

# The Correlation Between Parity and Quadratic Polynomials Mod 3

Frederic Green\*

Department of Mathematics and Computer Science

Clark University

Worcester, Massachusetts 01610

`fgreen@black.clarku.edu`

## Abstract

We prove exponentially small upper bounds on the correlation between parity and quadratic polynomials mod 3. One corollary of this is that in order to compute parity, circuits consisting of a threshold gate at the top, mod 3 gates in the middle, and AND gates of fan-in two at the inputs must be of size  $2^{\Omega(n)}$ . This is the first result of this type for general mod 3 subcircuits with ANDs of fan-in greater than 1. This yields an exponential improvement over a long-standing result of Smolensky, answering a question recently posed by Alon and Beigel. The proof uses a novel inductive estimate of the relevant exponential sums introduced by Cai, Green and Thierauf. The exponential sum and correlation bounds presented here are tight.

## 1 Introduction

After a flurry of exciting results in the 80's [FSS], [Yao 85], [Cai], [Has], [Raz], [Sm], circuit lower bounds have been few and far between in recent years. One reason for this is that some of the seemingly simplest problems on the “frontier” (e.g., to obtain lower bounds for ACC [Bar], or even just depth-3 circuits with Mod<sub>6</sub> gates) have proved to be deceptively difficult. While some of the difficulties are quite formidable (e.g., the natural proof [RR] barrier presented by TC<sup>0</sup>), there are still very good reasons to continue the effort for (presumably) less powerful circuits. Paramount among these reasons is to develop new lower bound *techniques*, especially those that show deep connections with powerful tools from other areas of mathematics. This paper represents another step in this direction.

Our chief interest in this paper is in circuits with a threshold or majority gate at the top, MOD gates in the middle and AND gates at the bottom (attached to the inputs). Following Alon and Beigel [AB], when the fan-in of the bottom AND gates is bounded by  $f(n)$ , we refer to these as “MAJ  $\circ$  MOD  $\circ$  AND <sub>$f(n)$</sub> ” circuits. These circuits are important for a number of reasons. Recall, for example, that they are very powerful. Allender [Al], using ideas from Toda's Theorem [Tod], showed that all of AC<sup>0</sup> can be simulated by quasipolynomial ( $2^{\log^{O(1)} n}$ ) size MAJ  $\circ$  MOD<sub>2</sub>  $\circ$  AND <sub>$(\log n)^{O(1)}$</sub>  circuits. It is well-known (e.g., [Has]) that both parity and the

---

\*Research supported in part by a grant from NWO, while the author was on sabbatical leave at CWI, Amsterdam, and by Army Research Office Grant DAAD19-02-1-0058.

majority function require exponential-size  $AC^0$ -type circuits, so  $MAJ \circ MOD_2 \circ AND_{(\log n)^{O(1)}}$  circuits are strictly more complex than  $AC^0$ . On the other hand, Yao [Yao 90] has shown (again, using many of the ideas and some of the methods of Toda's Theorem) that depth-3 threshold circuits of quasipolynomial size can simulate ACC. In fact, one can do this simulation with apparently weaker circuit models [BT], [GKRST] that still are at least as powerful as quasipolynomial size  $MAJ \circ MOD_2 \circ AND_{(\log n)^{O(1)}}$ . However, the relationship between  $MAJ \circ MOD_2 \circ AND_{(\log n)^{O(1)}}$  circuits and ACC remains unresolved. This is the central motivating problem we address. (See [Gr99] and [Gr00] for somewhat different perspectives.)

This problem shares some of the difficulties of finding lower bounds for depth 2 and depth 3 threshold circuits. Among the strongest lower bounds of this type is the result of Håstad and Goldmann [HG] that says that the generalized inner-product function requires exponential size  $MAJ \circ MAJ \circ AND_{O((1/2-\epsilon)\log n)}$  circuits. This implies, of course, a similar lower bound against  $MAJ \circ MOD_2 \circ AND_{(1/2-\epsilon)\log n}$  circuits computing generalized inner product. We suspect that even the simpler  $MOD_3$  function cannot be computed by such circuits, however, and the technique underlying the Håstad-Goldmann result is unlikely to resolve the central problem via this function (more detail is given below). A number of authors (e.g., [BM], [Gro], [KP]) have considered other depth-2 and depth-3 combinations of MAJ and MOD's and AND's, but to date little progress has been made on the combination with MOD's in the middle layer.

Another important reason to investigate  $MAJ \circ MOD_m \circ AND$  circuits is that, by the  $\epsilon$ -discriminator method of Hajnal et al. [HMPST], lower bounds for such circuits are equivalent to upper bounds on the ability of  $MOD_m \circ AND$  circuits to approximate given Boolean functions. This problem is interesting in its own right and a resolution may lead to a deeper understanding of ACC circuits. For example, there are still gaps in our understanding of the classes  $ACC(p)$  where  $p$  is prime. Smolensky [Sm] showed that if  $p$  is an odd prime, then  $ACC(p)$ -type circuits of "small" size (those that are below a certain exponential size) can agree with parity for at most a fraction  $1/2 + n^{o(1)}/\sqrt{n}$  of the input settings. By contrast, Håstad and Boppana [Has] showed that small  $AC^0$ -type circuits can agree with parity for at most a fraction  $1/2 + 2^{-n^{\Omega(1)}}$  of the input settings. Do  $ACC(p)$  circuits really give better approximations to parity, or is it possible to sharpen Smolensky's bound so that it is exponentially close to  $1/2$  as well?

Smolensky's theorem [Sm] implies that if  $p$  is an odd prime, then parity requires  $MAJ \circ MOD_p \circ AND_{(\log n)^{O(1)}}$  circuits of size  $\sqrt{n}/(2n^{o(1)})$ . Goldmann [Go] considered the case in which there are no AND gates on the bottom (i.e.,  $MAJ \circ MOD$  circuits), and showed that if  $q$  is a prime not dividing  $m$ , then the  $MOD_q$  function requires  $2^{\Omega(n)}$  size  $MAJ \circ MOD_m$  circuits. Cai, Green and Thierauf [CGT], and later (in a more general setting) Green [Gr99], considered the case in which the  $MOD \circ AND$  subcircuits compute symmetric functions. They showed that the  $MOD_q$  function requires  $2^{n^{\Omega(1)}}$  size  $MAJ \circ MOD_m \circ AND_{(\log n)^{O(1)}}$  circuits, provided the  $MOD_m \circ AND$  subcircuits compute symmetric functions. Recently, Alon and Beigel [AB] took a step toward extending this to the non-symmetric case. They did this by reducing the non-symmetric case to the symmetric case via a Ramsey-Theoretic argument. The result was that  $MOD_q$  requires  $2^{(\log n)^{\Omega(1)}}$  size  $MAJ \circ MOD_m \circ AND_2$  circuits, and  $\omega(1)$  size  $MAJ \circ MOD_m \circ AND_{O(1)}$  circuits. It seems unlikely, however, that Ramsey-Theoretic arguments will yield appreciably stronger results. Also note that Smolensky's technique [Sm] (which only works when  $m$  is a prime power) does not imply a stronger lower bound than  $\sqrt{n}/(2n^{o(1)})$  even if we restrict the fan-in on the AND-gates to be 2 and  $m$  to be 3.

In this paper, we introduce a technique that improves the bound exponentially in this case.

We extend Smolensky’s bound when the AND-gates have fan-in 2 to an exponential lower bound in the case that  $q = 2$  and  $m = 3$ : we show that parity requires  $\text{MAJ} \circ \text{MOD}_3 \circ \text{AND}_2$  circuits of size  $2^{\Omega(n)}$  (see Corollary 3.9). As in previous work, we accomplish this by putting an exponentially small upper bound on the ability of  $\text{MOD}_3 \circ \text{AND}_2$  circuits to approximate the parity function: such circuits can equal the parity function for at best a fraction  $\frac{1}{2} + 2^{-\Omega(n)}$  of all input settings (see Corollary 3.8). This answers a special case ( $q = 2$ ,  $m = 3$ , AND fan-in 2) of a question posed recently by Alon and Beigel [AB]. It represents the first extension of Smolensky’s [Sm] non-approximability results for parity by quadratic polynomials mod 3 to a value that is exponentially close to  $1/2$ .

Note that for composite  $m$ , the lower bound of Alon and Beigel [AB] remains the best that is known. Likewise, if  $m$  is any prime power other than the number 3, Smolensky’s bound [Sm] remains the best known.

Our approach is very different from that of [Sm] or [AB]. We directly evaluate the exponential sums originally introduced by Cai et al. [CGT]. In [CGT] it was shown that the correlation between parity and a  $\text{MOD}_3 \circ \text{AND}$  circuit can be written as an exponential sum (also variously known as a character sum or a generalized Gaussian sum). Evaluations of such sums were also instrumental in the communication complexity lower bound of Babai, Nisan and Szegedy [BNS] on which the Håstad-Goldmann [HG] result is based. Character sums, which originated with Gauss in the study of cyclotomic fields and quadratic reciprocity, have been intensively studied in the number theoretic literature (see, e.g., [LN] and [Sch]). Here we develop a new technique for evaluating the type of sums that arise in computing correlations. The Cauchy-Schwarz method used to great effect in [BNS], while very powerful, appears not to be sufficiently refined for our purposes. Instead we observe some very specific symmetry properties of the sum that can be exploited, via the triangle inequality and various identities involving the additive and multiplicative characters over  $\mathbf{Z}_3$ , to obtain accurate estimates inductively. The power of these simple symmetry arguments is a bit surprising. In fact, our bounds on the exponential sum as well as the correlation itself are the best possible.

The organization of the paper is as follows. In section 2, the terminology and notation for the paper is established, and we review how the problem of computing the circuit lower bounds reduces to the problem of computing upper bounds on the correlation [HMPST]. In turn, we also review how the latter reduces to the evaluation of an exponential sum [CGT]. In section 3, the evaluation of the exponential sum is presented, along with the main results. Tight upper bounds on the correlation itself are also given; while the main results do not require this, it underscores the *exactness* of the technique. In section 4, we address the question as to whether symmetric polynomials yield the highest correlation, which was posed in [AB]. Finally, it is curious that the technique of this paper at present appears to work only for parity versus  $\text{MOD}_3$ , and even then, only in the quadratic case. We explain and discuss these issues in section 5.

## 2 Preliminaries

A  $\text{MOD}_m$  gate takes  $n$  Boolean inputs  $x_1, \dots, x_n$  and outputs 1 if  $\sum_{i=1}^n x_i \not\equiv 0 \pmod{m}$ , and 0 otherwise. A MAJ gate also takes  $n$  inputs and outputs 1 iff more than half of the inputs are 1. Our results also apply to general threshold gates with weights bounded polynomially in the size of the input.

We adopt the convention that an  $n$ -tuple such as  $(x_1, \dots, x_n)$  is represented as a vector  $\mathbf{x}$ . Thus  $\mathbf{x} \in \{0, 1\}^n$  denotes that  $\mathbf{x} = (x_1, \dots, x_n)$  is an  $n$ -tuple of Boolean values.

As in [AB], if  $G$  is a type of Boolean gate and  $\mathcal{C}$  a class of circuits,  $G \circ \mathcal{C}$  denotes the class of circuits with  $\mathcal{C}$ -type circuits serving as inputs to  $G$ -type gates. In measuring the size of such circuits, the size of the  $\mathcal{C}$ -type subcircuits is to be regarded as a function of the number of inputs to the global  $G \circ \mathcal{C}$  circuit.

The *correlation*  $C_n(f_1, f_2)$  between two Boolean functions  $f_1, f_2 : \{0, 1\}^n \rightarrow \{0, 1\}$  is the number of agreements between  $f_1$  and  $f_2$  minus the number of disagreements, normalized by  $2^{-n}$ :

$$C_n(f_1, f_2) = \frac{1}{2^n} \sum_{\mathbf{x} \in \{0, 1\}^n} (-1)^{f_1(\mathbf{x}) + f_2(\mathbf{x})}. \quad (1)$$

The  $\epsilon$ -discriminator lemma of Hajnal et al. [HMPST] shows that the problem of proving lower bounds for a Boolean function  $f$  against circuits with a MAJ gate over subcircuits of a certain type, reduces to the problem of obtaining *upper* bounds on the correlation between  $f$  and one of the subcircuits. We use the lemma in the following form.

**Lemma 2.1.** Let  $T$  be a threshold circuit consisting of a majority gate over subcircuits  $c_1, \dots, c_s$ , each taking up to  $n$  inputs. Thus,  $T$  outputs 1 on input  $\mathbf{x} \in \{0, 1\}^n$  if and only if  $\sum_{i=1}^s c_i(\mathbf{x}) > s/2$ . Let  $T$  compute the Boolean function  $f : \{0, 1\}^n \rightarrow \{0, 1\}$ . Define the correlation  $C_n(f, c_i)$  as in equation (1). If  $|C_n(f, c_i)| \leq \epsilon$  for all  $1 \leq i \leq s$ , then  $s \geq \epsilon^{-1}$ .

Let  $\mathbf{Z}_m$  denote the ring of integers mod  $m$ .

A  $\text{MOD}_m \circ \text{AND}$  circuit is one consisting of a  $\text{MOD}_m$  gate over AND gates attached to the inputs. It is clear that for any  $\text{MOD}_m \circ \text{AND}$  circuit over the inputs  $x_1, \dots, x_n$ , there is a polynomial  $t \in \mathbf{Z}_m[x_1, \dots, x_n]$  such that the circuit outputs 1 iff  $t(x_1, \dots, x_n) \not\equiv 0 \pmod{m}$ . We call  $t$  the *defining polynomial* of the circuit.

It should generally be understandable from the context when quantities (e.g.)  $x, y$  are meant to be in  $\mathbf{Z}_m$ , or if they are meant to be reduced mod  $m$ , for some  $m$ . In this case, we replace the notation  $x \equiv y \pmod{m}$  and  $x \not\equiv y \pmod{m}$  by  $x = y$  and  $x \neq y$ , respectively.

Let  $\mathbf{F}$  be a finite field. A *multiplicative character* is a homomorphism  $\chi : \mathbf{F}^* \rightarrow \mathbf{C}$  from the multiplicative group  $\mathbf{F}^* = \mathbf{F} - \{0\}$  to the complex numbers. By definition, for nontrivial characters one extends the domain of  $\chi$  to include all of  $\mathbf{F}$  by taking  $\chi(0) = 0$ . (For the trivial character  $\varepsilon(\mathbf{F}^*) = 1$ , we take  $\varepsilon(0) = 1$ .) When  $\mathbf{F} = \mathbf{Z}_3$  (which will be true for most of this paper), there are only three field elements, which we write as  $\{0, 1, -1\}$ , and the unique nontrivial  $\chi$  takes a particularly simple form, namely,  $\chi(0) = 0$ ,  $\chi(1) = 1$ , and  $\chi(-1) = -1$ . Since  $\chi^2 = 1$  (when restricted to the domain  $\mathbf{Z}_3^*$ ), we refer to it as the *quadratic character* of  $\mathbf{Z}_3$ .

An additive character is a homomorphism  $\psi$  from the *additive* group of  $\mathbf{F}$  to the complex numbers. In the case of  $\mathbf{Z}_3$ , we use the additive character  $\psi(x) = \omega^x$ , where  $x \in \mathbf{Z}_3$ , and  $\omega$  is the primitive complex cube root of unity  $e^{2\pi i/3}$ . Note that  $\omega^2 = \bar{\omega}$ , where  $\bar{\omega}$  denotes the complex conjugate of  $\omega$ . Also recall the fact that, for  $k \in \mathbf{Z}_3$ ,

$$1 + \omega^k + \bar{\omega}^k = \begin{cases} 3 & \text{if } k = 0 \\ 0 & \text{otherwise.} \end{cases} \quad (2)$$

(Refer to [LN] for more information regarding characters.)

In [CGT], when  $f_1$  is the parity function  $\text{MOD}_2$  and  $f_2$  is the function computed by a  $\text{MOD}_3 \circ \text{AND}$  circuit, the correlation  $C_n(f_1, f_2)$  is written as an exponential sum involving the multiplicative and additive characters. Denote the function computed by the  $\text{MOD}_3 \circ \text{AND}$  circuit as  $f$ , and suppose the defining polynomial of  $f$  is  $r$ . Then,

$$C_n(\text{MOD}_2, f) = \frac{4}{3 \cdot 2^n} \text{Re} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{\sum_{j=1}^n x_j} \omega^{r(\mathbf{x})},$$

where “Re” denotes the real part. Again as in [CGT], making the change of variable  $x_i = (1/2)(1 - y_i)$  where  $y_i \in \{1, -1\}$ , the polynomial  $r$  becomes a new polynomial  $s$  in the  $y_i$  variables, of the same degree:

$$C_n(\text{MOD}_2, f) = \frac{4}{3 \cdot 2^n} \text{Re} \sum_{\mathbf{y} \in \mathbf{Z}_3^n} \chi\left(\prod_{i=1}^n y_i\right) \omega^{s(\mathbf{y})}. \quad (3)$$

Note that the sum can range over all of  $\mathbf{Z}_3$  rather than just  $\{1, -1\}$ , because the relation  $\chi(0) = 0$  eliminates any terms with any  $y_i = 0$ . Finally note that the polynomials  $r$  and  $s$  are multilinear.

Now if the AND’s in the original  $\text{MOD}_3 \circ \text{AND}$  circuit have fan-in at most 2, then the defining polynomial  $r$  is quadratic. Hence  $s$  is quadratic as well. We break up  $s$  into a homogeneous quadratic piece (i.e., a *quadratic form*)  $t(\mathbf{y})$ , and a linear form  $\mathbf{k} \cdot \mathbf{y}$ :

$$\begin{aligned} t(\mathbf{y}) &= \sum_{i=1}^{n-1} \sum_{j=i+1}^n k_{ij} y_i y_j, \\ \mathbf{k} \cdot \mathbf{y} &= \sum_{i=1}^n k_i y_i, \end{aligned}$$

where for all  $1 \leq i, j \leq n$ , the coefficients  $k_{ij}, k_i \in \mathbf{Z}_3$ . There may also be a constant term  $c \in \mathbf{Z}_3$ . Thus, with this notation established, our task is to find an upper bound on correlations of the following form:

$$C(t, \mathbf{k}, c, n) = \frac{4}{3} \text{Re}(S(t, \mathbf{k}, n) \omega^c), \quad (4)$$

where  $S(t, \mathbf{k}, n)$  is of the form:

$$S(t, \mathbf{k}, n) = \frac{1}{2^n} \sum_{\mathbf{y} \in \mathbf{Z}_3^n} \chi\left(\prod_{i=1}^n y_i\right) \omega^{t(\mathbf{y}) + \mathbf{k} \cdot \mathbf{y}}. \quad (5)$$

The reason for not including the constant  $c$  in the definition of  $S(t, \mathbf{k}, n)$  is that, as in [CGT], [Gr99], we prove exponentially small upper bounds on the *norm* of  $S(t, \mathbf{k}, n)$ . This immediately implies exponentially small upper bounds on the real part of  $S(t, \mathbf{k}, n) \omega^c$ , and hence (via equation (4)) on the correlation.

The notation  $S(t, \mathbf{k}, n)$  will always mean that  $t$  is a quadratic form and that  $\mathbf{k} \in \mathbf{Z}_3^n$ . Sometimes the vector  $\mathbf{k}$  will consist entirely of the 0 element of  $\mathbf{Z}_3$ , in which case we use the boldface notation  $\mathbf{0}$ . Similar conventions hold for  $C(t, \mathbf{k}, c, n)$ .

### 3 Evaluation of the Exponential Sum

We now obtain tight upper bounds on the norm of the exponential sum  $S(t, \mathbf{k}, n)$  as defined at the end of the previous section. Note that since by definition  $\chi(0) = 0$ , we can also write  $S$  as,

$$S(t, \mathbf{k}, n) = \frac{1}{2^n} \sum_{\mathbf{y} \in \{1, -1\}^n} \left( \prod_{i=1}^n y_i \right) \omega^{t(\mathbf{y}) + \mathbf{k} \cdot \mathbf{y}}. \quad (6)$$

It will be convenient to work with this form, although we will ultimately return to the original (equation (5)). For typographical reasons it will often be convenient to omit the explicit range of summation of a vector  $\mathbf{y}$ . In this case a sum over  $\mathbf{y}$  where  $\mathbf{y}$  is of length  $n$  is a sum over all  $\mathbf{y} \in \{1, -1\}^n$ .

Our main theorem is,

**Theorem 3.1.** For all  $n$ , the exponential sum  $S(t, \mathbf{k}, n)$  obeys,

$$|S(t, \mathbf{k}, n)| \leq \left( \frac{\sqrt{3}}{2} \right)^{\lceil n/2 \rceil}.$$

Furthermore, this upper bound can be achieved.

The proof of this theorem, which proceeds by induction on  $n$ , rests on a number of relations, given in the following lemmas. We start by noting some useful identities involving the additive and multiplicative characters.

**Lemma 3.2.** Let  $a, b \in \mathbf{Z}_3$ . Then the following identities hold:

- (i)  $\omega^a + \omega^{-a} = \omega^{a^2} + \omega^{-a^2}$ .
- (ii)  $\omega^a - \omega^{-a} = (\omega - \bar{\omega})\chi(a)$ .
- (iii)  $\chi(1+a)\omega^b + \chi(1-a)\omega^{-b} = \omega^{(a-b)^2} + \omega^{-(a+b)^2}$ .

**Proof:** Identities (i) and (ii) can be easily seen by plugging in the values  $\{0, 1, -1\}$  for  $a$ . One can verify identity (iii) in a similar way, but it is perhaps more satisfying to see how to derive it from (i) and (ii) algebraically. For notational convenience, let  $\chi_{\pm} = \chi(1-a) \pm \chi(1+a)$ . First observe that, by identity (ii),

$$\begin{aligned} \chi_+ &= \frac{1}{(\omega - \bar{\omega})} (\omega^{1-a} - \omega^{-1+a} + \omega^{1+a} - \omega^{-1-a}) \\ &= \frac{1}{(\omega - \bar{\omega})} (\omega(\omega^a + \omega^{-a}) - \bar{\omega}(\omega^a + \omega^{-a})) \\ &= \omega^a + \omega^{-a}. \end{aligned}$$

Similarly,

$$\begin{aligned} \chi_- &= \frac{1}{(\omega - \bar{\omega})} (\omega^{1-a} - \omega^{-1+a} - \omega^{1+a} + \omega^{-1-a}) \\ &= \frac{1}{(\omega - \bar{\omega})} (\omega^{-a}(\omega + \bar{\omega}) - \omega^a(\omega + \bar{\omega})) \\ &= \frac{\omega^a - \omega^{-a}}{(\omega - \bar{\omega})} = \chi(a), \end{aligned}$$

where we used the fact that  $\omega + \bar{\omega} = -1$  (see equation (2)). Solving the two resulting equations,

$$\begin{aligned}\chi(1-a) + \chi(1+a) &= \omega^a + \omega^{-a} \\ \chi(1-a) - \chi(1+a) &= \chi(a)\end{aligned}$$

for  $\chi(1-a)$  and  $\chi(1+a)$ , we obtain,

$$\begin{aligned}\chi(1-a) &= \frac{1}{2}(\omega^a + \omega^{-a} + \chi(a)) \\ \chi(1+a) &= \frac{1}{2}(\omega^a + \omega^{-a} - \chi(a)).\end{aligned}$$

Let  $A$  denote the quantity  $\chi(1+a)\omega^b + \chi(1-a)\omega^{-b}$ . Then, making free use of identities (i) and (ii) where necessary, and the fact that  $\chi(a)\chi(b) = \chi(ab)$ , we find,

$$\begin{aligned}A &= \frac{1}{2}[(\omega^a + \omega^{-a} - \chi(a))\omega^b + (\omega^a + \omega^{-a} + \chi(a))\omega^{-b}] \\ &= \frac{1}{2}[\omega^{a+b} + \omega^{-a+b} + \omega^{a-b} + \omega^{-a-b} - \chi(a)(\omega^b - \omega^{-b})] \\ &= \frac{1}{2}[\omega^{(a+b)^2} + \omega^{-(a+b)^2} + \omega^{(a-b)^2} + \omega^{-(a-b)^2} - (\omega - \bar{\omega})\chi(a)\chi(b)] \\ &= \frac{1}{2}[\omega^{(a+b)^2} + \omega^{-(a+b)^2} + \omega^{(a-b)^2} + \omega^{-(a-b)^2} - (\omega - \bar{\omega})\chi(ab)] \\ &= \frac{1}{2}[\omega^{(a+b)^2} + \omega^{-(a+b)^2} + \omega^{(a-b)^2} + \omega^{-(a-b)^2} - (\omega^{ab} - \omega^{-ab})].\end{aligned}$$

Expanding the expressions in the exponent (i.e.,  $(a+b)^2$  and  $(a-b)^2$ ) yields,

$$A = \frac{1}{2}[\omega^{ab}(-1 + \omega^{a^2+b^2} + \omega^{-a^2-b^2}) + \omega^{-ab}(1 + \omega^{a^2+b^2} + \omega^{-a^2-b^2})].$$

Now by equation (2),  $1 + \omega^k + \omega^{-k} = 0$  iff  $k \neq 0$ , and note that in  $\mathbf{Z}_3$ ,  $a = b = 0$  exactly when  $a^2 + b^2 = 0$ . Therefore, the quantity  $1 + \omega^{a^2+b^2} + \omega^{-a^2-b^2}$  is nonzero iff  $a = b = 0$ . The factor multiplying it ( $\omega^{-ab}$ ) can thus be replaced with  $\omega^{ab}$ . Thus,

$$\begin{aligned}A &= \frac{1}{2}[\omega^{ab}(1 + \omega^{a^2+b^2} + \omega^{-a^2-b^2}) + \omega^{ab}(-1 + \omega^{a^2+b^2} + \omega^{-a^2-b^2})] \\ &= \omega^{ab}(\omega^{a^2+b^2} + \omega^{-a^2-b^2}),\end{aligned}$$

from which (iii) follows immediately. □

We next give a simple but very useful symmetry property of  $S(t, \mathbf{k}, n)$ .

**Lemma 3.3.** For any  $n$ ,

$$S(t, \mathbf{k}, n) = (-1)^n S(t, -\mathbf{k}, n).$$

**Proof:** Let  $n$  be even. In the formula (6) for  $S(t, \mathbf{k}, n)$ , make the change of variable  $y_i \mapsto -y_i$ . Then, since  $n$  is even and the terms in  $t(\mathbf{y})$  are all of even degree, under this change of variable  $\prod_{i=1}^n y_i \mapsto \prod_{i=1}^n y_i$ , and  $t(\mathbf{y}) \mapsto t(\mathbf{y})$ , whereas  $\mathbf{k} \cdot \mathbf{y} \mapsto -\mathbf{k} \cdot \mathbf{y}$ . Hence  $S(t, \mathbf{k}, n) = S(t, -\mathbf{k}, n)$ .

On the other hand, if  $n$  is odd, under the same change of variable,  $\prod_{i=1}^n y_i \mapsto -\prod_{i=1}^n y_i$ , while  $t(\mathbf{k})$  and  $\mathbf{k} \cdot \mathbf{y}$  transform as they did before. Hence  $S(t, \mathbf{k}, n) = -S(t, -\mathbf{k}, n)$ .  $\square$

Observe that, as a consequence of Lemma 3.3, if  $n$  is odd then  $S(t, \mathbf{0}, n) = 0$ . Hence for odd  $n$ , a  $\text{MOD}_3 \circ \text{AND}$  circuit whose defining polynomial *expressed in terms of the  $y_i$  variables* is quadratic and homogeneous, has *zero* correlation with parity. In fact, the proof of Lemma 3.3 says that the resulting polynomial need not be quadratic; any polynomial all of whose terms are of even degree has zero correlation with parity if  $n$  is odd.

**Lemma 3.4.** If  $n$  is even, there exists a quadratic form  $t' \in \mathbf{Z}_3[y_1, \dots, y_n]$  such that,

$$|S(t, \mathbf{k}, n)| \leq |S(t', \mathbf{0}, n)|.$$

**Proof:** By Lemma 3.3,

$$\begin{aligned} S(t, \mathbf{k}, n) &= S(t, -\mathbf{k}, n) \\ &= \frac{1}{2} (S(t, \mathbf{k}, n) + S(t, -\mathbf{k}, n)) \\ &= \frac{1}{2^{n+1}} \sum_{\mathbf{y}} \left( \prod_{i=1}^n y_i \right) \omega^{t(\mathbf{y})} (\omega^{\mathbf{k} \cdot \mathbf{y}} + \omega^{-\mathbf{k} \cdot \mathbf{y}}). \end{aligned}$$

Using Lemma 3.2(i) with  $a = \mathbf{k} \cdot \mathbf{y}$ , the last equality implies,

$$S(t, \mathbf{k}, n) = \frac{1}{2^{n+1}} \sum_{\mathbf{y}} \left( \prod_{i=1}^n y_i \right) \omega^{t(\mathbf{y})} (\omega^{(\mathbf{k} \cdot \mathbf{y})^2} + \omega^{-(\mathbf{k} \cdot \mathbf{y})^2}).$$

Now since  $y_i^2 = 1$  for all  $i$ , we have that  $(\mathbf{k} \cdot \mathbf{y})^2 = t_k(\mathbf{y}) + c$  where  $t_k$  is a quadratic form and  $c$  is a constant (independent of  $\mathbf{y}$ ). Setting  $t^+(\mathbf{y}) = t(\mathbf{y}) + t_k(\mathbf{y})$  and  $t^-(\mathbf{y}) = t(\mathbf{y}) - t_k(\mathbf{y})$ , note that both  $t^+$  and  $t^-$  are quadratic forms. We thus have,

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

Hence, by the triangle inequality,

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

Taking  $t'$  to be  $t^+$  or  $t^-$ , depending on which of  $|S(t^+, \mathbf{0}, n)|$  or  $|S(t^-, \mathbf{0}, n)|$  is the maximum, the lemma follows.  $\square$

Lemma 3.4 shows that the inhomogeneous (quadratic plus linear) case reduces to the homogeneous quadratic case for even  $n$ . The next lemma shows that there is an intimate connection between the homogeneous quadratic case for even  $n$  and the inhomogeneous case for  $n - 1$ .

**Lemma 3.5.** Let  $n$  be even. Then there is a quadratic form  $t' \in \mathbf{Z}_3[y_2, \dots, y_n]$  and a  $\mathbf{k} \in \mathbf{Z}_3^{n-1}$  such that,

$$S(t, \mathbf{0}, n) = S(t', \mathbf{k}, n - 1).$$

**Proof:** For convenience, we introduce some notation. Write  $t$  as,

$$t(y_1, \dots, y_n) = t_2(y_2, \dots, y_n) + y_1(\mathbf{k}_1 \cdot \mathbf{y} \lfloor_2),$$

where  $t_2$  is the homogeneous part of  $t$  that only involves the variables  $y_2, \dots, y_n$ ,  $\mathbf{k}_1$  denotes the vector of coefficients  $k_{1j}$ ,  $\mathbf{y} \lfloor_2$  denotes the vector of variables  $(y_2, \dots, y_n)$ , and thus  $\mathbf{k}_1 \cdot \mathbf{y} \lfloor_2$  denotes  $\sum_{j=2}^n k_{1j} y_j$ .

We write the sum for  $S(t, \mathbf{0}, n)$  and do the sum over  $y_1$ :

$$\begin{aligned} S(t, \mathbf{0}, n) &= \frac{1}{2^n} \sum_{\mathbf{y}} \left( \prod_{i=1}^n y_i \right) \omega^{t_2(\mathbf{y} \lfloor_2) + y_1(\mathbf{k}_1 \cdot \mathbf{y} \lfloor_2)} \\ &= \frac{1}{2^n} \sum_{\mathbf{y} \lfloor_2} \left( \prod_{i=2}^n y_i \right) \omega^{t_2(\mathbf{y} \lfloor_2)} (\omega^{\mathbf{k}_1 \cdot \mathbf{y} \lfloor_2} - \omega^{-\mathbf{k}_1 \cdot \mathbf{y} \lfloor_2}) \\ &= \frac{1}{2} (S(t_2, \mathbf{k}_1, n-1) - S(t_2, -\mathbf{k}_1, n-1)) \\ &= S(t_2, \mathbf{k}_1, n-1), \end{aligned}$$

where, noting that  $n-1$  is odd, we applied Lemma 3.3 to obtain the last equality. Now taking  $t'$  to be  $t_2$  and  $\mathbf{k}$  to be  $\mathbf{k}_1$ , the result follows.  $\square$

Lemma 3.5 shows that the maximal sums for even  $n$  are *equal* to the maximal sums for  $n-1$ . Thus, in our inductive proof we gain no factors of  $\sqrt{3}/2$  in going from odd  $n$  to (even)  $n+1$ . These factors arise in going from *even*  $n$  to  $n+1$ , and thus the following lemma is the cornerstone of the proof.

**Lemma 3.6.** Let  $n$  be odd. Then there is a quadratic form  $t' \in \mathbf{Z}_3[y_2, \dots, y_n]$  such that,

$$|S(t, \mathbf{k}, n)| \leq \left( \frac{\sqrt{3}}{2} \right) |S(t', \mathbf{0}, n-1)|.$$

**Proof:** Proceeding as in the proof of Lemma 3.4, by Lemma 3.3,

$$\begin{aligned} S(t, \mathbf{k}, n) &= \frac{1}{2} (S(t, \mathbf{k}, n) - S(t, -\mathbf{k}, n)) \\ &= \frac{1}{2^{n+1}} \sum_{\mathbf{y}} \left( \prod_{i=1}^n y_i \right) \omega^{t(\mathbf{y})} (\omega^{\mathbf{k} \cdot \mathbf{y}} - \omega^{-\mathbf{k} \cdot \mathbf{y}}). \end{aligned}$$

Apply the identity from Lemma 3.2(ii), with  $a = \mathbf{k} \cdot \mathbf{y}$ . Then,

$$\begin{aligned} S(t, \mathbf{k}, n) &= \frac{1}{2^{n+1}} \sum_{\mathbf{y}} \left( \prod_{i=1}^n y_i \right) \omega^{t(\mathbf{y})} (\omega - \bar{\omega}) \chi(\mathbf{k} \cdot \mathbf{y}) \\ &= \frac{1}{2^n} \cdot \frac{(\omega - \bar{\omega})}{2} \sum_{\mathbf{y}} \chi(\mathbf{k} \cdot \mathbf{y}) \left( \prod_{i=1}^n y_i \right) \omega^{t(\mathbf{y})}. \end{aligned}$$

Now since  $S(t, \mathbf{0}, n) = 0$  (as we conclude either from Lemma 3.3 or the above relation, since  $\chi(0) = 0$ ), we may assume that some  $k_i$  is nonzero, since if all of the  $k_i$  are 0 the bound is trivially satisfied. Without loss of generality we may assume that  $k_1 \neq 0$ . To simplify

the expressions further, we may assume that  $k_1 = 1$ ; if  $k_1$  happens to be  $-1$ , we can flip the sign of  $y_1$  and obtain a sum of exactly the same type with  $k_1 = 1$ . Now to reduce this sum to  $n - 1$  variables, we first break up  $t$  as we did in the proof of Lemma 3.5. That is, write  $t(\mathbf{y}) = t_2(\mathbf{y}_{[2]}) + y_1 \mathbf{k}_1 \cdot \mathbf{y}_{[2]}$ , where as before  $\mathbf{y}_{[2]}$  denotes  $(y_2, \dots, y_n)$ , and  $\mathbf{k}_1 \cdot \mathbf{y}_{[2]}$  denotes  $\sum_{i=2}^n k_{1i} y_i$ . Next do the sum over  $y_1$ . Since  $\prod_{i=1}^n y_i$  is really  $\chi(\prod_{i=1}^n y_i)$ , we may write  $\chi(\mathbf{k} \cdot \mathbf{y}) \prod_{i=1}^n y_i = \chi(y_1 \mathbf{k} \cdot \mathbf{y}) \prod_{i=2}^n y_i$ . When  $y_1 = 1$ , we have  $y_1 \mathbf{k} \cdot \mathbf{y} = 1 + \mathbf{k} \cdot \mathbf{y}_{[2]}$ , and when  $y_1 = -1$ , we have  $y_1 \mathbf{k} \cdot \mathbf{y} = 1 - \mathbf{k} \cdot \mathbf{y}_{[2]}$ , where again,  $\mathbf{k} \cdot \mathbf{y}_{[2]}$  denotes  $\sum_{i=2}^n k_i y_i$ . (Note that  $\mathbf{k}$  and  $\mathbf{k}_1$  are not necessarily the same.) Let  $s_+(\mathbf{y})$  denote  $\chi(1 + \mathbf{k} \cdot \mathbf{y}_{[2]}) \omega^{\mathbf{k}_1 \cdot \mathbf{y}}$  and  $s_-(\mathbf{y})$  denote  $\chi(1 - \mathbf{k} \cdot \mathbf{y}_{[2]}) \omega^{-\mathbf{k}_1 \cdot \mathbf{y}}$ . Then,

$$S(t, \mathbf{k}, n) = \frac{1}{2^n} \cdot \frac{(\omega - \bar{\omega})}{2} \sum_{\mathbf{y}_{[2]}} \prod_{i=2}^n y_i \omega^{t_2(\mathbf{y}_{[2]})} (s_+(\mathbf{y}) + s_-(\mathbf{y})),$$

where

$$s_+(\mathbf{y}) + s_-(\mathbf{y}) = \chi(1 + \mathbf{k} \cdot \mathbf{y}_{[2]}) \omega^{\mathbf{k}_1 \cdot \mathbf{y}} + \chi(1 - \mathbf{k} \cdot \mathbf{y}_{[2]}) \omega^{-\mathbf{k}_1 \cdot \mathbf{y}}.$$

We now apply the crucial identity Lemma 3.2(iii), with the correspondence  $a = \mathbf{k} \cdot \mathbf{y}_{[2]}$  and  $b = \mathbf{k}_1 \cdot \mathbf{y}_{[2]}$ , in the above equation. We obtain,

$$s_+(\mathbf{y}) + s_-(\mathbf{y}) = \omega^{(\mathbf{k} \cdot \mathbf{y}_{[2]} - \mathbf{k}_1 \cdot \mathbf{y}_{[2]})^2} + \omega^{-(\mathbf{k} \cdot \mathbf{y}_{[2]} + \mathbf{k}_1 \cdot \mathbf{y}_{[2]})^2}.$$

Now the expression for  $S(t, \mathbf{k}, n)$  consists of two sums in  $n - 1$  variables entailing quadratic forms in the exponent (plus constants). That is, there are quadratic forms  $t^{(1)}, t^{(2)} \in \mathbf{Z}_3[y_2, \dots, y_n]$  and constants  $c_1, c_2 \in \mathbf{Z}_3$  such that,

$$S(t, \mathbf{k}, n) = \frac{(\omega - \bar{\omega})}{2} \cdot \frac{1}{2} \cdot (S(t^{(1)}, \mathbf{0}, n - 1) \omega^{c_1} + S(t^{(2)}, \mathbf{0}, n - 1) \omega^{c_2}). \quad (7)$$

Applying the triangle inequality as in Lemma 3.4, and using the fact that  $|\omega - \bar{\omega}| = \sqrt{3}$ , the result follows.  $\square$

We can now present the proof of the main theorem.

**Proof of Theorem 3.1:** We obtain an upper bound on  $|S(t, \mathbf{k}, n)|$  by induction on  $n$ . First consider  $n = 1$ . In this case, there is no quadratic piece and our sum has the form,

$$\frac{1}{2} \sum_{y \in \{1, -1\}} \chi(y) \omega^{ky},$$

where  $k \in \mathbf{Z}_3$ . If  $k = 0$ , this sum is 0. If  $k \neq 0$ , this is readily seen to have the value  $\pm(\omega - \bar{\omega})/2$  which, in turn, has norm  $\sqrt{3}/2$ , thus establishing the result for  $n = 1$ .

Now suppose  $n$  is even, and that the result holds for  $m = n - 1$ . By Lemma 3.4, there is a quadratic form  $t'$  such that

$$|S(t, \mathbf{k}, n)| \leq |S(t', \mathbf{0}, n)|.$$

By Lemma 3.5, there is a quadratic form  $t''$  and a  $\mathbf{k} \in \mathbf{Z}_3^{n-1}$  such that,

$$|S(t', \mathbf{0}, n)| = |S(t'', \mathbf{k}, n - 1)|.$$

Noting that  $\lceil (n-1)/2 \rceil = n/2 = \lceil n/2 \rceil$ , the inductive hypothesis says that

$$|S(t'', \mathbf{k}, n-1)| \leq \left(\frac{\sqrt{3}}{2}\right)^{\lceil n/2 \rceil},$$

which establishes the desired result for even  $n$ .

Now suppose  $n$  is odd, and that the result holds for  $m = n-1$ . Lemma 3.6 says there is a quadratic form  $t'$  such that,

$$|S(t, \mathbf{k}, n)| \leq \left(\frac{\sqrt{3}}{2}\right) |S(t', \mathbf{0}, n-1)|.$$

By the inductive hypothesis,  $|S(t', \mathbf{0}, n-1)| \leq (\sqrt{3}/2)^{m/2}$ . Thus,

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

which establishes the result for odd  $n$ .

It is easy to see that the bound is tight, since we can meet it as follows. For even  $n$ , the quadratic form

$$t(y_1, \dots, y_n) = y_1y_2 + y_3y_4 + y_5y_6 + \dots + y_{n-1}y_n \quad (8)$$

yields a maximum  $|S(t, \mathbf{0}, n)|$  (and therefore, by Lemma 3.4, a maximum  $|S(t, \mathbf{k}, n)|$ ). The computation is easy since the sum factors into  $n/2$  pieces, each of the form,

$$\frac{1}{4} \sum_{y_1, y_2 \in \{1, -1\}} \chi(y_1y_2) \omega^{y_1y_2},$$

which has norm  $\sqrt{3}/2$ . Similarly, for odd  $n$ , the (nonhomogeneous!) polynomial,

$$t(y_1, \dots, y_n) = y_1 + y_2y_3 + y_4y_5 + \dots + y_{n-1}y_n \quad (9)$$

yields the maximum norm for the exponential sum.  $\square$

It is interesting to observe that while the maximal quadratic polynomials for even  $n$  are quadratic forms (as indeed they must be in accordance with Lemma 3.4), the maximal quadratic polynomials for odd  $n$  have only *one* linear term. It is also notable that precisely the same polynomials arise in computing the number of zeroes of quadratic polynomials in finite fields of characteristic 2 (see, e.g., [LN], Chapter 6, Theorem 6.30).

By equation (4), Theorem 3.1 immediately implies an exponentially small upper bound on the correlation.

**Corollary 3.7.** For all  $n$ ,

$$|C(t, \mathbf{k}, c, n)| \leq \frac{4}{3} \cdot \left(\frac{\sqrt{3}}{2}\right)^{\lceil n/2 \rceil}.$$

We thus obtain the circuit lower bounds that result from the main theorem. By Corollary 3.7, we obtain immediately,

**Corollary 3.8.** Any  $\text{MOD}_3 \circ \text{AND}_2$  circuit can agree with parity for at most a fraction  $1/2 + 2^{-\Omega(n)}$  of the input settings.

By Corollary 3.7 and Lemma 2.1, we obtain,

**Corollary 3.9.** Circuits of type  $\text{MAJ} \circ \text{MOD}_3 \circ \text{AND}_2$  must have size  $2^{\Omega(n)}$  to compute parity.

We conclude this section with a result of a more technical nature. It is a fortuitous by-product of the proof that the bound in Theorem 3.1 is tight. However, the upper bound on the correlation in Corollary 3.7 is not tight, since the right-hand side can be irrational, whereas  $C(t, \mathbf{k}, c, n)$  is always rational. In the interest of completeness, and to do full justice to the title of this paper, we feel compelled to ask if it is possible to push through tight upper bounds for the correlation as well. Indeed, this can be done using the results and techniques of this section, as we now explain. It turns out that this is not as straightforward as one might think *à priori*. Indeed, the proof that follows also illustrates why the norm of the exponential sum appears to be a much more convenient quantity to work with than its real part. We arrive at the following refinement of Corollary 3.7.

**Theorem 3.10.** For all  $n$ ,

$$|C(t, \mathbf{k}, c, n)| \leq \left(\frac{3}{4}\right)^{\lceil n/4 \rceil - 1}.$$

Furthermore, this bound can be achieved.

**Proof:** We begin by explicitly evaluating  $S(t, \mathbf{k}, n)$  when the polynomials are the maximal ones given in equations (8) and (9). In these cases, we have simply,

$$S(t, \mathbf{k}, n) = \left(\frac{\omega - \bar{\omega}}{2}\right)^{\lceil n/2 \rceil} = \left(\frac{\sqrt{-3}}{2}\right)^{\lceil n/2 \rceil}. \quad (10)$$

First consider the case in which  $n \equiv 0 \pmod{4}$ . Then the maximal polynomial has  $\mathbf{k} = \mathbf{0}$ , the quantity  $S(t, \mathbf{0}, n)$  is real, and has absolute value,

$$|S(t, \mathbf{0}, n)| = \left(\frac{3}{4}\right)^{\lceil n/4 \rceil}.$$

Hence in this case

$$|C(t, \mathbf{0}, 0, n)| = \frac{4}{3} \text{Re} S(t, \mathbf{0}, n) = \left(\frac{3}{4}\right)^{\lceil n/4 \rceil - 1},$$

which establishes the result for  $n \equiv 0 \pmod{4}$ . Now, since  $n$  is even, it follows from Lemma 3.5 that the maximal value for  $S(t', \mathbf{k}', n-1)$  is the same as for  $S(t, \mathbf{0}, n)$ . Since  $\lceil (n-1)/4 \rceil = \lceil n/4 \rceil$ , this also establishes the result for  $n-1$ . Thus the assertion holds if  $n \equiv 0 \pmod{4}$  or  $n \equiv 3 \pmod{4}$ .

We now consider the case in which  $n \equiv 1 \pmod{4}$ . Again, as above, by Lemma 3.5 this takes care of the case  $n \equiv 2 \pmod{4}$  as well, so the assertion holds for all values of  $n$ . We prove the result for  $n \equiv 1 \pmod{4}$  by induction on  $n$  such that  $n \equiv 1 \pmod{4}$ . For  $n = 1$ , by equation (10), the maximal  $S(t, \mathbf{k}, n)$  is  $i\sqrt{3}/2$ . To obtain the correlation, we rotate this as close as possible to the real axis by choosing  $c = -1$ . Then,

$$C(t, \mathbf{k}, -1, 1) = \frac{4}{3} \operatorname{Re}(i\bar{\omega}\sqrt{3}/2) = \frac{2}{\sqrt{3}} \operatorname{Re}(i\bar{\omega}) = 1,$$

which is clearly maximal and proves the result for  $n = 1$ .

Now suppose the result is true for  $n - 4$  where  $n \equiv 1 \pmod{4}$ . That is, suppose, for any quadratic form  $t'$  in  $n - 4$  variables,  $\mathbf{k}' \in \mathbf{Z}_3^{n-4}$  and  $c' \in \mathbf{Z}_3$ , that

$$|C(t', \mathbf{k}', c', n - 4)| \leq \left(\frac{3}{4}\right)^{\lceil (n-4)/4 \rceil - 1}. \quad (11)$$

Consider the quantity  $S(t, \mathbf{k}, n)$ . Since  $n$  is odd, by the proof of Lemma 3.6, in particular equation (7), there are quadratic forms  $s^{(1)}, s^{(2)}$  in  $n - 1$  variables and constants  $c_1, c_2 \in \mathbf{Z}_3$  such that,

$$\begin{aligned} S(t, \mathbf{k}, n) &= \frac{(\omega - \bar{\omega})}{2} \cdot \frac{1}{2} \cdot (S(s^{(1)}, \mathbf{0}, n - 1)\omega^{c_1} + S(s^{(2)}, \mathbf{0}, n - 1)\omega^{c_2}) \\ &= \frac{\sqrt{-3}}{2} \cdot \frac{1}{2} \sum_{\ell=1}^2 S(s^{(\ell)}, \mathbf{0}, n - 1)\omega^{c_\ell}. \end{aligned}$$

Note that  $n - 1$  is even. By Lemma 3.5, there are quadratic forms  $t^{(1)}, t^{(2)}$  in  $n - 2$  variables, and vectors  $\mathbf{k}^{(1)}, \mathbf{k}^{(2)} \in \mathbf{Z}_3^{n-2}$  such that,

$$S(t, \mathbf{k}, n) = \frac{\sqrt{-3}}{2} \cdot \frac{1}{2} \sum_{\ell=1}^2 S(t^{(\ell)}, \mathbf{k}^{(\ell)}, n - 2)\omega^{c_\ell}.$$

Now that  $n - 2$  is odd, we apply equation (7) again, for  $S(t^{(1)}, \mathbf{k}^{(1)}, n - 2)$  and  $S(t^{(2)}, \mathbf{k}^{(2)}, n - 2)$  separately. There are quadratic forms  $u^{(1)}, u^{(2)}, u^{(3)}, u^{(4)}$  in  $n - 3$  variables, and constants  $a_1, a_2, a_3, a_4 \in \mathbf{Z}_3$  such that,

$$S(t, \mathbf{k}, n) = \left(\frac{\sqrt{-3}}{2}\right)^2 \cdot \frac{1}{4} \sum_{\ell=1}^4 S(u^{(\ell)}, \mathbf{0}, n - 3)\omega^{a_\ell}.$$

We employ Lemma 3.5 one final time, to conclude that there are quadratic forms  $v^{(1)}, v^{(2)}, v^{(3)}, v^{(4)}$  in  $n - 4$  variables, and vectors  $\mathbf{m}^{(1)}, \mathbf{m}^{(2)}, \mathbf{m}^{(3)}, \mathbf{m}^{(4)} \in \mathbf{Z}_3^{n-4}$  such that,

$$S(t, \mathbf{k}, n) = -\frac{3}{4} \cdot \frac{1}{4} \sum_{\ell=1}^4 S(v^{(\ell)}, \mathbf{m}^{(\ell)}, n - 4)\omega^{a_\ell}.$$

We multiply both sides of the above equation by  $(4/3)\omega^c$  and then apply the operator “Re” to both sides. Since “Re” is linear (i.e.,  $\operatorname{Re}(z_1 + z_2) = \operatorname{Re}(z_1) + \operatorname{Re}(z_2)$ , and  $\operatorname{Re}(az) = a\operatorname{Re}(z)$  if  $a$  is real), we find,

$$C(t, \mathbf{k}, c, n) = -\frac{3}{4} \cdot \frac{1}{4} \sum_{\ell=1}^4 C(v^{(\ell)}, \mathbf{m}^{(\ell)}, a'_\ell, n - 4),$$

for some  $a'_1, a'_2, a'_3, a'_4 \in \mathbf{Z}_3$ . Now apply the triangle inequality to this equation. Let  $|C(v^{(\ell_0)}, \mathbf{m}^{(\ell_0)}, a'_{\ell_0}, n-4)|$  denote the maximum of the four values appearing on the right-hand side, and let  $t' = v^{(\ell_0)}$ ,  $\mathbf{k}' = \mathbf{m}^{(\ell_0)}$ , and  $c' = a'_{\ell_0}$ . Then,

$$|C(t, \mathbf{k}, c, n)| \leq \frac{3}{4} |C(t', \mathbf{k}', c', n-4)|.$$

By the induction hypothesis (11),

$$|C(t, \mathbf{k}, c, n)| \leq \frac{3}{4} \cdot \left(\frac{3}{4}\right)^{\lceil (n-4)/4 \rceil - 1} = \left(\frac{3}{4}\right)^{\lceil n/4 \rceil - 1},$$

which establishes the upper bound on  $|C(t, \mathbf{k}, c, n)|$ . We can meet this bound by choosing the maximal polynomial (9) and choosing  $c$  to rotate  $S(t, \mathbf{k}, n)$  as close as possible to the real axis. This concludes the proof.  $\square$

## 4 Symmetric and Reducible Polynomials

Alon and Beigel [AB] (and, independently, this author) have asked if symmetric polynomials give the highest correlation, the degree being fixed. If this were the case, then the results of [CGT], [Gr99] would imply exponential lower bounds for  $\text{MAJ} \circ \text{MOD}_m \circ \text{AND}_{\text{polylog}}$  circuits. Note that the optimal polynomials written down in (8) and (9) are *not* symmetric. Is it nevertheless the case that some symmetric polynomial could give as high a correlation as the known maximal ones?

The answer is no. In this section we examine the case in which  $t(\mathbf{y})$  and  $\mathbf{k} \cdot \mathbf{y}$  are symmetric forms. In this case the correlation is much smaller than the tight upper bound of Theorem 3.1.

**Theorem 4.1.** If  $t$  is a symmetric quadratic form and  $\mathbf{k} \cdot \mathbf{y}$  is a symmetric linear form, then

$$|S(t, \mathbf{k}, n)| \leq 2 \cdot \left(\frac{\sqrt{3}}{2}\right)^n.$$

**Proof:** If  $t(\mathbf{y})$  is symmetric, then by a well-known theorem it can be written as an elementary symmetric polynomial:

$$t(\mathbf{y}) = c \sum_{i < j} y_i y_j,$$

for some  $c \in \mathbf{Z}_3$ . Assume that the  $y_i \in \{-1, 1\}$ , which suffices for the evaluation of  $S(t, \mathbf{k}, n)$ . Now observe that

$$\left(\sum_{i=1}^n y_i\right)^2 = \sum_{i \neq j} y_i y_j + n = -\sum_{i < j} y_i y_j + n,$$

by virtue of the fact that  $y_i^2 = 1$ . Thus, without loss of generality,

$$t(\mathbf{y}) = -c \left(\sum_{i=1}^n y_i\right)^2 + cn.$$

If  $\mathbf{k} \cdot \mathbf{y}$  is symmetric, then (similarly) we can write it as  $k \sum_{i=1}^n y_i$  for  $k \in \mathbf{Z}_3$ .

Now the sum  $S(t, \mathbf{k}, n)$  can be written as,

$$S(t, \mathbf{k}, n) = \frac{\omega^{cn}}{2^n} \sum_{\mathbf{y}} \prod_{i=1}^n y_i \omega^{-c(\sum_{i=1}^n y_i)^2 + k \sum_{i=1}^n y_i}.$$

We “reduce” this to the linear case as follows. Let  $a \in \mathbf{Z}_3$ . Then, using equation (2),

$$\omega^{-ca^2+ka} = \frac{1}{3} \sum_{\ell=0}^2 (1 + \omega^{a-\ell} + \omega^{-a+\ell}) \cdot \omega^{-c\ell^2+k\ell}.$$

Then, using the above relation with  $a = \sum_{i=1}^n y_i$ ,

$$\begin{aligned} S(t, \mathbf{k}, n) &= \frac{\omega^{cn}}{2^n} \cdot \frac{1}{3} \cdot \sum_{\ell=0}^2 \sum_{\mathbf{y}} \prod_{i=1}^n y_i (1 + \omega^{\sum_{i=1}^n y_i - \ell} + \omega^{-\sum_{i=1}^n y_i + \ell}) \omega^{-c\ell^2+k\ell} \\ &= \frac{\omega^{cn}}{2^n} \cdot \frac{1}{3} \cdot \sum_{\ell=0}^2 \sum_{\mathbf{y}} \prod_{i=1}^n y_i (\omega^{\sum_{i=1}^n y_i - \ell} + \omega^{-\sum_{i=1}^n y_i + \ell}) \omega^{-c\ell^2+k\ell}, \end{aligned}$$

where the last equality follows from the fact that  $\sum_{\mathbf{y}} \prod_{i=1}^n y_i = 0$ . It is straightforward to evaluate the resulting sum exactly, since the sum over  $\mathbf{y}$  breaks up into  $n$  factors:

$$S(t, \mathbf{k}, n) = \frac{\omega^{cn}}{2^n} \cdot \frac{1}{3} \cdot \sum_{\ell=0}^2 \left( \omega^{-\ell} (\omega - \bar{\omega})^n + \omega^{\ell} (\bar{\omega} - \omega)^n \right) \omega^{-c\ell^2+k\ell}$$

The right hand side consists of six terms each of norm  $(1/3)(\sqrt{3}/2)^n$ . By the triangle inequality, the theorem follows.  $\square$

Thus non-symmetric polynomials can yield a strictly greater correlation than symmetric polynomials. Note that in the course of the proof of the preceding theorem, we found that  $t$  is *reducible* (up to a constant term). Using this fact, it was then possible to reduce the evaluation of the sum to the evaluation of a sum involving a *linear* polynomial. The technique can easily be generalized to prove that  $|S(t, \mathbf{k}, n)| \leq c(\sqrt{3}/2)^n$  for some constant  $c$  whenever  $t$  is reducible. Hence the bound of Theorem 3.1 can only be met by irreducible polynomials.

Although symmetric polynomials do not give the highest correlation, the maximal polynomials nevertheless have a special form. In the terminology of [Gr99], they are *block symmetric*, that is, symmetric in *pairwise disjoint* subsets of the inputs. In [Gr99], it is shown that low-degree block-symmetric polynomials give an exponentially small correlation *in general*. Thus if it can be shown that block-symmetric polynomials give the highest correlation (the degree being fixed), the main problem of this paper will be solved. A further comment on this point appears in the final section.

## 5 Discussion

We believe that it will be possible to generalize the techniques of this paper to higher degree polynomials, as well as to other moduli than 3. Our motivation for reporting on the special case of parity versus  $\text{MOD}_3$  here is, in part, because the proof is simple enough to indicate, in broad outline, how a more general proof would proceed, but also sufficiently subtle so as to indicate where exactly the problems lie.

What are the difficulties? They exist on two fronts. Let us first consider extending the  $\text{MOD}_3$  result to higher-degree polynomials. For example, consider polynomials of degree 3. In this case, we immediately lose most of the nice symmetry properties (e.g., Lemma 3.3) that were instrumental in the proof. We need to exploit other properties of the sum. It is not clear what those properties are. The nature of the identity in Lemma 3.2(iii), and if some suitable generalization might be useful, is also unclear. The fact that Lemma 3.3 also holds when  $t$  is a polynomial with terms all of even degree strongly suggests there are other things to be discovered.

There is evidence that the answer for higher degrees may be quite simple. Let  $S(p, n)$  denote the generalization of  $S(t, \mathbf{k}, n)$  to higher degrees, that is,

$$S(p, n) = \frac{1}{2^n} \sum_{\mathbf{y} \in \mathbf{Z}_3^n} \chi\left(\prod_{i=1}^n y_i\right) \omega^{p(\mathbf{y})},$$

where  $p(\mathbf{y})$  is any polynomial. It is interesting to note that, if  $\deg(p) = 1$ , then  $|S(p, n)| \leq (\sqrt{3}/2)^n$  (see [Gr99] or the proof of Theorem 4.1), if  $\deg(p) = 2$ , then  $|S(p, n)| \leq (\sqrt{3}/2)^{\lceil n/2 \rceil}$  (Theorem 3.1), and that if  $\deg(p) = n$ , then  $|S(p, n)| \leq \sqrt{3}/2$  (implicit in the proof of Theorem 3.1, and also in [Gr99]). Furthermore, for any  $d$  we can find a polynomial  $p$  of degree  $d$  such that  $|S(p, n)| = (\sqrt{3}/2)^{\lceil n/d \rceil}$ . For example, if  $n$  is divisible by  $d$ , the following form meets this bound:

$$p(y_1, \dots, y_n) = y_1 y_2 \cdots y_d + y_{d+1} y_{d+2} \cdots y_{2d} + \dots + y_{n-d+1} y_{n-d+2} \cdots y_n.$$

We therefore conjecture the following:

**Conjecture 5.1.**

$$|S(p, n)| \leq \left(\frac{\sqrt{3}}{2}\right)^{\lceil n/\deg(p) \rceil}.$$

The polynomials meeting this bound are block-symmetric (see section 4). Hence implicit in this conjecture is the claim that block-symmetric polynomials give the highest correlation (at least in the case of  $\text{MOD}_3$ ).

Now consider the case of other moduli, for example  $\text{MOD}_5$ . Here, as elaborated in [Gr99], the relevant sums (over *Boolean* variables) are of the following form:

$$S = \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{\sum_{i=1}^n x_i} \zeta^{t(\mathbf{x})},$$

where  $\zeta = e^{2\pi i/5}$  is a primitive complex fifth root of unity. We can once again make the change of variable  $x_i = (1/2)(1 - y_i)$  where  $y_i \in \{1, -1\}$ . We can then re-write the sum in terms of the *quartic* multiplicative character  $\chi$  of  $\mathbf{Z}_5$ :

$$S = \sum_{\mathbf{y} \in \{1,0,-1\}^n} \chi\left(\prod_{i=1}^n y_i\right) \zeta^{t'(\mathbf{y})}. \quad (12)$$

If we start with a  $\text{MOD}_5 \circ \text{AND}_2$  circuit,  $t'$  will be quadratic. Now in fact Lemma 3.3 and Lemma 3.5 hold for this type of sum. But the proofs of Lemmas 3.4 and 3.6 no longer work.

Part of the problem is that  $S$  as given in equation (12) is a *partial* sum, i.e., the variables  $y_i$  do not range over the entire field  $\mathbf{Z}_5$ . It is possible to re-formulate the discriminator so as to obtain character sums that range over the complete field, by encoding field elements in the Boolean variables along the lines of [BS], [KP], and [Gr00]. However, the degrees of the polynomials are then higher than 2, and we are back to the problem of higher-degree polynomials.

Despite these problems, we believe at this point that they are not particularly difficult and that an appropriate algebraic setting will resolve them.

**Acknowledgements:** Parts of this paper were written during a sabbatical visit to CWI, Amsterdam. I thank Harry Buhrman and the others in his group for their hospitality. I am grateful to a number of people for discussions on this problem over a span of several years, especially Richard Beigel, Jin-Yi Cai, Randy Pruim, and Igor Shparlinski. I also thank Richard Beigel and Yao Yong for some valuable comments on the manuscript.

## References

- [AB] N. ALON AND R. BEIGEL, Lower bounds for approximations by low degree polynomials over  $\mathbf{Z}_m$ , in *Sixteenth Annual IEEE Conference on Computational Complexity*, IEEE Computer Society Press (2001) pp. 184–187.
- [Al] E. ALLENDER, A note on the power of threshold circuits. In *Proceedings of the 30th Symposium on Foundations of Computer Science*, (1989), 580-584.
- [Bar] D. BARRINGTON, Bounded-width polynomial-size branching programs recognize exactly those languages in  $\text{NC}^1$ , in *Journal of Computer and System Sciences* **38**, (1989), 150-164.
- [BM] R. BEIGEL AND A. MACIEL, Upper and lower bounds for some depth-3 circuit classes, in *Proceedings of the 12th IEEE Conference on Computational Complexity*, IEEE Computer Society Press (1997), pp. 149–157.
- [BNS] L. BABAI, N. NISAN AND M. SZEGEDY Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs, in *Journal of Computer and System Sciences*, **45:2** (1992), pp. 204-232.
- [BS] D. M. BARRINGTON AND H. STRAUBING, Complex polynomials and circuit lower bounds for modular counting. *Comput. Complexity* **4** (1994), 325–338.
- [BT] R. BEIGEL AND J. TARUI, On ACC, in *Computational Complexity* **4** (1994) 350–366.
- [Cai] 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.
- [CGT] J.-Y. CAI, F. GREEN, AND T. THIERAUF, On the correlation of symmetric functions, in *Mathematical Systems Theory* **29** (1996) 245-258.
- [FSS] M. FURST, J. B. SAXE, AND M. SIPSER, Parity, circuits, and the polynomial-time hierarchy, in *Mathematical Systems Theory*, **17** (1984) 13-27.
- [Go] M. GOLDMANN, A note on the power of majority gates and modular gates, in *Information Processing Letter*, **53** (1995), 321-327.

- [GKRST] F. GREEN, J. KÖBLER, K. REGAN, T. SCHWENTICK, AND J. TORÁN, The power of the middle bit of a  $\#P$  function, in *Journal of Computer and System Sciences* **50** (1995) 456-467.
- [Gr99] F. GREEN, Exponential sums and circuits with a single threshold gate and mod-gates, in *Theory of Computing Systems* **32** (1999) 453-466.
- [Gr00] F. GREEN, A complex-number fourier method for lower bounds on the Mod- $m$  degree, in *Computational Complexity*, **9** (2000) 16 - 38.
- [Gro] V. GROLMUSZ, A weight-size trade-off for circuits with mod  $m$  gates, in *Proceedings of the 26th ACM Symposium on Theory of Computing*, (1994), pp. 68-74.
- [Has] J. HÅSTAD, Computational limitations of small-depth circuits, the MIT press, Cambridge, 1987.
- [HG] J. HÅSTAD AND M. GOLDMANN, On the power of small-depth threshold circuits, in *Computational Complexity*, **1** (1991) 113-129.
- [HMPST] A. HAJNAL, W. MAASS, P. PUDLÁK, M. SZEGEDY, AND G. TURÁN, Threshold circuits of bounded depth, in *Proceedings 28th Annual IEEE Symposium on Foundations of Computer Science*, IEEE Computer Society Press (1987) 99-110.
- [KP] M. KRAUSE AND P. PUDLÁK, On the computational power of depth 2 circuits with threshold and modulo gates, in *Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing*, ACM Press (1994) 48-57.
- [LN] R. LIDL AND H. NIEDERREITER, Finite Fields, *Encyclopedia of Mathematics and its Applications*, Vol. 20, Cambridge University Press, Cambridge, 1983.
- [Raz] 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.
- [RR] A. A. RAZBOROV AND S. RUDICH, Natural proofs, in *Proc. 26th ACM Symp. on Theory of Computing*, Association for Computing Machinery, New York, (1994), pp. 204-213.
- [Sch] W. M. SCHMIDT, Equations over finite fields: An elementary approach, *Lecture Notes in Mathematics*, vol. 536, Springer, New York, 1976.
- [Sm] 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.
- [Tod] S. TODA. PP is as hard as the polynomial-time hierarchy. In *SIAM Journal on Computing* **20**, (1991) 865-877.
- [Yao 85] 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.
- [Yao 90] A. YAO, On ACC and threshold circuits. In *Proceedings of the 31st Symposium on Foundations of Computer Science*, (1990), 619-627.