Fourier conjectures, correlation bounds, and Majority*

Emanuele Viola†

May 6, 2021

Abstract

Recently several conjectures were made regarding the Fourier spectrum of low-degree polynomials. We show that these conjectures imply new correlation bounds for functions related to Majority. Then we prove several new results on correlation bounds which aim to, but don't, resolve the conjectures. In particular, we prove several new results on Majority which are of independent interest and complement Smolensky's classic result.

The recent "polarizing random walks" paradigm [CHHL18, CHLT19, CHH+20, CGL+20] constructs new pseudorandom generators against classes of functions with "bounded Fourier tails." For a function $f : \{0,1\}^n \to \{-1,1\}$ define

$$L_k(f) := \sum_{S\subseteq\{1,2,\dots,n\}:|S|=k} \left|\hat{f}(S)\right|,$$
$$M_k(f) := \sum_{S\subseteq\{1,2,\dots,n\}:|S|=k} \hat{f}(S),$$

where $\hat{f}(S) := \mathbb{E}_x f(x)\chi_S(x)$ for $\chi_S(x) := (-1)^{\sum_{i\in S} x_i}$ is the Fourier transform of f [O'D14]. These papers construct pseudorandom generators for functions with small L_k or M_k for several settings of parameters.

In an effort to use this framework to improve the state of pseudorandom generators against *low-degree polynomials* over $\mathbb{F}_2 = \{0,1\}$ [BV10a, Lov09, Vio09b, FSUV13], several conjectures have been put forth about polynomials. Let p be a degree-d polynomial over $\mathbb{F}_2$ in n variables. For $f := (-1)^p$ it has been conjectured (see [CHHL18, CHLT19, CGL+20]):

$$L_k(f) \le 2^{O(dk)} \qquad \forall k. \tag{1}$$
$$L_2(f) \le O(d^2), \tag{2}$$
$$M_k(f) \le 2^{o(dk)+O(k\log\log n)} \qquad \forall k \le O(\log n). \tag{3}$$

Conjecture (1) would not imply new pseudorandom generators, but would come close to matching the state-of-the-art using this framework – something which was eventually

*This paper includes the results in [Vio19]

†Supported by NSF CCF award 1813930.

achieved in [CGL$^+$20]. But conjectures (2) and (3) would imply new generators, improving on long-standing open problems. One interesting feature of this approach is that, unlike the influential approach by Nisan [Nis91], it is not based on *correlation bounds*. In particular, Conjecture (2) is not known to imply such bounds. Still, correlation bounds where shown to be *sufficient* for this approach in [CHH$^+$20].

We show that in fact correlation bounds are also *necessary*. That is, we show that this approach requires proving new correlation bounds for polynomials. This is new information about Conjecture (2). Conjecture (3) was shown in [CGL$^+$20] to imply new pseudorandom generators with good dependence on the error, and the latter are known to imply new correlation bounds for a function in NP [Vio09b]. We give a direct proof of this implication which yields a function in P (and other parameter improvements). In fact, we show that even weaker versions of the conjectures, such as $M_2 \leq o(\sqrt{n})$ for polynomials of degree $\log_2 n$, already imply new correlation bounds.

Correlation bounds. We say that a function $f : \{0,1\}^n \to \{-1,1\}$ has δ-*advantage (or* $(1-\delta)$-*error) (probabilistic) degree* d if there is a distribution P on polynomials $p : \{0,1\}^n \to \{0,1\}$ over $\mathbb{F}_2$ of degree d such that for every input x we have $\mathbb{P}[(-1)^{P(x)} = f(x)] \geq \delta$. By Yao's min-max argument [Yao77], a function f has δ-advantage degree d iff for every distribution D on $\{0,1\}^n$ it has δ-advantage degree d under D, meaning there exists a polynomial p over $\mathbb{F}_2$ of degree d such that $\mathbb{P}[(-1)^{p(D)} = f(D)] \geq \delta$. If f has range $\{0,1\}$ instead of $\{-1,1\}$ we use the same notation except $(-1)^{P(x)}$ is replaced simply by $P(x)$.

For two functions f and g from $\{0,1\}^n$ to $\{-1,1\}$ we define their *correlation* under a distribution D by $\mathbb{E}[f(D)g(D)]$, which we note equals $2(\mathbb{P}[f(D) = g(D)] - 1/2)$ and so it is (twice) the distance of $1/2$ from the advantage.

Since the classical works by Razborov and Smolensky [Raz87, Smo87] the best-available explicit probabilistic-degree lower bound for degree $d \geq \log_2 n$ gives error at best

$$1/2 - \Omega(d/\sqrt{n}) \tag{4}$$

which holds for the Majority function on n bits. In particular, it is consistent with our knowledge that every explicit function has $(1/2+1/\sqrt{n})$-advantage degree $\log_2 n$ (while non-constructively there exist functions which do not even have advantage exponentially close to $1/2$ for polynomial degree). For recent progress on functions computable in exponential-time classes see [Vio].

Proving correlation bounds is a fundamental open problem whose solution stands in the way of progress on a striking variety of fronts, including: circuit lower bounds, multiparty communication complexity, and matrix rigidity. For more on this long-standing challenge and a discussion of the just-mentioned implications, we refer the reader to [Vio09a, Vio17, Vio].

The conjectures imply new correlation bounds. We show that bounds on M_k imply new probabilistic-degree lower bounds for an explicit function h_k. We now define h_k and state our results.

Let $g_k : \{0,1\}^n \to \mathbb{Z}$ and $h_k : \{0,1\}^n \to \{-1,1\}$ be defined as

$$g_k(x) := \sum_{S:|S|=k} \chi_S(x),$$
$$h_k(x) := \mathrm{Sign}(g_k(x)),$$

where $\mathrm{Sign}(i) = 1$ if $i > 0$ and -1 otherwise (the value on $i = 0$ is arbitrary).

Theorem 1. *Let F be a distribution on functions from $\{0,1\}^n$ to $\{-1,1\}$ such that $\mathbb{P}[F(x) = h_k(x)] \geq 1/2+\epsilon$ for every x. Then there is an outcome f of F such that $M_k(f) \geq 2\epsilon \cdot e^{-k}\sqrt{\binom{n}{k}}$.*

To illustrate the theorem, consider first $k = 2$, in which case the conclusion becomes $M_2(f) \geq \Omega(\epsilon n)$. This means that showing even just $M_2(p) \leq o(\sqrt{n})$ for every degree-d polynomial requires showing that h_2 does not have $(1/2 + \Omega(1/\sqrt{n}))$-advantage degree d. This would improve the tradeoff (4) mentioned above when $d \geq \log_2 n$. Conjecture (2) implies the stronger bound $M_2(p) \leq O(d^2)$ for every degree-d polynomial p. This would mean that h_2 does not even have $(1/2 + cd^2/n)$-advantage degree d for a constant c, a quadratic improvement on the tradeoff (4). Consider now the case of larger k. Assuming that h_k has $(1/2+\epsilon)$-advantage degree d, and assuming Conjecture (3) and using the bound $\binom{n}{k} \geq (n/k)^k$ we obtain

$$2\epsilon \cdot e^{-k}\left(\frac{n}{k}\right)^{k/2} \leq 2\epsilon \cdot e^{-k}\sqrt{\binom{n}{k}} \leq 2^{o(dk)+O(k\log\log n)}.$$

This implies $\epsilon \leq 2^{k(o(d)+O(\log\log n)-0.5\log_2(n/k))}$. For $k = \log_2 n$ this yields new correlation bounds. Indeed, let $d := \log_2 n$. Then because $o(d)$, $\log\log n$, and $\log(k)$ are all $o(\log n)$ we obtain

$$\epsilon \leq 2^{-\Omega(k\log n)} = 2^{-\Omega(\log^2 n)}$$

which improves on the tradeoff (4).

Proof. Note that for any function f, by linearity of expectation, we have

$$M_k(f) = \mathbb{E}_x f(x) g_k(x).$$

Fix any x and let $\mathbb{P}[F(x) = h_k(x)]$ be equal to $1/2 + \epsilon_x \geq 1/2 + \epsilon$. We can write

$$\mathbb{E}_F[F(x)g_k(x)] = (1/2+\epsilon_x)\cdot \mathrm{Sign}(g_k(x))\cdot g_k(x) + (1/2-\epsilon_x)\cdot(-\mathrm{Sign}(g_k(x)))\cdot g_k(x),$$

holding even if $g_k(x) = 0$. Note that $\mathrm{Sign}(g_k(x)) \cdot g_k(x) = |g_k(x)|$. Hence

$$\mathbb{E}_F[F(x)g_k(x)] = (1/2+\epsilon_x)|g_k(x)| + (1/2-\epsilon_x)(-|g_k(x)|) = 2\epsilon_x|g_k(x)| \geq 2\epsilon|g_k(x)|.$$

This gives $\mathbb{E}_{x,F}F(x)g_k(x) \geq \mathbb{E}_x 2\epsilon|g_k(x)|$. In particular, there exists an outcome f such that

$$\mathbb{E}_x f(x)g_k(x) \geq 2\epsilon\mathbb{E}_x|g_k(x)|.$$

There remains to bound $\mathbb{E}_x|g_k(x)|$. We make use of *hypercontractivity* from the analysis of Boolean functions. Because g_k is a polynomial of degree k, by Theorem 9.22 in [O'D14] we have

$$\mathbb{E}_x|g_k(x)| \geq e^{-k}\sqrt{\mathbb{E}_x|g_k(x)|^2}.$$

Now observe that

$$\mathbb{E}_x|g_k(x)|^2 = \mathbb{E}_x \sum_{S,T:|S|=|T|=k} \chi_S(x)\chi_T(x) = \mathbb{E}_x \sum_{S,T:|S|=|T|=k} \chi_{S\oplus T}(x) = \binom{n}{k},$$

where $\oplus$ is symmetric difference. The last equality holds because the terms where $S \neq T$ have expectation zero, and the others have expectation one. The result follows. □

A natural question is whether Theorem 1 holds even for functions that correlate with h_k under the uniform distribution. We show that it does not.

Theorem 2. *Let n be a power of 2. For any integer s between 0 and $\sqrt{n}/2$ there is a function $f : \{0,1\}^n \to \{-1,1\}$ such that $\mathbb{P}[f(x) = h_2(x)] \geq 1/2 + \Omega(s/\sqrt{n})$ but $M_2(f) \leq O(s^2)$.*

To get a sense of the parameters let $\mathbb{P}[f(x) = h_2(x)] = 1/2 + \epsilon$. Then $M_2(f)$ is only $O(\epsilon^2 n)$ as opposed to $\Omega(\epsilon n)$ in Theorem 1. In particular, if $s = O(1)$ and $\epsilon = \Theta(1/\sqrt{n})$ we get $M_2(f) = O(1)$ as opposed to $\Omega(\sqrt{n})$ in Theorem 1.

We have shown that understanding the probabilistic degree of the functions h_k is also important for the feasibility of recent approaches to pseudorandom generators against polynomials. We obtain new bounds on the probabilistic degree of the functions h_k which however fall short of resolving whether the correlation bounds in the conclusion of Theorem 1 hold or not. We begin with studying h_1 which is essentially the majority function Maj. The results are of independent interest, and a natural step to tackle h_k for larger k. Indeed, below we use techniques developed for Maj to give new results on h_2.

We point out that the probabilistic degree tradeoff of Majority is not known. Given the tremendous interest in this function, this may come as a surprise. One might be tempted to think that Smolensky's tradeoff (4) is tight. We can show that it is indeed tight *under the uniform distribution.*

Theorem 3. *Majority has $(1/2+\Omega(d/\sqrt{n}))$-advantage degree d under the uniform distribution.*

Recall this means that there are degree-d polynomials p over $\mathbb{F}_2$ such that $\mathbb{P}_x[p(x) = \mathrm{Maj}(x)] \geq 1/2 + \Omega(d/\sqrt{n})$, where x is uniform in $\{0,1\}^n$. Such a result was only known for $d = O(1)$ or $d = \Omega(\sqrt{n})$, see [Vio09a].

However, there are harder distributions. We beat Smolensky's bound for degree one. While such polynomials are simple, in light of Theorem 3 this result already requires a non-uniform distribution.

Theorem 4. *Majority does not have $(1/2 + c/n)$-advantage degree one, for some constant c. This bound is tight up to the value of c.*

We now turn to constructions of probabilistic polynomials for majority. This problem is related to the so-called *coin problem,* defined next.

Definition 5. For $\delta \in [0,1]$ we denote by N^t_δ the distribution over $\{0,1\}^t$ where the bits are i.i.d. and each comes up 1 with probability δ. We say that a distribution F on boolean functions on t bits $(1/2+\alpha)$-*solves the* δ-*coin problem with advantage* α if the following is true:

(1) $\mathbb{P}[F(N^t_\delta) = 1] \geq 1/2 + \alpha$; and

(2) $\mathbb{P}[F(N^t_{1-\delta}) = 0] \geq 1/2 + \alpha$.

The study of the coin problem for low-degree polynomials goes back to [SV10] (see also the thesis [Vio06]) and has been the subject of several recent works including [LSS+19, GII+19, Sri20]. This problem has also been studied in a variety of other models; the terminology "coin problem" was coined in [BV10b].

However, these works consider large advantage $\alpha = \Omega(1)$. By contrast, we are interested in the setting where α is close to 0. We give tight bounds in this setting, showing that with degree d the best we can do is to boost the bias by d.

Theorem 6. *There is a distribution on polynomials of degree $O(d)$ that $(1/2+d\epsilon)$-solves the $(1/2+\epsilon)$-coin problem, whenever $d\epsilon < c$ for an absolute constant c. Moreover, this is tight up to the constant in the $O(.)$.*

Computing Majority on n bits for odd n can be randomly reduced to solving the $(1/2+1/n)$-coin problem, simply by selecting uniform bits from the input. Hence, Theorem 6 shows that Majority has $(1/2+d/n)$-advantage degree $\leq O(d)$. We improve the advantage to $\Omega(d^2/n)$, and conjecture that this is tight.

Theorem 7. *Majority on n bits, for odd n, has $(1/2+d^2/n)$-advantage degree $\leq O(d)$.*

Conjecture 8. *Theorem 7 is tight. A "hard" distribution can be uniform on the inputs of Hamming weights $n/2+2^{\ell-1}$ and $n/2-2^{\ell-1}$ where $d < 2^\ell$.*

To understand the choice of the hard distribution, recall that *symmetric* polynomials of degree $d < 2^\ell$ only depend on the weight of the input modulo 2^ℓ (see Lemma 11). For example, for $\ell = 1$ symmetric polynomials of degree $1 < 2$ only depend on the input weight modulo 2. The two Hamming weights in the conjecture are congruent modulo 2^ℓ; hence any symmetric polynomial of degree $< 2^\ell$ has correlation zero.

Finally, we turn to h_2. One can reduce h_2 to a majority on $\binom{n}{2}$ bits, and then apply Theorem 7 to obtain advantage $1/2+\Omega(d^2/n^2)$. We improve this to $1/2+\Omega(d^2/n^{3/2})$, under a condition on n.

Theorem 9. *Let ℓ be the smallest integer such that $d \leq 2^\ell$. Suppose that the remainder of $\sqrt{n}$ divided by $2^{\ell+100}$ is not in $[0,2d] \cup [2^{\ell+100}-2d, 2^{\ell+100}]$.*

Then h_2 has $(1/2+d^2/n^{3/2})$-advantage degree $O(d)$.

This result is not strong enough to disprove Conjecture (2). For that we require advantage $1/2+\omega(d^2/n)$.

The rest of the paper is organized as follows. After some preliminaries in Section 1 we prove the statements in the same order in which we discussed them, except that the proof of Theorem 2 is in Section 7.

1 Preliminaries

In this section we collect several results which are used in later proofs.

The following lemma shows that the majority of several i.i.d. Bernoulli random variables increases their bias, even in the regime where the bias is very small to start with.

Lemma 10. $\mathbb{P}[\mathrm{Maj}(N^t_{1/2+\alpha}) = 1] \geq 1/2 + \Omega(\alpha\sqrt{t})$, *whenever* $\sqrt{t}\alpha < c$ *for an absolute constant* c.

We are not aware of a source from which this result can be easily extracted, so we provide a proof. But Jarosław Błasiok let us know that this lemma appears as Lemma 8 in [TMB+17].

Proof. We prove $\mathbb{P}[\mathrm{Maj}(N^t_{1/2+\alpha}) = 1] - \mathbb{P}[\mathrm{Maj}(N^t_{1/2+\alpha}) = 0] \geq \Omega(\alpha\sqrt{t})$. The former difference can be written as

$$\sum_{i=1/2}^{t/2} \binom{t}{t/2+i} \left((1/2+\alpha)^{t/2+i}(1/2-\alpha)^{t/2-i} - (1/2-\alpha)^{t/2+i}(1/2+\alpha)^{t/2-i}\right),$$

where the sum is for $i = 1/2, 1+1/2, 2+1/2, \ldots, t/2$.

Collecting a 2^t factor and writing z for 2α this equals

$$2^{-t}\sum_{i=1/2}^{t/2} \binom{t}{t/2+i} \left((1+z)^{t/2+i}(1-z)^{t/2-i} - (1-z)^{t/2+i}(1+z)^{t/2-i}\right).$$

Further collecting $(1-z)^{t/2}(1+z)^{t/2} = (1-z^2)^{t/2}$ we rewrite it as

$$2^{-t}(1-z^2)^{t/2}\sum_{i=1/2}^{t/2} \binom{t}{t/2+i} \left(\left(\frac{1+z}{1-z}\right)^i - \left(\frac{1-z}{1+z}\right)^i\right).$$

Note that $\left(\frac{1+z}{1-z}\right) > 1$ and so $\left(\frac{1+z}{1-z}\right)^i - \left(\frac{1-z}{1+z}\right)^i$ is positive and increasing with i. Hence for any s we can bound below the expression by

$$2^{-t}(1-z^2)^{t/2}\sum_{i=s}^{t/2} \binom{t}{t/2+i} \left(\left(\frac{1+z}{1-z}\right)^s - \left(\frac{1-z}{1+z}\right)^s\right).$$

Moreover, let us write

$$\left(\frac{1+z}{1-z}\right)^s - \left(\frac{1-z}{1+z}\right)^s = (1+x)^s - (1-y)^s$$

where $x = 2z/(1-z)$ and $y = 2z/(1+z)$. We bound below the right-hand side by

$$1 + xs - e^{-ys} \geq 1 + xs - (1 - ys + (ys)^2) = s(x+y) - y^2s^2.$$

We pick $s = \sqrt{t}/100 + 1/2$. The above expression is $\Omega(\sqrt{t}\alpha)$ as long as $\sqrt{t}\alpha = \Theta(st)$ is sufficiently small. Moreover, we have

$$2^{-t}(1-z^2)^{t/2}\sum_{i=s}^{t/2} \binom{t}{t/2+i} \geq \Omega(1).$$

This holds because $(1-z^2)^{t/2} \geq \Omega(1)$ and the sum of binomial coefficients is also $\Omega(2^{-t})$ using Stirling's approximation to the binomial coefficient. $\square$

We use the following characterization of symmetric polynomials which is Theorem 2.4 in [BGL06] and follows from Lucas' theorem.

Lemma 11. *Let $f : \{0,1\}^n \to \{0,1\}$ be a symmetric function that only depends on the input Hamming weight modulo 2^ℓ. Then f is computable by a symmetric $\mathbb{F}_2$ polynomial of degree $< 2^\ell$. Conversely, any function $f : \{0,1\}^n \to \{0,1\}$ computable by a symmetric $\mathbb{F}_2$ polynomial of degree $< 2^\ell$ only depends on the input Hamming weight modulo 2^ℓ.*

Then we need constructions of probabilistic polynomials for symmetric functions, obtained in [AW15]. The bounds in the earlier paper [Sri13] would also suffice for the main points in this paper. See also [STV19] for a recent characterization.

Lemma 12. *[AW15] Let $f : \{0,1\}^n \to \{0,1\}$ be symmetric. Then f has $(1-\epsilon)$-advantage degree $O(\sqrt{n \log(1/\epsilon)})$, for any ϵ.*

2 Proof of Theorem 3

The main proof is for odd n. If n is even we can use the polynomial $p'(x_0, x_1, \ldots, x_{n-1}) := p(x_0, x_1, \ldots, x_{n-2})(1 - x_{n-1})$ where p is the polynomial with the highest correlation γ with majority on input length $n-1$. The correlation of p' with majority is $> \gamma/2$.

We now proceed with the main proof. We can assume without loss of generality that d is a power of 2 and $\leq 0.1\sqrt{n}$. The polynomial witnessing the correlation will be *symmetric.* For a symmetric function $f : \{0,1\}^n \to \{0,1\}$ write $f_w : \{0,1,\ldots,n\} \to \{0,1\}$ for $f(x) = f_w(|x|)$ where $|x|$ is the Hamming weight of x. The correlation between a symmetric polynomial p and $(-1)^{\text{Maj}}$ can be written as

$$2^{-n} \sum_{i=0}^{n} \binom{n}{i} (-1)^{p_w(i)} (-1)^{Maj_w(i)}.$$

To construct p we use Lemma 11 for $\ell = \log_2(2d)$. That shows that for any $f_w : \{0,1,\ldots,n\} \to \{0,1\}$ that depends only on the input modulo 2^ℓ there is a symmetric polynomial $p : \{0,1\}^n \to \{0,1\}$ of degree 2^ℓ such that $p_w = f_w$.

The definition of f_w and hence p is as follows. Define Block i to be the $2d$ integers $2di+0, 2di+1, \ldots, 2di+2d-1$. Let i^* be the smallest i such that Block i contains an integer larger than $n/2$. Let t be the number of integers less than $n/2$ in Block i^*. (If $n+1$ is a power of 2 we have $t = 0$, and below there is no residual chunk.) Define f_w to be 1 on the smallest t inputs, 0 on the next t, 0 on the next $d-t$, and finally 1 on the next $d-t$. Here's an example for $n = 17, d = 2, t = 1, i^* = 2$; the last row shows the division in blocks:

weight	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$(-1)^{Maj_w}$	-	-	-	-	-	-	-	-	-	+	+	+	+	+	+	+	+	+
$(-1)^{p_w}$	-	+	+	-	-	+	+	-	-	+	+	-	-	+	+	-	-	+

Note that p_w is by construction anti-symmetric in the sense, different from above, that: $p_w(i) = 1 - p_w(n-i)$. The same is true for Maj_w. Therefore $g(i) := (-1)^{p_w(i)}(-1)^{Maj_w(i)}$

is symmetric, that is $g(i) = g(n-i)$. Hence we only need to consider the bigger half of the Hamming weights. Majority is always 1, and so we can rewrite the correlation as

$$2^{-n} \cdot 2 \cdot \sum_{i=0}^{(n-1)/2} \binom{n}{(n+1)/2+i} (-1)^{p_w((n+1)/2+i)}.$$

Enumerate the above binomial coefficients starting from the biggest one for $i = 0$. The term $(-1)^{p_w((n+1)/2+i)}$ will be $+1$ on the first $t + (d-t) = d$, then -1 on the next d, then again $+1$ on the next d, and so on. We group the coefficients in chunks of length $2d$; in each chunk the term is $+1$ for the first half and -1 for the second half. The number of coefficients is $(n+1)/2$. Hence we have $\lfloor (n+1)/4d \rfloor$ chunks, plus a residual truncated chunk of length $\ell < 2d$.

Hence we can write the correlation as follows.

$$2^{-n} \cdot 2 \cdot \sum_{i=0}^{\lfloor (n+1)/4d \rfloor - 1} \sum_{j=0}^{d-1} \left(\binom{n}{(n+1)/2 + 2di + j} - \binom{n}{(n+1)/2 + 2di + j + d} \right)$$
$$+ 2^{-n} \cdot 2 \cdot \sum_{i=0}^{\ell - 1} \binom{n}{n-i} (-1)^{p_w((n+1)/2+i)}.$$

By, say, a Chernoff bound the absolute value of the latter summand $+2^{-n} \cdots$ is at most $2^{-\Omega(n)}$, using that $\ell < 2d = O(\sqrt{n})$. Now consider the first summand. Because the binomials are decreasing in size, each difference is positive. Hence we obtain a lower bound if we reduce the range of i. We reduce it to $\lfloor \sqrt{n}/d \rfloor$. So the correlation is at least

$$2^{-n} \cdot 2 \cdot \sum_{i=0}^{\lfloor \sqrt{n}/d \rfloor} \sum_{j=0}^{d-1} \left(\binom{n}{(n+1)/2 + 2di + j} - \binom{n}{(n+1)/2 + 2di + j + d} \right) - 2^{-\Omega(n)}.$$

The next lemma bounds below the difference of two such binomial coefficients.

Lemma 13. *For $s \le 4\sqrt{n}$ and $d \le 0.1\sqrt{n}$ we have:* $2^{-n} \left(\binom{n}{n/2+s} - \binom{n}{n/2+s+d} \right) \ge \Omega(sd/n^{3/2})$.

We apply the lemma with $s = 1/2 + 2di + j$ which note is $\le 1/2 + 2\sqrt{n} + 0.1\sqrt{n} \le 3\sqrt{n}$. The correlation is at least

$$\sum_{i=0}^{\lfloor \sqrt{n}/d \rfloor} \sum_{j=0}^{d-1} \Omega((1/2 + 2di + j)d/n^{3/2}) - 2^{-\Omega(n)} \ge \sum_{k=0}^{\Omega(\sqrt{n})} \Omega(kd/n^{3/2}) - 2^{-\Omega(n)} \ge \Omega(d/\sqrt{n}).$$

To justify the first inequality we use $1/2 + 2di + j \ge di + j$ and then do the change of variable $k = di + j$. For the second we use that the sum of all k up to $\Omega(\sqrt{n})$ is $\Omega(n)$. This concludes the proof except for the lemma.

Proof of lemma We have

$$\binom{n}{n/2+s} - \binom{n}{n/2+s+d}$$
$$=\frac{n!}{(n/2+s)!(n/2-s)!} - \frac{n!}{(n/2+s+d)!(n/2-s-d)!}$$
$$=\frac{n!}{(n/2+s)!(n/2-s)!}\left[1 - \frac{(n/2-s)(n/2-s-1)\cdots(n/2-s-d+1)}{(n/2+s+d)(n/2+s+d-1)\cdots(n/2+s+1)}\right].$$

The ratio inside the square bracket is at most

$$\frac{(n/2-s)^d}{(n/2)^d} = (1-2s/n)^d \le e^{-2sd/n} \le 1 - sd/n,$$

where the last inequality holds because $2sd/n \le 1$.

The binomial coefficient outside of the square bracket is

$$\binom{n}{n/2+s} \ge \frac{2^{nh(1/2+s/n)}}{\sqrt{8n(1/2+s/n)(1/2-sn)}} \ge \Omega\left(\frac{2^{n(1-O(s^2/n^2))}}{\sqrt{n}}\right) \ge \Omega\left(\frac{2^n}{\sqrt{n}}\right).$$

Here h is the binary entropy function, and the first inequality can be found as Lemma 17.5.1 in [CT06]. The second and third inequalities follow from the approximation $h(1/2+x) \ge 1-4x^2$, valid for every x, and $s = O(\sqrt{n})$.

The lemma follows by combining the two bounds.

3 Proof of Theorem 4

First let us discuss tightness. To show tightness for odd n we simply output a uniformly selected bit. For even n this works for all inputs except those of Hamming weight $= n/2$. To fix this, we modify the distribution on polynomials to equal 1 with probability $1/n$. On input of weight $= n/2$ we get the right value with probability $1/n + (1-1/n)(1/2) \ge 1/2 + \Omega(1/n)$. On inputs of Hamming weight $\neq n/2$ we also get the right value with probability $(1-1/n)(1/2+1/n) \ge 1/2 + \Omega(1/n)$.

We now move to negative results. First we note that we can reduce the case of even n to that of odd n: simply append a bit whose value is that of majority on balanced inputs. This does not change the value of majority, and has negligible effect on the advantage. Hence it suffices to prove a negative result for even n, and we do so in the rest of this section.

We select as the hard distribution the distribution D which is uniform on inputs of Hamming weight $n/2+1$ and $n/2-1$. Our goal is to show that for every fixed degree-one polynomial f we have $\mathbb{P}[f(D) = \mathrm{Maj}(D)] \le 1/2 + O(1/n)$. Using *generating functions* we obtain a proof which is nearly calculation-free, requiring only elementary bounds on binomials. Let $m = n/2$ and $f = x_1 + x_2 + \cdots + x_k$ for a parameter k. Let

$$b(n,m,k) = \sum_{i=0}^{k} (-1)^i \binom{m}{i}\binom{n-m}{k-i}.$$

Note that $b(n,m,k)/\binom{n}{k}$ is the probability that a uniform set of size k has odd intersection with a fixed set of size m, minus the probability that it has even intersection. By the definition of D and f one obtains that $|\mathbb{P}[f(D) = \mathrm{Maj}(D)] - 1/2|$ is at most big-Oh of

$$\alpha(n, n/2-1, k) := \left| \frac{1}{\binom{n}{k}} (b(n, n/2-1, k) - b(n, n/2+1, k)) \right|.$$

Note that we can assume that f has no constant term because we are taking absolute values in the expression $|\mathbb{P}[f(D) = \mathrm{Maj}(D)] - 1/2|$.

First we use generating functions to obtain a closed form for $b(n,m,k)$. Recall the generating functions (see e.g. [GKP94] for background on this technique)

$$(1+z)^n = \sum_{i \geq 0} \binom{n}{i} z^i,$$
$$(1-z)^n = \sum_{i \geq 0} \binom{n}{i} (-1)^i z^i.$$

We have

$$(1-z)^m (1+z)^{n-m} = \sum_{i \geq 0, j \geq 0} \binom{m}{i} \binom{n-m}{j} (-1)^i z^{i+j} = \sum_{k \geq 0} b(n,m,k) z^k.$$

If $m = n/2 - t$ the left-hand side can be written as

$$\begin{aligned} &(1-z)^{n/2-t}(1+z)^{n/2-t}(1+z)^{2t} \\ =&(1-z^2)^{n/2-t}(1+z)^{2t} \\ =&\sum_{i \geq 0} (-1)^i \binom{n/2-t}{i} z^{2i} (1+z)^{2t}. \end{aligned}$$

Similarly, if $m = n/2 + t$ then it can be written as

$$\begin{aligned} &(1-z)^{n/2-t}(1+z)^{n/2-t}(1-z)^{2t} \\ =&\sum_{i \geq 0} (-1)^i \binom{n/2-t}{i} z^{2i} (1-z)^{2t}. \end{aligned}$$

Specializing to $t = 1$ we obtain

$$\begin{aligned} &\sum_{k \geq 0} (b(n, n/2-1, k) - b(n, n/2+1, k)) z^k \\ =&\sum_{i \geq 0} (-1)^i \binom{n/2-1}{i} z^{2i} \left((1+z)^2 - (1-z)^2\right) \\ =&\sum_{i \geq 0} (-1)^i \binom{n/2-1}{i} z^{2i} \cdot 4z \\ =&4 \sum_{i \geq 0} (-1)^i \binom{n/2-1}{i} z^{2i+1}. \end{aligned}$$

Equating coefficients of z^k yields

$$b(n, n/2-1, k) - b(n, n/2+1, k) = 4(-1)^{(k-1)/2}\binom{n/2-1}{(k-1)/2}$$

if k is odd, otherwise the left-hand side is zero.

Hence we get

$$\alpha = 4\binom{n/2-1}{(k-1)/2}/\binom{n}{k}$$

if k is odd, and $\alpha = 0$ if k is even.

There remains to bound the right-hand side. First, we can assume that $k \leq n/2$ because replacing k with $n-k$ does not change the value of α. If $k = 0, 1$ we readily have $\alpha = O(1/n)$, using that n is even. Otherwise we can use the bounds

$$(n/k)^k \leq \binom{n}{k} \leq (en/k)^k$$

to again show $\alpha = O(1/n)$. We have

$$\alpha \leq 4\left(\frac{n}{(k-1)}\right)^{(k-1)/2}\left(\frac{k}{n}\right)^k = 4\sqrt{\frac{k}{n}}\left(\sqrt{\frac{1}{k-1}} \cdot \frac{k}{\sqrt{n}}\right)^k.$$

We can conclude by noticing that if $k \leq 100\log_2 n$ then this is at most $\operatorname{poly}\log n/n^{1.5} \leq O(1/n)$, using $k \geq 2$; while if $k \geq 100\log_2 n$ using that $k \leq n/2$ and $k-1 \geq 0.99k$ we have

$$\alpha \leq O(1) \cdot \left(\frac{\sqrt{k}}{\sqrt{0.99n}}\right)^k \leq O(1)(\sqrt{0.5/0.99})^k \leq O(1)(3/4)^k \leq 1/n.$$

4 Proof of Theorem 6

The theorem follows immediately from the following more general lemma, which we will also use later.

Lemma 14. *There is a distribution P on polynomials on $s = O(d^2)$ bits of degree $O(d)$ such that for every $\epsilon \in [-1/2, 1/2]$, $\epsilon \leq 1/d$, we have $\mathbb{P}[P(N^s_{1/2+\epsilon}) = \operatorname{Sign}(\epsilon)] \geq 1/2 + \Omega(d\epsilon)$.*

Proof. Let $P'' : \{0,1\}^s \to \{0,1\}$ be the probabilistic polynomial of degree $O(d)$ from Theorem 12 which computes Maj on every input with probability 0.99, with input length $s = O(d^2)$ which is assumed to be odd without loss of generality.

We modify P'' so that the probability that it makes a mistake on input x only depends on $||x| - n/2|$. That is, it is the same on every two inputs of weights $n/2 + i$ and $n/2 - i$. First, let P' pick a random permutation of the input bits, and then apply P''. The probability that P' makes a mistake only depends on $|x|$. Second, define P that on input x tosses a coin, and if it is heads it outputs $P'(x)$, and if it is tails it complements x to obtain $\neg x$, runs $P'(\neg x)$, and flips the answer. Because $\operatorname{Maj}(x) = 1 - \operatorname{Maj}(\neg x)$ on inputs of odd length, the probability that it makes a mistake on input x only depends on $||x| - n/2|$

For an input y of Hamming weight i, denote

$$m_i := \mathbb{P}[P(y) \neq \mathrm{Maj}(y)].$$

We conclude the proof assuming $\epsilon \geq 0$. This will cover the case $\epsilon < 0$ as well, since $\mathbb{P}[P(N^s_{1/2-\epsilon}) = 0] = \mathbb{P}[P(N^s_{1/2+\epsilon}) = 1]$.

Let $p_i := \mathbb{P}[|N^s_{1/2+\epsilon}| = i]$. We can write

$$\begin{aligned}
\mathbb{P}[P(N^s_{1/2+\epsilon}) = 1] &= \sum_{i>s/2} p_i \cdot (1 - m_i) + \sum_{i<s/2} p_i \cdot m_i \\
&= \sum_{i>s/2} (p_i \cdot (1 - m_i) + p_{s-i} \cdot m_{s-i}) \\
&= \sum_{i>s/2} (p_i - m_i(p_i - p_{s-i}))\,.
\end{aligned}$$

Where the last equality holds because by construction $m_i = m_{n-i}$ for every i.

Because $\epsilon \geq 0$ and $i > s/2$, the factor $(p_i - p_{s-i})$ is positive. Hence we bound the sum below if we replace m_i with its maximum value 0.01, obtaining

$$\sum_{i>s/2} (p_i - 0.01(p_i - p_{s-i})) = \mathbb{P}[\mathrm{Maj}(N^s_{1/2+\epsilon}) = 1](1 - 0.01) + 0.01 \cdot \mathbb{P}[\mathrm{Maj}(N^s_{1/2+\epsilon}) = 0].$$

Writing $\mathbb{P}[\mathrm{Maj}(N^s_{1/2+\epsilon}) = 0] = 1 - \mathbb{P}[\mathrm{Maj}(N^s_{1/2+\epsilon}) = 1]$ this becomes

$$\mathbb{P}[\mathrm{Maj}(N^s_{1/2+\epsilon}) = 1](1 - 2 \cdot 0.01) + 0.01.$$

By Lemma 10, $\mathbb{P}[\mathrm{Maj}(N^s_{1/2+\epsilon}) = 1] \geq 1/2 + \Omega(d\epsilon)$. Hence we conclude

$$\mathbb{P}[P(N^s_{1/2+\epsilon}) = 1] \geq (1/2 + \Omega(d\epsilon))(1 - 2 \cdot 0.01) + 0.01 = 1/2 + \Omega(d\epsilon).$$

□

At first sight, it may seem suspicious that we can tolerate constant error in the polynomials for majority. Some intuition why this might be OK follows. If $\mathbb{P}[P(N^s_{1/2+\epsilon}) = 1]$ is close to 1, constant error won't bother us, since we are only aiming for advantage close to 1/2. On the other hand, if that probability is close to 1/2, the loss will recouped thanks to the symmetrization. That is, mistakes will be made on $N^s_{1/2-\epsilon}$ with the same probability, boosting the correctness.

To prove that this result is tight, suppose there is a distribution on degree-d polynomials that solves the $(1/2+\epsilon)$-coin problem with advantage $1/2+\alpha$. If we sample $O(1/\alpha)^2$ times independently these polynomials, and compute the majority, a Chernoff bound shows that we obtain advantage 0.99. By Lemma 12 the majority computation can be done with error 1/100 by a probabilistic polynomial of degree $O(1/\alpha)$. Composing this with the degree-d polynomial we obtain a probabilistic polynomial of degree $O(d/\alpha)$ which solves the $(1/2+\epsilon)$-coin problem with advantage 0.98. By averaging we can fix the polynomial and still maintain advantage 0.96. Now we can appeal to a result proved in [LSS+19] which shows that any such polynomial has degree $\Omega(1/\epsilon)$. Hence, $d/\alpha \geq \Omega(1/\epsilon)$. In other words, $\alpha \leq O(d\epsilon)$, as desired.

5 Proof of Theorem 7

By Yao's argument mentioned in the introduction, it suffices to show that for every distribution Z on $\{0,1\}^n$ there exists a polynomial which computes Maj correctly with probability $1/2 + \Omega(d^2/n)$ over Z. By averaging, it suffices to give, for any Z, a distribution $P = P(Z)$ on polynomials that computes Maj correctly with the same probability over both the input drawn from Z and P. Our polynomials will depend only on the Hamming weight $|Z|$ of Z.

Case: $\mathbb{P}[||Z| - n/2| \geq d] \geq 0.01$**.** Let $M : \{0,1\}^{O(d^2)} \to \{0,1\}$ be the probabilistic polynomial of degree $O(d)$ from Lemma 14. Define $P(x)$ to compute M on an odd number $s := O(d^2)$ bits y selected uniformly at random from x. We first analyze the performance of this polynomial on any fixed input x of Hamming weight $w = n(1/2 + \epsilon)$. Note that y has the distribution $N^s_{1/2+\epsilon}$

We have

$$\mathbb{P}[P(x) = \text{Maj}(x)] = \mathbb{P}[M(N^s_{1/2+\epsilon}) = \text{Sign}(\epsilon)] \geq 1/2 + \Omega(d\epsilon),$$

By Lemma 14.

Now we use the assumption on Z. With probability $\Omega(1)$, we have $|\epsilon| \geq d/n$, in which case the probability is $\geq 1/2 + \Omega(d^2/n)$. In every other case, the probability is at least 1/2. Overall, $\mathbb{P}[P(Z) = \text{Maj}(Z)] \geq 1/2 + \Omega(d^2/n)$, concluding this case.

Case: $\mathbb{P}[||Z| - n/2| \leq d] \geq 0.99$**.** Let P be the polynomial of degree $O(d)$ from Lemma 11 that computes Maj on every input whose Hamming weight w has distance $\leq d$ from $n/2$. In this case, we have $\mathbb{P}[P(Z) = \text{Maj}(Z)] \geq \mathbb{P}[||Z| - n/2| \leq d] \geq 0.99$.

6 Proof of Theorem 9

As in the proof of Theorem 7, it suffices to show that for every distribution Z on $\{0,1\}^n$ there exists a distribution on polynomials which computes h_2 well over Z. Our polynomials will again depend only on the Hamming weight $|Z|$ of Z.

From the definition of g_2 we have that on inputs x with $n/2 + t$ zeroes and $n/2 - t$ ones we have

$$g_2(x) = 2t^2 - n/2.$$

As a function of t, this is a parabola which roots at $t = \pm\sqrt{n/4} = \pm n \cdot r$ where $r := 1/\sqrt{4n}$. Let $L := [-nr - d, -nr + d] \bigcap \mathbb{Z}$ and $R := [nr - d, nr + d] \bigcap \mathbb{Z}$ be the integers at distance $\leq d$ from either root.

Case: $\mathbb{P}[|Z| - n/2 \in L \bigcup R|] \geq 0.99$**.** In this case we use polynomials of degree $O(d)$ from Lemma 11 to compute h_2 correctly on $L \bigcup R$. This definition is possible if the elements in L and R are not congruent modulo $2^{\ell+100}$. That is, we require that for every x, y of absolute value at most d the values $-nr + x$ and $nr + y$ are not congruent modulo $2^{\ell+100}$. For this it suffices that the remainder of $2nr = \sqrt{n}$ divided by $2^{\ell+100}$ is not in $[0, 2d] \cup [2^{\ell+100} - 2d, 2^{\ell+100}]$, given by assumption.

Case: $\mathbb{P}[|Z| - n/2 \in L \bigcup R|] < 0.01$. Consider the following process. With probability $1/(1+4r^2)$ pick two uniform elements from the input and output their XOR; otherwise output zero. On any input with weight $1/2+\alpha$ the probability the process outputs 1 is

$$1/2+\epsilon := \frac{1/2+2\alpha^2}{1+4r^2} = \frac{1/2+2(r+\alpha-r)^2}{1+4r^2} = 1/2+\frac{2\left((\alpha-r)^2+2r(\alpha-r)\right)}{1+4r^2} = 1/2+\frac{2\left(\alpha^2-r^2\right)}{1+4r^2}.$$

Note $\epsilon = 0$ exactly when $\alpha = \pm r$, and $\epsilon < 0$ exactly when α is between these two roots.

Now repeat the process s times to generate $N^s_{1/2+\epsilon}$, and run the polynomial from Lemma 14 on them.

On any input, we compute correctly with probability $\geq 1/2$.

Assume now the input weight is not in $L \bigcup R$. Let $c := 2/(1+4r^2)$.

If $|\alpha| \geq r + d/n$ then $\epsilon \geq c(d^2/n^2 + 2rd/n) = \Omega(rd/n)$.

If $|\alpha| \leq r - d/n$ then $\epsilon \leq c(d^2/n^2 - 2rd/n) = -\Omega(rd/n)$.

In either case, by Lemma 14 we compute h_2 correctly with probability $1/2 + d \cdot \Omega(rd/n) = 1/2 + \Omega(d^2/n^{3/2})$.

7 Proof of Theorem 2

We essentially define f to have correlation zero with h_2 on every Hamming weight, except for s Hamming weights where the value of g_2 is as small as possible. Let $M := \{n/2 + \sqrt{n}/2, n/2+\sqrt{n}/2-1, \ldots, n/2+\sqrt{n}/2-s+1\}$ and let Z_i be the inputs with i zeroes. For $x \in Z_i$ and $i \in M$ let $f(x) = h_2(x) = -1$. For $x \in Z_0$ let, say, $f(x) = 1$ and for $x \in Z_n$ let $f(x) = -1$. For any other Z_i, divide the inputs in Z_i in two equals parts, which is possible by Lucas' theorem because n is a power of 2. Let f be 1 on one part and -1 on the other.

Consider $\mathbb{E}_x[f(x)h_2(x)]$. We have $\mathbb{E}_x[f(x)h_2(x)|x \in Z_0 \cup Z_n] = 0$, and $\mathbb{E}_x[f(x)h_2(x)|x \in Z_i] = 0$ if $i \notin M$ and $i \neq 0$ and $i \neq n$, by definition. Otherwise the expectation is 1. Hence $\mathbb{E}_x[f(x)h(x)]$ is the probability that $x \in Z_i$ for some $i \in M$. Assuming $s \leq \sqrt{n}/2$ this probability is $\geq \Omega(s) \cdot \mathbb{P}[x \in Z_{n/2+\sqrt{n}/2}]$. The latter probability is $\Omega(1/\sqrt{n})$ using the standard bound $\binom{n}{n/2+\sqrt{n}/2} = \Theta(2^n/\sqrt{n})$ which can be verified using Stirling's approximation. Hence $\mathbb{E}_x[f(x)h_2(x)] \geq \Omega(s/\sqrt{n})$, and so $\mathbb{P}[f(x) = h_2(x)] \geq 1/2 + \Omega(s/\sqrt{n})$.

Now consider $\mathbb{E}_x[f(x)g_2(x)]$. Again, this is zero unless the number of zeroes of x lies in M. Note that $g_2(x) = 2t^2 - n/2$ on inputs in $Z_{n/2+t}$. The maximum value of $|g_2(x)|$ for inputs with weights in M is for $t = \sqrt{n}/2 - s + 1$ which yields value $|2(\sqrt{n}/2 - s+1)^2 - n/2| = |2(-s+1)^2 + (-s+1)\sqrt{n}| \leq O(s^2 + s\sqrt{n})$. For $s \leq \sqrt{n}/2$ the latter is $O(s\sqrt{n})$. The chance that the number of zeroes of x lies in M is $\Theta(s/\sqrt{n})$ as noted before. Hence we get $M_2(f) \leq O(s\sqrt{n} \cdot s/\sqrt{n}) \leq O(s^2)$.

Acknowledgment. I am grateful to Chin Ho Lee for pointing out the work [CGL+20] to me, and to an anonymous reviewer for suggesting the use of hypercontractivity to bound $\mathbb{E}|g_k(x)|$ in the proof of Theorem 1 (alternatively one can reason along the lines of the proof of Theorem 4).

A preliminary version of this paper had Theorem 7 only for $d \geq \Omega(n^{1/3})$, and the degree bound was $O(d\sqrt{\log n})$. Jarosław Błasiok pointed out to us how to improve the proof to obtain Theorem 7. The proof in the preliminary version was similar, but rather than

performing a case analysis, detected the two cases explicitly with an auxiliary polynomial, which led to $d \geq \Omega(n^{1/3})$. It also used the polynomials for Maj with polynomially-small error, as opposed to constant, which led to the extra $\sqrt{\log n}$ factor. Following these ideas, we also improved the results on the coin problem and h_2. We are very grateful to Jarosław Błasiok for letting us include the improved results!

References

[AW15] Josh Alman and Ryan Williams. Probabilistic polynomials and hamming nearest neighbors. In *IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 136–150, 2015.

[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.

[BV10a] Andrej Bogdanov and Emanuele Viola. Pseudorandom bits for polynomials. *SIAM J. on Computing*, 39(6):2464–2486, 2010.

[BV10b] Joshua Brody and Elad Verbin. The coin problem, and pseudorandomness for branching programs. In *51th IEEE Symp. on Foundations of Computer Science (FOCS)*, 2010.

[CGL+20] Eshan Chattopadhyay, Jason Gaitonde, Chin Ho Lee, Shachar Lovett, and Abhishek Shetty. Fractional pseudorandom generators from any fourier level. *CoRR*, abs/2008.01316, 2020.

[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.

[CHHL18] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett. Pseudorandom generators from polarizing random walks. In *CCC*, volume 102 of *LIPIcs*, pages 1:1–1:21. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018.

[CHLT19] Eshan Chattopadhyay, Pooya Hatami, Shachar Lovett, and Avishay Tal. Pseudorandom generators from the second fourier level and applications to AC0 with parity gates. In *ACM Innovations in Theoretical Computer Science conf. (ITCS)*, pages 22:1–22:15, 2019.

[CT06] Thomas Cover and Joy Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[FSUV13] Bill Fefferman, Ronen Shaltiel, Christopher Umans, and Emanuele Viola. On beating the hybrid argument. *Theory of Computing*, 9:809–843, 2013.

[GII+19] Alexander Golovnev, Rahul Ilango, Russell Impagliazzo, Valentine Kabanets, Antonina Kolokolova, and Avishay Tal. $\mathrm{AC}^0[p]$ lower bounds against MCSP via the coin problem. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece*, volume

132 of *LIPIcs*, pages 66:1–66:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[GKP94] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik. *Concrete Mathematics: A Foundation for Computer Science, 2nd Ed.* Addison-Wesley, 1994.

[Lov09] Shachar Lovett. Unconditional pseudorandom generators for low degree polynomials. *Theory of Computing*, 5(1):69–82, 2009.

[LSS+19] Nutan Limaye, Karteek Sreenivasaiah, Srikanth Srinivasan, Utkarsh Tripathi, and S. Venkitesh. A fixed-depth size-hierarchy theorem for $\mathrm{AC}^0[\oplus]$ via the coin problem. In *ACM Symp. on the Theory of Computing (STOC)*, pages 442–453. ACM, 2019.

[Nis91] Noam Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica. An Journal on Combinatorics and the Theory of Computing*, 11(1):63–70, 1991.

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions.* Cambridge University Press, 2014.

[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.

[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.

[Sri13] Srikanth Srinivasan. On improved degree lower bounds for polynomial approximation. In *FSTTCS*, volume 24 of *LIPIcs*, pages 201–212. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2013.

[Sri20] Srikanth Srinivasan. A robust version of hegedus's lemma, with applications. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proccedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 1349–1362. ACM, 2020.

[STV19] Srikanth Srinivasan, Utkarsh Tripathi, and S. Venkitesh. On the probabilistic degrees of symmetric boolean functions, 2019.

[SV10] Ronen Shaltiel and Emanuele Viola. Hardness amplification proofs require majority. *SIAM J. on Computing*, 39(7):3122–3154, 2010.

[TMB+17] Charalampos E. Tsourakakis, Michael Mitzenmacher, Jaroslaw Blasiok, Ben Lawson, Preetum Nakkiran, and Vasileios Nakos. Predicting positive and negative links with noisy queries: Theory & practice. *CoRR*, abs/1709.07308, 2017.

[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. The complexity of hardness amplification and derandomization. *Ph.D. thesis, Harvard University*, 2006.

[Vio09a] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

[Vio09b] Emanuele Viola. The sum of d small-bias generators fools polynomials of degree d. *Computational Complexity*, 18(2):209–217, 2009.

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

[Vio19] Emanuele Viola. Matching Smolensky's correlation bound with majority. Available at http://www.ccs.neu.edu/home/viola/, 2019.

[Yao77] Andrew Chi-Chih Yao. Probabilistic computations: Toward a unified measure of complexity (extended abstract). In *IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 222–227. IEEE Computer Society, 1977.