# On the Correlation of Symmetric Functions *

Jin-Yi Cai †
University of Buffalo

Frederic Green‡
Clark University

Thomas Thierauf §
Universität Ulm

**Abstract**

The *correlation* between two Boolean functions of $n$ inputs is defined as the number of times the functions agree minus the number of times they disagree, all divided by $2^n$. In this paper, we compute, in closed form, the correlation between any two *symmetric* Boolean functions. As a consequence of our main result, we get that every symmetric Boolean function having an odd period has an *exponentially small* correlation (in $n$) with the parity function. This improves a result of Smolensky [12] restricted to symmetric Boolean functions: the correlation between parity and any circuit consisting of a $\text{Mod}_q$ gate over AND-gates of small fan-in, where $q$ is odd and the function computed by the sum of the AND-gates is symmetric, is bounded by $2^{-\Omega(n)}$.

In addition, we find that for a large class of symmetric functions the correlation with parity is *identically* zero for infinitely many $n$. We characterize exactly those symmetric Boolean functions having this property.

## 1 Introduction

$\text{AC}^{(0)}$ circuits cannot compute the parity function as shown in the seminal work of Furst, Saxe, and Sipser [5] and Ajtai [1]. In a breakthrough result, Yao [14] showed that in fact $\text{AC}^{(0)}$ type circuits (i.e., bounded-depth circuits containing AND, OR and NOT gates) must have exponential size to compute parity. A simpler proof and nearly optimal lower bounds were obtained by Håstad [7]. As originally pointed out in [5], these bounds imply the existence of an oracle separating PH from PSPACE. In order to prove the separation relative to a random oracle, Cai [4] showed that $\text{AC}^{(0)}$ type circuits below a certain exponential size cannot even *approximate* parity, in that the error approaches 50% asymptotically. Babai [2] subsequently gave an elegant and much simpler proof. More specifically, it is shown that $\text{AC}^{(0)}$ type circuits, below a certain exponential size, can agree with parity no more than a fraction $1/2 + f(n)$ of the $2^n$ inputs, where $f(n) = 2^{-n^{\Omega(1)}}$. (This was implicit in [4] and Håstad and Boppana, as reported in [7], have the best constant involved.) One of the interesting consequences of this sharp result is that circuits consisting of a single majority

*Supported in part by NSF grant CCR-9057486.

†Department of Computer Science, State University of New York at Buffalo, Buffalo, NY 14260. Supported in part by an Alfred T. Sloan Fellowship in computer science.

‡Clark University, Department of Mathematics & Computer Science, Worcester, Massachusetts 01610. Work done in part while visiting Princeton University.

§Universität Ulm, Abteilung Theoretische Informatik, Oberer Eselsberg, 89069 Ulm, Germany. Work done in part while visiting Princeton University and the University of Rochester. Supported in part by DFG Postdoctoral Stipend Th 472/1-1 and by NSF grant CCR-8957604.

gate over $\mathrm{AC}^{(0)}$-type circuits cannot compute parity, unless the circuits are of exponential size [6].

If we allow, for example, $\mathrm{Mod}_3$ gates in addition in the $\mathrm{AC}^{(0)}$ subcircuits, it was shown by Smolensky [12], extending techniques of Razbarov [10], that the fraction of agreement between parity and bounded-depth circuits containing AND, OR, NOT and $\mathrm{Mod}_3$ gates, below a certain exponential size, is no more than $1/2 + f(n)$, where $f(n) = 1/n^{1/2-o(1)}$. Thus, the bound for $f(n)$ is weaker for this type of circuit. It is therefore natural to ask if the $1/n^{1/2-o(1)}$ bound can be tightened, as in the $\mathrm{AC}^{(0)}$ case, to $2^{-n^{\Omega(1)}}$. To reduce the problem to its simplest form, consider a circuit consisting of a $\mathrm{Mod}_3$ gate over AND gates of small fan-in. Even in this case it is not known if the agreement with parity is exponentially close to 1/2. (This is also sufficient, since the Razborov approximation is exponentially close.) However, it is not clear whether Smolensky's techniques can be used to improve the known bound below $O(1/\sqrt{n})$.

The sum of the inputs going into a $\mathrm{Mod}_q$ gate can be interpreted as a polynomial in the input variables. Thus the problem can be stated more precisely as follows: For any natural number $q$ define the Boolean function $M_q : N \to \{0,1\}$ such that $M_q(k) = 1$ if $k \not\equiv 0 \pmod q$ and 0 otherwise. For a polynomial $p : \{0,1\}^n \to \mathbf{N}$, how well can $M_q(p(x_1, \ldots, x_n))$ approximate parity?

In this paper, we consider a restricted version of this problem, in which we assume the polynomials $p$ are *symmetric*. Thus the question we address is: for a *symmetric* polynomial $p : \{0,1\}^n \to \mathbf{N}$ of low degree, how well can $M_q(p(x_1, \ldots, x_n))$ approximate parity?

In a recent paper, which was in part an inspiration for this one, Barrington, Beigel, and Rudich [3] also considered the computational power of symmetric polynomials which represent Boolean functions in this way. They give a surprising upper bound (and a matching lower bound) for the degree of a symmetric polynomial $p$ such that $M_q(p(x_1, \ldots, x_n))$ computes the OR function. Their results suggest the very interesting possibility that in general $\mathrm{Mod}_q$ gates might be more powerful when $q$ is composite than when $q$ is prime. In addition, for a *general* polynomial $p$ (not necessarily symmetric), they prove the first lower bounds on the degree of $p$ for $M_q(p)$ to compute the $M_{q'}$ function when $q$ and $q'$ are composite and there is a prime divisor of $q'$ that is not a divisor of $q$. Our problem is different. We wish to estimate the error rather than finding exact agreement. For the latter reason, we do not consider the OR function, since a constant polynomial would give almost complete agreement.

As a measure of how well one Boolean function can approximate another we use the notion of correlation. Let $g_1, g_2 : \{0,1\}^n \to \{0,1\}$ be two Boolean functions over the inputs $\{x_1, \ldots, x_n\}$ where $x_i \in \{0,1\}$. The *correlation* $C_n(g_1, g_2)$ between $g_1$ and $g_2$ is the difference between the number of times $g_1$ and $g_2$ agree and the number of times they disagree, divided by $2^n$. Since $g_1, g_2$ take on values in $\{0,1\}$, this can be written as,

$$C_n(g_1, g_2) = 2^{-n} \sum_{\{x_1,\ldots,x_n\} \in \{0,1\}^n} (-1)^{g_1(x_1,\ldots,x_n)+g_2(x_1,\ldots,x_n)}.$$

In these terms, the result of Cai and Håstad says that if $g$ is the Boolean function computed by an $\mathrm{AC}^{(0)}$ circuit, and $\oplus$ denotes the parity function, then $C_n(g, \oplus) = 2^{-n^{\Omega(1)}}$. Smolensky's result says that if $q$ is an odd prime and if $p$ denotes any polynomial of low degree (e.g., *polylog*$(n)$), then $C_n(M_q(p), \oplus) = 1/n^{1/2-o(1)}$.

Our main result is that if $p$ is any low-degree symmetric polynomial, the correlation is indeed exponentially small. That is, if $q$ is odd, and $p$ is symmetric and of low degree (e.g., *polylog* $(n)$ or even $n^{o(1)}$), then $C_n(M_q(p), \oplus) = 2^{-\Omega(n)}$ (see Corollary 3.4). This is actually a corollary of a general result, which gives a *closed form* expression for the correlation between any two symmetric Boolean functions. This result is given in Section 3 (see Theorem 3.1). In Section 4, we show that for a wide class of symmetric polynomials the correlation with parity is *exactly* 0 for infinitely many values of $n$. Our techniques allow a detailed analysis of the correlation, so that we can characterize exactly all those symmetric Boolean functions having this property (Theorem 4.1). We demonstrate, for elementary symmetric polynomials, how the zeroes in the correlation as a function of $n$ can be computed when this property holds.

## 2 Preliminaries

A function $g : \{0,1\}^n \to \mathbf{N}$ over Boolean variables $\{x_1, \ldots, x_n\}$ is *symmetric*, if the function value of $g$ remains unchanged for any permutation of the input variables. As a consequence, any symmetric function depends only on the sum of its inputs. Hence, we can write it as $g(x_1, \ldots, x_n) = f(\sum_{j=1}^n x_j)$ for some function $f : \mathbf{Z} \to \mathbf{Z}$ which we say *represents* $g$. If $g$ is a Boolean function, i.e., $g : \{0,1\}^n \to \{0,1\}$, then we also require $f$ to map to $\{0,1\}$.

The *elementary symmetric polynomial* $e_d(x_1, \ldots, x_n)$ or $e_d(x)$ of degree $d$ over Boolean variables $\{x_1, \ldots, x_n\}$ is the sum of all monomials of the form $\prod_{j \in S} x_i$ where $S \subseteq \{1, \ldots, n\}$ and $||S|| = d$. It is clear that if the number of variables that are 1 is $k$, then $e_d(x) = \binom{k}{d}$. Any symmetric Boolean function of degree $d$ can be written as a linear combination of the elementary symmetric polynomials of degree $\leq d$.

Let $D \in \mathbf{N}$, $D > 0$. We say $f : \mathbf{Z} \to \mathbf{Z}$ is *periodic with period* $D$ if $f(k + D) = f(k)$, for any $k \in \mathbf{Z}$. Unless otherwise noted, when we refer to *the* period of a function, we mean the smallest period. Of course any multiple of the period $D$ is also a period, and it is not hard to see that any period must be a multiple of the smallest one. We say the symmetric Boolean function $g : \{0,1\}^n \to \{0,1\}$ is *periodic with period* $D$ if $D \leq n$ and there is a function $f$ that represents $g$ such that $f$ is periodic with period $D$. (Note that in fact such a function $f$, if it exists, is uniquely determined.)

For example, define $M_q : \mathbf{Z} \to \{0,1\}$ as

$$M_q(k) = \begin{cases} 1, & \text{if } k \not\equiv 0 \pmod{q} \\ 0, & \text{otherwise.} \end{cases}$$

In [3] it is noted that if $p$ is a polynomial of degree $d$ and the number of distinct prime factors of $q$ is $r$, then the period of $M_q(p(x_1, \ldots, x_n))$ is $D = \Theta(d^r)$.

While a symmetric, periodic Boolean function $g : \{0,1\}^n \to \{0,1\}$ has a finite domain, the function $f$ representing $g$ is defined on $\mathbf{Z}$. Therefore, when we consider $n$ as variable in later sections, we are referring to $f$ instead of $g$. Note that in turn, $f$ defines a sequence of symmetric Boolean functions $g_m : \{0,1\}^m \to \{0,1\}$, for each $m \in \mathbf{N}$. Regarding the correlation, we will also write $C_n(f, g')$ for $C_n(g, g')$, where $g'$ is another Boolean function.

## 3 General Symmetric Functions

Let $q_1, q_2 \in \mathbf{N}$ and $p_1$ and $p_2$ be symmetric polynomials. We derive in this section a formula for $C_n(M_{q_1}(p_1), M_{q_2}(p_2))$. In fact, we don't need any special properties of these functions. Our proof depends only on the periodicity of $M_{q_1}(p_1)$ and $M_{q_2}(p_2)$, and therefore, we consider the correlation between any two symmetric Boolean functions in terms of their periods.

**Theorem 3.1.** Let $g_1,\ g_2 : \{0,1\}^n \to \{0,1\}$ be symmetric Boolean functions represented by $f_1$ and $f_2$, respectively, and let $D$ be a period of $f_1 + f_2$. Let $\xi$ denote the $D^{th}$ root of unity $e^{2\pi i/D}$ and $\lambda_j = 1 + \xi^{-j}$. Then

$$C_n(g_1, g_2) \ = \ \frac{1}{2^n D} \sum_{k=0}^{D-1} (-1)^{f_1(k)+f_2(k)} \sum_{j=0}^{D-1} \xi^{kj} \lambda_j^n.$$

*Proof.* Since $g_1$ and $g_2$ are symmetric, the correlation between $g_1$ and $g_2$ becomes

$$C_n(g_1, g_2) \ = \ 2^{-n} \sum_{k=0}^{n} (-1)^{f_1(k)+f_2(k)} \binom{n}{k}.$$

Since $D$ is a period of $f_1 + f_2$, we can partition this sum into $D$ sums, one for each remainder modulo $D$, as follows. For $k = 0, \ldots, D-1$ let

$$r_k(n) \ = \ \sum_{j \ \equiv \ k \ (\mathrm{mod}\ D)} \binom{n}{j}.$$

Then we have

$$C_n(g_1, g_2) \ = \ 2^{-n} \sum_{k=0}^{D-1} (-1)^{f_1(k)+f_2(k)} r_k(n).$$

The proof is completed by the following lemma, showing that each $r_k$ can be written as claimed in the theorem. □

**Lemma 3.2.** $r_k(n) = \frac{1}{D} \sum\limits_{j=0}^{D-1} \xi^{kj} \lambda_j^n, \quad$ for $k = 0, \ldots, D-1$.

*Proof.* Using the recurrence relation for the binomial coefficients, we have

$$r_k(n) \ = \ \sum_{j \ \equiv \ k \ (\mathrm{mod}\ D)} \left[ \binom{n-1}{j} + \binom{n-1}{j-1} \right] \ = \ r_k(n-1) + r_{k-1}(n-1)$$

for all $k \in \{0, \ldots, D-1\}$, where index $k-1$ is taken modulo $D$. Let us define vector $\mathbf{r}(n)$ as

$$\mathbf{r}(n) \ = \ \begin{pmatrix} r_0(n) \\ r_1(n) \\ \cdot \\ \cdot \\ \cdot \\ r_{D-1}(n) \end{pmatrix}.$$

By the above recurrence relation, we can compute $\mathbf{r}(n)$ by multiplying $\mathbf{r}(n-1)$ with some appropriately defined matrix $\mathbf{M}$,

$$\mathbf{r}(n) \;=\; \mathbf{M}\,\mathbf{r}(n-1),$$

where $\mathbf{M}$ is the $D \times D$ matrix

$$\mathbf{M} \;=\; \begin{pmatrix} 1 & 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 1 \\ 1 & 1 & 0 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & & & & & & & & \cdot \\ \cdot & & & & & & & & \cdot \\ \cdot & & & & & & & & \cdot \\ 0 & 0 & 0 & 0 & \cdot & \cdot & \cdot & 1 & 1 \end{pmatrix}.$$

Hence, we get $\mathbf{r}(n) = \mathbf{M}^n\mathbf{r}(0)$, where the components of $\mathbf{r}(0)$ are $r_0(0) = 1$ and $r_k(0) = 0$ for $k = 1, \ldots, D-1$. It remains to compute the $n$-th power of the matrix $\mathbf{M}$. The simplest way to do this is to diagonalize $\mathbf{M}$. The eigenvalues of $\mathbf{M}$ are the $\lambda_j$, for $j = 0, \ldots, D-1$, and an eigenvector corresponding to $\lambda_j$ is

$$\begin{pmatrix} 1 & \xi^{-j} & \xi^{-2j} & \cdot & \cdot & \cdot & \xi^{-(D-1)j} \end{pmatrix}^T.$$

Since the eigenvectors are linearly independent, we actually can diagonalize $\mathbf{M}$. The diagonalizing matrix $\mathbf{V}$ is defined as having the $D$ eigenvectors as its columns, $(\mathbf{V})_{k,j} = \xi^{-kj}$, which is a Vandermonde matrix. The diagonal matrix $\mathbf{\Delta}$ has the eigenvalues as its diagonal entries, the $j$-th diagonal entry of $\mathbf{\Delta}$ being the eigenvalue for the eigenvector in the $j$-th column of $\mathbf{V}$, $\lambda_j$.

It is easy to verify that $\frac{1}{\sqrt{D}}\mathbf{V}$ is unitary (i.e., $\mathbf{V}\mathbf{V}^* = \mathbf{V}^*\mathbf{V} = D\,\mathbf{I}$, where $\mathbf{V}^*$ denotes the Hermitian conjugate of $\mathbf{V}$ and $\mathbf{I}$ is the identity matrix) using the fact that

$$\sum_{j=0}^{D-1} \xi^{kj} \;=\; \begin{cases} D, & \text{if } k = 0, \\ 0, & \text{otherwise.} \end{cases}$$

Hence $\mathbf{M} = \frac{1}{D}\mathbf{V}^*\mathbf{\Delta}\mathbf{V}$, and $\mathbf{M}^n = \frac{1}{D}\mathbf{V}^*\mathbf{\Delta}^n\mathbf{V}$. Therefore, we get

$$\mathbf{r}(n) \;=\; \frac{1}{D}\mathbf{V}^*\mathbf{\Delta}^n\mathbf{V}\mathbf{r}(0) \;=\; \frac{1}{D}\mathbf{V}^*\mathbf{\Delta}^n\mathbf{V}\begin{pmatrix} 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix} \;=\; \frac{1}{D}\mathbf{V}^*\mathbf{\Delta}^n\begin{pmatrix} 1 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ 1 \end{pmatrix} \;=\; \frac{1}{D}\mathbf{V}^*\begin{pmatrix} \lambda_0^n \\ \lambda_1^n \\ \lambda_2^n \\ \cdot \\ \cdot \\ \cdot \\ \lambda_{D-1}^n \end{pmatrix}.$$

From the definition of $\mathbf{V}$, the lemma now follows immediately. □

The sum in Theorem 3.1 can also be written as

$$C_n(g_1, g_2) \;=\; \frac{1}{2^n D}\sum_{j=0}^{D-1} s_j\lambda_j^n,$$

where

$$s_j = \sum_{k=0}^{D-1} (-1)^{f_1(k)+f_2(k)} \xi^{kj}.$$

Observe that the largest eigenvalue is $\lambda_0 = 2$, and that all other eigenvalues are smaller. In fact, the second largest eigenvalue $\lambda_1$ has norm $|1+\xi| = 2\cos(\pi/D)$. Thus, while the largest term in the above sum (when $j = 0$) is constant $s_0/D$ (i.e., independent of $n$, if $D$ is constant), the second largest term (when $j = 1$) has norm $\frac{|s_1|}{D}\cos(\pi/D)^n$ which is exponentially small compared with the first term (if $D$ is a constant or a slowly growing function in $n$). This yields,

**Corollary 3.3.** Let $g_1$, $g_2 : \{0,1\}^n \to \{0,1\}$ be symmetric Boolean functions represented by $f_1$ and $f_2$, respectively, and let $D$ be a period of $f_1 + f_2$. Let $s_0 = \sum_{k=0}^{D-1}(-1)^{f_1(k)+f_2(k)}$. Then

$$|\, C_n(g_1, g_2) - \frac{s_0}{D} \,| = O(\cos(\pi/D)^n).$$

We can now easily prove the main corollary of this section, which states that the fraction of the time that any symmetric function with a small odd period can agree with parity is exponentially close to 1/2.

**Corollary 3.4.** Let $g : \{0,1\}^n \to \{0,1\}$ be a symmetric Boolean function with odd period $D$. Let $\oplus$ denote the parity function. Then

$$|\, C_n(g, \oplus) \,| = O(\cos(\pi/(2D))^n) = O\left((1 - \frac{1}{2}(\frac{\pi}{2D})^2)^n\right).$$

*Proof.* Let $f$ represent $g$. Observe that $M_2$ represents $\oplus$. Since $D$ is odd, the period of $f + M_2$ is $2D$. Furthermore, we have $(-1)^{f(k)+M_2(k)} = (-1)^{f(k)+k} = -(-1)^{f(k+D)+k+D}$, and hence

$$s_0 = \sum_{k=0}^{2D-1} (-1)^{f(k)+k} = 0.$$

Now, the claim follows from Corollary 3.3. $\square$

Let us consider a sequence of symmetric functions $g_n : \{0,1\}^n \to \{0,1\}$ having different (odd) periods $D(n)$. It follows from Corollary 3.4 that $C_n(g_n, \oplus)$ is exponentially small in $n$ as long as $D(n) = O(n^{1/2-\epsilon})$, for some $\epsilon > 0$.

If we choose $g_n = M_q(p_n)$, for odd $q$ and some symmetric polynomial $p_n$ of degree $d(n)$, then the period of $g_n$ is odd (see Theorem 4.7 below) and is bounded by $O(d(n)^{\log q})$. Therefore, when the degree $d(n)$ is bounded by $O(n^{\frac{1}{2\log q}-\epsilon})$, for some $\epsilon > 0$, then $|C_n(M_q(p_n), \oplus)| = 2^{-\Omega(n)}$.

## 4 Zeroes in the Correlation With Parity

In the previous section, we have seen that the correlation of parity with any symmetric function of small, odd period must be exponentially small. Remarkably, we find that for many symmetric functions the correlation is identically zero for infinitely many $n$, spaced at regular intervals if the period is constant. When a function has this property, we can compute the zeroes (i.e., those values of $n$ for which the correlation is zero). In this section, we first characterize which symmetric functions have this property. Then we turn our attention to a special class of functions (the elementary symmetric polynomials modulo an odd number) to illustrate how to compute the zeroes.

It is easy to see that the correlation of a constant function with parity is zero for all $n$. For any non-constant symmetric function, the following theorem characterizes almost all $n$ for which the correlation with parity is zero.

**Theorem 4.1.** Let $f : \mathbf{Z} \to \{0,1\}$ be a non-constant function with odd period $D$. There exists an integer $n_0$[1] such that for any $n > n_0$, the following conditions are equivalent.

(a) $C_n(f, \oplus) = 0$,

(b) $f(k) \equiv n + 1 + f(n-k) \pmod 2$, for $k = 0, \ldots, D-1$.

*Proof.* Let $\xi$ denote the $2D^{th}$ root of unity $e^{\pi i/D}$ and $\lambda_j = 1+\xi^{-j}$. Then, by Theorem 3.1,

$$\begin{aligned} 2^n C_n(f, \oplus) &= \frac{1}{2D} \sum_{j=0}^{2D-1} \sum_{k=0}^{2D-1} (-1)^{f(k)+k}\, \xi^{kj} \lambda_j^n \\ &= \frac{1}{D} \sum_{j=0}^{D-1} \mathrm{Re}\left( \sum_{k=0}^{2D-1} (-1)^{f(k)+k}\, \xi^{kj} \lambda_j^n \right), \end{aligned}$$

where the second equality holds because $\xi^{2D-j} = \overline{\xi}^j$ and $\lambda_{2D-j} = \overline{\lambda}_j$, so that the second half of the $j$-sum ($D \le j \le 2D-1$) is the complex conjugate of the first half. Let us define

$$\begin{aligned} s_j &= \sum_{k=0}^{2D-1} (-1)^{f(k)+k}\, \xi^{kj}, \\ t_j(n) &= \mathrm{Re}(s_j \lambda_j^n), \end{aligned}$$

for $j = 0, \ldots, 2D-1$. Then we have

$$2^n C_n(f, \oplus) = \frac{1}{D} \sum_{j=0}^{D-1} t_j(n).$$

Note that if $j$ is even, we have that $s_j = 0$, and hence $t_j(n) = 0$. This holds because $\xi^{(k+D)j} = \xi^{kj}$ for even $j$, and $(-1)^{k+D} = -(-1)^k$. Note also that for any $0 \le j \le D-1$, we have $t_j(n) = t_{2D-j}(n)$ and that $t_D(n) = 0$ since $\lambda_D = 0$.

The proof is completed by the following three lemmas. ☐

When $C_n(f, \oplus) = 0$, there are potentially two reasons for this: either all the $t_j(n)$ are zero or several nonzero $t_j(n)$ cancel each other. Our first lemma states that the latter cannot happen for large enough $n$.

[1] In fact, $n_0$ depends only on $D$, and not on $f$.

**Lemma 4.2.** There exists an integer $n_0$ such that for any $n > n_0$,

$$C_n(f, \oplus) = 0 \iff t_j(n) = 0, \quad \text{for all } 0 \le j \le 2D-1.$$

*Proof.* Since $t_j(n) = t_{2D-j}(n)$, it suffices to argue for $0 \le j \le D-1$. Suppose $C_n(f, \oplus) = 0$. We can express $t_j(n)$ as[2]

$$t_j(n) \quad = \quad |s_j|\,|2\cos(\frac{\pi j}{2D})|^n \cos(\arg(s_j) - \frac{\pi n j}{2D}). \tag{1}$$

Clearly, we have $|t_j(n)| \le |s_j|\,|2\cos(\frac{\pi j}{2D})|^n$. On the other hand, since the cosine is periodic in $n$, for any $j$ there exists a constant $c_j > 0$ (i.e., $c_j$ does not depend on $n$) such that

$$t_j(n) \ne 0 \implies |t_j(n)| \ge c_j\,|2\cos(\frac{\pi j}{2D})|^n.$$

Hence, each $|t_j(n)|$ is either zero or in a constant range of $|2\cos(\frac{\pi j}{2D})|^n$. (Note that $s_j$ doesn't depend on $n$.)

Because $|2\cos(\frac{\pi j}{2D})|^n$ dominates $|2\cos(\frac{\pi(j+1)}{2D})|^n$ for large $n$ and $j < D$, any $t_j(n) \ne 0$ dominates all the $t_{j'}(n)$ for $j < j' < D$. Thus, if $j_0$ is the least $j$ such that $t_j(n) \ne 0$, then the subsequent terms cannot cancel $t_{j_0}(n)$, and hence, $C_n(f, \oplus) \ne 0$. Therefore, $t_j(n) = 0$ for all $0 \le j \le D-1$. □

Using equation (1), we can characterize when a $t_j(n)$ is zero in terms of the $s_j$. Since $|2\cos(\frac{\pi j}{2D})|^n$ (and hence $t_j(n)$) is zero for $j = D$, we have to exclude the case $j = D$ in the next lemma.

**Lemma 4.3.** Let $0 \le j \le 2D-1$, $j \ne D$. Then $t_j(n) = 0 \iff s_j = -\xi^{nj}\overline{s_j}$.

*Proof.* If $s_j = 0$, then the lemma is trivial. Otherwise, for any $j \ne D$,

$$\begin{aligned}
t_j(n) = 0 \quad &\iff \quad \cos(\arg(s_j) - \frac{\pi n j}{2D}) = 0 \\
&\iff \quad \exists\, l \;\; \arg(s_j) - \frac{\pi n j}{2D} \;=\; \frac{\pi}{2} + l\pi \\
&\iff \quad \exists\, l \;\; e^{2i\arg(s_j)} \;=\; e^{2i\,(\frac{\pi n j}{2D} + \frac{\pi}{2} + l\pi)} \\
&\iff \quad |s_j|\, e^{i\arg(s_j)} \;=\; -|s_j|\, e^{-i\arg(s_j)} e^{\frac{\pi i}{D} n j} \\
&\iff \quad s_j \;=\; -\xi^{nj}\overline{s_j}.
\end{aligned}$$

□

**Lemma 4.4.** The following conditions are equivalent.

(i) $s_j = -\xi^{nj}\overline{s_j}$, for $j = 0, \ldots, 2D-1$, $j \ne D$,

(ii) $f(k) \equiv n + 1 + f(n-k) \pmod 2$, for $k = 0, \ldots, D-1$.

[2] Any complex number $z \ne 0$ can uniquely be written as $z = |z|(\cos\varphi + i\sin\varphi) = |z|e^{i\varphi}$, where $0 \le \varphi \le 2\pi$. $\varphi$ is called the *argument of* $z$, $\varphi = \arg z$. Hence $\mathrm{Re}(z) = |z|\cos\arg(z)$.

*Proof.* Since $(-1)^{f(k)+k}\,\xi^{-kj}$ has period $2D$, we have

$$\begin{aligned}
-\xi^{nj}\overline{s_j} &= -\xi^{nj}\sum_{k=0}^{2D-1}(-1)^{f(k)+k}\,\xi^{-kj} \\
&= -\xi^{nj}\sum_{k=n}^{n+2D-1}(-1)^{f(k)+k}\,\xi^{-kj} \\
&= (-1)^{n+1}\sum_{k=n}^{n+2D-1}(-1)^{f(k)+n-k}\,\xi^{(n-k)j} \\
&= \sum_{k'=0}^{2D-1}(-1)^{n+1+f(n-k')+k'}\,\xi^{k'j},
\end{aligned}$$

where the last equality was obtained by changing the summation variable to $k' = n-k$. Now, if condition (ii) is true, then it is clear that

$$s_j = \sum_{k=0}^{2D-1}(-1)^{n+1+f(n-k)+k}\,\xi^{kj},$$

which yields condition (i).

Conversely, if condition (i) is true then, for any $0 \le j \le 2D-1$, $j \ne D$,

$$\sum_{k=0}^{2D-1}(-1)^{f(k)+k}\,\xi^{kj} = \sum_{k=0}^{2D-1}(-1)^{n+1+f(n-k)+k}\,\xi^{kj}. \tag{2}$$

Note that these sums are the Fourier transforms of the functions $(-1)^{k+f(k)}$ and $(-1)^{k+n+1+f(n-k)}$, respectively. Therefore, if equation (2) held for all $j$, i.e., including $j = D$, then we could immediately conclude that the functions are equal. But it is not obvious that equation (2) holds for $j = D$ when $n$ is even. Nevertheless, we can perform an inverse Fourier transform by using the relation

$$\sum_{j=0, j\ne D}^{2D-1}\xi^{(k-k')j} = \begin{cases} 2D-1 & \text{if } k = k' \\ (-1)^{k-k'+1} & \text{otherwise.} \end{cases}$$

Now multiply the left and right hand sides of equation (2) by $\xi^{-k'j}$ and sum over $j$ from 0 to $2D-1$, excluding $j = D$. This yields, for any $0 \le k' \le D-1$,

$$2D(-1)^{f(k')} - \sum_{k=0}^{2D-1}(-1)^{f(k)} = 2D(-1)^{n+1+f(n-k')} - \sum_{k=0}^{2D-1}(-1)^{n+1+f(n-k)}.$$

Note that the last sum in this equation is equal to $(-1)^{n+1}\sum_{k=0}^{2D-1}(-1)^{f(k)}$. Hence, we get

$$(-1)^{f(k')} = (-1)^{n+1+f(n-k')} + \frac{1}{2D}(1+(-1)^n)\sum_{k=0}^{2D-1}(-1)^{f(k)}. \tag{3}$$

To show condition (ii), it suffices to prove that the second term of the right hand side of equation (3) is 0. This is certainly true when $n$ is odd. Let $n$ be even. Then equation (3) becomes

$$(-1)^{f(k')} + (-1)^{f(n-k')} = \frac{1}{D} \sum_{k=0}^{2D-1} (-1)^{f(k)}.$$

Observe that the right hand side is independent of $k'$, and hence both sides are. The left hand side can be $\pm 2$ or 0. If it is $\pm 2$, then $f$ is constant, which contradicts the hypothesis of the theorem. Hence, the left hand side is 0 and we conclude that $\sum_{k=0}^{2D-1}(-1)^{f(k)} = 0$. Thus, the second term of the right hand side of equation (3) is indeed zero, and condition (ii) follows. (Observe that $s_D = \sum_{k=0}^{2D-1}(-1)^{f(k)+k}\xi^{kD} = \sum_{k=0}^{2D-1}(-1)^{f(k)} = 0$. Hence, condition (i) implies that in fact $s_j = -\xi^{nj}\overline{s_j}$, for all $0 \leq j \leq 2D-1$.) $\square$

Observe that in both conditions (i) and (ii) in the last lemma, we can equivalently replace $n$ by $m$, where $m$ $(0 \leq m < 2D)$ is the residue of $n$ modulo $2D$. Likewise, we can make this replacement in Theorem 4.1(b). Therefore, to determine whether $C_n(f, \oplus)$ is zero for infinitely many $n$, it is only necessary to find an $m$ such that $0 \leq m \leq 2D-1$ and

$$f(k) \equiv m + 1 + f(m-k) \pmod 2, \quad \text{for } k = 0, \ldots, D-1. \tag{4}$$

**Corollary 4.5.** Let $f : \mathbf{Z} \to \{0,1\}$ be a non-constant function with odd period $D$. There is an $m \in \{0, \ldots, 2D-1\}$ such that equation (4) holds iff $C_n(f, \oplus) = 0$ for all (large enough) $n$ such that $n \equiv m \pmod{2D}$.

Next, we show that if there exists an $m$ for which equation (4) holds, then it is unique. Thus, in fact, *all* zeros in the correlation of $f$ with parity are at the points $n_l = m + 2l\,D$, for a fixed $m$, from a certain size of $l$ on. Note that there may be additional zeroes for small values of $n$.

**Proposition 4.6.** Let $f : \mathbf{Z} \to \{0,1\}$ be a function with odd period $D$. Then equation (4) holds for at most one $m \in \{0, \ldots, 2D-1\}$.

*Proof.* Suppose there are $m_0, m_1$, where $0 \leq m_0 < m_1 < 2D$, such that $f(k) \equiv m_j + 1 + f(m_j - k) \pmod 2$, for all $k$ and $j = 0, 1$. It follows that $f(m_0 - k) \equiv m_1 - m_0 + f(m_1 + 2D - k) \pmod 2$, for all $k$. Let $k' = m_0 + 2D - k$. Then

$$f(k') \equiv m_1 - m_0 + f(k' + m_1 - m_0) \pmod 2$$

for any $k'$.

Next, we argue that $m_1 - m_0$ must be even. Suppose $m_1 - m_0$ is odd. Then $f(k') \equiv 1 + f(k' + m_1 - m_0) \pmod 2$ for all $k'$. Hence, applying this a second time with the argument $k' + m_1 - m_0$ instead of $k'$, we get $f(k') \equiv 1 + 1 + f(k' + 2(m_1 - m_0)) \equiv f(k' + 2(m_1 - m_0)) \pmod 2$, and therefore $f(k') = f(k' + 2(m_1 - m_0))$ for any $k' \geq 0$. By our assumption $2(m_1 - m_0) > 0$, and hence it is a period of $f$. Recall that any period of $f$ must be a multiple of the smallest period $D$. Since $D$ is odd, $m_1 - m_0$ must be a multiple of $D$. Furthermore, since $m_1 - m_0 < 2D$, it follows that $m_1 - m_0 = D$. But then $f(k') \equiv 1 + f(k' + D) \pmod 2$, which contradicts the fact that $D$ is the period of $f$.

Since $m_1 - m_0$ is even, we have $f(k') = f(k' + m_1 - m_0)$ for any $k' \geq 0$. Suppose $m_1 - m_0 > 0$. Then it is a period of $f$ and therefore a multiple of $D$. Since $D$ is odd, $m_1 - m_0$ is also a nonzero multiple of $2D$. But this contradicts the fact that $0 < m_1 - m_0 < 2D$. We conclude that $m_0 = m_1$. □

We now compute the zeroes in the correlation between parity and any elementary symmetric polynomial modulo an odd number $q$. When $q$ is prime it is easy to see, by Lucas' theorem (see [13]), that the period of $\binom{k}{d}$ mod $q$ is $q^b$ (in $k$), where $b$ is the smallest integer such that $d < q^b$. The formula for the period of the binomial coefficients modulo $q$ when $q$ is composite is more complicated and is given in the following theorem proved by S. Zabek [15].

**Theorem 4.7.** **[15]** Let $q = p_1^{a_1} \cdots p_r^{a_r}$, where the $p_j$'s are the prime factors of $q$, $d > 0$, and $b_j = \lfloor log_{p_j}(d) \rfloor$. Then the period of $\binom{k}{d}$ mod $q$ is $\prod_{j=1}^{r} p_j^{a_j + b_j}$.

It suffices to note here that when $q$ is odd the period is a product of its prime factors and is therefore odd. Note also that the period of $\binom{k}{d}$ mod $q$ is a multiple of the period of $M_q(e_d)$, and hence, this period is odd too.

It follows from Corollary 3.4 that for any $d$, $M_q(e_d(x))$ has exponentially small correlation with parity. Furthermore, we have

**Theorem 4.8.** Let $q$ be odd and $D$ be the period of $M_q(e_d(x))$. Then, for sufficiently large $n$, $C_n(M_q(e_d), \oplus) = 0$ iff $n = lD + d - 1$, where $l$ is any integer such that $l \equiv d \pmod 2$.

*Proof.* In order to apply Theorem 4.1, we need to derive an appropriate symmetry property of the binomial coefficients. We use the following basic idendity which holds for any integer $k$.

$$\binom{k}{d} = \binom{d-1-k}{d}(-1)^d,$$

and therefore

$$M_q(\binom{k}{d}) = M_q(\binom{d-1-k}{d}).$$

Define $m$ to be $d-1$, if $d$ is even and $D+d-1$, if $d$ is odd, so that $m$ is odd. (Recall that $D$ is odd.) Then we have for any integer $k$

$$M_q(\binom{k}{d}) \equiv m + 1 + M_q(\binom{m-k}{d}) \pmod 2.$$

Now, the claim follows from Theorem 4.1 and Proposition 4.6. □

# 5 Conclusions and Open Problems

We have investigated the correlation between two symmetric Boolean functions. Our technique is to use exponential sums to estimate this important quantity. For the class of symmetric functions, we are able to obtain closed form solutions for the sum. The more interesting result would be to give a similar estimate for any low degree polynomials modulo an odd integer against the parity function, say. The use of exponential sums points to the possibility of applying more sophisticated techniques. There is a strong connection between our sum and the (generalized) Gauss sum or Kloosterman sum (see, e.g., [8]) which we briefly illustrate below.

Consider a polynomial $f(x_1, \ldots, x_n)$ with integer coefficients and degree $d$ on $n$ boolean variables. We consider the correlation between, e.g., this polynomial modulo 3 and the parity function $\oplus$. Let $\omega$ be the third root of unity $e^{2\pi i/3}$. Then

$$\begin{aligned} C_n(f, \oplus) &= 2^{-n+1} \sum_{\{x_1,\ldots,x_n\}\in\{0,1\}^n} \frac{\omega^{f(x_1,\ldots,x_n)} + \omega^{-f(x_1,\ldots,x_n)} + 1}{3} (-1)^{\sum_{j=1}^n x_j} \\ &= \frac{1}{2^{n-2}3} \mathrm{Re} \sum_{\{x_1,\ldots,x_n\}\in\{0,1\}^n} \omega^{f(x_1,\ldots,x_n)} (-1)^{\sum_{j=1}^n x_j}. \end{aligned}$$

If we let $\chi$ be a nontrivial character modulo 3, by rearranging $-1, 1$ for $1, 0$, we have

$$C_n(f, \oplus) = \frac{1}{2^{n-2}3} \mathrm{Re} \sum_{\{x_1,\ldots,x_n\}\in\mathbf{F}_3^n} \omega^{f(x_1,\ldots,x_n)} \chi(x_1) \cdots \chi(x_n),$$

which is precisely the real part of a generalized Gauss sum.

A lot of work has been done in order to estimate sums of this type, especially those results connected with the theorems and conjectures of Weil and Deligne (see [11],[9] for more information). The sums encountered there are usually of the type where one has a fixed number of variables, and considers the sum as the base field is successively extended to degree $n$. In contrast, we have the situation where the number of the variables $n$ is growing but the field is fixed. It would be nice to be able to apply some of their techniques here. At the same time a solution to our problem without their machinery would also be of independent interest to number theory.

### Acknowledgements

We wish to thank Noga Alon, Dave Barrington, Don Coppersmith, Nick Katz, Neal Koblitz, Laci Lovasz, Victor Miller, Andrew Odlyzko, Pete Winkler and Andrew Yao for discussions.

## References

[1] M, Ajtai, $\Sigma_1^1$-formulae on finite structures, *Annals of Pure and Applied Logic* **24** (1983) 1-48.

[2] L. Babai, A random oracle separates PSPACE from the polynomial-time hierarchy, *Information Processing Letters* **26** (1987) 51-53.

[3] D. M. Barrington, R. Beigel, and S. Rudich, Representing Boolean functions as polynomials modulo composite numbers, *Proceedings of the 24th ACM Symposium on Theory of Computing* (1992) 455-461.

[4] J.-Y. Cai, With probability one, a random oracle separates PSPACE from the polynomial-time hierarchy *Journal of Computer and System Science* **38** (1989) 68-85.

[5] M. Furst, J. B. Saxe and M. Sipser, Parity, circuits and the polynomial-time hierarchy, *Mathematical Systems Theory* **17** (1984) 13-27.

[6] F. Green, An oracle separating $\oplus$P from $\mathrm{PP}^{\mathrm{PH}}$, *Information Processing Letters* **37** (1991) 149-153.

[7] J. Håstad, Computational limitations of small-depth circuits, the MIT press, Cambridge, 1987.

[8] K. Ireland and M. Rosen, A classical introduction to modern number theory, Second Edition, Springer-Verlag, New York, 1990.

[9] N. Katz, Sommes Exponentielles, *Astérisque*, 79, 1980.

[10] A. A. Razborov, Lower bounds on the size of bounded depth networks over a complete basis with logical addition, *Matematicheskie Zametki* **41** (1987) 598-607. English translation in *Mathematical Notes of the Academy of Sciences of the USSR* **41** (1987) 333-338.

[11] W. M. Schmidt, Equations over finite fields: An elementary approach, *Lecture Notes in Mathematics*, vol. 536, Springer, New York, 1976.

[12] R. Smolensky, Algebraic methods in the theory of lower bounds for Boolean circuit complexity, in *Proceedings of the 19th Annual ACM Symposium on Theory of Computing* (1987) 77-82.

[13] C. Smorynski, Logical Number Theory, Volume I, Springer-Verlag, 1991.

[14] A.C. Yao, Separating the polynomial-time hierarchy by oracles, in *Proceedings of the 26th Annual IEEE Symposium on Foundations of Computer Science* (1985) 1-10.

[15] S. Zabek, Sur la périodicité modulo $m$ des suites de nombres $\binom{n}{k}$, *Ann. Univ. Mariae Curie-Sklodowska*, A10 (1956) 37-47.