^{(\ell)}| = qD$ is that these vectors are all equal. However, for $k = 0$ we get the number $\zeta_p^{r(0)}$, whereas for $k = 1$ we get $\zeta_{qD}^{D+\ell} \zeta_p^{r(1)}$. Since D is even and ℓ is odd, $D + \ell$ is odd. Therefore, $D + \ell \not\equiv qD/2$ modulo qD, using that $d \geq 2$ and so $D \geq 4$. This implies that $\zeta_{qD}^{D+\ell} \zeta_p^{r(1)} \neq \zeta_p^{r(0)}$. □

We note that the upper bound $|\sigma^{(\ell)}| < qD$ can be generalized to any odd q for sufficiently large D. Indeed, reasoning as in the proof we get that $|\sigma^{(\ell)}| < qD$ implies $\zeta_{qD}^{D+\ell} = \zeta_2^b$ for some $b \in \mathbb{Z}_2$. In turn, this is equivalent to $\zeta_{qD}^{D+\ell} \zeta_{qD}^{-qbD/2} = 1$. Since $p = 2$, $D = 2^h$ for some h. Hence this last equality is equivalent to $\ell + 2^h - qb2^{h-1} \equiv 0 \pmod{q2^h}$. This in turn implies that $\ell \equiv 0 \pmod{2^{h-1}}$. If $\ell = c$, this is a clear contradiction for sufficiently large D (since $1 \leq c \leq q - 1$). On the other hand, if $\ell = c + q(D - 1) = c + q(2^h - 1)$, then $c - q \equiv 0 \pmod{2^{h-1}}$ or, equivalently, $q - c \equiv 0 \pmod{2^{h-1}}$. But $1 \leq |q - c| \leq q - 1$, so again we arrive at a contradiction for large enough D.

Using the same reasoning presented in the proof of Theorem 1.2, Theorem 4.2 implies that block-symmetric polynomials, for sufficiently large blocks, correlate worse than symmetric.

Theorem 1.4 (Symmetric mod 2 beats large-block-symmetric in computing Mod 3.)**.** *For any fixed degree d, block-symmetric polynomials modulo* 2 *with sufficiently large blocks have worse correlation with the Mod*$_3$ *function than symmetric.*

5 Step-wise decay and switch-symmetric

In this section we give a different family of polynomials that beats symmetric at correlating with parity. Here it is convenient to think of variables over $-1, 1$ as opposed to $0, 1$.

Let

$$S(t,n) = \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \zeta_p^{t(x)},$$

where t is a polynomial in $\mathbb{Z}_p[x_1, \ldots, x_n]$.

Definition 5.1. *A polynomial is* even *if it only contains monomials of even degree. A polynomial is* odd *if it only contains monomials of odd degree.*

We first prove the following theorem in §5.1.

Theorem 5.2. *For every even n, even d, and odd p: $\max_t |S(t, n-1)| = \max_t |S(t,n)|$ where each maximum is over polynomials mod p of degree d.*

Moreover, let $t \in \mathbb{Z}_p[x_2, \ldots, x_n]$ be a polynomial in $n-1$ variables. Write $t = e + k$ where e is even and k is odd. Then $|S(t, n-1)| = |S(e + x_1 k, n)|$.

Then we argue in §5.2 that Theorem 5.2 is incompatible with the assumption that symmetric polynomials are optimal, for certain degrees which include some not covered by the block-symmetric result. And we derive an explicit family of polynomials that beat symmetric.

5.1 Proof of Theorem 5.2

We rely on two Lemmas below which are similar to Lemmas 3.4 and 3.5 in [Gre04]. Throughout this section p denotes any fixed odd integer.

Lemma 5.3 (Even w.l.o.g.)**.** *Let n be even. Let $t \in \mathbb{Z}_p[x_1, ..., x_n]$ be a polynomial. Write $t = e + k$, where e is even, k odd. Then*

$$|S(t,n)| \leq \max\{|S(e + x_1 k, n)|, |S(e - x_1 k, n)|\}.$$

Proof. We have:

$$\begin{aligned}
S(t,n) &= \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \zeta_p^{e(x)+k(x)} \\
&= \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \zeta_p^{e(x)-k(x)} \\
&= \frac{1}{2} \cdot \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \zeta_p^{e(x)} (\zeta_p^{k(x)} + \zeta_p^{-k(x)}) \\
&= \frac{1}{2} \cdot \frac{1}{2^n} \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^{n} x_i \right) \zeta_p^{e(x)} (\zeta_p^{x_1 k(x)} + \zeta_p^{-x_1 k(x)}),
\end{aligned}$$

where in the second equality we made the substitution $x_i \mapsto -x_i$, and in the last we used the fact[1] that $\zeta_p^{k(x)} + \zeta_p^{-k(x)} = \zeta_p^{x_1 k(x)} + \zeta_p^{-x_1 k(x)}$ for $x_1 \in \{1, -1\}$. Now by the triangle inequality,

$$\begin{aligned} |S(t,n)| &\leq \frac{1}{2} \cdot \frac{1}{2^n} \left| \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^n x_i \right) \zeta_p^{e(x)+x_1 k(x)} \right| + \frac{1}{2} \cdot \frac{1}{2^n} \left| \sum_{x \in \{1,-1\}^n} \left(\prod_{i=1}^n x_i \right) \zeta_p^{e(x)-x_1 k(x)} \right| \\ &= \frac{1}{2} |S(e + x_1 k, n)| + \frac{1}{2} |S(e - x_1 k, n)|, \end{aligned}$$

as desired. □

Lemma 5.4 (($n-1$)-var same as n-var, even). *Let n be even. Let $t \in \mathbb{Z}_p[x_2, ..., x_n]$ be $t = e + k$ where e is even, k odd. Then the (even) polynomial $e + x_1 k \in \mathbb{Z}_p[x_1, \ldots, x_n]$ satisfies*

$$S(e + x_1 k, n) = S(e + k, n - 1).$$

Conversely, let $t \in \mathbb{Z}_p[x_1, ..., x_n]$ be even. Write t as $t = e + x_1 k$, then

$$S(t, n) = S(e + k, n - 1).$$

Proof. Let $t(x) = e_2(x) + x_1 k_2(x)$ be even, where $e_2 \in \mathbb{Z}_p[x_2, \ldots, x_n]$ and $k_2 \in \mathbb{Z}_p[x_2, \ldots, x_n]$ only depend on $x_2, \ldots, x_n$. Then, performing the sum over x_1,

$$\begin{aligned} S(t,n) =& \frac{1}{2^n} \sum_{x \in \{1,-1\}^{n-1}} \left(\prod_{i=2}^n x_i \right) \zeta_p^{e_2(x)} \cdot \zeta_p^{k_2(x)} - \frac{1}{2^n} \sum_{x \in \{1,-1\}^{n-1}} \left(\prod_{i=2}^n x_i \right) \zeta_p^{e_2(x)} \cdot \zeta_p^{-k_2(x)} \\ =& \frac{1}{2^{n-1}} \sum_{x \in \{1,-1\}^{n-1}} \left(\prod_{i=2}^n x_i \right) \zeta_p^{e_2(x)+k_2(x)}, \end{aligned}$$

where in the second equality we apply the transformation $x_i \mapsto -x_i$ to the second summand, which note keeps e_2 the same, but flips the sign of k_2 and $\prod_{i=2}^n x_i$.

This establishes both implications, since we can work forwards or backwards in the chain of equalities, and e_2 and k_2 are completely general polynomials of $n-1$ variables (consisting of even and odd degree monomials, respectively). □

In the above two lemmas observe that, if $deg(t) = d$ where d is even, then $deg(x_1 k) \leq d$. The combination of the lemmas and this observation shows that for n even, the values $|S(t, n-1)|$ over t of degree d are the same as the values $S(t,n)$ over t of degree d. This proves the first claim in Theorem 5.2. The second claim is Lemma 5.4.

[1] This trick is due to E. M. Luks [Luk03].

5.2 Switch-symmetric beats symmetric

We call a polynomial t *optimal* if it maximizes $|S(t,n)|$ among a pre-specified set of polynomials. Theorem 5.2 shows that, for even degrees, the correlation of optimal polynomials decays “in steps.” Perhaps surprisingly, the correlation of symmetric polynomials mod 3 with parity also exhibits this behavior for degree 6 and 8 for every n we managed to compute. Hence, for example, the belief that symmetric polynomials are optimal for degree 6 is consistent with the theorem.

For other degrees and moduli however we can prove that for all sufficiently large n the correlation does not decay in steps, and hence symmetric polynomials cannot be optimal.

Moreover, using the second claim in Theorem 5.2 we can get our hands on a specific family of polynomials that beat symmetric. We define this family next.

Definition 5.5. *A* switch-symmetric *polynomial $t \in \mathbb{Z}_p[x_1,\ldots,x_n]$ is a polynomial of the form $t = x_1 s + s'$ where $s, s' \in \mathbb{Z}_p[x_2,\ldots,x_n]$ are symmetric polynomials.*

Theorem 1.5 (Switch-symmetric beats symmetric)**.** *Let $(d,p) \in \{(4,3),(10,3),(6,5)\}$. For all sufficiently large, even n there exists a degree-d switch-symmetric polynomial mod p over n variables that correlates with parity better than degree-d symmetric polynomials.*

Proof. We have computed by brute force the maximum values of $|\beta|$ for (d,p). Refer to Table 1 (further discussed in Section 6) for the computed values in the case of $p = 3$. We have verified that this value is independent from n. Recalling now Expression (6), and the fact that $(\alpha_\ell/\alpha_1) < 1$ for $\ell > 1$, and that the $|\beta_\ell|$ only depend on a finite number of values of n and hence are bounded, we see that the correlation of optimal symmetric polynomials over n variables is strictly less than that over $n-1$ variables. By the second part of Theorem 5.2 we can devise a switch-symmetric polynomial over n variables that has the same correlation as the optimal symmetric polynomial over $n-1$ variables, thus proving the theorem. □

Note that from the above argument switch-symmetric beats symmetric by only a constant factor, and only for even n, as opposed to the exponential factor of block symmetric, which also applies to every n. However, it is conceivable that this constant-factor saving could be boosted to an exponential saving that beats even block-symmetric polynomials, by forming block-switch-symmetric polynomials: polynomials divided up in blocks, where in each bock you have a switch-symmetric polynomial. But at the moment the different ranges of d in our results on switch- and block-symmetric polynomials obstruct their combination.

6 Computer search

Table 1 reports the maximum values of β in Eq. (8) for $p = 3$. These values are computed going over every symmetric polynomial (represented as $d+1$ coefficients), and exploiting the fact that β only depends on $n \mod 4D$, as is evident from Equation (8). No particular optimization was used in this computation, which can be reproduced easily.

$d = 2, D = 3$	$\lvert\beta\rvert \approx \begin{cases} 3.4641 & \text{if } n \text{ even} \\ 3 & \text{if } n \text{ odd} \end{cases}$
$3 \leq d \leq 4, D = 9$	$\lvert\beta\rvert \approx 7.5963$
$d = 5, D = 9$	$\lvert\beta\rvert \approx \begin{cases} 8.5192 & \text{if } n \text{ even} \\ 8.6382 & \text{if } n \text{ odd} \end{cases}$
$d = 6, D = 9$	$\lvert\beta\rvert \approx \begin{cases} 8.7714 & \text{if } n \text{ even} \\ 8.6382 & \text{if } n \text{ odd} \end{cases}$
$d = 7, D = 9$	$\lvert\beta\rvert \approx \begin{cases} 9.6877 & \text{if } n \text{ even} \\ 9.8229 & \text{if } n \text{ odd} \end{cases}$
$d = 8, D = 9$	$\lvert\beta\rvert \approx \begin{cases} 9.9745 & \text{if } n \text{ even} \\ 9.8229 & \text{if } n \text{ odd} \end{cases}$
$9 \leq d \leq 10, D = 27$	$\lvert\beta\rvert \approx 22.379$
$11 \leq d \leq 14, D = 27$	$\lvert\beta\rvert \approx \begin{cases} 22.652 & \text{if } n \text{ even} \\ 22.686 & \text{if } n \text{ odd} \end{cases}$
$15 \leq d \leq 16, D = 27$	$\lvert\beta\rvert \approx \begin{cases} 25.410 & \text{if } n \text{ even} \\ 25.449 & \text{if } n \text{ odd} \end{cases}$
$d = 17, D = 27$	$\lvert\beta\rvert \approx \begin{cases} 25.754 & \text{if } n \text{ even} \\ 25.798 & \text{if } n \text{ odd} \end{cases}$

Table 1: Values of $|\beta|$ for $p = 3$ and various degrees.

We see that $|\beta|/D > 1$ for $d = 7, 8$. Our (analytical) results include $d = 8$. Optimizing our proofs it should be possible to analyze $d = 7$ analytically as well.

The next tables consider arbitrary (not necessarily symmetric) polynomials. These results require non-trivial performance optimizations. They are obtained and can be reproduced with the code *poly.c* available on Emanuele Viola's webpage.

Table 2 lists all the polynomials in n variables of degree d modulo 2 that maximize the correlation with the Mod_3 function, for various values of d and n. We set the constant term to 0 since it does not affect correlation. We also report the correlation.

In all the values that we managed to compute, symmetric polynomials maximize the correlation. (We actually also verified this for $n = 9, 10$ and $d = 2$, but using a more complicated code that we omit.) This evidence for $d = 2$ is in stark contrast with the one for other moduli [Gre04, DMRS06], where symmetric is not optimal for any $n \leq 10$.

Below we denote by $s(d)$ the elementary symmetric polynomial of degree d.

Next in Table 3 we report the results for polynomials mod $p = 3$ vs. the mod $q = 2$ function. In order to make it easier to compare our results with the previous ones in the literature, e.g. [Gre04, DMRS06], in this setting we actually think of the variables as ranging over $\{-1, 1\}$ as opposed to $\{0, 1\}$. One can always switch between the two with a linear transformation, so this does not change the correlation, but it does change the polynomials. For concreteness, we mention this means that we are computing

$$C(n, d, 3, 2) := \frac{1}{2^n} \max_f \left| \sum_{x \in \{-1,1\}^n} \omega_3^{f(x)} \cdot \prod_i x_i \right| .$$

	d = 2	d = 3	d = 4	d = 5
n = 2	$s(1)$ $\sqrt{9}/2^2$ ≈ 0.7500			
n = 3	$s(1)$ $s(2)$ $\sqrt{27}/2^3$ ≈ 0.6495	$s(3) + s(1)$ $s(3) + s(2)$ $\sqrt{31}/2^3$ ≈ 0.6960		
n = 4	$s(2)$ $s(2) + s(1)$ $\sqrt{97}/2^4$ ≈ 0.6156	$s(3) + s(2)$ $\sqrt{121}/2^4$ ≈ 0.6875	$s(3) + s(2)$ $\sqrt{121}/2^4$ ≈ 0.6875	
n = 5	$s(2) + s(1)$ $\sqrt{363}/2^5$ ≈ 0.5954	$s(3)$ $s(3) + s(2)$ $\sqrt{381}/2^5$ ≈ 0.6100	$s(4) + s(3) + s(1)$ $\sqrt{441}/2^5$ ≈ 0.6563	$s(5) + s(4) + s(2) + s(1)$ $s(5) + s(3) + s(2)$ $\sqrt{463}/2^5$ ≈ 0.6724
n = 6	$s(2)$ $s(2) + s(1)$ $\sqrt{1351}/2^6$ ≈ 0.5743	$s(3)$ $\sqrt{1521}/2^6$ ≈ 0.6094		
n = 7	$s(2)$ $\sqrt{5043}/2^7$ ≈ 0.5548			
n = 8	$s(2)$ $s(2) + s(1)$ $\sqrt{18817}/2^8$ ≈ 0.5358			

Table 2: Correlations for $q = 3$ versus polynomials mod 2.

	d = 3	d = 4
n = 3	$s(3)$ $\sqrt{48}/2^3$ ≈ 0.8660	
n = 4	$s(3)+s(2)+s(1)$ $s(3)-s(2)+s(1)$ $\sqrt{171}/2^4$ ≈ 0.8173	$s(4)$ $\sqrt{192}/2^4$ ≈ 0.8660
n = 5	$s(3)+s(1)$ $\sqrt{675}/2^5$ ≈ 0.8119	

Table 3: Correlations for parity versus polynomials mod 3.

The results are listed up to multiplying a variable by -1, and up to adding a constant term – two operations that it is easy to see do not affect C.

For context, we mention that for any n and $d = 2$ the optimal polynomials are characterized [GR10]. Up to a constant term and permutation of the variables, the optimal polynomials are

$$\pm x_1x_2 \pm x_3x_4 \pm \cdots \pm x_{n-1}x_n$$

if n is even, and

$$\pm x_1x_2 \pm x_3x_4 \pm \cdots \pm x_{n-2}x_{n-1} + x_n$$

if n is odd.

A similar characterization is given in [DMRS06] for $n \leq 10$ and any odd p.

7 Missing proofs and details from §3

In this section we prove Theorem 3.1, restated next. Then we show that it cannot be improved, for $p = 3$. Finally we restate and prove Lemma 3.3.

Theorem 3.1. *Let p, c be any integers, and let D be any odd integer. Let $v = (D-1)/2 = \lfloor D/2 \rfloor$, $u_1 = \lfloor v/2 \rfloor$ and $u_2 = \lceil v/2 \rceil$. If n is even there exists an $r : \mathbb{Z}_D \to \mathbb{Z}_p$ such that,*

$$\beta = (-1)^{n/2} \frac{2}{\sin\left(\frac{\pi}{D}\right)} \left[\sin\left(\frac{2u_1+1}{D}\pi\right) - \zeta_p^c \sin\left(\frac{2u_2}{D}\pi\right) \right]. \tag{15}$$

If n is odd there exists an $r : \mathbb{Z}_D \to \mathbb{Z}_p$,

$$\beta = (-1)^{(n-1)/2}(1-\zeta_p^c)\frac{\sin\left(\frac{v\pi}{D}\right)}{\sin\left(\frac{\pi}{2D}\right)}. \tag{14}$$

Proof. If n is even, write $n = 2m$. Then,

$$\beta = 2\sum_{k=0}^{D-1}(-1)^k\zeta_p^{r(k)}\cos\left(\frac{k-m}{D}\pi\right).$$

A change of variable $k \mapsto k+m$ gives,

$$\beta = 2\sum_{k=-m}^{D-m-1}(-1)^{k+m}\zeta_p^{r(k+m)}\cos\left(\frac{k}{D}\pi\right).$$

It is now convenient to extend r to a periodic function with period D defined over the integers. So for any k, we have $r(k+m) = r(D+k+m)$. We also have $(-1)^{D+k} = -(-1)^k$ (since D is odd) and $\cos\left(\frac{D+k}{D}\pi\right) = \cos\left(\pi + \frac{k}{D}\pi\right) = -\cos\left(\frac{k}{D}\pi\right)$, hence $(-1)^{D+k}\zeta_p^{r(D+k+m)}\cos\left(\frac{D+k}{D}\pi\right) = (-1)^k\zeta_p^{r(k+m)}\cos\left(\frac{k}{D}\pi\right)$. Thus the terms in the above sum for $-m \leq k < 0$ are identical to the terms we get from $D-m \leq k < D$. Therefore,

$$\beta = 2(-1)^m\sum_{k=0}^{D-1}(-1)^k\zeta_p^{r(k+m)}\cos\left(\frac{k}{D}\pi\right). \tag{14}$$

Define the function $r : \mathbb{Z}_D \to \mathbb{Z}_p$ as follows:

$$r(k+m) = \begin{cases} 0 & \text{if } (-1)^k\cos\left(\frac{k}{D}\pi\right) \geq 0, \\ c & \text{if } (-1)^k\cos\left(\frac{k}{D}\pi\right) < 0. \end{cases}$$

Note that, since D is odd, and $\cos(\pi-\theta) = -\cos(\theta)$,

$$(-1)^{D-k}\cos\left(\frac{D-k}{D}\pi\right) = -(-1)^k\cos\left(\pi - \frac{k}{D}\pi\right) = (-1)^k\cos\left(\frac{k}{D}\pi\right).$$

This implies that $r(D-k+m) = r(k+m)$. Using this we can thus group respective terms with $1 \leq k \leq v = (D-1)/2$ with those such that $v+1 \leq k \leq 2v = D-1$. In particular, note that when $k \leq v$, $\cos\left(\frac{k}{D}\pi\right) > 0$, so that in this range the value of $r(k+m)$ is entirely determined by $(-1)^k$. That is, when $1 \leq k \leq v$ is even, $\zeta_p^{r(k+m)} = 1$ and when $1 \leq k \leq v$ is odd, then $\zeta_p^{r(k+m)} = \zeta_p^c$. The respective terms for $D-k$, with $k \leq v$, are identical. The contribution to β for $k=0$ is $2(-1)^m$. Summarizing, we have,

$$\begin{aligned}\beta(-1)^m &= 4\sum_{k=1}^{v}(-1)^k\zeta_p^{r(k+m)}\cos\left(\frac{k}{D}\pi\right) + 2 \\ &= 4\left[\sum_{k\equiv 0 \pmod 2, 1\leq k\leq v}\cos\left(\frac{k}{D}\pi\right) - \zeta_p^c\sum_{k\equiv 1 \pmod 2, 1\leq k\leq v}\cos\left(\frac{k}{D}\pi\right)\right] + 2. \end{aligned} \tag{15}$$

We now show how to evaluate each of the sums in Eq. (15). If $k > 0$ is even and $\le v = \lfloor D/2 \rfloor$, then $k = 2\ell$ where $\ell \le \lfloor v/2 \rfloor = u_1$. Thus the first sum is,

$$\sum_{k\equiv 0 \pmod 2, k\le v} \cos\left(\frac{k}{D}\pi\right) = \sum_{\ell=1}^{u_1}\cos\left(\frac{2\pi\ell}{D}\right) = \sum_{\ell=1}^{u_1}\Re\left(\zeta_{2D}^{2\ell}\right) = \Re\left(\sum_{\ell=1}^{u_1}\zeta_D^{\ell}\right).$$

The geometric series yields,

$$\sum_{\ell=1}^{u_1}\zeta_D^{\ell} = \sum_{\ell=0}^{u_1}\zeta_D^{\ell} - 1 = \frac{\zeta_D^{u_1+1}-\zeta_D}{\zeta_D-1} = \zeta_D\frac{\zeta_D^{u_1}-1}{\zeta_D-1} = \zeta_{2D}^{u_1+1}\frac{\zeta_{2D}^{u_1}-\zeta_{2D}^{-u_1}}{\zeta_{2D}-\zeta_{2D}^{-1}} = \zeta_{2D}^{u_1+1}\frac{\sin\left(\frac{\pi u_1}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}.$$

Since $\Re(\zeta_{2D}^{u_1+1}) = \cos\left(\frac{u_1+1}{D}\pi\right)$, we find,

$$\sum_{k\equiv 0 \pmod 2, k\le v} \cos\left(\frac{k}{D}\pi\right) = \frac{\sin\left(\frac{\pi u_1}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}\cos\left(\frac{u_1+1}{D}\pi\right). \tag{16}$$

We proceed similarly for the second sum in Eq. (15). Note here that if $k \le v = \lfloor D/2 \rfloor$ where k is odd, then we can write $k = 2\ell - 1$ where now $\ell \le \lceil v/2 \rceil = u_2$. Thus,

$$\sum_{k\equiv 1 \pmod 2, k\le v} \cos\left(\frac{k}{D}\pi\right) = \sum_{\ell=1}^{u_2}\cos\left(\frac{2\ell-1}{D}\pi\right) = \Re\left(\zeta_{2D}^{-1}\sum_{\ell=1}^{u_2}\zeta_D^{\ell}\right) = \Re\left(\zeta_{2D}^{u_2}\right)\frac{\sin\left(\frac{\pi u_2}{D}\right)}{\sin\left(\frac{\pi}{D}\right)},$$

which yields,

$$\sum_{k\equiv 1 \pmod 2, k\le v} \cos\left(\frac{k}{D}\pi\right) = \cos\left(\frac{u_2}{D}\pi\right)\frac{\sin\left(\frac{\pi u_2}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}. \tag{17}$$

Plugging Eqs. (16) and (17) into Eq. (15) yields,

$$\beta(-1)^m = 4\left[\frac{\sin\left(\frac{u_1\pi}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}\cos\left(\frac{u_1+1}{D}\pi\right) - \zeta_p^c\frac{\sin\left(\frac{u_2\pi}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}\cos\left(\frac{u_2}{D}\pi\right)\right] + 2. \tag{18}$$

We obtain Eq. (12) from Eq. (18) via the elementary trigonometric identities $\sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y)$ and $\cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y)$. Combining the first and last term in Eq. (18), we obtain,

$$\begin{aligned}
4\frac{\sin\left(\frac{u_1\pi}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}\cos\left(\frac{u_1+1}{D}\pi\right) + 2 &= 4\frac{\sin\left(\frac{u_1\pi}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}\left(\cos(\frac{u_1\pi}{D})\cos(\frac{\pi}{D}) - \sin(\frac{u_1\pi}{D})\sin(\frac{\pi}{D})\right) + 2 \\
&= 2\frac{\sin(\frac{2u_1\pi}{D})\cos(\frac{\pi}{D}) - 2\sin^2(\frac{u_1\pi}{D})\sin(\frac{\pi}{D}) + \sin(\frac{\pi}{D})}{\sin(\frac{\pi}{D})} \\
&= 2\frac{\sin(\frac{2u_1\pi}{D})\cos(\frac{\pi}{D}) + \cos(\frac{2u_1\pi}{D})\sin(\frac{\pi}{D})}{\sin(\frac{\pi}{D})} \\
&= 2\frac{\sin(\frac{(2u_1+1)\pi}{D})}{\sin(\frac{\pi}{D})}
\end{aligned}$$

Similarly, the coefficient of ζ_p^c in the second term in Eq. (18) is,

$$4\frac{\sin\left(\frac{u_2\pi}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}\cos\left(\frac{u_2}{D}\pi\right) = 2\frac{\sin\left(\frac{2u_2\pi}{D}\right)}{\sin\left(\frac{\pi}{D}\right)}.$$

Combining these terms in Eq. (18) yields Eq. (12).

We next treat the case of odd n. Write $n = 2m+1$. Then, using the same reasoning as for Eq. (14),

$$\beta = 2(-1)^m \sum_{k=0}^{D-1} (-1)^k \zeta_p^{r(k+m)} \cos\left(\frac{k}{D}\pi - \frac{\pi}{2D}\right). \tag{19}$$

Define the function $r : \mathbb{Z}_D \to \mathbb{Z}_p$ as,

$$r(k+m) = \begin{cases} 0 & \text{if } (-1)^k \cos\left(\frac{k}{D}\pi - \frac{\pi}{2D}\right) \geq 0, \\ c & \text{if } (-1)^k \cos\left(\frac{k}{D}\pi - \frac{\pi}{2D}\right) < 0. \end{cases}$$

The terms for $k = 0$ and $k = 1$ yield the same cosine factor (i.e., $\cos(\pi/(2D))$) but, due to the $(-1)^k$, different $r(k+m)$ values. Thus the contribution to the sum in Eq. (19) from $k = 0$ and $k = 1$ is $(1 - \zeta_p^c)\cos(\pi/(2D))$. The remaining terms, $2 \leq k \leq D-1$, group together more neatly than for n even. To see this, note that,

$$\cos\left(\frac{D-(k-1)}{D}\pi - \frac{\pi}{2D}\right) = \cos\left(\pi - \frac{k\pi}{D} + \frac{\pi}{D} - \frac{\pi}{2D}\right) = -\cos\left(\frac{k\pi}{D} - \frac{\pi}{2D}\right).$$

Thus $(-1)^k \cos\left(\frac{k\pi}{D} - \frac{\pi}{2D}\right)$ and $(-1)^{D-(k-1)} \cos\left(\frac{D-(k-1)}{D}\pi - \frac{\pi}{2D}\right)$ have opposite sign, so $r(k+m)$ and $r(D-(k-1)+m)$ have different values. Furthermore, for any k, $2 \leq k \leq v = \lfloor D/2 \rfloor$, the terms for k and $D-(k-1)$ sum to $(1-\zeta_p^c)\cos(k\pi/D - \pi/(2D))$. Summarizing, we find,

$$\beta = 2(-1)^m (1 - \zeta_p^c) \sum_{k=1}^{v} \cos\left(\frac{k\pi}{D} - \frac{\pi}{2D}\right)$$

We use the same technique to evaluate β in this case, reducing the sum of cosines to a geometric series.

$$
\begin{aligned}
\frac{\beta}{2(-1)^m(1-\zeta_p^c)} &= \Re\left(\zeta_{4D}^{-1}\sum_{k=1}^{v}\zeta_{2D}^k\right)\\
&= \Re\left(\zeta_{4D}^{-1}\frac{\zeta_{2D}^{v+1}-\zeta_{2D}}{\zeta_{2D}-1}\right)\\
&= \Re\left(\zeta_{4D}\frac{\zeta_{2D}^{v}-1}{\zeta_{2D}-1}\right)\\
&= \Re\left(\zeta_{4D}\zeta_{4D}^{v-1}\frac{\zeta_{4D}^{v}-\zeta_{4D}^{-v}}{\zeta_{4D}-\zeta_{4D}^{-1}}\right)\\
&= \Re\left(\zeta_{4D}^{v}\frac{\sin\left(\frac{v}{2D}\pi\right)}{\sin\left(\frac{\pi}{2D}\right)}\right)\\
&= \frac{\cos\left(\frac{v}{2D}\pi\right)\sin\left(\frac{v}{2D}\pi\right)}{\sin\left(\frac{\pi}{2D}\right)}.
\end{aligned}
$$

Finally, the identity $\sin(2\theta) = 2\sin(\theta)\cos(\theta)$ yields Eq. (13). □

The choices for r given in the proof of Theorem 3.1 seem to be optimal, at least intuitively (in fact, this was the basis for those choices). In the case $p = 3$ we can prove this. We use the notation $\omega = \zeta_3$.

Theorem 7.1 (Optimality of $\beta^\star$). *Let $p = 3$ and consider any function r in the Equation (8) for β. Then $|\beta| \leq |\beta^\star|$ for $c = 1$.*

Proof. We start with the form for β given in Eq. (8). Write,

$$
\begin{aligned}
\beta/2 &= \sum_{k=0}^{D-1}(-1)^k\omega^{r(k)}\cos(\pi(n-2k)/2D)\\
&= \left(\sum_{k:r(k)=0} +\omega\sum_{k:r(k)=1} +\overline{\omega}\sum_{k:r(k)=2}\right)(-1)^k\cos(\pi(n-2k)/2D)\\
&= A_0+\omega A_1+\overline{\omega}A_2,
\end{aligned}
$$

where for $i = 0, 1, 2$, we define $A_i = \sum\limits_{k:r(k)=i}(-1)^k\cos(\pi(n-2k)/2D)$. Note each A_i is real. Then,

$$|\beta/2|^2 = (A_0 + A_1 + A_2)^2 - 3(A_0A_1 + A_0A_2 + A_1A_2).$$

In order to maximize $|\beta|$, we must therefore minimize the expression $A_0A_1 + A_0A_2 + A_1A_2$. Now by the proof of Theorem 3.1, there is a setting for r such that $A_2 = 0$ and A_0 and A_1 have opposite signs. In fact, for this setting of r, $A_0 + A_1 = 0$. Because the quantity $A_0 + A_1 + A_2$ is invariant under changes in r, it follows that for all settings of r, $A_0 + A_1 + A_2 = 0$. Now since there is some setting of r such that $A_0A_1 < 0$, there must be such a term in the optimal case. Thus, in general, assume wlog that the signs of A_0 and A_1 are different, that $A_2 \neq 0$, and that $sign(A_1) = sign(A_2)$. Define $A'_1 = A_1 + A_2$. Then $A_0A_1 + A_0A_2 + A_1A_2 = A_0A'_1 + A_1A_2 > A_0A'_1$ (since $A_1A_2 > 0$). Hence we may assume that the optimal value has $A_2 = 0$. By the preceding argument, we also have $A_0 + A_1 = 0$, so that it follows that $A_0 = -A_1$. Hence, $|\beta|$ is at most $|A_0| \cdot |1 - \omega|$. We thus obtain the optimal value for β (i.e., A_0) by choosing r such that the quantity $(-1)^k \cos(\pi(n-2k)/2D)$ has the same sign for all k such that $r(k) = 0$ (and, for A_1, for all k such that $r(k) = 1$). This is precisely the choice made in the proof of Theorem 3.1. □

We now restate and prove Lemma 3.3.

Lemma 3.3 (Bounds on $\beta^\star$)**.** *Let* $c := (p-1)/2$. *Then:*
For any p, *we have* $\lim_{D\to\infty} |\beta^\star(D)/D| = 4\sin(\pi c/p)/\pi \geq 2\sqrt{3}/\pi > 1.102$.
For $p = D = 3$, *we have* $|\beta^\star| = 3$ *for* n *even, and* $|\beta^\star| = 2\sqrt{3}$ *if* n *is odd.*
Finally, for any $p \geq 3$ *and* $D \geq 5$, *we* $|\beta^\star|/D > 1.04$.

Proof. If n is even, first note that $\lim_{D\to\infty}(2/\sin(\pi/D))/D = \lim_{D\to\infty}(2D/\pi)/D = 2/\pi$. Secondly, $\lim_{D\to\infty} \sin\left(\frac{2u_1+1}{D}\pi\right) = \lim_{D\to\infty} \sin\left(\frac{2u_2}{D}\pi\right) = \sin(\pi/2) = 1$. Combining these, and taking the limit of $|\beta|$ as given in Eq. (12), yields $\lim_{D\to\infty}(|\beta|/D) = 2|1 - \zeta_p^c|/\pi = 4\sin(\pi c/p)/\pi$. If n is odd, Eq. (13) and the fact that $\lim_{D\to\infty} \sin(v\pi/D) = \sin(\pi/2) = 1$, and a similar calculation to the above, yields the same limit for $|\beta|/D$. To conclude the first bound note that $\sin(\pi c/p) = \sin\left(\frac{\pi}{2}(1 - 1/p)\right) \geq \sin\left(\frac{\pi}{3}\right) = \sqrt{3}/2$.

The case of $p = D = 3$ can be seen by direct computation from Eqs. (12, 13).

The remaining gate is $p \geq 3$ and $D \geq 5$. First consider even n. Note that for $a, b \in \mathbb{R}$, $|a - b\zeta_p^c| = \sqrt{a^2 + b^2 - 2ab\cos(2\pi c/p)}$. Since $\cos(2\pi c/p) = \cos(\pi - \pi/p) = -\cos(\pi/p)$, and for $p \geq 3$, $\cos(\pi/p) \geq 1/2$, we conclude that $|a - b\zeta_p^c| \geq \sqrt{a^2 + b^2 + ab}$, we then find from Eq. (12),

$$|\beta^\star(p,D)| \geq \frac{2}{\sin\left(\frac{\pi}{D}\right)}\sqrt{\sin\left(\frac{2u_1+1}{D}\pi\right)^2 + \sin\left(\frac{2u_2}{D}\pi\right)^2 + \sin\left(\frac{2u_1+1}{D}\pi\right)\sin\left(\frac{2u_2}{D}\pi\right)}.$$

Since $\sin(\pi/D) < \pi/D$ for any D, we have $2/\sin(\pi/D) > 2D/\pi$. Each of the sine terms inside the square root (e.g., $\sin\left(\frac{2u_1+1}{D}\pi\right)$) defines a non-decreasing sequence indexed by D that approaches $\sin(\pi/2)$. The minimal terms in these sequences are thus given by $D = 5$, in which case $u_1 = u_2 = 2$. Thus each of the sine terms under the square root is at least $\sin^2(2\pi/5)$. Therefore,

$$\frac{|\beta^\star(p,D)|}{D} \geq \frac{2}{\pi}\sqrt{3\sin^2(2\pi/5)} = \frac{2\sqrt{3}}{\pi}\sin(2\pi/5) > 1.04. \tag{20}$$

The odd n case is somewhat simpler. Here we note that $1/\sin\left(\frac{\pi}{2D}\right) > 2D/\pi$ and that $\sin\left(\frac{v\pi}{D}\right) > \sin\left(\frac{2\pi}{5}\right)$. Substituting these into Eq. (13) yields Eq. (20). □

8 Open problems

Are the optimal polynomials modulo $p = 2$ for the Mod $q = 3$ function symmetric for every degree? Again, the results in §6 support this fact, which would be a major step forward.

Less ambitiously, are symmetric polynomials optimal for $p = 3, q = 2, d = 3$?

We conjecture that the dependence of the maximum value of $|\beta|$ on n is limited to n modulo 2, regardless of d. Theorem 3.1 establishes this for $d = p^t - 1$.

We conjecture that for any degree of the form $d = p^h + 1$ switch-symmetric polynomial mod p correlate better than symmetric.

Do block-switch-symmetric polynomials ever beat block-symmetric?

For any fixed d and say $p = 3, q = 2$, determine the basis α so that the correlation is $(\alpha \pm o(1))^n$. Note Theorem 1.2 obtains improved lower bounds on α for infinitely many d. Can we have matching upper and lower bounds?

Determine for each $d \in (3^t, 3^{t-1})$ which of symmetric, block-symmetric, and switch-symmetric correlates best.

This work focuses on the leading coefficient $\beta = \beta_1$. A natural next step is to consider other β_i as well and obtain improved bounds.

9 Acknowledgements

F.G. gratefully acknowledges the hospitality of Steve Homer and the Computer Science Department of Boston University.

References

[AB01] Noga Alon and Richard Beigel. Lower bounds for approximations by low degree polynomials over Z_m. In *IEEE Conf. on Computational Complexity (CCC)*, pages 184–187, 2001.

[AW08] Scott Aaronson and Avi Wigderson. Algebrization: a new barrier in complexity theory. In *40th ACM Symp. on the Theory of Computing (STOC)*, pages 731–740, 2008.

[BGL06] Nayantara Bhatnagar, Parikshit Gopalan, and Richard J. Lipton. Symmetric polynomials over Z_m and simultaneous communication protocols. *J. of Computer and System Sciences*, 72(2):252–285, 2006.

[BGS75] Theodore Baker, John Gill, and Robert Solovay. Relativizations of the *P=?NP* question. *SIAM J. Comput.*, 4(4):431–442, 1975.

[BK10] Joppe Bos and Marcelo Kaihara. Playstation 3 computing breaks 2^{60} barrier: 112-bit prime ECDLP solved, 2010.

[BNS92] László Babai, Noam Nisan, and Márió Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Comput. System Sci.*, 45(2):204–232, 1992.

[Bou05] Jean Bourgain. Estimation of certain exponential sums arising in complexity theory. *C. R. Math. Acad. Sci. Paris*, 340(9):627–631, 2005.

[CGT96] Jin-Yi Cai, Frederic Green, and Thomas Thierauf. On the correlation of symmetric functions. *Mathematical Systems Theory*, 29(3):245–258, 1996.

[DMRS06] Eduardo Dueñez, Steven J. Miller, Amitabha Roy, and Howard Straubing. Incomplete quadratic exponential sums in several variables. *J. Number Theory*, 116(1):168–199, 2006.

[GR10] Frederic Green and Amitabha Roy. Uniqueness of optimal mod 3 circuits for parity. *Journal of Number Theory*, 130:961 – 975, 2010.

[Gre99] Frederic Green. Exponential sums and circuits with a single threshold gate and mod-gates. *Theory Comput. Syst.*, 32(4):453–466, 1999.

[Gre04] Frederic Green. The correlation between parity and quadratic polynomials mod 3. *J. Comput. System Sci.*, 69(1):28–44, 2004.

[GRS05] Frederic Green, Amitabha Roy, and Howard Straubing. Bounds on an exponential sum arising in Boolean circuit complexity. *C. R. Math. Acad. Sci. Paris*, 341(5):279–282, 2005.

[HMP$^+$93] András Hajnal, Wolfgang Maass, Pavel Pudlák, Márió Szegedy, and György Turán. Threshold circuits of bounded depth. *J. Comput. System Sci.*, 46(2):129–154, 1993.

[Luk03] Eugene M. Luks. Private communication, 2003.

[Rad09] Stanislaw Radziszowski. Small ramsey numbers, 2009. Dynamic Survey.

[Raz87] Alexander Razborov. Lower bounds on the dimension of schemes of bounded depth in a complete basis containing the logical addition function. *Mat. Zametki*, 41(4):598–607, 1987. English translation in Mathematical Notes of the Academy of Sci. of the USSR, 41(4):333-338, 1987.

[RR97] Alexander Razborov and Steven Rudich. Natural proofs. *J. of Computer and System Sciences*, 55(1):24–35, August 1997.

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *19th ACM Symp. on the Theory of Computing (STOC)*, pages 77–82. ACM, 1987.

[Smo93] Roman Smolensky. On representations by low-degree polynomials. In *34th IEEE IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 130–138, 1993.

[Vio09] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

[VW08] Emanuele Viola and Avi Wigderson. Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols. *Theory of Computing*, 4:137–168, 2008.

[Wil07] Ryan Williams. *Algorithms and Resource Requirements for Fundamental Problems.* PhD thesis, Carnegie Mellon University, 2007.

A Other notions of correlation

In this section we briefly discuss other notions of correlation that appear in the literature, and explain how they relate to the exponential sum.

Let $f, g : \{0,1\}^n \to \{0,1\}$ be Boolean functions over n variables. A notion of "correlation" between f and g is defined as

$$C(f,g) = \Pr[f(x) = 1 | g(x) = 1] - \Pr[f(x) = 1 | g(x) = 0], \tag{21}$$

where the probability is taken over x chosen uniformly at random from $\{0,1\}^n$. In this paper we study the case in which f is defined as follows: Let $p \in \mathbb{Z}$, and t be a polynomial in the n Boolean variables $x_1, \ldots, x_n$. Then,

$$f(x) = \begin{cases} 1 & \text{if } t(x) \not\equiv 0 \pmod p, \\ 0 & \text{otherwise.} \end{cases}$$

The target function g is defined in terms of the Hamming weight of the inputs mod q for some $q \in \mathbb{Z}$.

$$g(x) = \begin{cases} 1 & \text{if } \sum_{i=1}^n x_i \not\equiv 0 \pmod q, \\ 0 & \text{otherwise.} \end{cases}$$

We always assume q and p to be relatively prime, and usually take both q and p to be primes; we will specify when these conditions apply.

In [CGT96], [Gre99], it was shown how, in this case, $C(f,g)$ can be expressed in terms of exponential sums. (In fact the quantity considered in [Gre99] was not the same as $C(f,g)$, but as observed in [AB01] and explicitly proved in [Bou05], a derivation similar to the one in [Gre99] works for the choice of f, g given above.) To this end, for any $u \in \mathbb{Z}$, define the primitive complex u^{th} root of unity $\zeta_u = e^{2\pi i/u}$. Then, following a computation similar to one given in [Bou05] (in which the only difference was that $f(x)$ is 0 iff $t(x) \equiv 0 \pmod p$)), we find,

$$C(f,g) = \frac{1}{2^n} \frac{q}{q-1} \sum_{a=1}^{m-1} \sum_{b=1}^{q-1} \sum_{x \in \{0,1\}^n} \zeta_q^{b \sum_{i=1}^n x_i} \zeta_p^{at(x)}. \tag{22}$$

Note that, due to the a and b sums, there are $(q-1)(p-1)$ sums, each one over n variables. We are ultimately interested in exponential upper bounds on $|C(f,g)|$, which hold if such bounds hold for each of the a, b terms.

In the important settings $q = 2$ and $p = 3$ (i.e., mod 3 polynomials vs. parity), or $q = 3$ and $p = 2$, which are sufficient for all the main results in this paper, one needs only to consider $a = b = 1$. This is because $\zeta_3^2 = \bar{\zeta}_3$, so different values of a and b only conjugate the correlation.

For $p > 3$ we also note that, when proving an upper bound for every polynomial, the value of a can be absorbed in $t(x)$, and so again one can assume $a = 1$ without loss of generality.

Our object of study is therefore Definition 1.