Lecture Notes November 1, 2026

Exponential Correlation Bounds for Polynomials

Lecturer: Hamed Hatami

Lecture overview

Proving correlation bounds for explicit functions against low-degree polynomials is a central problem in theoretical computer science. For decades, Smolensky's $O(d/\sqrt{n})$ bound for majority remained the best known bound for polynomials of degree $d \geq \log n$.

In these notes, we present a recent result of [CHL+26] that improves this to an exponentially small bound: Taking the XOR of majorities on blocks of $\Theta(d^2)$ bits gives correlation $e^{-\Omega(n/d^2)}$ with every polynomial of degree at most d over any field. The proof is an extension of Smolensky's dimension argument. For simplicity, we present it only over $\mathbb{F}_2$.

Outline.

- Section 2: Smolensky's dimension argument and the $O(d/\sqrt{n})$ bound for majority.
- Section 3: the exponential bound for XOR of majorities.

1 Introduction

The *correlation* between a boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and a polynomial $P \in \mathbb{F}_2[x_1, \ldots, x_n]$ is

$$\operatorname{corr}(f, P) := \left|\mathbb{E}_x (-1)^{f(x)+P(x)}\right| = \left|2 \Pr_x[f(x) = P(x)] - 1\right|.$$

Hence, a correlation at most ε means that P agrees with f on at most a $\frac{1}{2} + \frac{\varepsilon}{2}$ fraction of the inputs.

A random Boolean function, with high probability, has exponentially small correlation with every low-degree polynomial. Indeed, for a fixed P, if f is random, then the values $(-1)^{f(x)+P(x)}$ are 2^n independent uniform random signs. Since $\operatorname{corr}(f, P)$ is the absolute value of their average, by the Chernoff bound

$$\Pr_f\left[\operatorname{corr}(f, P) \geq 2^{-n/3}\right] \leq e^{-\Omega(2^{n/3})}.$$

On the other hand, there are only $2^{\binom{n}{\leq d}}$ polynomials of degree at most d. When $d = o(n)$, this is $2^{2^{o(n)}}$, so by the union bound, the probability that any one of them has correlation larger than $2^{-n/3}$ with f is $2^{-\Omega(2^{n/3})}$.

Constructing *explicit* functions with small correlation with low-degree polynomials, however, has been a major challenge in complexity theory. Such functions are highly sought after for several reasons.

First, low-degree polynomials are easy to compute in many natural computational models, such as small circuits, branching programs, and multiparty communication protocols. Thus, proving that a function is hard to approximate by low-degree polynomials is a prerequisite for showing that it is hard to approximate in these models.

Second, the Razborov–Smolensky method [Raz87, Smo87] shows that small constant-depth circuits can be approximated by polynomials of polylogarithmic degree. Hence, a function with small correlation with all such polynomials cannot be computed by these circuits. Strong enough correlation bounds also yield pseudorandom generators that fool low-degree polynomials, via the Nisan–Wigderson paradigm [NW94]. They are also closely tied to matrix rigidity and to number-on-forehead communication complexity; see Viola's survey [Vio09].

The classical bound. Smolensky's $O(d/\sqrt{n})$ correlation bound for majority [Smo87, Smo93] (see Theorem 2.3 below) remained the benchmark for decades. It is nontrivial for degrees up to about $\sqrt{n}$, but it never gives correlation smaller than $1/\sqrt{n}$. In fact, already for degree $d = \log_2 n$, no explicit function was known to have correlation less than $1/\sqrt{n}$ [Vio09].

The new bound. The recent theorem of [CHL+26] breaks this barrier. Taking the XOR of majorities on blocks of $\Theta(d^2)$ bits gives correlation $e^{-\Omega(n/d^2)}$ with every polynomial of degree at most d. For example, for $d = \log_2 n$ this is $e^{-\Omega(n/\log^2 n)}$, compared with the previous $1/\sqrt{n}$.

Comparison with repeated Cauchy–Schwarz. The other classical approach, going back to Babai, Nisan, and Szegedy [BNS92], uses repeated applications of the Cauchy–Schwarz inequality. In modern language, it bounds $\operatorname{corr}(f, P)$ by the Gowers uniformity norm $\|(-1)^f\|_{U^{d+1}}$ for every polynomial P of degree at most d. However, the U^{d+1} norm is a 2^{d+1}-th root of an average, and for ± 1-valued functions this average is always at least 2^{-n}. Hence $\|(-1)^f\|_{U^{d+1}} \geq 2^{-n/2^{d+1}}$, which makes these bounds useless once $d \geq \log_2 n$.

Notation. For $x \in \mathbb{F}_2^n$, write $|x| := |\{i : x_i = 1\}|$. For $S \subseteq [n]$, write $x^S := \prod_{i \in S} x_i$, with $x^\varnothing \equiv 1$. We treat these monomials as functions and write $x^S(y) = \prod_{i \in S} y_i$ for $y \in \mathbb{F}_2^n$.

For $\mathcal{A} \subseteq \mathbb{F}_2^n$, we write $\mathbb{F}_2^{\mathcal{A}}$ for the $|\mathcal{A}|$-dimensional $\mathbb{F}_2$-vector space of functions $\mathcal{A} \to \mathbb{F}_2$. Functions on $\mathbb{F}_2^n$ are regarded as elements of $\mathbb{F}_2^{\mathcal{A}}$ by restriction. For example, we say that a set of polynomials spans $\mathbb{F}_2^{\mathcal{A}}$ if their restrictions to $\mathcal{A}$ do.

2 Smolensky's classical bound

We identify each $y \in \mathbb{F}_2^n$ with its support $\{i : y_i = 1\}$, so $x^S(y) = 1 \Leftrightarrow S \subseteq y$.

> **Lemma 2.1.** *For every $\mathcal{A} \subseteq \mathbb{F}_2^n$, the monomials $\{x^S : S \in \mathcal{A}\}$ form a basis for $\mathbb{F}_2^{\mathcal{A}}$.*

Proof. There are $|\mathcal{A}|$ monomials and the space has dimension $|\mathcal{A}|$, so it suffices to prove linear independence. List the elements of $\mathcal{A}$ as $S_1, \ldots, S_r$ in non-increasing order of size. It suffices to show that, for each j, the monomial x^{S_j} is not in the span of $x^{S_1}, \ldots, x^{S_{j-1}}$. Indeed, $x^{S_j}(S_j) = 1$, while $x^{S_i}(S_j) = 0$ for every $i < j$, since $S_i \not\subseteq S_j$. □

Put $m := \lfloor n/2 \rfloor$, and define $\mathrm{Maj}\colon \mathbb{F}_2^n \to \mathbb{F}_2$ by

$$\mathrm{Maj}(x) := \begin{cases} 0 & \text{if } |x| \leq m, \\ 1 & \text{if } |x| > m. \end{cases}$$

The following proposition shows that if we are allowed to multiply monomials by Maj, then every function has an expansion using only monomials of degree at most m.

Proposition 2.2. *Every $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ can be written as*

$$f = p + q\,\mathrm{Maj}, \qquad \deg(p), \deg(q) \le m.$$

Proof. Let $\mathcal{M}_0 := \mathrm{Maj}^{-1}(0)$ and $\mathcal{M}_1 := \mathrm{Maj}^{-1}(1)$. By Lemma 2.1, every $g\colon \mathcal{M}_0 \to \mathbb{F}_2$ agrees on $\mathcal{M}_0$ with a polynomial of degree at most m, since every element of $\mathcal{M}_0$ has weight at most m.

The same holds for $\mathcal{M}_1$. Indeed, flipping all the bits maps $\mathcal{M}_1$ into $\mathcal{M}_0$, that is, $\mathcal{M}_1 + \mathbf{1} \subseteq \mathcal{M}_0$. So for $g\colon \mathcal{M}_1 \to \mathbb{F}_2$ there is r of degree at most m with $r(y) = g(y+\mathbf{1})$ on $\mathcal{M}_1 + \mathbf{1}$, and then $r(x+\mathbf{1})$ has degree at most m and agrees with g on $\mathcal{M}_1$.

Now choose p of degree at most m agreeing with f on $\mathcal{M}_0$, and q of degree at most m agreeing with $f - p$ on $\mathcal{M}_1$. Then $p + q\,\mathrm{Maj}$ equals $p = f$ on $\mathcal{M}_0$, and $p + (f-p) = f$ on $\mathcal{M}_1$. □

Theorem 2.3 (Smolensky [Smo87, Smo93])**.** *For every integer $d \ge 1$, every polynomial $P \in \mathbb{F}_2[x_1, \dots, x_n]$ of degree at most d satisfies*

$$\Pr_{x \in \mathbb{F}_2^n}[\mathrm{Maj}(x) = P(x)] \le \frac{1}{2} + \frac{2d}{\sqrt{n}}.$$

Proof. If $d > m$, the claimed bound is trivial, so assume $d \le m$. Let

$$\mathcal{T} := \{x \in \mathbb{F}_2^n : P(x) = \mathrm{Maj}(x)\}.$$

By Proposition 2.2, every $f : \mathcal{T} \to \mathbb{F}_2$ can be expressed as $p + q\,\mathrm{Maj}$, with $\deg(p), \deg(q) \le m$. Since $P = \mathrm{Maj}$ on $\mathcal{T}$,

$$f(x) = p(x) + P(x)q(x) \qquad (x \in \mathcal{T}).$$

Thus every function on $\mathcal{T}$ lies in the span of monomials of degree at most $m + d$. Counting these monomials, and using the estimate $\binom{n}{m} \le 2^n/\sqrt{n}$, we obtain

$$|\mathcal{T}| \le \sum_{j=0}^{m+d} \binom{n}{j} \le 2^{n-1} + (d+1)\binom{n}{m} \le 2^n \left(\frac{1}{2} + \frac{2d}{\sqrt{n}}\right).$$ □

3 Exponential correlation for XOR of majorities

For $X = (X_1, \dots, X_k) \in (\mathbb{F}_2^\ell)^k$, define

$$\mathrm{Maj}_\ell^{\oplus k}(X) := \mathrm{Maj}(X_1) + \cdots + \mathrm{Maj}(X_k),$$

where each majority is taken on ℓ bits and the sum is in $\mathbb{F}_2$. The main theorem of this lecture is the following.

Theorem 3.1 (Exponential correlation [CHL+26])**.** *For integers $\ell, k, d \ge 1$, every polynomial P of degree at most d satisfies*

$$\Pr_{X \in (\mathbb{F}_2^\ell)^k}\left[\mathrm{Maj}_\ell^{\oplus k}(X) = P(X)\right] \le \frac{1}{2} + \left(\frac{4d}{\sqrt{\ell}}\right)^k.$$

For simplicity, we only prove the theorem for odd ℓ. Throughout this section, write $\ell = 2m+1$ and $n = \ell k$, and split the coordinates into k blocks of size ℓ. For $S \subseteq [n]$, let S_i be its intersection with block i. For $x = (X_1, \dots, X_k) \in (\mathbb{F}_2^\ell)^k$, write

$$\mathrm{Maj}_i(x) \coloneqq \mathrm{Maj}(X_i), \qquad \mathrm{Maj}^I \coloneqq \prod_{i \in I} \mathrm{Maj}_i \quad (I \subseteq [k]).$$

First, we prove a block version of Proposition 2.2; for $k = 1$, it is exactly Proposition 2.2.

Proposition 3.2. *Every $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is in the linear span of*

$$\mathcal{B} \coloneqq \left\{ x^S \,\mathrm{Maj}^I : S \subseteq [n],\ |S_i| \le m \text{ for every } i,\ I \subseteq [k] \right\}.$$

Proof. Since monomials span all functions, it suffices to show that every monomial lies in the span of $\mathcal{B}$. Every monomial factors as $x^U = \prod_{i=1}^k x^{U_i}$. Applying Proposition 2.2 in each block gives

$$x^{U_i} = p_i + q_i \,\mathrm{Maj}_i, \qquad \deg(p_i), \deg(q_i) \le m,$$

where p_i, q_i depend only on block i. Multiplying and expanding expresses x^U as a linear combination of elements of $\mathcal{B}$. □

Fix a polynomial P of degree at most d, and let

$$\mathcal{T} \coloneqq \{x \in \mathbb{F}_2^n : P(x) = \mathrm{Maj}_\ell^{\oplus k}(x)\}.$$

Given $S \subseteq [n]$, let

$$L(S) \coloneqq \{i \in [k] : |S_i| \le m - 2d\} \quad \text{and} \quad j(S) \coloneqq \min L(S),$$

with $j(S) = \infty$ if $L(S) = \varnothing$. We call the blocks in $L(S)$ the *low* blocks of S, and the other blocks *high*.

Proof idea of Theorem 3.1

We bound $|\mathcal{T}|$ by showing that $\mathbb{F}_2^{\mathcal{T}}$ is spanned by a small set $\mathcal{B}^* \subseteq \mathcal{B}$ defined as

$$\mathcal{B}^* \coloneqq \{x^S \,\mathrm{Maj}^I \in \mathcal{B} : j(S) \notin I\}.$$

To show that every $f \in \mathbb{F}_2^{\mathcal{T}}$ is a linear combination of elements of $\mathcal{B}^*$, we start with an expansion of f as a linear combination of elements of $\mathcal{B}$, guaranteed by Proposition 3.2. Whenever we face a term $x^S \,\mathrm{Maj}^I \in \mathcal{B} \setminus \mathcal{B}^*$, we have $j \coloneqq j(S) \in I$, and we replace Maj_j using

$$\mathrm{Maj}_j = P + \sum_{i \ne j} \mathrm{Maj}_i \qquad \text{on } \mathcal{T}, \tag{1}$$

which holds by the definition of $\mathcal{T}$. We then expand. Some of the new terms may have blocks of degree larger than m, and we rewrite each such block using Proposition 2.2, so that all the resulting terms are in $\mathcal{B}$. We will show that every newly created term $x^{S'} \,\mathrm{Maj}^{I'}$ is either in $\mathcal{B}^*$ or satisfies $w(S') < w(S)$, where the *potential* w is defined as

$$w(S) \coloneqq 2|S| + (2d+1)|L(S)|, \tag{2}$$

that is, twice the degree of the monomial x^S plus a bonus of $2d+1$ for each low block.

Lemma 3.3. *The set $\mathcal{B}^*$ spans $\mathbb{F}_2^{\mathcal{T}}$.*

Proof. Throughout the proof all identities are on $\mathcal{T}$. By Proposition 3.2, it suffices to show that every $x^S \operatorname{Maj}^I \in \mathcal{B}$ lies in the span of $\mathcal{B}^*$. We prove this by induction on the potential $w(S)$ defined in (2).

If $j(S) \notin I$, the term already belongs to $\mathcal{B}^*$. Otherwise, put $j = j(S) \in I$, and write the multilinear expansion of P as

$$P = \sum_{U \in \mathcal{P}} x^U, \qquad |U| \le d.$$

Substituting Maj_j with the right hand side of (1) in $x^S \operatorname{Maj}^I$ gives

$$x^S \operatorname{Maj}^I = \sum_{U \in \mathcal{P}} x^{S \cup U} \operatorname{Maj}^{I \setminus \{j\}} + \sum_{i \neq j} x^S \operatorname{Maj}^{(I \setminus \{j\}) \cup \{i\}}.$$

Every term in the second sum belongs to $\mathcal{B}^*$, since S is unchanged, so $j(S) = j$, and $j \notin (I \setminus \{j\}) \cup \{i\}$.

Next, fix $U \in \mathcal{P}$ and consider the corresponding term $x^{S \cup U} \operatorname{Maj}^{I \setminus \{j\}}$ in the first sum. This term need not belong to $\mathcal{B}$, since some blocks may have $|S_i \cup U_i| > m$. In each such block, apply Proposition 2.2 to rewrite the block as

$$x^{S_i \cup U_i} = p_i + q_i \operatorname{Maj}_i, \qquad \deg(p_i), \deg(q_i) \le m.$$

Expanding and using $\operatorname{Maj}_i^2 = \operatorname{Maj}_i$ gives a linear combination of terms $x^{S'} \operatorname{Maj}^{I'} \in \mathcal{B}$. Each resulting term satisfies the following two properties.

(a) $\boldsymbol{j \notin I'}$**:** Since block j is low for S,

$$|S_j \cup U_j| \le |S_j| + d \le m - d \le m.$$

So block j is not rewritten, and Maj_j remains absent.

(b) **If $\boldsymbol{j(S') \in I'}$, then $\boldsymbol{w(S') < w(S)}$:** Suppose $j(S') \in I'$. By (a), $j(S') \neq j$. So either block j has changed from low to high, or some block $i < j$ has changed from high to low. In either case, at least one block has changed its status.

We compare $w(S')$ with $w(S)$ in two steps. Passing from S to $S \cup U$ increases the degree contribution $2|S|$ by at most $2d$. Passing from $S \cup U$ to S' only rewrites blocks, and rewriting never increases the degree of a block. So blocks whose status is unchanged incur no further increase. For the blocks that change status:

- A low-to-high change removes a bonus of $2d + 1$.
- A high-to-low change can only happen in a rewritten block, since blocks that are not rewritten only grow. Such a block goes from degree at least $m + 1$ to degree at most $m - 2d$, so its degree contribution drops by at least $2(2d + 1)$, while its bonus increases by only $2d + 1$.

Since at least one block changes status, the potential decreases:

$$w(S') \le w(S) + 2d - (2d + 1) < w(S).$$

Consequently, each resulting term either belongs to $\mathcal{B}^*$ or is covered by the induction hypothesis. □

Proof of Theorem 3.1. By Lemma 3.3, $|\mathcal{T}| \leq |\mathcal{B}^*|$, so it suffices to count the elements of $\mathcal{B}^*$.

Since $\ell = 2m+1$, the number of choices for each S_i is $\binom{\ell}{\leq m} = 2^{\ell-1}$, so there are $(2^{\ell-1})^k = 2^{n-k}$ choices of S. For each S, we retain half of the 2^k choices of I, except when every block is high, in which case we retain all of them.

A high block satisfies $m - 2d < |S_i| \leq m$. This leaves at most $2d$ possible sizes, each giving at most $\binom{\ell}{m}$ choices of S_i. So each block has at most $2d\binom{\ell}{m}$ high choices of S_i. We obtain the desired bound:

$$|\mathcal{T}| \leq 2^{n-1} + 2^{k-1}\left(2d\binom{\ell}{m}\right)^k \leq 2^n\left(\frac{1}{2} + \frac{1}{2}\left(\frac{4d}{\sqrt{\ell}}\right)^k\right). \qquad \square$$

References

[BNS92] László Babai, Noam Nisan, and Mário Szegedy, *Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs*, Journal of Computer and System Sciences **45** (1992), no. 2, 204–232.

[CHL+26] Eshan Chattopadhyay, Pooya Hatami, Chin Ho Lee, Shachar Lovett, Avishay Tal, and Emanuele Viola, *Exponential correlation bounds for polynomials*, 2026, arXiv:2609.28839.

[NW94] Noam Nisan and Avi Wigderson, *Hardness vs randomness*, Journal of Computer and System Sciences **49** (1994), no. 2, 149–167.

[Raz87] Alexander A. Razborov, *Lower bounds on the size of bounded depth circuits over a complete basis with logical addition*, Mathematical Notes of the Academy of Sciences of the USSR **41** (1987), no. 4, 333–338.

[Smo87] Roman Smolensky, *Algebraic methods in the theory of lower bounds for Boolean circuit complexity*, Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, pp. 77–82.

[Smo93] Roman Smolensky, *On representations by low-degree polynomials*, Proceedings of the 34th Annual Symposium on Foundations of Computer Science (FOCS), 1993, pp. 130–138.

[Vio09] Emanuele Viola, *Correlation bounds for polynomials over* $\{0,1\}$, SIGACT News **40** (2009), no. 1, 27–44.