# On correlation bounds against polynomials

Peter Ivanov[*] Liam Pavlovic[*] Emanuele Viola[*]

July 2, 2022

**Abstract**

We study the fundamental challenge of exhibiting explicit functions that have small correlation with low-degree polynomials over $\mathbb{F}_2$. Our main contributions include:

1. In STOC 2020, CHHLZ introduced a new technique to prove correlation bounds. Using their technique they established new correlation bounds for low-degree polynomials. They conjectured that their technique generalizes to higher degree polynomials as well. We give a counterexample to their conjecture, in fact ruling out weaker parameters and showing what they prove is essentially the best possible.

2. We advocate an alternative approach for proving correlation bounds with the central "mod functions," consisting of proving two steps: (I) the polynomials that maximize correlation are symmetric, and (II) symmetric polynomials have small correlation. Contrary to related results in the literature, we conjecture that (I) is true. We argue that this approach is not affected by existing "barrier results."

3. We prove our conjecture for quadratic polynomials. Specifically, we determine the maximum possible correlation between quadratic polynomials modulo 2 and the functions $(x_1, \ldots, x_n) \to z^{\sum x_i}$ for any $z$ on the complex unit circle; and show that it is achieved by symmetric polynomials. To obtain our results we develop a new proof technique: we express correlation in terms of directional derivatives and analyze it by slowly restricting the direction.

4. We make partial progress on the conjecture for cubic polynomials, in particular proving tight correlation bounds for cubic polynomials whose degree-3 part is symmetric.

[*] Supported by NSF grant CCF-2114116. Liam Pavlovic supported by Research Experience for Undergraduates (REU) supplement.

# 1 Introduction and our results

Exhibiting explicit functions that have small *correlation* with low-degree polynomials modulo 2 is a fundamental challenge in complexity theory. This challenge is generally referred to as "proving correlation bounds" and progress on it is a prerequisite for progress on a striking variety of other long-standing problems: circuit lower bounds [Vio09b, Vio17], Valiant's rigidity challenge [Vio], number-on-forehead communication complexity [Vio, Vio17], and even recently-made conjectures on the Fourier spectrum of low-degree polynomials [Vio21].

After many years, the state-of-the-art on this challenge has not changed much since seminal works from at least thirty years ago. Two bounds are known for degree $d$ polynomials. First, the results by Razborov and Smolensky from the 80's give correlation $O(d/\sqrt{n})$ [Raz87, Smo87, Smo93]; second, the result by Babai, Nisan, and Szegedy [BNS92] on number-on-forehead communication protocols yields correlation $\exp(-\Omega(n/d2^d))$. A slight improvement to $\exp(-\Omega(n/2^d))$ appears in [Vio06]. Thus, the first bound applies to large degrees but yields weak correlation, while the second bound yields exponentially small correlation, but only applies to degrees less than $\log n$. Achieving correlation less than $1/\sqrt{n}$ for polynomials of degree $\log n$ remains open, for any explicit function. Remarkably, solving this specific setting of parameters is required for long-sought progress on any of the challenges mentioned in the previous paragraph.

**The conjecture [CHH$^+$20].** In STOC 2020, Chattopadhyay, Hatami, Hosseini, Lovett, and Zuckerman introduced a novel technique with which they established new correlation bounds for low-degree polynomials. The key ingredient in the approach in [CHH$^+$20] is a structural result about the Fourier spectrum of low-degree polynomials over $\mathbb{F}_2$. They show that for any $n$-variate polynomial $p$ over $\mathbb{F}_2$ of degree $\leq d$, there is a set $S$ of variables such that almost all of the Fourier mass of $p$ lies on Fourier coefficients that intersect with $S$, and the size of $S$ is exponential in $d$. Further, they conjecture that the size of $S$ needs to be just polynomial in $d$.

We give a counterexample to their conjecture. In fact, we shall rule out weaker parameters and show what they prove is essentially the best possible. This appears in Section 2.

**Mod functions.** A natural candidate for achieving small correlation are the $Mod_\phi$ functions which map inputs of Hamming weight $w$ to the complex point on the unit circle with angle $w\phi$. These $Mod_\phi$ are closely related to the boolean mod $m$ functions which indicate if the input Hamming weight is divisible by $m$. Specifically, one can bound the correlation with mod $m$ for odd $m$ by the correlations with the $Mod_\phi$ functions for $\phi = 2\pi k/m$ for $k = 1, 2, \ldots, (m-1)/2$ (see Lemma 36). In turn, as discussed below, an early motivation for studying the correlation with mod $m$ was proving circuit lower bounds.

We now formally define these notions and then discuss previous results.

**Definition 1.** For any angle $\phi \in [0, 2\pi]$ the function $Mod_\phi \colon \{0,1\}^n \to \mathbb{C}$ is defined as

$$Mod_\phi(x) := e^{\phi\sqrt{-1}\sum_i x_i}.$$

The correlation of a polynomial $p : \{0,1\}^n \to \{0,1\}$ with $Mod_\phi$ is

$$C_\phi(p) := \left|\mathbb{E}_{x\in\{0,1\}^n}(-1)^{p(x)} Mod_\phi(x)\right|.$$

For any integer $m$ we define the boolean Mod $m$ function $BMod_m : \{0,1\}^n \to \{0,1\}$ as

$$BMod_m(x) := \begin{cases} 1 & \text{if } \sum_{i=1}^n x_i \neq 0 \bmod m \\ 0 & \text{if } \sum_{i=1}^n x_i = 0 \bmod m. \end{cases}$$

The correlation between a polynomial $p : \{0,1\}^n \to \{0,1\}$ and $BMod_m$ is:

$$B_m(p) := \left|\mathbb{E}_{x:BMod_m(x)=0}(-1)^{p(x)} - \mathbb{E}_{x:BMod_m(x)=1}(-1)^{p(x)}\right|.$$

Most or all of the works in this area, including this paper, is concerned with the $Mod_\phi$ functions. And most of the works use correlation bounds with $Mod_\phi$ functions for various $\phi$ to obtain corresponding correlation bounds with the mod $m$ functions. In particular, the two correlation bounds stated above hold for $Mod_{2\pi/3}$. The first bound essentially appears in Smolensky's paper. For the second bound, Bourgain first proved [Bou05] correlation $\exp(-\Omega(n/c^d))$ with $Mod_{2\pi/m}$, with a correction in [GRS05]. Nisan later pointed out that such bounds also follow from [BNS92]. The constant $c$ is optimized to 4 in [Vio06]. For more discussion and background we refer to the survey [Vio09b], where the reader may find proofs of both bounds, including Nisan's derivation from [BNS92].

**Exact results.** Unlike other models of computation such as circuits, polynomials seem simple enough that one may try to obtain *exact* results. That is, one may try to precisely characterize the polynomials that achieve the maximum correlation. Twenty years ago, a remarkable paper by Green [Gre04], which is an inspiration for this work, took precisely such a step. Green, and the subsequent work [GR10], precisely characterized the quadratic polynomials modulo *three* that achieve the maximum correlation with the $Mod_{2\pi/2}$ function, i.e., parity. Compared to our discussion above, the moduli in [Gre04] are swapped. Green considers polynomials modulo 3 instead of 2, and bounds the correlation with $Mod_{2\pi/2}$ instead of $Mod_{2\pi/3}$. Extending Green's result to other moduli has resisted attacks, see [Gre04, DMRS06]. While these works do not explicitly consider polynomials modulo 2, difficulties also arise trying to port Green's proof to our setting. In fact, jumping ahead, we will show that the answer is different, arguably explaining the difficulties.

**Symmetry.** Aiming for exact results, a natural question to ask is whether, for some fixed degree, the polynomials modulo 2 that correlate best with $Mod_\phi$ are *symmetric.* Indeed, this question has been asked by many authors; it appears explicitly for example in the 2001 paper by Alon and Beigel [AB01]. A positive answer would have dramatic consequences since symmetric polynomials modulo 2, even of large degree, have exponentially small correlation with, say, $Mod_{2\pi/3}$. Thus, if one could prove that symmetric polynomials correlate best, one would obtain long-sought correlation bounds.

However, until now the evidence for this has been negative. The maximizing polynomials in [Gre04, GR10] are *not* symmetric. Moreover, the work [GKV17] has shown that for a large range of parameters, symmetric polynomials modulo 3 do *not* correlate best with parity (and are not even close). One of the families of polynomials that are shown to outperform symmetric in these works is that of *block-symmetric* polynomials, which are sums of symmetric polynomials on disjoint sets of variables. However, naive conjectures regarding the optimality of block-symmetric or other families of polynomials fail, and we are not aware of any natural family of polynomials modulo 3 that is a candidate to maximizing correlation with parity. The only available evidence that symmetric polynomials correlate best with mod functions are computer experiments up to 10 variables reported in [GKV17].

**Our results: A new approach to proving correlation bounds.** Departing from previous proofs, in this work we propose the following approach to proving correlation bounds with mod functions. It consists of two steps:

(I) Prove that symmetric polynomials correlate best with mod functions, and

(II) Prove that symmetric polynomials have exponentially small correlation with mod functions.

Regarding (I), we put forth the following conjecture:

**Conjecture 2.** *For every $d, n, \phi$ degree-$d$ symmetric polynomials correlate best with the $Mod_\phi$ function on $n$ bits.*

We verify (II) in Section 7. The result is folklore. We remark that [CGT96] proves a similar result, but in the case of symmetric polynomials mod $m$ and the mod 2 function. However, changing moduli can yield different results, as shown by this paper.

**Our approach vs. "barriers" to lower bounds.** Over the years many "barriers" have been proposed for progress on lower bounds. Barriers based on oracles or relativization [BGS75, AW08] are not known to apply – they mostly concern uniform models of computation. The Natural Proofs barrier [RR97] (see also [NRR02, MV15]) is also not known to apply since we do not have candidate pseudorandom functions that correlate with low-degree polynomials.

More recently, in an exciting work, Bhowmick and Lovett [BL15] proposed a new barrier specifically for proving correlation bounds. They consider an extension of polynomials called *non-classical polynomials.* In short, in a non-classical polynomial of degree $d$ monomials can have rational coefficients (with denominators depending on the degree) and the output of the polynomial is considered as an element in the torus $[0, 1]$. The work [BL15] shows that the proofs of most correlation bounds (such as those mentioned at the beginning of this introduction) also apply to non-classical polynomials. Moreover, for non-classical polynomials these bounds are actually tight! For example, there are non-classical polynomials of degree just $O(\log n)$ that correlate well with mod functions.

We argue that non-classical polynomials do not constitute an obstacle for our approach above. The main reason is that the non-classical polynomials in [BL15] – including those for mod functions – are actually symmetric. Hence, one could conceivably prove (I) above without distinguishing classical from non-classical polynomials. Moreover, the proof of (II) above already distinguishes classical from non-classical polynomials.

**Our results: Proof of Conjecture 2 for $d = 2$.** A main technical contribution of this work is a proof of our Conjecture 2 in the case of degree two. That is, in contrast with the previous proofs discussed above, we show that, among quadratic polynomials modulo 2, those that correlate best with the $Mod_\phi$ functions are symmetric. Let us first define the elementary symmetric polynomials of degree 1 and 2.

**Definition 3** (Elementary symmetric polynomials)**.** Let

$$e^1(x_1,\ldots,x_n) := \sum_{i=1}^{n} x_i,$$
$$e^2(x_1,\ldots,x_n) := \sum_{i<j}^{n} x_i x_j.$$

**Example 4.** Let $\phi = 2\pi/3$ and $\omega = e^{\phi\sqrt{-1}}$. We have:

$$C_\phi(0) = \left|\mathop{\mathbb{E}}_{x\in\{0,1\}^n} \omega^{\sum_i x_i}\right| = \left|\mathop{\mathbb{E}}_{x_1\in\{0,1\}} \omega^{x_1}\right|^n = \left|\frac{1+\omega}{2}\right|^n = \left(\frac{1+\cos\phi}{2}\right)^{n/2} = \left(\frac{1}{2}\right)^n,$$
$$C_\phi(e^1) = \left|\mathop{\mathbb{E}}_{x\in\{0,1\}^n} (-1)^{\sum_i x_i}\omega^{\sum_i x_i}\right| = \left|\mathop{\mathbb{E}}_{x_1\in\{0,1\}} (-1)^{x_1}\omega^{x_1}\right|^n = \left|\frac{1-\omega}{2}\right|^n = \left(\frac{1-\cos\phi}{2}\right)^{n/2} = \left(\frac{\sqrt{3}}{2}\right)^n,$$

$C_\phi(BMod_3) \geq 1/2,$

where the last inequality this follows because the absolute value of the real component of $(-1)^{BMod_3(x)}\omega^{\sum_i x_i}$ is $\geq 1/2$ for every $x$.

We next state our first result. Henceforth all polynomials in this paper have coefficients in $\{0,1\}$ and operate modulo two. We characterize the quadratic polynomials that maximize $C_\phi$ *for any angle* $\phi \in [0, 2\pi]$. Additionally, we show the correlation of other quadratic polynomials is a multiplicative factor smaller.

It is in fact sufficient to restrict our attention to angles $\phi \in [0, \pi/2]$ thanks to a simple symmetry argument presented in Section 3. When $\phi \in [0, \pi/4]$ then the constant zero polynomial maximizes correlation. Our main contribution is that when $\phi \in (\pi/4, \pi/2]$ the correlation is maximized by either $e^2$ or $e^2 + e^1$, depending on the value of $n$ mod 4.

We define the quantity

$$v_\phi := 2^{-n-1} \cdot ((1+\sin\phi)^n + (1-\sin\phi)^n)$$

which plays a key role in this paper.

**Theorem 5.** *Fix any angle $\phi \in [0, \pi/2]$. For all large enough $n$, the maximum $C_\phi(p)$ over quadratic polynomials $p$ is attained by a symmetric polynomial. In more detail:*

1. *Suppose $\phi \in (\pi/4, \pi/2]$.*
   (a) *For $n$ even we have $C_\phi(e^2) = C_\phi(e^2 + e^1) = \sqrt{v_\phi}$.*
   (b) *For $n \equiv 1 \bmod 4$ we have $C_\phi(e^2) = \sqrt{v_\phi + (\cos(\phi)/2)^n}$, $C_\phi(e^2+e^1) = \sqrt{v_\phi - (\cos(\phi)/2)^n}$.*
   (c) *For $n \equiv 3 \bmod 4$ we have $C_\phi(e^2) = \sqrt{v_\phi - (\cos(\phi)/2)^n}$, $C_\phi(e^2+e^1) = \sqrt{v_\phi + (\cos(\phi)/2)^n}$.*
   (d) *For any quadratic polynomial $p$ besides $e^2$, $e^2 + e^1$ we have $C_\phi(p) \leq \sqrt{1 - \Omega(\sin\phi - \cos\phi)} \cdot \sqrt{v_\phi}$.*

2. *Suppose $\phi \in [0, \pi/4]$. Then $C_\phi(0) = \left(\frac{1+\cos\phi}{2}\right)^{n/2}$ and for any quadratic polynomial $p \neq 0$ we have $C_\phi(p) \leq (1 - \Omega(1)) \cdot C_\phi(0)$.*

Note that $\sqrt{v_\phi - (\cos(\phi)/2)^n} \geq (1 - o(1))\sqrt{v_\phi}$ and so the theorem shows that the correlation of non-symmetric polynomials is a constant-factor smaller than optimal.

An important message of this paper is that $C_\phi$ is maximized by *symmetric* polynomials. This contrasts with previous works, and gives hope that this may hold for larger degrees as well. If that is the case one would obtain long-sought correlation bounds, as discussed previously.

**Boolean correlation.** We now turn our attention to the boolean $BMod_m$ function. As mentioned earlier, most or all papers bounding the corresponding correlation $B_m$, including this one, proceed by first bounding $C_\phi$ for several corresponding values of $\phi$ and then using that information to bound $B_m$. Indeed, $C_\phi$ is a better-behaved quantity to work with. In turn, an early motivation for studying $B_m$ is the so-called *discriminator lemma* [HMP+93]. The lemma implies that if there is a circuit consisting of a majority of $s$ functions that computes $BMod_m$ then one of those functions $p$ has $B_m(p) \geq 1/s$. Thus, one can use upper bounds on $B_m$ to obtain lower bounds for such circuits.

In this paper we determine up to constant factors the maximum of $B_m$ over quadratic polynomials. This is Item 1 in the next theorem. In fact, we obtain more precise information. Item 2 determines (exactly) the maximum value when $n$ is congruent to $m, 3m \bmod 4m$: either $e^2$ or $e^2 + e^1$ maximizes $B_m$, and moreover it will achieve the upper bound on $B_m$ from Item 1. Our inability to determine the maximum value of $B_m$ for every $n$ is reflected in Item 3, which shows when $n$ is congruent to $0, 2m \bmod 4m$ this maximum is not achieved by symmetric polynomials.

**Theorem 6.** *Fix any odd $m \geq 3$, let $\phi := 2\pi/m$, $\ell_1 \in \{\frac{m-1}{4}, \frac{m+1}{4}\}$ denote the integer closest to $\frac{m}{4}$, and set $\Psi := 2m/(m-1)\sqrt{v_{\ell_1\phi}}$. The following holds for large enough $n$. Let $B_m^*$ denote the maximum $B_m(p)$ over all quadratic $p$.*

1. *For any $n$,*
$$\Psi(1/\sqrt{2} - o(1)) \leq B_m^* \leq \Psi(1 + o(1)).$$

2. *If $n \equiv m, 3m \bmod 4m$ then*
$$B_m^* = \max_{s \in \{e^2, e^2+e^1\}} B_m(s) = \Psi(1 - o(1)).$$

3. *If $n \equiv 0, 2m \bmod 4m$ then*
$$(1 + \Omega(1)) \max_{s \in \{0, e^1, e^2, e^2+e^1\}} B_m(s) < \max_{s' \in \{e^2, e^2+e^1\}} B_m(x_1 + s'(x_2, \dots, x_n)).$$

Note that the polynomial in the right-hand side of Item 3 is not symmetric. We conjecture that this polynomial is in fact optimal (for the corresponding values of $n$). Our techniques yield slightly stronger results for specific $m$ and $n$, but for simplicity we only state the above theorem that applies for any odd $m \geq 3$. In particular, when $m = 3$, it is possible to determine for every value of $n$ whether symmetric polynomials maximize $B_3$.

Previous techniques could at best determine this maximum up to polynomial factors. Hence we also improve polynomially the corresponding circuit lower bounds obtained via the discriminator lemma – this is a straightforward application that we do not state formally.

Green's work [Gre04] also determines exactly the maximum correlation between quadratic polynomials modulo 3 and the parity function. Our setting appears somewhat complicated by the fact that the $BMod_m$ functions are not balanced for odd $m$.

**Results and directions for $d = 3$.** We conjecture that Theorem 5 can be extended to show that for any cubic polynomial $p$ and any $\phi$, $C_\phi(p) \le \max_{s \in \{0, e^1, e^2, e^2+e^1\}} C_\phi(s)$. In other words, the correlation over all cubic polynomials is still maximized by a quadratic symmetric. This would prove Conjecture 2 for $d = 3$ as well.

We make progress on this conjecture by proving this indeed holds when $p$ is the sum of an arbitrary quadratic polynomial and a symmetric degree-3 polynomial. This is done in Section 8.

**Techniques and organization for the proof of Theorem 5.** We begin by rewriting the correlation squared in a convenient form, involving derivatives of the polynomial and of the mod function. Bounding the correlation in terms of derivatives is natural and done in several previous works, see e.g. discussion of the 'squaring trick' in [Vio09a, Chapter 1]. However, a key difference is that these previous works typically take repeated derivatives until the polynomial becomes constant, use the Cauchy-Schwartz inequality, and are lossy. By contrast, we take a single derivative, avoid Cauchy-Schwartz, and give an exact expression. To reiterate, these previous works provide asymptotic correlation bounds for larger degree polynomials, while we provide an *exact bound* for quadratic polynomials.

Let us fix some quadratic polynomial $p$, and for concreteness consider the complex mod 3 function $Mod_\phi := e^{\phi\sqrt{-1}\sum_i x_i}$ where $\phi := 2\pi/3$. Let us write $p_y$ for the derivative $p(x + y) + p(x)$ of $p$ in the direction $y \in \{0,1\}^n$. We can similarly consider the derivative of $Mod_\phi$ in direction $y$. This is $Mod_{\phi,y}(x) := \omega^{\sum_i x_i - \sum_i (x_i \oplus y_i)}$. We can now write

$$C_\phi^2(p) = \mathbb{E}_y \mathbb{E}_x (-1)^{p_y(x)} Mod_{\phi,y}(x).$$

Writing $c_y(p)$ for the inner expectation – where $c$ stands for *contribution* in direction $y$ – we can rewrite the correlation square as $\mathbb{E}_y c_y(p)$. This derivation is done in Section 3. Using this, we then show in Section 4 that $C_\phi^2(s)$ admits a particularly nice expression where $s$ is either $e^2, e^2 + e^1$. Supposing $n$ is even for simplicity we have:

$$\mathbb{E}_y c_y(s) = 2^{-n} \sum_{y \in E} (\sin\phi)^{w(y)}. \tag{1}$$

We sketch how this expression arises. The derivatives of $s$ are very structured. Specifically, $s_y$ is the linear polynomial $\sum_{i:y_i=1} x_i$ if the Hamming weight of $y$ is even; otherwise it is $\sum_{i:y_i=0} x_i$. On the other hand, $Mod_{\phi,y}$ only depends on the variables corresponding to the bits set to 1 by $y$. This implies that for any $y$ of odd weight, the contribution $c_y(s)$ will equal $\prod_{i:y_i=0}[\cdot] \prod_{i:y_i=1} \mathbb{E}_{x_i}[(-1)^{x_i}] = 0$. For any $y$ of even weight, similar considerations show that $c_y(s) = (\sin\phi)^{w(y)}$. Together this implies (1).

Recall our goal is to prove that $\mathbb{E}_y c_y(p) \le \mathbb{E}_y c_y(s)$ for any quadratic $p$, which we formally show in Section 5. We reason by slowly conditioning on the bits of $y$. To give some intuition, we illustrate how this is done for the first bit. Suppose for simplicity that in $p$, the only quadratic term containing $x_1$ is $x_1x_2$. We show that the following holds:

$$\mathbb{E}_{y:y_1=0}|c_y(p)| \leq \mathbb{E}_{y:y_1=0}c_y(s). \tag{2}$$

Let us first analyze $\mathbb{E}_{y:y_1=0}|c_y(p)|$. We bound it by conditioning on $y_2$, the direction bit corresponding to $x_2$.

If $y_2 = 1$ we mimic the reasoning for symmetric polynomials in case of odd-weight derivative which we have seen above. Specifically, $x_1$ appears in $p_y(x)$, but $Mod_{\phi,y}$ does not depend on $x_1$ because $y_1 = 0$. Hence $c_y(p) = 0$.

The more challenging case is when $y_2 = 0$. We start by noting the inner term in (1) is in fact an upper bound. In other words, for any $p, y$ we have

$$|c_y(p)| \leq (\sin\phi)^{w(y)}. \tag{3}$$

Briefly, this follows because $Mod_{\phi,y}$ only depends on the variables corresponding to the 1 bits of $y$ and $|c_y(p)|$ is maximized when $p_y$ is the linear polynomial on these $w(y)$ variables. Applying (3) in the case $y_2 = 0$ implies that

$$\sum_{y:y_1=0} |c_y(p)| \leq \sum_{y:y_1=0,y_2=0} (\sin\phi)^{w(y)}.$$

Now we analyze $\mathbb{E}_{y:y_1=0}c_y(s)$. We know $c_y(s) = (\sin\phi)^{w(y)}$ if $y$ is even and 0 if $y$ is odd. Since $y_1 = 0$ and by conditioning on $y_2$ we have

$$\sum_{y:y_1=0} c_y(s) = \sum_{y:y_1=0,y_2=0,y_3+\cdots+y_n=0} (\sin\phi)^{w(y)} + \sum_{y:y_1=0,y_2=1,y_3+\cdots+y_n=1} (\sin\phi)^{w(y)}.$$

To compare this to $\mathbb{E}_{y:y_1=0}|c_y(p)|$ we can condition on $y_3 + \cdots + y_n$ and write

$$\sum_{y:y_1=0} |c_y(p)| \leq \sum_{y:y_1=0,y_2=0,y_3+\cdots+y_n=0} (\sin\phi)^{w(y)} + \sum_{y:y_1=0,y_2=0,y_3+\cdots+y_n=1} (\sin\phi)^{w(y)}.$$

Since the left hand terms in both expressions are equal, to prove (2) it remains to show

$$\sum_{y:y_1=0,y_2=0,y_3+\cdots+y_n=1} (\sin\phi)^{w(y)} \leq \sum_{y:y_1=0,y_2=1,y_3+\cdots+y_n=1} (\sin\phi)^{w(y)}.$$

Unfortunately, the above inequality does not hold. Note the right-hand side equals the left-hand side times a factor $\sin(\phi) < 1$. For the proof to go through, we need to improve the left-hand side. To do so, we crucially rely on the *handshaking lemma* from graph theory as follows.

For any $y$, we can determine the derivative $p_y(x)$ by examining the graph $G_{p,y}$, where nodes represent the variables corresponding to the 1 bits of $y$, and edges represent the quadratic terms of $p$ on those $w(y)$ variables. Indeed, $x_i$ appears in $p_y(x)$ iff $x_i$ has odd degree in $G_{p,y}$.

Now consider some $y$ such that $w(y)$ (and hence the number of nodes in $G_{p,y}$) is odd. The handshaking lemma says that the number of nodes in a graph with odd degree must be even. This implies that $p_y(x)$ contains at most $w(y)-1$ variables corresponding to the 1 bits of $y$. This yields the following improvement to (3), that holds whenever $w(y)$ is odd:

$$|c_y(p)| \leq (\sin\phi)^{w(y)-1}. \tag{4}$$

To apply this in our setting, note for every $y$ that satisfies $y_1 = 0, y_2 = 0, y_3 + \cdots + y_n = 1$, $w(y)$ is odd. This allows us to improve our previous bound to

$$\sum_{y:y_1=0} |c_y(p)| \leq \sum_{y:y_1=0,y_2=0,y_3+\cdots+y_n=0} (\sin\phi)^{w(y)} + \sum_{y:y_1=0,y_2=0,y_3+\cdots+y_n=1} (\sin\phi)^{w(y)-1}.$$

To finish the proof it suffices to show

$$\sum_{y:y_1=0,y_2=0,y_3+\cdots+y_n=1} (\sin\phi)^{w(y)-1} \leq \sum_{y:y_1=0,y_2=1,y_3+\cdots+y_n=1} (\sin\phi)^{w(y)}.$$

This inequality now holds due to the $(\sin\phi)^{-1}$ factor we just gained. To summarize, we have just shown (2) holds when $p$ contains $x_1x_2$ but no other quadratic terms with $x_1$.

**Opening more bits.** If we were to show $\mathbb{E}_{y:y_1=1}|c_y(p)| \leq \mathbb{E}_{y:y_1=1}c_y(s)$ then we could conclude the proof. However, it is not clear how to condition on $y_1 = 1$. In the previous argument, conditioning on $y_1 = 0$ crucially allowed us to observe that $c_y(p) = 0$ whenever $y_2 = 1$, which eliminated half the directions. It turns out we can make a similar observation whenever at least one direction bit is conditioned to 0. So in the next step we instead show $\mathbb{E}_{y:y_1=1,y_2=0}|c_y(p)| \leq \mathbb{E}_{y:y_1=1,y_2=0}c_y(s)$.

We are able to continue this process as long as there are variables that, roughly speaking, appear in at least a few quadratic terms (for the precise conditions see Lemmas 28, 29).

When we can no longer continue, suppose we have opened the $j$ direction bits $y_1, \ldots y_j$. To conclude the proof it remains to show that

$$\mathbb{E}_{y:y_1=1,\ldots,y_j=1}|c_y(p)| \leq \mathbb{E}_{y:y_1=1,\ldots,y_j=1}c_y(s).$$

Since we were not able to open any more bits, that means $x_{j+1}, \ldots x_n$ appear in just a few quadratic terms. We again consider the graph $G_p$, where the $n$ nodes represent variables and the edges represent quadratic terms of $p$. The nodes corresponding to $x_{j+1}, \ldots, x_n$ have low degree. When $j$ is small, this implies there is a large independent set in $G_p$, which is another way of saying that $p$ has a large linear subpolynomial. We can use this to then prove from scratch that $\mathbb{E}_{y:y_1=1,\ldots y_j=1}|c_y(p)|$ will be sufficiently small (Lemma 32).

When $j$ is large, we apply (3) to every $y$ to bound $\mathbb{E}_{y:y_1=1,\ldots y_j=1}|c_y(p)|$ (Lemma 31). However, the resulting bound *does not yield* the desired inequality $\mathbb{E}_{y:y_1=1,\ldots,y_j=1}|c_y(p)| \leq \mathbb{E}_{y:y_1=1,\ldots,y_j=1}c_y(s)$. We explain how we overcome this obstacle below.

**Slackness.** Although we get exact results in the end, we emphasize that some steps in the proof do not yield exact bounds, but are approximate. For example, after we open the first bit we in fact show a strict inequality between $\mathbb{E}_{y:y_1=0}|c_y(p)|$ and $\mathbb{E}_{y:y_1=0}c_y(s)$ when $p$ is non-symmetric (Lemma 30). This gives us a "buffer" between $\mathbb{E}_y|c_y(p)|$ and $\mathbb{E}_yc_y(s)$, which is reflected in the statement of Item 1(d) in Theorem 5.

This extra factor is not just additional information, but is in fact critical for the proof since the final step might be lossy, as mentioned above. The buffer gained will be much larger than the upper bound we derive for $\mathbb{E}_{y:y_1=1,\ldots,y_j=1}|c_y(p)|$ in the large $j$ case, which allows us to conclude the proof.

## 2 The CHHLZ conjecture

In this section we present the new technique in [CHH$^+$20], their conjecture, and our counterexample. The key ingredient in the approach in [CHH$^+$20] is a structural result about the Fourier spectrum of low-degree polynomials over $\mathbb{F}_2$. They show that for any $n$-variate polynomial $p$ over $\mathbb{F}_2$ of degree $\leq d$, there is a set $S$ of variables such that almost all of the Fourier mass of $p$ lies on Fourier coefficients that intersect with $S$, and the size of $S$ is exponential in $d$. This remarkable result allows them to prove new correlation bounds. Further, they conjecture that the size of $S$ needs to be just polynomial in $d$.

Next we present their conjecture in more detail, and then our results. The main quantity used in [CHH$^+$20] is "local correlation" which they define as follows:

**Definition 7** (Local correlation, [CHH$^+$20])**.** For any $F : \{0,1\}^n \to \{-1,1\}$,

$$\Delta_S(F) := \mathbb{E}_{x^{\overline{S}}}\left[(\mathbb{E}_{x^S}[F(x)] - \mathbb{E}[F])^2\right].$$

For a polynomial $p : \mathbb{F}_2^n \to \mathbb{F}_2$ we write $e(p)$ for $(-1)^p$ which takes values in $\{-1,1\}$. Next we state their conjecture:

**Conjecture 8** ([CHH$^+$20, Conjecture 1.14])**.** *For every polynomial $p$ of degree $d$ there exists a set $S$ of $\leq poly(d, \log(1/\epsilon))$ variables such that $\Delta_S(e(p)) \leq \epsilon$.*

In fact CHHLZ make a stronger conjecture (Conjecture 1.15 in [CHH$^+$20]), where a single set $S$ is found that works for an entire space of dimension $k$ of polynomials. This generality is critical in proving their new correlation bounds. However, we shall give a counterexample even for $k = 1$. In fact, we shall rule out even much weaker parameters and show that what they prove is essentially the best possible. Specifically, we show that for $d = O(\log n)$ and constant $\epsilon$, one needs $|S| \geq n/\log^{O(1)} n$.

**Theorem 9.** *There exists a polynomial $p$ of degree $d = O(\log n)$ such that $\Delta_S(e(p)) \geq \Omega(1)$ for any $S$ of size $\leq c \cdot n/\log^2 n$, where $c > 0$ is an absolute constant.*

The rest of this section is devoted to the proof of this theorem. The idea behind it is quite natural in hindsight, and highlights the expressive power of polynomials of degree $O(\log n)$.

**Definition 10.** [BL85] (cf. [O'D07], Proposition 4.12) We define TRIBES : $\{0,1\}^n \to \{0,1\}$ to be a read-once monotone DNF where every term has size $w$ so that $|\mathbb{E}_x[\text{TRIBES}(x)] - 1/2| \leq O(\log n)/n$. This makes $w = \log n - \log\log n + O(1)$.

The next result shows the probability TRIBES is fixed to 1 after a uniform assignment to $x^{\overline{S}}$ is approximately the same as after a uniform assignment to $x$, where $S \subset [n]$ is a subset of nearly linear size. This property was also used in [HIV22] to show separations between DNFs composed with parity gates and parity decision trees.

**Lemma 11.** *Fix any $S \subset [n]$ such that $|S| \leq O(n/\log^2 n)$. Then*

$$\mathbb{P}_{x^{\overline{S}}}[\mathrm{TRIBES}(x) \text{ not fixed }] \leq 1/2 + o(1).$$

*Proof.* The set $S$ can intersect at most $|S|$ AND terms. The probability over a uniform assignment to $x^{\overline{S}}$ that TRIBES$(x)$ is fixed to 1 is at least the probability one of the untouched AND terms is set to 1. Hence,

$$\begin{aligned}\mathbb{P}_{x^{\overline{S}}}[\mathrm{TRIBES}(x) = 1] &\geq 1 - (1 - 2^{-w})^{n/w - |S|}. \\ &= 1 - \frac{\mathbb{P}_x[\mathrm{TRIBES}(x) = 0]}{(1 - 2^{-w})^{|S|}} \\ &\geq 1 - (1/2 + O(\log n)/n)(1 + 1/\Omega(\log n)) \\ &\geq 1/2 - 1/\Omega(\log n).\end{aligned}$$

where the second $\geq$ follows since $(1 - 2^{-w})^{|S|} \geq 1 - |S|/2^w \geq 1 - 1/\Omega(\log n)$ and the fact $1/(1-x) \geq 1 + x$. □

We next show that TRIBES can be approximated by a low-degree polynomial. This can be seen as a special case of Razborov's classical approximation [Raz87].

**Lemma 12.** *There exists a $O(\log n)$ degree polynomial $p$ such that*

$$\mathbb{E}_x[e(\mathrm{TRIBES}(x))e(p(x))] \geq 1/2 + \Omega(1).$$

*Proof.* We will construct a distribution $D$ of $O(\log n)$ degree polynomials such that for any $x$, $\mathbb{P}_{q \sim D}[q(x) \neq \mathrm{TRIBES}(x)] \leq 1/4$. This would allow us to conclude, since by averaging there must a polynomial $p \in D$ such that $\mathbb{P}_x[p(x) \neq \mathrm{TRIBES}(x)] \leq 1/4$.

To construct $D$, first note the $n/w$ *AND* terms can be computed by degree $w$ monomials $m_1(x), \ldots, m_{n/w}(x)$. To sample $q \sim D$, we uniformly sample $T_1, T_2 \subseteq [n/w]$ and set

$$q(x) := 1 - (1 - \bigoplus_{i \in T_1} m_i(x)) \wedge (1 - \bigoplus_{i \in T_2} m_i(x)).$$

Since $T_1, T_2$ are chosen uniformly, for any $x$ such that $(m_1(x), \ldots m_{n/w}(x)) \neq 0$ we have $\mathbb{P}_{q \sim D}[q(x) = 0] = 1/4$ . And for any $x$ such that $(m_1(x), \ldots m_{n/w}(x)) = 0$ we have $\mathbb{P}_{q \sim D}[q(x) = 1] = 0$. Together this implies for any $x$, $\mathbb{P}_{q \sim D}[q(x) \neq \mathrm{TRIBES}(x)] \leq 1/4$. □

We are now ready to prove the main result.

*Proof of Theorem 9.* First we note that if $\Delta_S(e(p)) \leq \epsilon$ then by Markov's inequality

$$\mathbb{P}_{x^{\overline{S}}}\left[|\mathbb{E}_{x^S}[e(p(x))] - \mathbb{E}[e(p)]| > \epsilon^{1/4}\right] \leq \epsilon^{1/2}. \tag{5}$$

Then, using $T(x)$ to denote TRIBES$(x)$ for brevity, we can write

$$\begin{aligned}\mathbb{E}_x\left[e(T(x))e(p(x))\right] &= \mathbb{E}_x\left[e(T(x)) \cdot (e(p(x)) - \mathbb{E}[e(p)])\right] + \mathbb{E}[e(T)]\mathbb{E}[e(p)] \\ &\leq \mathbb{E}_x\left[e(T(x)) \cdot (e(p(x)) - \mathbb{E}[e(p)])\right] + O(\log n)/n\end{aligned}$$

where the $\le$ follows since $|\mathbb{E}[e(T)]| \le O(\log n)/n$ by the definition of TRIBES.

After a uniform assignment to $x^{\overline{S}}$, let $E_1$ denote the event $|\mathbb{E}_{x^S}[e(p(x))] - \mathbb{E}[e(p)]| \le \epsilon^{1/4}$ and let $E_2$ denote the event that TRIBES$(x)$ is fixed. Then we have

$$\begin{aligned}\mathbb{E}_x\left[e(T(x)) \cdot (e(p(x)) - \mathbb{E}[e(p)])\right] &\le \mathbb{E}_{x^{\overline{S}}}\left[\left|\mathbb{E}_{x^S}\left[e(T(x)) \cdot (e(p(x)) - \mathbb{E}[e(p)])\right]\right|\right] \\ &\le \mathbb{E}_{x^{\overline{S}}}\left[\left|\mathbb{E}_{x^S}\left[e(T(x)) \cdot (e(p(x)) - \mathbb{E}[e(p)])|E_1E_2\right]\right|\right] + \mathbb{P}[\neg E_1] + \mathbb{P}[\neg E_2] \\ &\le \epsilon^{1/4} + \epsilon^{1/2} + 1/2 + o(1).\end{aligned}$$

For the last inequality, note that $\mathbb{E}_{x^S}[e(T(x)) \cdot (e(p(x)) - \mathbb{E}[e(p)])|E_1E_2] = \mathbb{E}_{x^S}[e(p(x)) - \mathbb{E}[e(p)]|E_1]$ since TRIBES$(x)$ is fixed conditioned on $E_2$. We bound $\mathbb{P}[\neg E_1]$ by (5) and $\mathbb{P}[\neg E_2]$ by Lemma 11. Setting $\epsilon$ to a small enough constant contradicts Lemma 12 and concludes the proof of Theorem 9. □

# 3 Derivatives

In this section we rewrite $C_\phi(p)^2$ in terms of the correlation of the derivatives of $p$ with $Mod_\phi$, and use this viewpoint to derive several basic facts which will be used later. Fix any $\phi \in [0, 2\pi]$, let $\omega = e^{\phi\sqrt{-1}}$, and from here on we let $\sigma := \sin\phi, \gamma := \cos\phi$.

We begin by using the fact that $|z|^2 = z\overline{z}$ for any complex number, where $\overline{z}$ is the complex conjugate, to rewrite the correlation square $C_\phi^2(p)$ as

$$\mathbb{E}_x(-1)^{p(x)}\omega^{\sum_i x_i} \cdot \overline{\mathbb{E}_y(-1)^{p(y)}\omega^{\sum_i y_i}}.$$

Replacing $y$ with $x \oplus y$ and noting that $\overline{(-1)^{p(y)}\omega^{\sum_i y_i}} = (-1)^{p(y)}\omega^{-\sum_i y_i}$ we can rewrite the correlation square with the following expression:

$$\mathbb{E}_y\mathbb{E}_x(-1)^{p(x)+p(x\oplus y)}\omega^{\sum_i x_i - \sum_i (x_i \oplus y_i)}.$$

The inner expectation over $x$ plays an important role and so we introduce a definition.

**Definition 13.** The *contribution* of polynomial $p$ in the *direction $y$*, or the *$y$-contribution* of $p$, is $c_y(p) := \mathbb{E}_x(-1)^{p(x)+p(x\oplus y)}\omega^{\sum_i x_i - \sum_i (x_i \oplus y_i)}$.

Note $c_y(p)$ is always defined with respect to an angle $\phi$, which will always be clear from context. Repeating what was said above,

$$C_\phi(p)^2 = \mathbb{E}_y c_y(p).$$

The polynomial $p(x) + p(x \oplus y)$ that appears in $c_y(p)$ is the *derivative* of $p$ in *direction $y$*, denoted $p_y$. When $p$ is quadratic, this derivative is linear. Hence, $p_y(x) = \sum_{i \le n} p_{y,i}x_i + p_{y,0}$ where for every $y$, $p_{y,i} \in \{0, 1\}$ are is the coefficient of $x_i$, and $p_{y,0}$ is the constant.

Because $p_y(x)$ is linear, for fixed $y$ the expectation over $x$ is actually the expectation of *independent* functions of the $x_i$ and so the $y$-contribution can be written as

$$(-1)^{p_{y,0}} \prod_{i=1}^{n} \mathbb{E}_{x_i}(-1)^{p_{y,i}x_i}\omega^{x_i - (x_i \oplus y_i)}.$$

Each of the expectations $\mathbb{E}_{x_i}(-1)^{p_{y,i}x_i}\omega^{x_i-(x_i\oplus y_i)}$ above takes one of four different values, depending on the four possibilities for $p_{y,i}$ and $y_i$. These values play a crucial role in this paper and we present them next. Note that if $y_i = 0$ then $x_i - (x_i \oplus y_i) = 0$ and so the $\omega$ factor disappears.

**Proposition 14.** *We have the following four possible values for* $\mathbb{E}_{x_i}(-1)^{p_{y,i}x_i}\omega^{x_i-(x_i\oplus y_i)}$*:*

| $p_{y,i}$ | $y_i$ | $\mathbb{E}_{x_i}(-1)^{p_{y,i}x_i}\omega^{x_i-(x_i\oplus y_i)}$ |
|---|---|---|
| 0 | 0 | $= 1$ |
| 1 | 0 | $= \mathbb{E}_{x_i}(-1)^{x_i} = 0$ |
| 0 | 1 | $= \mathbb{E}_{x_i}\omega^{x_i-(x_i\oplus 1)} = \frac{1}{2}\left(\omega^{-1}+\omega\right) = \gamma$ |
| 1 | 1 | $= \mathbb{E}_{x_i}(-1)^{x_i}\omega^{x_i-(x_i\oplus 1)} = \frac{1}{2}\left(\omega^{-1}-\omega\right) = -\sqrt{-1}\cdot\sigma$ |

**Restricting to $\phi \in [0, \pi/2]$.** We now justify our previous assertion that we can restrict our attention to angles $\phi \in [0, \pi/2]$. First, if $\phi \in [\pi/2, 3\pi/2]$ then we can sum $e^1$ to $p$. Then $C_\phi(p + e^1) = C_{\pi+\phi}(p)$ and $\pi + \phi \in [-\pi/2, \pi/2]$. Next, if $\phi \in [-\pi/2, 0]$ then $C_\phi(p) = C_{-\phi}(p)$ and now $\phi \in [0, \pi/2]$.

**Definition 15.** We denote the Hamming weight of $x \in \{0,1\}^n$ by $w(x)$.

Looking at the table above we can obtain the following bound on $c_y(p)$ in terms of the weight of the derivative.

**Claim 16** (Weight bound on contribution)**.** *For any $y \in \{0,1\}^n$ and any $\phi$ we have* $|c_y(p)| \le \max\{\sigma,\gamma\}^{w(y)}$.

We conclude this section by giving a quick illustration of how this framework can be used to compute the maximum correlation for $\phi \in [0, \pi/4]$. Note that Theorem 5 proves a stronger result, showing that non-symmetric polynomials have correlation a constant-factor smaller than optimal. For such $\phi$ we are going to show that the constant polynomial, which is symmetric, maximizes $C_\phi$. By Example 4,

$$C_\phi^2(0) = 2^{-n}\left(1+\gamma\right)^n.$$

We show this is an upper bound for any quadratic polynomial $p$. We have

$$C_\phi^2(p) \le \mathbb{E}_y|c_y(p)|,$$

where $c_y$ is as in Definition 13. By Claim 16, since $\gamma > \sigma$, we have

$$|c_y(p)| \le \gamma^{w(y)}.$$

Hence,

$$C_\phi^2(p) \le 2^{-n}\sum_{i=0}^{n}\binom{n}{i}\gamma^i = 2^{-n}(1+\gamma)^n,$$

by the binomial theorem.

# 4 Correlation of symmetric polynomials

We use the information from Section 3 to compute the maximal correlation of symmetric quadratic polynomials, and note an important "no-cancellation" property which will guide the rest of the proof.

We first apply Proposition 14 to determine the *contributions of symmetric polynomials.* The derivatives of $e^1$ are simply the constant term $e^1_{y,0} = \sum_i y_i$. We now analyze the derivatives of $e^2$. The coefficient $e^2_{y,i}$ for $i \geq 1$ equals to $\sum_{j \neq i} y_j$ and the constant term $e^2_{y,0}$ equals $\sum_{i<j} y_i y_j$. Combining this information with the above we can characterize the $y$-contributions of symmetric polynomials.

**Lemma 17** (Contributions of symmetric polynomials)**.** *For any $\phi \in [0, \pi/2]$ and any $y \in \{0,1\}^n$ we have:*

1. *If $w(y)$ is even then $c_y(s) = \sigma^{w(y)}$ for either $s = e^2 + e^1$ or $s = e^2$.*
2. *If $w(y)$ is odd and $w(y) < n$ then $c_y(s) = 0$ for either $s = e^2 + e^1$ or $s = e^2$.*
3. *If $w(y) = n$ and $n \equiv 1 \bmod 4$ then $c_y(s) = +\gamma^n$ for $s = e^2$ and $c_y(s) = -\gamma^n$ for $s = e^1 + e^2$.*
4. *If $w(y) = n$ and $n \equiv 3 \bmod 4$ then $c_y(s) = -\gamma^n$ for $s = e^2$ and $c_y(s) = +\gamma$ for $s = e^1 + e^2$.*

*Proof.* Refer to Proposition 14.

If $w(y)$ is even, the expectations over $x_i$ with $y_i = 0$ contribute 1 since the corresponding coefficient $s_{y,i}$ (the coefficient of $x_i$ in the derivative polynomial $s_y$) is 0. This corresponds to the first row of Proposition 14. The other expectations contribute $(-\sqrt{-1})\sigma$. This corresponds to the last row of Proposition 14. In addition, we have the constant term. For $e^2$ this term is $(-1)^{\binom{w(y)}{2}} = (-1)^{w(y)^2/2 - w(y)/2} = (-1)^{-w(y)/2}$ using that $w(y)$ is even. For $e^2 + e^1$ the constant term is $(-1)^{\binom{w(y)}{2} + w(y)}$ which again equals $(-1)^{-w(y)/2}$ because $w(y)$ is even. Hence the $y$-contribution equals

$$(-1)^{-w(y)/2} \cdot ((-\sqrt{-1})\sigma)^{w(y)} = \sigma^{w(y)}$$

where the last equality follows again because $w(y)$ is even.

If $w(y)$ is odd and less than $n$ then some $y_i$ is zero. The corresponding $s_{y,i}$ equals $w(y)$, which is odd. So the contribution is zero, by the second row of Proposition 14.

Finally, consider $w(y) = n$ when $n$ is odd. Note that $s_{y,i} = n - 1$ which is even. By the third row of Proposition 14, the expectation of $x$ is $\gamma^n$ times the constant term. For $s = e^2$ the constant term is $(-1)^{\binom{n}{2}} = (-1)^{n(n-1)/2}$ which is 1 if $n \equiv 1 \mod 4$ and $-1$ otherwise. For $s = e^2 + e^1$ the constant term is $(-1)^{\binom{n}{2}+n} = (-1)^{n(n-1)/2+1}$ which is $-1$ if $n \equiv 1 \mod 4$ and 1 otherwise. □

Lemma 17 yields an expression for the maximum $C_\phi(s)$ attained by symmetric quadratic polynomials $s$. It is best to express this correlation using the quantity $v_\phi$ that we redefine in a way that is more convenient for the main proof.

**Definition 18** $(E, O, v)$**.** Let $E \subseteq \{0,1\}^n$ be the set of $n$-bit strings of even Hamming weight, and let $O$ be the set of strings of odd weight. Define

$$v_\phi := 2^{-n} \sum_{y \in E} \sigma^{w(y)}.$$

The equivalence between this definition and the one in the introduction is given by the following claim, which we will use often.

**Claim 19** (Odd-even sum)**.** *For any number $d$ we have:*
$\sum_{y:y\in E} d^{w(y)} = \sum_y d^{w(y)}(1+(-1)^{w(y)})/2 = \frac{(1+d)^n+(1-d)^n}{2}$,
$\sum_{y:y\in O} d^{w(y)} = \sum_y d^{w(y)}(1-(-1)^{w(y)})/2 = \frac{(1+d)^n-(1-d)^n}{2}$.

*Proof.* In each line, the second equality follows from the binomial theorem. □

For example, $v_{2\pi/3} = \Theta((1+\sqrt{3}/2)/2)^n$, where $(1+\sqrt{3}/2)/2 = 0.933\ldots$. We now give the maximal correlation of a symmetric quadratic polynomial.

**Corollary 20.** *Fix $\phi \in [\pi/2, \pi/4)$ and let $C^*_\phi$ be the maximum $C_\phi$ attained by a symmetric quadratic polynomial on $n$ bits for large enough $n$. We have:*
$C^*_\phi = \sqrt{v_\phi}$ *if $n$ is even. This is attained by both $e^2$ and $e^1 + e^2$.*
$C^*_\phi = \sqrt{v_\phi + 1/4^n}$ *if $n$ is odd. This is attained by $e^2$ if $n \equiv 1 \mod 4$ and by $e^1 + e^2$ if $n \equiv 3 \mod 4$.*

*Proof.* By Example 4, $C_\phi(e^1) < C_\phi(0) = \left(\frac{1+\gamma}{2}\right)^{n/2}$. By the definition of $v_\phi$, $\sqrt{v_\phi} \geq \Omega\left(\left(\frac{1+\sigma}{2}\right)^{n/2}\right)$ which is greater for $n$ large enough since $\sigma > \gamma$ when $\phi \in [\pi/2, \pi/4)$. The proof now follows from Lemma 17. □

**(No) cancellations** Note an interesting fact holds for the symmetric polynomial that maximizes $C_\phi$: *the $y$-contributions are always real and non-negative*, for any $y$. This is not true in general. For a simple example, take $p = e^2, n = 3 \bmod 4$, and $w(y) = n$. Then $c_y(p)$ is negative. This leads to cancellations in the correlation. However, for the symmetric polynomial that maximizes correlation, the inner expectation is always non-negative and there are *no cancellations.*

This fact shows that for the symmetric polynomials $p$ that maximize correlation, the correlation square $C^2_\phi(p)$ can be equivalently written as

$$\mathbb{E}_y |c_y(p)|;$$

that is, we can take absolute values of the contributions "for free". Note that by the triangle inequality, for *any* polynomial $p$ the above expression is an *upper bound* on the correlation. We used this when showing the constant polynomial maximizes $C_\phi$ for $\phi \in [0, \pi/4]$. For the symmetric polynomials that maximize correlation, it turns out that this bound can be attained.

In the proof of Theorem 5 we shall mostly be working with this quantity, which does not depend on the linear part of $p$. This is because the derivative of a linear polynomial is a constant depending only on $y$, which disappears when taking absolute values. Hence we can assume that $p$ does not contain linear terms.

# 5 Proof of Theorem 5

The next two results are needed to prove the first, main item of Theorem 5. First we deal with polynomials that are missing at least one degree two monomial.

**Theorem 21.** *Let $\phi \in (\pi/4, \pi/2]$ and $p$ be a quadratic polynomial that is not equal to $e^2 + \ell$ for some linear polynomial $\ell$. Then $\mathbb{E}_y |c_y(p)| \le (1 - \Omega(\sigma - \gamma))v_\phi$.*

Next we deal with non-symmetric polynomials that possess all degree two monomials. Note we use the quantity $\mathbb{E}_y c_y(p)$ instead.

**Lemma 22.** *Let $\phi \in (\pi/4, \pi/2]$ and $p$ be a polynomial that is equal to $e^2 + \ell$ where $\ell$ is a linear polynomial not equal to a constant or $e^1$. Then $\mathbb{E}_y c_y(p) \le (1 - \Omega(1))v_\phi$.*

Assuming these are true, we prove the first item of Theorem 5.

*Proof of Theorem 5 Item 1.* Follows from Corollary 20, Theorem 21, and Lemma 22. □

We next give similar results that are needed to prove the second item of Theorem 5.

**Lemma 23.** *Let $\phi \in [0, \pi/4]$ and $p$ be a quadratic polynomial that is not linear. Then $\mathbb{E}_y |c_y(p)| \le (1 - \Omega(1)) \left(\frac{1+\gamma}{2}\right)^n$.*

**Lemma 24.** *Let $\phi \in [0, \pi/4]$ and $p$ be a linear polynomial that is not equal to the constant polynomial. Then $\mathbb{E}_y c_y(p) \le (1 - \Omega(1)) \left(\frac{1+\gamma}{2}\right)^n$.*

*Proof of Theorem 5 Item 2.* Follows from Lemma 23, Lemma 24, and Example 4 which says $C_\phi^2(0) = \left(\frac{1+\gamma}{2}\right)^n$. □

## 5.1 Proof of Theorem 21

Our proof strategy is to *slowly restrict the direction* $y$, to try to connect the corresponding contributions with the target value $v_\phi$.

**Definition 25.** A *restriction* $r$ is an element of $\{0, 1, *\}^n$. The *weight* $w(r)$ of $r$ is the number of ones, and $S(r)$ is the number of stars. We also view $r$ as a function $r : \{0, 1\}^{S(r)} \to \{0, 1\}^n$ mapping assignments to stars to $n$-bit strings, and we write $ry$ for $r(y)$. For a restriction $r$ we call $x_i$ a $b \in \{0, 1, *\}$ variable if the $i$th bit of $r$ is $b$.

We emphasize that $r$ restricts the space of directions $y$, not $x$. So for example if $x_i$ is a 0 variable then the corresponding directional bit $y_i$ has been restricted to 0 – but $x_i$ is never restricted. We next introduce restricted versions of the quantities in Theorem 21.

**Definition 26** ($c(p, r)$ and $v_\phi(r)$)**.** Let $r$ be a restriction. For a polynomial $p$ we define

$$c(p, r) := \mathbb{E}_{y \in \{0,1\}^{S(r)}} |c_{ry}(p)|.$$

Note that $c(p, r)$ is defined with respect to the angle $\phi$ since $c_{ry}(p)$ is. We also define

$$v_\phi(r) := 2^{-S(r)} \sum_{y \in \{0,1\}^{S(r)} : ry \in E} \sigma^{w(ry)},$$

where we sum over all derivatives $ry$ of even weight.

For any $r \in \{0,1\}^n$ we have $c(p,r) = |c_r(p)|$. Also,

$$\mathbb{E}_y|c_y(p)| = c(p,*^n),$$
$$v_\phi = v_\phi(*^n).$$

Using the above notation our goal is to show that

$$c(p,*^n) \leq (1 - \Omega(\sigma - \gamma))v_\phi.$$

**Polynomials as graphs** We associate to a quadratic polynomial $p$ the *graph* over the variables where $x_i$ and $x_j$ are connected iff monomial $x_ix_j$ is present in $p$. Note this graph only depends on the monomials of degree 2 of $p$. The *degree* of a variable shall refer to the degree as a node in this graph. We shall also talk of variables being connected, etc.

**Example 27.** Let $n = 3, r = (1 * 0) \in \{0,1,*\}^3, p = x_1x_2 + x_2x_3$. The $*$ variable $x_2$ is connected to the 1 variable $x_1$ and to the 0 variable $x_3$.

We now proceed with the proof of Theorem 21. In all upcoming statements, $p$ is an arbitrary quadratic polynomial on $n$ variables, $\phi \in (\pi/4, \pi/2]$, and we set $n$ and a parameter $t$ large enough so that both $t$ and $n/t$ are large enough depending on $\phi$. The minimal $n$ for which our proof of Theorem 5 holds increases as $\phi$ approaches $\pi/4$ (where $\sigma$ approaches $\gamma$).

We next state several lemmas and prove Theorem 21 assuming them. The first two lemmas show that $c(p,r) \leq v_\phi(r)$ under various conditions on $p$ and $r$.

**Lemma 28.** *Let $r \in \{0,1,*\}^n$ be a restriction. Suppose there exists a 0 variable that is connected to an odd number of 1 variables. Then $c(p,r) \leq v_\phi(r)$.*

**Lemma 29.** *Let $r \in \{0,1,*\}^n$ be a restriction. Suppose there exists a 0 variable that is connected to an even number of 1 variables and at least $t$ $*$ variables. Then $c(p,r) \leq v_\phi(r)$.*

The next lemma shows that if $p$ is missing a degree two monomial then $v_\phi(0*^{n-1})$ gains an advantage over $c(p, 0*^{n-1})$. It can be considered a strengthening of Lemma 29 under an additional constraint.

**Lemma 30** (Buffer)**.** *Let $r = 0*^{n-1}$. Suppose the 0 variable is connected to at least $t$ $*$ variables and at most $n-2$ $*$ variables. Then $c(p,r) \leq v_\phi(r) - \left(\frac{\sigma-\gamma}{16}\right) v_\phi$.*

We shall use the above lemmas to slowly restrict directions, beginning with Lemma 30 and then iteratively applying either Lemma 28 or Lemma 29. This process stops when we cannot find variables that satisfy the hypothesis of either Lemma 28 or Lemma 29.

When this happens, we consider two cases based on the number of variables restricted. In the first case, when the number is large, we give an upper bound on $c(p,r)$. This suffices because of the buffer afforded to us by Lemma 30.

**Lemma 31** (Opened majority)**.** *Let $r = 1^j*^{n-j}$ for some $j \geq n/2$. Then $c(p,r) < 2^j \left(\frac{\sigma-\gamma}{1000}\right) v_\phi$.*

In the second case, when the number of restricted variables is small, the polynomial has structure that we can utilize to again show $c(p,r) \leq v_\phi(r)$. Specifically, in the graph of the polynomial many variables have small degree.

**Lemma 32** (Low degree loses)**.** *Let $r = 1^j *^{n-j}$ for some $j < n/2$. Suppose every $*$ variable is connected to at most $t$ other $*$ variables. Then $c(p, r) \leq v_\phi(r)$.*

We will need the following variant of Lemma 32 for an edge case in the main proof.

**Lemma 33.** *Let $r = *^n$. Suppose there are at least $n - t$ variables connected to at most $t$ other variables. Then $c(p, r) \leq (1 - (\sigma - \gamma))v_\phi$.*

Assuming these lemmas we can prove Theorem 21.

*Proof of Theorem 21.* We consider two cases based on the existence of a variable of certain degree in the graph of $p$. In the first case, when $p$ is a 'typical' polynomial, we suppose the existence of a variable with degree in $[t, n-2]$ (corresponding to the hypothesis of Lemma 30). Let us denote this variable $x_1$ for ease. We "open" the directional bit corresponding to $x_1$. That is, we condition $\mathbb{E}_y|c_y(p)|$ depending on the value of $y_1$:

$$c(p, *^n) = \frac{1}{2}\left(c(p, 0*^{n-1}) + c(p, 1*^{n-1})\right).$$

Correspondingly, it holds that

$$v_\phi(*^n) = \frac{1}{2}\left(v_\phi(0*^{n-1}) + v_\phi(1*^{n-1})\right).$$

Then we iteratively open up $*$ variables in the term where the restriction has no zeroes, as long as we can find a $*$ variable that is connected to an odd number of 1 variables or that is connected to an even number of 1 variables and at least $t$ other $*$ variables. We can write the terms corresponding to the variables that were opened (up to permutation of variables):

$$c(p, *^n) = \frac{1}{2}c(p, 0*^{n-1}) + \frac{1}{4}c(p, 10*^{n-2}) + \cdots + \frac{1}{2^j}c(p, 1^j*^{n-j}),$$

for some $1 \leq j \leq n$ depending on $p$. We also write the corresponding terms for $v_\phi$:

$$v_\phi(*^n) = \frac{1}{2}v_\phi(0*^{n-1}) + \frac{1}{4}v_\phi(10*^{n-2}) + \cdots + \frac{1}{2^j}v_\phi(1^j*^{n-j}).$$

We compare the terms in the right-hand sides in the two equations above. For the first term, we have $\frac{1}{2}c(p, 0*^{n-1}) \leq \frac{1}{2}v_\phi(0*^{n-1}) - (\frac{\sigma-\gamma}{32})v_\phi$ by Lemma 30. For all the other terms except the last one, we have that the $c(p, r)$ terms is at most the corresponding $v_\phi(r)$ term by either Lemma 28 or Lemma 29. Now we analyze the last terms depending on the value of $j$. Note that each $*$ variable is connected to at most $t$ other $*$ variables.

If $1 \leq j < n/2$ we apply Lemma 32 which says $c(p, 1^j*^{n-j}) \leq v_\phi(p, 1^j*^{n-j})$ and conclude as $v_\phi(*^n) - c(p, *^n) \geq \frac{\sigma-\gamma}{32}v_\phi$ .

If $j \geq n/2$ then $\frac{1}{2^j}c(p, 1^j*^{n-j}) \leq (\frac{\sigma-\gamma}{1000})v_\phi$ by Lemma 31 and we conclude as $v_\phi(*^n) - c(p, *^n) \geq \left(\frac{\sigma-\gamma}{32} - \frac{\sigma-\gamma}{1000}\right)v_\phi$.

This finishes the proof of when $p$ has a node with degree in $[t, n-2]$. For the second case, suppose that every node has degree at most $t-1$ or degree exactly $n-1$. We then claim there are $\leq t-1$ nodes with degree $n-1$. Supposing this is true we can immediately conclude by Lemma 33.

Now we verify the desired claim. Suppose there are $z$ nodes of degree $n-1$ with $z \geq t$. Each of these nodes is connected to every other node, so every node in the graph has degree at least $z \geq t$. By the supposition, every node in the graph has degree $n-1$. This contradicts the hypothesis that $p \neq e^2 + \ell$. □

Next we give proofs of the technical lemmas.

### 5.1.1 Proof of Lemma 28

Fix a 0 variable $x_i$ that is connected to an odd number of 1 variables. Let $T$ denote the indices of the $*$ variables connected to $x_i$ and let $U$ denote the indices of the remaining $*$ variables. Write $y = (y^T, y^U)$ for the corresponding bits of $y$.

Note that by Proposition 14, $c_{ry}(p) = 0$ if $w(y^T)$ is even (because the coefficient of $x_i$ would be odd). And if $w(y^T)$ is odd we apply the upper bound $|c_{ry}(p)| \leq \sigma^{w(ry)}$ from Claim 16. Combining these two things yields:

$$\begin{aligned} c(p,r) &= 2^{-S(r)} \sum_{y^T \in O, y^U} |c_{ry}(p)| \\ &\leq 2^{-S(r)} \sum_{y^T \in O, y^U} \sigma^{w(ry)}. \end{aligned}$$

Now we compare this value with the expression for $v_\phi$. Let us assume that $w(r)$ is even. Then

$$v_\phi(r) = 2^{-S(r)} \sum_{y \in E} \sigma^{w(ry)}.$$

Hence to prove $c(p,r) \leq v_\phi(r)$ it suffices to show

$$\sum_{y^T \in O, y^U} \sigma^{w(y)} \leq \sum_{y \in E} \sigma^{w(y)}.$$

Note in the above two expressions we can assume $|T| > 0$ since otherwise the left hand-side will be 0 and we would be immediately done. Then by conditioning on the parity of $y^U$ in each side it suffices to show

$$\sum_{y^T \in O, y^U \in E} \sigma^{w(y)} + \sum_{y^T \in O, y^U \in O} \sigma^{w(y)} \leq \sum_{y^T \in E, y^U \in E} \sigma^{w(y)} + \sum_{y^T \in O, y^U \in O} \sigma^{w(y)}.$$

The second sum in each side is the same, and the first sum in the right-hand side is bigger than the first sum in the left-hand side by Claim 19. This concludes the case of when $w(r)$ is even.

When $w(r)$ is odd

$$v_\phi(r) = 2^{-S(r)} \sum_{y \in O} \sigma^{w(ry)}.$$

Then it suffices to show

$$\sum_{y^T \in O, y^U \in E} \sigma^{w(y)} + \sum_{y^T \in O, y^U \in O} \sigma^{w(y)} \leq \sum_{y^T \in E, y^U \in O} \sigma^{w(y)} + \sum_{y^T \in O, y^U \in E} \sigma^{w(y)}.$$

The inequality holds again by Claim 19.

### 5.1.2 Proof of Lemma 29

The high-level approach is similar to the proof of Lemma 28, but we utilize the following improvement of Claim 16 when the weight of the derivative is odd. The improvement comes from the handshaking lemma.

**Claim 34.** *Let $y \in \{0,1\}^n$. Then $|c_y(p)|$ is either 0 or $\sigma^e \gamma^{w(y)-e}$, where $e$ is an even integer and $0 \leq e \leq w(y)$.*

*Proof.* Consider the graph $G$ with $w(y)$ nodes which are the 1 variables and the edges represent monomials. Let $S, T$ be the nodes in $G$ that have odd, even degree respectively. Note that nodes in $S$ contribute a $\sigma$ factor, while the nodes in $T$ contribute a $\gamma$ factor. The remaining $n - w(y)$ 0 variables not in $G$ contribute either 1 or 0.

So to finish the proof it suffices to show that $|S|$ must be even. The sum of all the degrees in $G$ is $|S| \cdot \mathit{odd} + (|V| - |S|) \cdot \mathit{even} = |S| \cdot \mathit{odd} + \mathit{even}$. In any graph, the sum of degrees is even, hence $|S|$ is always even. □

To prove Lemma 29 we exploit that if $w(ry)$ is odd then the exponent of the $\sigma$ factor is $< w(ry)$. Fix the 0 variable $x_i$ that is connected to an even number of 1 variables and to at least $t$ $*$ variables. Let $T$, $U$ denote the same as in the previous proof. The $ry$ contribution is zero if $w(y^T)$ is odd (because the coefficient of $x_i$ in the $ry$ derivative would be $\mathit{even} + \mathit{odd} = \mathit{odd}$). So then

$$\begin{aligned} c(p,r) &= 2^{-S(r)} \sum_{y^T \in E, y^U} |c_{ry}(p)| \\ &= 2^{-S(r)} \Big( \sum_{y^T \in E, y^U \in E} |c_{ry}(p)| + \sum_{y^T \in E, y^U \in O} |c_{ry}(p)| \Big). \end{aligned}$$

Suppose that $w(r)$ is even. For the first term, where $y^T \in E, y^U \in E$, we use Claim 16. For the second term, where $y^T \in E, y^U \in O$, $w(ry) = \mathit{even} + \mathit{even} + \mathit{odd} = \mathit{odd}$. By Claim 34, the max contribution of $ry$ in the second term is $\leq \sigma^{w(ry)-1}\gamma$. So we can bound

$$c(p,r) \leq 2^{-S(r)} \Big( \sum_{y^T \in E, y^U \in E} \sigma^{w(ry)} + \frac{\gamma}{\sigma} \sum_{y^T \in E, y^U \in O} \sigma^{w(ry)} \Big).$$

We compare this to

$$\begin{aligned} v_\phi(r) &= 2^{-S(r)} \sum_{y \in E} \sigma^{w(ry)} \\ &= 2^{-S(r)} \Big( \sum_{y^T \in E, y^U \in E} \sigma^{w(ry)} + \sum_{y^T \in O, y^U \in O} \sigma^{w(ry)} \Big). \end{aligned}$$

The sums over $y^T \in E, y^U \in E$ are the same. Hence to show $c(p,r) \leq v_\phi(r)$ it suffices to show

$$\begin{aligned}
\frac{\gamma}{\sigma} \sum_{y^T \in E, y^U \in O} \sigma^{w(y)} &\leq \sum_{y^T \in O, y^U \in O} \sigma^{w(y)} \\
\iff \frac{\gamma}{\sigma} \sum_{y^T \in E} \sigma^{w(y^T)} &\leq \sum_{y^T \in O} \sigma^{w(y^T)} \\
\iff (\sigma/\gamma + 1)\,(1-\sigma)^{|T|} &\leq (\sigma/\gamma - 1)\,(1+\sigma)^{|T|} \\
\iff \frac{\sigma+\gamma}{\sigma-\gamma} &\leq \left(\frac{1+\sigma}{1-\sigma}\right)^{|T|}.
\end{aligned}$$

The second to last $\iff$ follows by applying Claim 19 and rearranging. The last inequality holds for $t$ large enough, since $|T| \geq t$ and the left hand term will be some fixed positive number since $\phi \in (\pi/4, \pi/2]$. This concludes the $w(r)$ even case.

Now suppose $w(r)$ is odd. Proceeding similarly as before, we have

$$c(p,r) \leq 2^{-S(r)}(\frac{\gamma}{\sigma} \sum_{y^T \in E, y^U \in E} \sigma^{w(ry)} + \sum_{y^T \in E, y^U \in O} \sigma^{w(ry)}).$$

Which we need to compare with

$$\begin{aligned}
v_\phi(r) &= 2^{-S(r)} \sum_{y \in O} \sigma^{w(ry)} \\
&= 2^{-S(r)}( \sum_{y^T \in E, y^U \in O} \sigma^{w(ry)} + \sum_{y^T \in O, y^U \in E} \sigma^{w(ry)}).
\end{aligned}$$

Now the sums over $y^T \in E, y^U \in O$ are the same. So then it suffices to show

$$\frac{\gamma}{\sigma} \sum_{y^T \in E} \sigma^{w(y^T)} \leq \sum_{y^T \in O} \sigma^{w(y^T)}$$

which we have already verified.

### 5.1.3 Proof of Lemma 30

The proof starts identically as the proof of Lemma 29, but then we strengthen the analysis to give a strict inequality. Let $T$ denote the set of $*$ variables connected to $x_1$, and let $U$ denote the $*$ variables not connected to $x_1$. We have $|T| + |U| = n - 1$ and by hypothesis $t \leq |T| \leq n - 2$. We remark the strengthened analysis only works because of the condition $|T| \leq n - 2$.

We have the following derivation, where the first inequality follows from the same steps as in $w(r)$ even case of the previous proof. Let $a = 1+\sigma, b = 1-\sigma$, and $\delta = \gamma/\sigma$.

$$\begin{aligned}
2^{n-1}\left(v_\phi(0*^{n-1}) - c(p, 0*^{n-1})\right) &\geq \sum_{y^T \in O, y^U \in O} \sigma^{w(y)} - \frac{\gamma}{\sigma} \sum_{y^T \in E, y^U \in O} \sigma^{w(y)}. \\
&= \sum_{y^U \in O} \sigma^{w(y^U)} \cdot \Big(\sum_{y^T \in O} \sigma^{w(y^T)} - \delta \sum_{y^T \in E} \sigma^{w(y^T)}\Big) \\
&= \frac{a^{|U|} - b^{|U|}}{2} \cdot \frac{(1-\delta)a^{|T|} - (1+\delta)b^{|T|}}{2} \\
&\geq \frac{a^{|U|}}{4} \cdot \frac{(1-\delta)a^{|T|}}{4} \\
&= \frac{(1-\delta)a^{n-1}}{16}.
\end{aligned}$$

We elaborate on the last $\geq$. First, note that if $|U| = 0$ the inequality would not be valid since the entire expression would be equal to 0. Second, we verify that

$$\begin{aligned}
\frac{(1+\delta)b^{|T|}}{2} &\leq \frac{(1-\delta)a^{|T|}}{4} \\
\iff 2 \cdot \frac{\sigma+\gamma}{\sigma-\gamma} &\leq \left(\frac{1+\sigma}{1-\sigma}\right)^{|T|}.
\end{aligned}$$

The last inequality holds for $t$ large enough, since $|T| \geq t$. Note this is almost the same inequality that is in the proof of Lemma 29. Lastly, we verify that

$$\begin{aligned}
\frac{b^{|U|}}{2} &\leq \frac{a^{|U|}}{4} \\
\Leftarrow 2 &\leq \frac{1+\sigma}{1-\sigma}.
\end{aligned}$$

The $\Leftarrow$ holds since $|U| > 0$ and the last inequality is equivalent to $\sigma \geq 1/3$ which holds since $\sigma = \sin(\phi) \geq \sin(\pi/4) = 1/\sqrt{2} \geq 1/3$.

We continue the derivation, applying similar logic:

$$\begin{aligned}
\frac{(1-\delta)a^{n-1}}{16} &\geq \frac{(1-\delta)a^{n-1} + (1-\delta)b^{n-1}}{32} \\
&\geq \frac{(1-\delta)a^{n} + (1-\delta)b^{n}}{32a} \\
&= \frac{(1-\delta)}{16a} \cdot 2^n v_\phi.
\end{aligned}$$

Dividing both sides by $2^{n-1}$ we obtain

$$\begin{aligned}
v_\phi(0*^{n-1}) - c(p, 0*^{n-1}) &\geq \frac{(1-\delta)}{8a} \cdot v_\phi \\
&\geq \frac{\sigma-\gamma}{16} \cdot v_\phi.
\end{aligned}$$

where the last $\geq$ follows since $a = 1+\sigma \leq 2$, $(1-\delta) = \frac{\sigma-\gamma}{\sigma} \geq \sigma - \gamma$ because $\sigma \leq 1$.

### 5.1.4 Proof of Lemma 31

Applying Claim 16 we can say

$$\begin{aligned} c(p, 1^j *^{n-j}) &\le 2^{-(n-j)}\sigma^j \sum_y \sigma^{w(y)} \\ &= 2^{-(n-j)}\sigma^j (1+\sigma)^{n-j}. \end{aligned}$$

On the other hand,

$$2^j v_\phi(*^n) \ge 2^{-(n-j+1)}(1+\sigma)^n.$$

So it suffices to show that

$$\begin{aligned} &\frac{\sigma^j(1+\sigma)^{n-j}}{2^{n-j}} \le \frac{\sigma-\gamma}{1000}\frac{(1+\sigma)^n}{2^{n-j+1}} \\ \iff\quad &\frac{2000}{\sigma-\gamma} \le \left(\frac{1+\sigma}{\sigma}\right)^j, \end{aligned}$$

where we divided by $\sigma - \gamma > 0$. The last inequality holds for $n$ large enough since $j \ge n/2$ and $\sigma > 0$.

### 5.1.5 Proof of Lemma 32

Consider the subgraph induced by the $*$ variables. There are $n-j \ge n/2$ nodes in it of degree $\le t$. By a greedy argument, this implies an independent set of size $\ge (n-j)/(t+1) \ge n/4t$. Let $T$ denote the variables in the independent set and let $S$ denote the remaining $*$ variables. Note $|S| + |T| = n - j$ and the remaining $j$ variables are 1 variables.

For any fixing $y^S$ of $S$, let $p^T(y^S) \in \{0,1\}^{|T|}$ denote the coefficients of the variables in $T$ based on the partial restriction $1^j y^S *^{|T|}$. This is a valid definition because $T$ is an independent set, and so $p^T(y^S)$ is unaffected by any fixing $y^T$ of $T$. By Proposition 14, if for some fixing $y^T$ there is a variable $x_j$ in $T$ such that $p^T_j(y^S) = 1$ but $y^T_j = 0$ then the contribution is 0. Using also the other values in the table in Proposition 14, for any fixed $y^S$ we can let $\psi := w(p^T(y^S))$ and bound the contribution over $y^T$ as follows:

$$\begin{aligned} 2^{|T|}c(p, 1^j y^S *^{|T|}) &\le \sigma^{j+w(y^S)+\psi} \sum_{z\in\{0,1\}^{|T|-\psi}} \gamma^{w(z)} \\ &= \sigma^{j+w(y^S)+\psi}(1+\gamma)^{|T|-\psi} \\ &\le \sigma^{j+w(y^S)}(1+\gamma)^{|T|}. \end{aligned}$$

The last $\le$ follows since $\sigma < 1 \le 1+\gamma$. By summing over all possible fixings $y^S$ and applying the previous bound we can bound $c(p, 1^j *^{n-j})$ as follows:

$$\begin{aligned} 2^{n-j}c(p, 1^j *^{n-j}) &\le \sigma^j (1+\gamma)^{|T|} \sum_{y^S} \sigma^{w(y^S)} \\ &= \sigma^j(1+\gamma)^{|T|}(1+\sigma)^{|S|} \\ &\le \sigma^j(1+\gamma)^{n/4t}(1+\sigma)^{(n-j)-n/4t}. \end{aligned}$$

The last $\leq$ holds since $\sigma > \gamma$ and $|T| \geq n/4t$. On the other hand,

$$\begin{aligned} 2^{n-j} v_\phi(1^j *^{n-j}) &= \sum_{y:1^j y \in E} \sigma^{j+w(y)} \\ &\geq \sigma^j \frac{(1+\sigma)^{n-j}}{4}. \end{aligned}$$

So then it suffices to show

$$\begin{aligned} \sigma^j (1+\gamma)^{n/4t}(1+\sigma)^{(n-j)-n/4t} &< \sigma^j \frac{(1+\sigma)^{n-j}}{4} \\ \iff (1+\gamma)^{n/4t} &< \frac{(1+\sigma)^{n/4t}}{4} \\ \iff 4 &< \left(\frac{1+\sigma}{1+\gamma}\right)^{n/4t}. \end{aligned}$$

Since $\sigma > \gamma$ when $\phi \in (\pi/4, \pi/2]$, the last inequality holds for $n/t$ large enough.

### 5.1.6 Proof of Lemma 33

The proof is nearly identical to the proof of Lemma 32. The hypothesis implies the existence of an independent set of size $\geq (n-t)/(t+1) \geq (n-t)/2t$ in the graph consisting of all the variables. Following the same logic as before, we can upper bound $c(p, *^n)$ by

$$2^n c(p, *^n) \leq (1+\gamma)^{(n-t)/2t}(1+\sigma)^{n-(n-t)/2t}.$$

On the other hand,

$$2^n v_\phi \geq \frac{(1+\sigma)^n}{2}.$$

Then it suffices to show

$$\begin{aligned} (1+\gamma)^{(n-t)/2t}(1+\sigma)^{n-(n-t)/2t} &< (1-(\sigma-\gamma))\frac{(1+\sigma)^n}{2} \\ \iff \frac{2}{(1-(\sigma-\gamma))} &< \left(\frac{1+\sigma}{1+\gamma}\right)^{(n-t)/2t}. \end{aligned}$$

Recall that $n/t$ is arbitrarily large, so $(n-t)/2t$ is also arbitrarily large and the inequality holds.

## 5.2 Proof of Lemma 22

We can perform a similar analysis as in the proof of Lemma 17. As before $c_y(p) = 0$ if $w(y)$ is odd. But now if $w(y)$ even, letting $T$ denote the set of variables that appear in the linear polynomial $\ell$, the contribution is

$$\begin{aligned} c_y(p) &= (-1)^{-w(y)/2+w(y^T)} \cdot ((-\sqrt{-1})\sigma)^{w(y)} \\ &= (-1)^{w(y^T)}\sigma^{w(y)}. \end{aligned}$$

So a derivative makes a positive contribution if $w(y)$ is even and $w(y^T)$ is even, and a negative one if $w(y)$ is even and $w(y^T)$ is odd. Let $U$ be the complement of $T$. By hypothesis, $1 \le |T|, |U| \le n-1$. We can sum over the positive contributions and subtract the negative ones to get the expression

$$2^n \cdot \mathbb{E}_y c_y(p) = \sum_{y^T \in E, y^U \in E} \sigma^{w(y)} - \sum_{y^T \in O, y^U \in O} \sigma^{w(y)}.$$

On the other hand,

$$2^n \cdot v_\phi = \sum_{y^T \in E, y^U \in E} \sigma^{w(y)} + \sum_{y^T \in O, y^U \in O} \sigma^{w(y)}.$$

Combining the two expressions and letting $a = (1+\sigma), b = (1-\sigma)$, we get

$$\begin{aligned} 2^n \left(v_\phi - \mathbb{E}_y c_y(p)\right) &= 2 \sum_{y^T \in O, y^U \in O} \sigma^{w(y)} \\ &= \frac{1}{2}\left(a^{|T|} - b^{|T|}\right)\left(a^{|U|} - b^{|U|}\right) \\ &\ge \frac{1}{2} \frac{a^{|T|}}{2} \frac{a^{|U|}}{2} \\ &= \frac{a^n}{8}. \end{aligned}$$

The second = follows by Claim 19, and the $\ge$ after that follows since $1 \le |T|, |U|$ by hypothesis and $2b < a$.

### 5.3 Proof of Lemma 23

Since $p$ is not linear there is at least one node with degree $\ge 1$ in the polynomial graph. Let us denote this node $x_1$ for ease, and let $T, U$ denote the nodes connected, not connected to $x_1$ respectively. We write $y = (y^T, y^U)$ for the corresponding bits of $y$. Just like in the proof of Theorem 21 we condition on the value of $y_1$ to get

$$c(p, *^n) = \frac{1}{2}\left(c(p, 0*^{n-1}) + c(p, 1*^{n-1})\right).$$

We bound the second term by applying Claim 16 which says $c_{ry}(p) \le \gamma^{w(ry)}$ using that $\phi \in [0, \pi/4]$:

$$\begin{aligned} 2^{n-1} c(p, 1*^{n-1}) &\le \sum_{y \in \{0,1\}^{n-1}} \gamma^{1+w(y)} \\ &= \gamma\left(1+\gamma\right)^{n-1}. \end{aligned}$$

To deal with the first term, we proceed similarly as we did in the proof of Lemma 28. Note that $|T| \ge 1$, and if $w(y^T)$ is odd then $c_{1y}(p) = 0$. If $w(y^T)$ is even then as before we use the bound $c_{ry}(p) \le \gamma^{w(ry)}$. These two things yield

$$\begin{aligned}
2^{n-1}c(p, 0*^{n-1}) &\le \sum_{y^T \in E, y^U} \gamma^{w(y)} \\
&= \left( \frac{(1+\gamma)^{|T|} + (1-\gamma)^{|T|}}{2} \right) (1+\gamma)^{|U|} \\
&\le 3/4(1+\gamma)^{n-1}.
\end{aligned}$$

The last $\le$ follows as $|T| \ge 1$ and $1 - \gamma < \frac{1+\gamma}{2}$ when $1/\sqrt{2} \le \gamma$. Altogether this gives

$$2^n c(p, *^n) \le (3/4 + \gamma)(1+\gamma)^{n-1}.$$

So it only remains to show $(3/4 + \gamma) \le (1 - \Omega(1))(1+\gamma)$ which holds because $\gamma \le 1$.

## 5.4 Proof of Lemma 24

Let $T$ denote the set of variables that appear in the linear polynomial $p$ and let $U$ denote the remaining variables. Applying the same logic as in Example 4 we have

$$\begin{aligned}
\mathbb{E}_y c_y(p) &= \left( \frac{1-\gamma}{2} \right)^{|T|} \left( \frac{1+\gamma}{2} \right)^{|U|} \\
&\le \left( \frac{1-\gamma}{2} \right) \left( \frac{1+\gamma}{2} \right)^{n-1}.
\end{aligned}$$

The $\le$ follows since $|T| \ge 1$ and $1 + \gamma > 1 - \gamma$ when $\phi \in [0, \pi/4]$.

So it only remains to show $(1 - \gamma) \le (1 - \Omega(1))(1+\gamma)$ which holds because $\gamma \ge 1/\sqrt{2}$.

# 6 Boolean correlation

In this section we prove Theorem 6. Recall that $C_\phi$ is defined as the absolute value of a sum. We need to analyze this sum more carefully, so we define it next.

**Definition 35.** $E_\phi(p) := \mathbb{E}_{x \in \{0,1\}^n} (-1)^{p(x)} \omega^{\sum_i x_i}$. Note that $|E_\phi(p)| = C_\phi(p)$.

We now give an overview of the upcoming technical results. In the proof of Theorem 6, we will use Lemma 39, which relates $B_m(p)$ to the quantity $|Real(E_\phi(p))|$ for a specific angle $\phi$, and Corollary 41, which allows us to compute $|Real(E_\phi(s))|$ for $s = e^2, e^2 + e^1$. Together these two results will enable us to compute $B_m(s)$ for $s = e^2, e^2 + e^1$.

On the other hand, combining Lemma 39 with Theorem 5 lets us bound $B_m(p)$ when $p$ is not symmetric, since Theorem 5 bounds $C_\phi(p)$ and $|Real(E_\phi(p))| \le |E_\phi(p)| = C_\phi(p)$.

Proposition 36 and Claims 37, 38 are used to prove Lemma 39, and Lemma 40 is needed for Corollary 41.

For the rest of the section, fix any odd $m \ge 3$, set $\phi = 2\pi/m$, $\omega = e^{\phi\sqrt{-1}}$. We start with the following standard fact:

**Proposition 36.** *Let $b$ be the fraction of $n$-bit strings whose weight is divisible by $m$. For any $p$,*

$$B_m(p) = \frac{1}{b(1-b)} \left| \frac{2}{m} \cdot \sum_{k=1}^{(m-1)/2} Real(E_{k\phi}(p)) + \frac{1}{m} - b \right|$$

*where $Real(z)$ denotes the real part of the complex number $z$.*

*Proof.* Let $s(k) := \sum_{j=0}^{m} \omega^{jk} = 1 + \omega^k + \cdots + \omega^{(m-1)k}$ and note that $S(k) = m$ if $k \equiv 0 \mod m$ and $S(k) = 0$ otherwise. Using this notation we can write

$$B_m(p) = \left| \mathbb{E}_x (-1)^{p(x)} \frac{s(w(x))}{m} \cdot \frac{1}{b} - \mathbb{E}_x (-1)^{p(x)} \left(1 - \frac{s(w(x))}{m}\right) \cdot \frac{1}{1-b} \right|.$$

Collecting terms this is

$$\left| \mathbb{E}_x (-1)^{p(x)} \left( \frac{s(w(x))}{m} \cdot \frac{1}{b} - \left(1 - \frac{s(w(x))}{m}\right) \cdot \frac{1}{1-b} \right) \right|.$$

Using the definition of $s$ this equals

$$\left| \mathbb{E}_x (-1)^{p(x)} \left[ \left( \sum_{j=1}^{m} \omega^{jw(x)} \right) \left( \frac{1}{mb} + \frac{1}{m(1-b)} \right) + \frac{1}{mb} - \left(1 - \frac{1}{m}\right) \frac{1}{1-b} \right] \right|.$$

Also,

$$\frac{1}{mb} - \left(1 - \frac{1}{m}\right) \frac{1}{1-b} = \frac{1-mb}{mb(1-b)}.$$

Furthermore, $\omega^{jw(x)} + \omega^{(m-j)w(x)} = 2Real(\omega^{jw(x)})$ for each $j$. After factoring out $1/b(1-b)$ the result follows. □

Observe that in the statement of Lemma 36, if we replaced $b$ with $1/m$ then the terms that don't multiply $\omega$ would be 0. However, $b \neq 1/m$ but it will be very close. We use the following bound [1] that's implicit in [BHLV19].

**Claim 37.** $|b - 1/m| < \cos(\pi/m)^n$.

Now let $\ell_1 \in \{\frac{m-1}{4}, \frac{m+1}{4}\}$ denote the integer closest to $\frac{m}{4}$. The next result suggests we should focus on $Real(E_{\ell_1\phi}(p))$.

**Claim 38.** *Fix any odd $m \geq 3$ and $k \in \{1..., (m-1)/2\} : k \neq \ell_1$. Then for all large enough $n$ and any quadratic $p$,*

$$|Real(E_{k\phi}(p))| = o(\sqrt{v_{\ell_1\phi}}).$$

[1] When $m = 3$ the claim says $|b - 1/m| < 2^{-n}$ but we do not use this.

*Proof.* By Theorem 5, for any $k$ it holds that

$$C_{k\phi}(p) \le \max_{s\in\{0,e^1,e^2,e^2+e^1\}} C_{k\phi}(s) \le \max\left\{O\left(\left(\frac{1+|\sin(k\phi)|}{2}\right)^{n/2}\right), \left(\frac{1+|\cos(k\phi)|}{2}\right)^{n/2}\right\}.$$

Next we claim that if $k \in \{1..., (m-1)/2\}, k \neq \ell_1$ then $\max\{|\sin(k\phi)|, |cos(k\phi)|\} < \sin(\ell_1\phi)$. If this holds we can conclude since $\sqrt{v_{\ell_1\phi}} = \Omega((\frac{1+\sin(\ell_1\phi)}{2})^{n/2})$ and $|Real(E_{k\phi}(p))| \le C_{k\phi}(p)$.

To verify the claim, note for $k \neq \ell_1$, $|\sin(k\phi)|$ is maximized when $k = \ell_2$, where $\ell_2$ denotes the second closest integer to $m/4$. Since $m$ is odd, $\ell_2 \in \{\frac{m-3}{4}, \frac{m+3}{4}\}$ which implies $\sin(\ell_2\phi) < \sin(\ell_1\phi)$.

And $|\cos(k\phi)|$ is maximized for $k = (m-1)/2$ and $|\cos(k\phi)| = |\cos(\pi - \pi/m)| = \cos(\pi/m)$. We can now conclude as $\cos(\pi/m) < \sin(\ell_1\phi) = \sin(\pi/2 \pm \pi/2m) = \cos(\pi/2m)$. □

The next result, which combines Claim 37, 38 with Proposition 36, says we can approximate $B_m(p)$ using just $|Real(E_{\ell_1\phi}(p))|$.

**Lemma 39.** *For all large enough $n$ and any quadratic $p$,*

$$\left|B_m(p) - \frac{2m}{m-1}\,|Real(E_{\ell_1\phi}(p))|\right| \le o(\sqrt{v_{\ell_1\phi}}).$$

*For $m = 3$ this can be improved to*

$$\left|B_3(p) - 3\left|Real(E_{2\pi/3}(p))\right|\right| \le O(2^{-n}).$$

*Proof.* By Claim 37 and noting that $\cos(\pi/m)^n = o(\sqrt{v_{\ell_1\phi}})$ we have

$$\left|\frac{1}{b(1-b)} - \frac{m^2}{m-1}\right| = o(\sqrt{v_{\ell_1\phi}}).$$

Applying the triangle inequality and Claim 38 we also have

$$\left|\left|\sum_{k=1}^{(m-1)/2} Real(E_{k\phi}(p))\right| - \left|Real(E_{\ell_1\phi}(p))\right|\right| \le \sum_{k\neq\ell_1}\left|Real(E_{k\phi}(p))\right| \le m\cdot o(\sqrt{v_{\ell_1\phi}}).$$

Inserting the previous two inequalities into Lemma 36 implies

$$|B_m(p) - 2m/(m-1)|Real(E_{\ell_1\phi}(p))|| \le O(m)o(\sqrt{v_{\ell_1\phi}}).$$

We can now conclude since we consider $m$ fixed. □

We are naturally interested in computing $B_m(s)$ for $s = e^2, e^2+e^1$ and the next lemma allows us to do so by giving an expression for $E_{\ell_1\phi}(s)$. In Section 4 we determined $C_{\ell_1\phi}(s) = |E_{\ell_1\phi}(s)|$, but this no longer suffices as we need to understand the angle of $E_{\ell_1\phi}(s)$ in order to compute $|Real(E_{\ell_1\phi}(s))|$.

**Lemma 40.** *For any $k \in \{1, 2, \ldots, m-1\}$ we have:*

$$E_{k\phi}(e^2) = 2^{-(n+1)}\left[(1+i)(1-i\omega^k)^n + (1-i)(1+i\omega^k)^n\right],$$
$$E_{k\phi}(e^2+e^1) = 2^{-(n+1)}\left[(1-i)(1-i\omega^k)^n + (1+i)(1+i\omega^k)^n\right].$$

*Proof.* We prove Item 1. Since $(-1)^{e^2(x)} = (-1)^{\binom{w(x)}{2}}$ we can write

$$E_{k\phi}(e^2) = \sum_{j=0}^{n} \binom{n}{j} (-1)^{\binom{j}{2}} \omega^{kj}.$$

We also have

$$\sum_{j=0 \bmod 4} \binom{n}{j}\omega^{kj} = \sum_{j=0}^{n} \binom{n}{j}\omega^{kj}\left(\frac{1+i^j}{2}\right)\left(\frac{1+(-1)^j}{2}\right)$$
$$\sum_{j=2 \bmod 4} \binom{n}{j}\omega^{kj} = \sum_{j=0}^{n} \binom{n}{j}\omega^{kj}\left(\frac{1-i^j}{2}\right)\left(\frac{1+(-1)^j}{2}\right).$$

So this implies

$$\sum_{j=0 \bmod 4} \binom{n}{j}\omega^{kj} - \sum_{j=2 \bmod 4} \binom{n}{j}\omega^{kj} = \frac{1}{2}\left[(1+\omega^k i)^n + (1+\omega^k(-i))^n\right].$$

Doing the analogous for $j = 1, 3 \mod 4$ gives

$$\sum_{j=1 \bmod 4} \binom{n}{j}\omega^{kj} - \sum_{j=3 \bmod 4} \binom{n}{j}\omega^{kj} = \frac{1}{2}\left[-i(1+\omega^k i)^n + i(1+\omega^k(-i))^n\right].$$

The proof of Item 2 is similar. □

The next result result reduces the problem of computing $|Real(E_{\ell_1\phi}(s)|$ to the problem of computing $|\cos(\chi \pm \pi/4)|$ for a certain angle $\chi$. The angle $\chi \pm \pi/4$ arises because it is the angle of the vector $(1 \pm i)(1 - i\omega^{\ell_1})^n$, which is the dominant term in the previous expressions for $E_{\ell_1\phi}(s)$. The last equality below then allows us to relate $|Real(E_{\ell_1\phi}(s)|$ to $\sqrt{v_{\ell_1\phi}}$.

**Corollary 41.** *Let $\chi = \frac{n\pi}{4m}, -\frac{n\pi}{4m}$ when $\ell_1 = \frac{m+1}{4}, \frac{m-1}{4}$ respectively. Let $\gamma = \sqrt{2}|1 - i\omega^{\ell_1}|^n$. For all large enough $n$, the following holds:*

1. $\left|2^{n+1}|Real(E_{\ell_1\phi}(e^2))| - |\cos(\chi + \pi/4)|\gamma\right| = o(1)$
2. $\left|2^{n+1}|Real(E_{\ell_1\phi}(e^2+e^1))| - |\cos(\chi - \pi/4)|\gamma\right| = o(1)$,
3. $\left|2^{n+1}\sqrt{v_{\ell_1\phi}} - \gamma\right| = o(1)$.

*Proof.* We show the first equality when $\ell_1 = \frac{m+1}{4}$. The $\ell_1 = \frac{m-1}{4}$ case is symmetrical.

By definition $\omega^{\ell_1} = e^{\sqrt{-1}(2\pi/m)(m+1)/4} = e^{\sqrt{-1}(\pi/2+\pi/2m)}$, hence $-i\omega^{\ell_1} = e^{\sqrt{-1}(\pi/2m)}$. This implies $(1 - i\omega^{\ell_1}) = |1 - i\omega^{\ell_1}|e^{\sqrt{-1}(\pi/4m)}$. Additionally, $1 + i = \sqrt{2}e^{\sqrt{-1}(\pi/4)}$. So then

$$\begin{aligned}(1+i)(1-i\omega^{\ell_1})^n &= \sqrt{2}e^{\sqrt{-1}(\pi/4)} \cdot |1 - i\omega^{\ell_1}|^n e^{\sqrt{-1}(\pi/4m)n} \\ &= \gamma e^{\sqrt{-1}(n\pi/4m+\pi/4)}.\end{aligned}$$

We can now conclude by Lemma 40, the fact $|Real(e^{\sqrt{-1}\phi})| = |\cos\phi|$ for any $\phi$, and noting $|1+i\omega^{\ell_1}|^n = o(1)$ since $|1+i\omega^{\ell_1}| < 1$ when $m$ is odd. The second inequality is done similarly.

The third inequality follows by Lemma 40, the facts $|E_{\ell_1\phi}(p)| = C_{\ell_1\phi}(p)$, $|1+i\omega^{\ell_1}|^n = o(1)$, and since when $s = e^2, e^2 + e^1$, $\left|C_{\ell_1\phi}(s) - \sqrt{v_{\ell_1\phi}}\right| \leq o(1)$ by Lemma 17. □

## 6.1 Proof of Theorem 6

### 6.1.1 Proof of Item 1

First we prove the upper bound. Lemma 39 implies that

$$B_m(p) \leq 2m/(m-1)\,|Real(E_{\ell_1\phi}(p))| + o(\sqrt{v_{\ell_1\phi}}).$$

The upper bound now follows since $|Real(E_{\ell_1\phi}(p))| \leq |E_{\ell_1\phi}(p)| = C_{\ell_1\phi}(p) \leq (1+o(1))\sqrt{v_{\ell_1\phi}}$. The last inequality holds by Theorem 5.

Next we prove the lower bound by showing

$$\max_{s\in\{e^2,e^2+e^1\}} B_m(s) \geq (2m/(m-1) - o(1))\sqrt{\frac{v_{\ell_1\phi}}{2}}. \tag{6}$$

Lemma 39 implies that

$$B_m(s) \geq 2m/(m-1)\,|Real(E_{\ell_1\phi}(s))| - o(\sqrt{v_{\ell_1\phi}}).$$

Then we claim that for either $s = e^2$ or $s = e^2 + e^1$,

$$|Real(E_{\ell_1\phi}(s))| \geq (1 - o(1))\sqrt{\frac{v_{\ell_1\phi}}{2}}.$$

The previous two inequalities imply Equation 6.

To verify the claim, note that since $\cos(\pi/4) = 1/\sqrt{2}$, at least one of the next two inequalities hold for any angle $\chi$:

$$\begin{aligned}\cos(\chi + \pi/4) &\geq 1/\sqrt{2}, \\ \cos(\chi - \pi/4) &\geq 1/\sqrt{2}.\end{aligned}$$

We then conclude by Corollary 41.

### 6.1.2 Proof of Item 2

We present the $n \equiv 3m \bmod 4m, \ell_1 = \frac{m+1}{4}$ case. In the proof we show that $E_{\ell_1}(e^2)$ is essentially real, which means $|Real(E_{\ell_1}(e^2))|$ equals $\sqrt{v_{\ell_1\phi}}$ by Corollary 41. On the other hand, for any non-symmetric $p$, $C_{\ell_1\phi}(p)$ is a constant factor smaller than $\sqrt{v_{\ell_1\phi}}$ by Theorem 5. This suffices as $|E_{\ell_1\phi}(p)| = C_{\ell_1\phi}(p)$, and note the angle of $E_{\ell_1\phi}(p)$ does not even matter.

So first we show

$$B_m(e^2) \geq (2m/(m-1) - o(1))\sqrt{v_{\ell_1\phi}}.$$

This follows by Lemma 39 and the claim that

$$\left|Real(E_{\ell_1\phi}(e^2))\right| \geq (1-o(1))\sqrt{v_{\ell_1\phi}}.$$

To verify the claim, note when $n \equiv 3m$ mod $4m$, $n\pi/4m = (3m + k4m)\pi/4m \equiv 3\pi/4 + k\pi \bmod 2\pi$ for some integer $k$. Hence $\cos(n\pi/4m + \pi/4) = \cos((k+1)\pi) = \pm 1$. We then conclude by Corollary 41. Note $\cos(n\pi/4m - \pi/4) = 0$, so $B_m(e^2 + e^1) < B_m(e^2)$.

On the other hand, for any $p \neq e^2, e^2 + e^1$ we show

$$B_m(p) \leq 2m/(m-1)\sqrt{1 - \Omega(\sin(\ell_1\phi) - \cos(\ell_1\phi))} \cdot \sqrt{v_{\ell_1\phi}}.$$

This follows by Lemma 39 and Theorem 5 which states

$$C_{\ell_1\phi}(p) \leq \sqrt{1 - \Omega(\sin(\ell_1\phi) - \cos(\ell_1\phi))} \cdot \sqrt{v_{\ell_1\phi}}.$$

This yields the desired inequality since $|Real(E_{\ell_1\phi}(p))| \leq C_{\ell_1\phi}(p)$.

If $p = e^1, 0$ we show

$$\max_{s \in \{0, e^1\}} B_m(s) \leq (2m/(m-1)) \cdot o(\sqrt{v_{\ell_1}}). \tag{7}$$

This follows by Lemma 39 and noting for $s = e^1, 0$, $C_{\ell_1\phi}(s) = (\frac{1+\cos(\ell_1\phi)}{2})^{n/2} = o(\sqrt{v_{\ell_1\phi}})$ since $\cos(\ell_1\phi) < \sin(\ell_1\phi)$.

The $n \equiv 3m, \ell_1 = \frac{m-1}{4}$ case is similar except we use $e^2 + e^1$ instead of $e^2$. The $n \equiv m$ cases are analogous.

### 6.1.3 Proof of Item 3

We present the $n \equiv 0 \bmod 4m, \ell_1 = \frac{m+1}{4}$ case. First note that Equations 6 and 7 imply it suffices to prove $\max_{s \in \{e^2, e^2+e^1\}} B_m(s) < B_m(q)$ for some non-symmetric $q$. We will show that $E_{\ell_1\phi}(e^2), E_{\ell_1\phi}(e^2 + e^1)$ are both maximally imaginary as allowed by Equation 6. Next, consider $q := x_1 + e^2(x_2, \ldots, x_n)$. $C_{\ell_1\phi}(q)$ is close to, but less than $C_{\ell_1\phi}(s)$ for $s = e^2, e^2 + e^1$. However, $E_{\ell_1\phi}(q)$ will be more real which is enough to compensate for this difference and show that $|Real(E_{\ell_1\phi}(s))| < |Real(E_{\ell_1\phi}(q))|$.

So first we show that for either $s = e^2, e^2 + e^1$,

$$B_m(s) \leq (2m/(m-1) + o(1)) \cdot \sqrt{\frac{v_{\ell_1\phi}}{2}}.$$

This follows by Lemma 39 and the claim that for either $s = e^2, e^2 + e^1$,

$$|Real(E_{\ell_1\phi}(s))| \le (1 + o(1))\sqrt{\frac{v_{\ell_1\phi}}{2}}.$$

To verify the claim, since $n \equiv 0 \bmod 4m$, then $n\pi/4m \equiv k\pi \bmod 2\pi$. Hence $\cos(n\pi/4m \pm \pi/4m) = \pm 1/\sqrt{2}$. We then conclude by Corollary 41.

On the other hand, we show that

$$B_m(q) > (2m/(m-1) - o(1)) \cdot \frac{(1 + \tan(\pi/4m))\sqrt{v_{\ell_1\phi}}}{\sqrt{2}}.$$

Note $1 + \tan(\pi/4m) > 1$ for $m \ge 3$. The inequality holds by Lemma 39 and the claim

$$|Real(E_{\ell_1\phi}(q))| \ge (1 - o(1)) \cdot \frac{(1 + \tan(\pi/4m))\sqrt{v_{\ell_1\phi}}}{\sqrt{2}}.$$

To show the claim, we start by rewriting $E_{\ell_1\phi}(q)$ by conditioning on $x_1$ (below $e^2$ is on $n-1$ variables):

$$E_{\ell_1\phi}(q) = \frac{(1 - \omega^{\ell_1})}{2} E_{\ell_1\phi}(e^2).$$

An analogous version of Corollary 41 Item 1 holds for $e^2$ on $n-1$ variables:

$$\left| 2^n |Real(E_{\ell_1\phi}(e^2))| - \left| \cos\left(\frac{(n-1)\pi}{4m} + \frac{\pi}{4}\right) \right| \frac{\gamma}{|1 - i\omega^{\ell_1}|} \right| = o(1).$$

Since $-\omega^{\ell_1} = e^{\sqrt{-1}(-\pi/2+\pi/2m)}$ we have $(1 - \omega^{\ell_1}) = |1 - \omega^{\ell_1}| e^{\sqrt{-1}(-\pi/4+\pi/4m)}$. Combining this with the previous equality implies that

$$\left| 2^{n+1} |Real(E_{\ell_1\phi}(q))| - \left| \cos\left(\frac{(n-1)\pi}{4m} + \frac{\pi}{4m}\right) \right| \frac{|1 - \omega^{\ell_1}|}{|1 - i\omega^{\ell_1}|}\gamma \right| = o(1)$$
$$\iff \left| 2^{n+1} |Real(E_{\ell_1\phi}(q))| - \frac{|1 - \omega^{\ell_1}|}{|1 - i\omega^{\ell_1}|}\gamma \right| = o(1).$$

The $\iff$ follows as $\cos(n\pi/4m) = \pm 1$ when $n \equiv 0 \bmod 4m$.

To conclude, by Corollary 41 it suffices to show

$$\frac{1 + \tan(\pi/4m)}{\sqrt{2}} = \frac{|1 - \omega^{\ell_1}|}{|1 - i\omega^{\ell_1}|}.$$

Using the identity $|1 + e^{\sqrt{-1}\phi}| = 2|cos(\phi/2)|$, we have $|1 - i\omega^{\ell_1}| = 2\cos(\pi/4m)$ and $|1 - \omega^{\ell_1}| = 2|\cos(-\pi/4 + \pi/4m)| = 2\cos(\pi/4 - \pi/4m) = \sqrt{2}(\cos(\pi/4m) + \sin(\pi/4m))$ where the last step holds as $cos(a - b) = \cos a \cos b + \sin a \sin b$. Hence the equality holds.

The $n \equiv 0$, $\ell_1 = \frac{m-1}{4}$ case is similar except $q$ will be $e^2(x_2, \dots, x_n)$ instead. The $n \equiv 2m$ cases are analogous.

# 7 Symmetric correlates poorly with mod $m$

For completeness, we show that symmetric polynomials mod 2 correlate poorly with the complex mod $m$ function. To get a sense of the parameters below, fix $m = 3$ and apply the identities $\cos x \leq 1 - x^2/6$ and $(1-x)^n \leq e^{-xn}$. This yields $C_\phi(s) \leq O(d)2^{-\Omega(n/d^2)}$, so if Conjecture 2 were true this would imply exponentially small correlation bounds for any $O(\log n)$ degree polynomial - a long-standing open problem.

**Theorem 42.** *Let $\phi = 2\pi k/m$ for some odd $m$ and $k \in \{1, \dots m-1\}$. Then for any degree $d$ symmetric polynomial $s$,*

$$C_\phi(s) \leq 2md \cdot \cos\left(\frac{\pi}{2md}\right)^n.$$

*Proof.* Let $\delta$ be an integer such that $2^{\delta-1} \leq d < 2^\delta$. It is shown in [BGL06] that $s(x)$ is determined by the weight of $x$ mod $2^\delta$. Hence we can write

$$(-1)^{s(x)} = \sum_{i=0}^{2^\delta-1} c_i \mathbf{1}_{w(x) \equiv i \bmod 2^\delta}$$

where $c_i \in \{-1, 1\}$ for each $i$. Then we can write the correlation as

$$\begin{aligned} C_\phi(s) &= \left| \mathbb{E}_x[Mod_\phi(x) \cdot \sum_{i=0}^{2^\delta-1} c_i \mathbf{1}_{w(x)\equiv i \bmod 2^\delta}] \right| \\ &= \left| \sum_{i=0}^{2^\delta-1} \mathbb{E}_x\left[Mod_\phi(x) \cdot c_i \mathbf{1}_{w(x)\equiv i \bmod 2^\delta}\right] \right|. \end{aligned}$$

Letting $\omega = e^{\sqrt{-1}\cdot 2\pi/m}$, for any $i$ we have

$$\mathbb{E}_x\left[Mod_\phi(x) \cdot \mathbf{1}_{w(x)\equiv i \bmod 2^\delta}\right] = \sum_{j=0}^{m-1} \omega^{(i+j2^\delta)k} \mathbb{P}_x[w(x) \equiv i + j2^\delta \bmod m2^\delta].$$

We next use a slightly generalized version of Claim 37: □

**Claim 43.** *For any $k, m$, $|\mathbb{P}_x[w(x) \equiv k \bmod m] - 1/m| \leq \cos(\pi/m)^n$.*

*Proof.* Combining this with the fact $\sum_{j=0}^{m-1} \omega^{(i+j2^\delta)k} = 0$ implies that

$$\left|\mathbb{E}_x\left[Mod_\phi(x) \cdot \mathbf{1}_{w(x)\equiv i \bmod 2^\delta}\right]\right| \leq m(\cos(\pi/m2^\delta))^n.$$

Hence

$$C_\phi(s) \leq \sum_{i=0}^{2^\delta-1} \left|\mathbb{E}_x\left[Mod_\phi(x) \cdot c_i \mathbf{1}_{w(x)\equiv i \bmod 2^\delta}\right]\right| \leq m2^\delta \cos(\pi/m2^\delta))^n.$$

We can now conclude the proof since $2^\delta \leq 2d$. □

# 8 Structured cubic loses to quadratic

In this section we show that any cubic polynomial with a symmetric degree 3 part has correlation that is a constant factor worse than the optimal achieved by quadratic polynomials.

**Theorem 44.** *Suppose $t = e^3 + q$ for some arbitrary quadratic $q$. Then for any $\phi$,*

$$C_\phi(t) \leq (1 - \Omega(1)) \max_{s \in \{0, e^1, e^2, e^2+e^1\}} C_\phi(s).$$

We prove this by applying the derivative framework from Section 3. First, we analyze for every direction $y$ what the derivative $e^3_y$ will be and use this to bound the contribution $|c_y(e^3)|$. Then we show that for any $y$, adding the derivative $q_y$ (which will be linear) to $e^3_y$ can only decrease the contribution. In other words, we show $|c_y(t)| \leq |c_y(e^3)|$ for every $y$. This allows us to use our bounds on $|c_y(e^3)|$ to bound $C_\phi(t)$.

We first list some preliminary results we will need for the proof of Theorem 44. We characterize the Fourier coefficients of $e^2, e^2 + e^1$:

**Fact 45.** *Let $s$ denote either $e^2, e^2 + e^1$ on $n$ variables. Then for any $U \subseteq [n]$,*

1. *If $n$ is even then $\widehat{s}(U) \in \{2^{-n/2}, -2^{-n/2}\}$.*
2. *If $n$ is odd then $\widehat{s}(U) \in \{0, 2^{-(n-1)/2}, -2^{-(n-1)/2}\}$.*

**Fact 46.** *Let $p$ be an arbitrary polynomial and let $\ell$ be a linear polynomial. Then $|bias(e(p + \ell))| = |\widehat{e(p)}(L)|$, where $L \subseteq [n]$ denotes the variables in $\ell$.*

Next we state a simple result that says if for some arbitrary polynomial $p$ and direction $y$, the bias of $p_y$ is small after an arbitrary restriction to the 1-variables, then the contribution $|c_y(p)|$ must be small.

Below and for the remainder of the section, we let $V_1, V_0 \subseteq [n]$ denote the indices of the 1, 0-variables respectively with respect to a fixed direction $y$.

**Proposition 47.** *Fix some polynomial $p$ and direction $y \in \{0,1\}^n$. Suppose for any restriction $r \in \{0,1\}^{|V_1|}$ of the 1-variables,*

$$\left|\mathbb{E}_{x : x^{V_1} = r}(-1)^{p_y(x)}\right| \leq \delta.$$

*Then*

$$|c_y(p)| \leq \delta$$

*Proof.* We have

$$\begin{aligned} c_y(p) &= \mathbb{E}_x[(-1)^{p_y(x)} Mod_{\phi,y}(x)] \\ &= \mathbb{E}_{x^{V_1}}[Mod_{\phi,y}(x) \cdot \mathbb{E}_{x^{V_0}}[(-1)^{p_y(x)}]] \\ &\leq \delta. \end{aligned}$$

The second $=$ follows since $Mod_{\phi,y}(x)$ only depends on the 1-variables. The $\leq$ follows since $|Mod_{\phi,y}(x)| = 1$ and by the hypothesis on $p_y$. □

Next we characterize the derivatives of $e^3$ which depend on the weight of $y$ mod4. We abuse notation and let $e^i(V_j)$ denote the polynomial $e^i$ defined on the variables indexed by $V_j$.

**Proposition 48.** *Fix any direction $y \in \{0,1\}^n$ and consider the derivative $e^3_y$.*

1. *If $w(y) \equiv 0 \bmod 4$ then*
$$e^3_y = e^1(V_1) + e^1(V_1)e^1(V_0).$$

2. *If $w(y) \equiv 2 \bmod 4$ then*
$$e^3_y = e^1(V_1)e^1(V_0) + e^1(V_0).$$

3. *If $w(y) \equiv 1 \bmod 4$ then*
$$e^3_y = e^2(V_1) + e^2(V_0).$$

4. *If $w(y) \equiv 3 \bmod 4$ then*
$$e^3_y = (e^2 + e^1)(V_1) + (e^2 + e^1)(V_0) + 1.$$

*Proof.* We can write $e^3 = e^3(V_1) + e^2(V_1)e^1(V_0) + e^1(V_1)e^2(V_0) + e^3(V_0)$. Firstly note the term $e^3(V_0)$ does not affect $e^3_y$. Secondly, the term $e^1(V_1)e^2(V_0)$ only contributes $e^2(V_0)$ to $e^3_y$ when $|V_1| = w(y)$ is odd.

Thirdly, we deal with $e^2(V_1)e^1(V_0)$. Note that $e^1(V_0)$ has a coefficient of $\binom{w(y)}{2}$ in $e^3_y$, which is odd when $w(y) \equiv 2, 3 \bmod 4$. Now let $x_i$ denote a 1-variable. Then $x_i e^1(V_0)$ has a coefficient of $\binom{w(y)-1}{1}$, hence $e^1(V_1)e^1(V_0)$ appears when $w(y)$ is even.

Lastly, we deal with $e^3(V_1)$. Note $x_i$ has a coefficient of $\binom{w(y)-1}{2}$, hence $e^1(V_1)$ appears if $w(y) \equiv 0, 3 \bmod 4$. Let $x_j$ denote a second 1-variable. Then $x_i x_j$ has a coefficient of $\binom{w(y)-2}{1}$ hence $e^2(V_1)$ appears if $w(y)$ is odd. The constant 1 has a coefficient of $\binom{w(y)}{3}$ which is odd when $w(y) \equiv 3 \bmod 4$. □

**Lemma 49.** *Suppose $t = e^3 + q$ for some arbitrary quadratic $q$.*

1. *If $w(y) \in E$ then*
$$|c_y(t)| \le \frac{|\sigma|^{w(y)} + |\gamma|^{w(y)}}{2}.$$

2. *If $w(y) \in O$ then*
$$|c_y(t)| \le \frac{2^{w(y)}}{2^{n-1}}.$$

*Proof.* As a warmup, we first prove the $t = e^3$ case. Suppose $w(y) \equiv 0 \bmod 4$. By Proposition 48, if $x^{V_0} \in E$ then $e^3_y = e^1(V_1)$. If $x^{V_0} \in O$ then $e^3_y = 0$. Hence

$$\begin{aligned} c_y(e^3) &= 2^{-n}\Big(\sum_{x:x^{V_0} \in E} \sigma^{w(y)} + \sum_{x:x^{V_0} \in O} \gamma^{w(y)}\Big) \\ &= \frac{\sigma^{w(y)} + \gamma^{w(y)}}{2}. \end{aligned}$$

The $w(y) \equiv 2 \bmod 4$ case is similar. If $x^{V_0} \in E$ then $e_y^3 = 0$. Otherwise, $e_y^3 = e^1(V_0) + 1$. Hence $c_y(e^3) = \frac{-\sigma^{w(y)}+\gamma^{w(y)}}{2}$. This conclude the $w(y) \in E$ case.

Now suppose $w(y) \in O$. Fact 45 implies that for $s = e^2(V_0), (e^2 + e^1)(V_0)$, $|bias(e(s))| = |\widehat{e(s)}(\emptyset)| \le 2^{-(n-w(y)-1)}$. Since $e_y^3$ is disjoint on $V_0, V_1$, Proposition 47 implies that $|c_y(e^3)| \le 2^{-(n-w(y)-1)}$.

This concludes the $t = e^3$ case. Now suppose $t = e^3 + q$ for some quadratic $q$. Note that for any direction $y$, $p_y$ has the same quadratic terms as $e_y^3$ and $q_y$ only affects the linear terms in $p_y$. Let us write $q_y = u(V_1) + v(V_0)$, where $u(V_1), v(V_0)$ are linear polynomials over the $1, 0$-variables respectively.

First suppose $y \equiv 0 \bmod 4$. We now consider restricting the 1-variables. If $x^{V_1} \in E$ then $t_y^3 = c + v(V_0)$ where $c$ is some constant. If $x^{V_1} \in O$ then $t_y^3 = c + (e^1 + v)(V_0)$. Note that if $0 \neq v(V_0) \neq e^1(V_0)$, then the bias of the restricted function will be 0 for both cases. Hence by Proposition 47, $c_y(t) = 0$ and we are done. If $v(V_0) = e^1(V_0)$ then this is symmetrical to when $v(V_0) = 0$. Hence we can assume that $v(V_0) = 0$.

From here, we switch back to restricting the 0-variables. If $x^{V_0} \in E$ then $e_y^3 = (e^1+u)(V_1)$, and if $x^{V_0} \in O$ then $e_y^3 = u(V_1)$. Suppose $u(V_1)$ contains $k$ variables. Then $|c_y(t)| \le |\sigma|^{w(y)-k}|\gamma|^k$ whenever $x^{V_0} \in E$ and $|c_y(t)| \le |\sigma|^k|\gamma|^{w(y)-k}$ otherwise. Hence

$$|c_y(t)| \le \frac{|\sigma|^{w(y)-k}|\gamma^k| + |\sigma|^k|\gamma|^{w(y)-k}}{2}.$$

Assume that $|\sigma| > |\gamma|$ (the other case is similar). We can now conclude as

$$\begin{aligned} \frac{|\sigma|^{w(y)-k}|\gamma|^k + |\sigma|^k|\gamma|^{w(y)-k}}{2} &\le \frac{|\sigma|^{w(y)} + |\gamma|^{w(y)}}{2} \\ \iff \frac{|\gamma|^{w(y)-k}(|\sigma|^k - |\gamma|^k)}{2} &\le \frac{|\sigma|^{w(y)-k}(|\sigma|^k - |\gamma|^k)}{2} \\ \iff |\gamma| &\le |\sigma|. \end{aligned}$$

The $w(y) \equiv 2 \bmod 4$ case is analogous.

Now suppose $w(y) \equiv 1 \bmod 4$. After an arbitrary restriction to $x^{V_1}$, we have $e_y^3 = e^2(V_0) + v(V_0) + c$ for some constant $c$. Combining Facts 45, 46 implies that $|bias((-1)^{e_y^3})| \le 2^{-(n-w(y)-1)}$ after any restriction to $x^{V_1}$. We can now conclude by applying Proposition 47. The $w(y) \equiv 3 \bmod 4$ case is analogous. □

We are now ready to prove Theorem 44. We bound the overall contribution by applying Lemma 49 for every fixed direction $y$.

*Proof of Theorem 44.* By Lemma 49 we have

$$\begin{aligned} \sum_y |c_y(t)| &= \sum_{y:w(y)\in E} |c_y(t)| + \sum_{y:w(y)\in O} |c_y(t)| \\ &\le \sum_{y:w(y)\in E} \frac{|\sigma|^{w(y)} + |\gamma|^{w(y)}}{2} + \sum_{y:w(y)\in O} 2^{-(n-w(y)-1)} \\ &= \frac{(1+|\sigma|)^n + (1-|\sigma|)^n}{4} + \frac{(1+|\gamma|)^n + (1-|\gamma|)^n}{4} + \frac{3^n-1}{2^n}. \end{aligned}$$

Note that for any $\phi$, $\max\{1+|\sigma|, 1+|\gamma|\} \geq 1 + 1/\sqrt{2} > 3/2$. Now suppose that $\phi$ is such that $|\sigma| > |\gamma|$. Then

$$C_\phi^2(t) \leq 2^{-n}\frac{(1+o(1))(1+|\sigma|)^n}{4}.$$

On the other hand by Theorem 5 we know that

$$\max_{s\in\{e^2, e^2+e^1\}} C_\phi^2(s) \geq 2^{-n}\frac{(1+|\sigma|)^n}{2}.$$

Next suppose that $\phi$ is such that $|\sigma| \leq |\gamma|$. Then

$$C_\phi^2(t) \leq 2^{-n}\frac{(2+o(1))(1+|\gamma|)^n}{4}.$$

However by Theorem 5,

$$\max_{s\in\{0,e^1\}} C_\phi^2(s) = 2^{-n}(1+|\gamma|)^n.$$

□

**Acknowledgment.** We are grateful to Brenden Collins for collaborating during the initial stages of this project.

# 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. on Computing*, 4(4):431–442, 1975.

[BHLV19] Ravi Boppana, Johan Håstad, Chin Ho Lee, and Emanuele Viola. Bounded independence versus symmetric tests. *ACM Trans. Computation Theory*, 11(4):21:1–21:27, 2019.

[BL85] Michael Ben-Or and Nathan Linial. Collective coin flipping, robust voting schemes and minima of Banzhaf values. In *26th Symposium on Foundations of Computer Science*, pages 408–416, Portland, Oregon, 21–23 October 1985. IEEE.

[BL15] Abhishek Bhowmick and Shachar Lovett. Nonclassical polynomials as a barrier to polynomial lower bounds. In *IEEE Conf. on Computational Complexity (CCC)*, pages 72–87, 2015.

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

[Bou05] Jean Bourgain. Estimation of certain exponential sums arising in complexity theory. *Comptes Rendus Mathématique. Académie des Sciences. 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.

[CHH$^+$20] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, Shachar Lovett, and David Zuckerman. XOR lemmas for resilient functions against polynomials. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *ACM Symp. on the Theory of Computing (STOC)*, pages 234–246. ACM, 2020.

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

[GKV17] Frederic Green, Daniel Kreymer, and Emanuele Viola. Block-symmetric polynomials correlate with parity better than symmetric. *Computational Complexity*, 26(2):323–364, 2017. Available at http://www.ccs.neu.edu/home/viola/.

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

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

[GRS05] Frederic Green, Amitabha Roy, and Howard Straubing. Bounds on an exponential sum arising in Boolean circuit complexity. *Comptes Rendus Mathématique. Académie des Sciences. Paris*, 341(5):279–282, 2005.

[HIV22] Xuangui Huang, Peter Ivanov, and Emanuele Viola. Affine extractors and ac0-parity. In *Workshop on Randomization and Computation (RANDOM)*, 2022.

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

[MV15] Eric Miles and Emanuele Viola. Substitution-permutation networks, pseudorandom functions, and natural proofs. *J. of the ACM*, 62(6), 2015.

[NRR02] Moni Naor, Omer Reingold, and Alon Rosen. Pseudorandom functions and factoring. *SIAM J. Comput.*, 31(5):1383–1404, 2002.

[O'D07] Ryan O'Donnell. Analysis of boolean functions, 2007. Lecture notes. Available at http://www.cs.cmu.edu/ odonnell/boolean-analysis/.

[Raz87] Alexander Razborov. Lower bounds on the dimension of schemes of bounded depth in a complete basis containing the logical addition function. *Akademiya Nauk SSSR. Matematicheskie 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.

[Vio] Emanuele Viola. New lower bounds for probabilistic degree and AC0 with parity gates. *Theory of Computing.* Available at http://www.ccs.neu.edu/home/viola/.

[Vio06] Emanuele Viola. New correlation bounds for GF(2) polynomials using Gowers uniformity. *Electronic Colloquium on Computational Complexity*, Technical Report TR06-097, 2006. www.eccc.uni-trier.de/.

[Vio09a] Emanuele Viola. Correlation bounds for polynomials over $\{0,1\}$. *SIGACT News, Complexity Theory Column*, 40(1), 2009.

[Vio09b] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

[Vio17] Emanuele Viola. Challenges in computational lower bounds. *SIGACT News, Open Problems Column*, 48(1), 2017.

[Vio21] Emanuele Viola. Fourier conjectures, correlation bounds, and majority. In *Coll. on Automata, Languages and Programming (ICALP)*, 2021. Available at http://www.ccs.neu.edu/home/viola/.