

Exponential Correlation Bounds for Polynomials: A Lecture

Hamed Hatami

October 29, 2026

Abstract

Proving correlation bounds for explicit functions against low-degree polynomials is a fundamental challenge in theoretical computer science. For decades, Smolensky's $O(d/\sqrt{n})$ bound for majority remained the best known 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 $\mathbb{F}_2$.

1 Introduction

Define the *correlation* between a boolean function $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ and a polynomial $P \in \mathbb{F}_2[x_1, \dots, x_n]$ by

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

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

A random Boolean function has exponentially small correlation with every low-degree polynomial with high probability. Indeed, for a fixed P , if f is random, then the values $(-1)^{f(x)+P(x)}$, for $x \in \mathbb{F}_2^n$, are i.i.d. random variables, each equal to ± 1 with probability $\frac{1}{2}$. Since $\text{corr}(f, P)$ is the absolute value of their average, by the Chernoff bound

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

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

Constructing explicit examples, however, has been a major challenge in complexity theory. Low-degree polynomials are easy to compute in many natural computational models, such as small circuits, branching programs, and multiparty communication protocols. Thus, before we can prove that a function is hard to approximate in these models, we must first show that it is hard to approximate by low-degree polynomials.

Furthermore, the Razborov–Smolensky method shows that small constant-depth circuits can be approximated by low-degree polynomials [Raz87, Smo87], so a function with small correlation with all low-degree polynomials cannot be computed by such circuits. Strong enough correlation bounds also yield pseudo-random 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 a 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 the Gowers uniformity norm: for every polynomial P of degree at most d , it bounds $\text{corr}(f, P)$ by $\|(-1)^f\|_{U^{d+1}}$.

For example, the generalized inner product $\sum_{j=1}^t \prod_{i=1}^{d+1} x_{i,j}$ on $n = (d+1)t$ variables has correlation $e^{-\Omega(n/d^{d+1})}$ with every polynomial of degree at most d [BNS92], and the best known bound of this kind is $e^{-\Omega(n/2^d)}$ [Vio06]. The loss comes from the fact that the U^{d+1} norm is a 2^{d+1} -th root of an average, which makes these bounds useless once $d \geq \log_2 n$.

Convention. 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 $x^\emptyset \equiv 1$. We treat these monomials as functions as 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 $\mathcal{A} \rightarrow \mathbb{F}_2$. 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 $S_1, \dots, S_r$ in nonincreasing order of size. We show that, for each j , the monomial x^{S_j} is not in the span of $x^{S_1}, \dots, x^{S_{j-1}}$. Indeed, $x^{S_j}(S_j) = 1$, while $x^{S_i}(S_j) = 0$ for every $i < j$, since $S_i \not\subseteq S_j$. $\square$

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

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

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 $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ can be written as*

$$f = p + q \text{Maj}, \quad \deg(p), \deg(q) \leq m.$$

Proof. Let $\mathcal{M}_0 := \text{Maj}^{-1}(0)$ and $\mathcal{M}_1 := \text{Maj}^{-1}(1)$. By Lemma 2.1, every $g: \mathcal{M}_0 \rightarrow \mathbb{F}_2$ 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 $g: \mathcal{M}_1 \rightarrow \mathbb{F}_2$ 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 $p + q \text{Maj}$ equals $p = f$ on $\mathcal{M}_0$, and $p + (f - p) = f$ on $\mathcal{M}_1$. $\square$

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

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

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

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

By [Proposition 2.2](#), every $f : \mathcal{T} \rightarrow \mathbb{F}_2$ can be expressed as $p + q \text{Maj}$, with $\deg(p), \deg(q) \leq m$. Since $P = \text{Maj}$ on $\mathcal{T}$,

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

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 $\binom{n}{m} \leq 2^n / \sqrt{n}$, we obtain

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

3 Exponential correlation for XOR of majorities

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

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

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 $\ell, k, d \geq 1$, every polynomial P of degree at most d satisfies*

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

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

$$\text{Maj}_i(x) := \text{Maj}(X_i), \quad \text{Maj}^I := \prod_{i \in I} \text{Maj}_i \quad (I \subseteq [k]).$$

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

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

$$\mathcal{B} := \{x^S \text{Maj}^I : S \subseteq [n], |S_i| \leq m \text{ for every } i, I \subseteq [k]\}.$$

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

$$x^{U_i} = p_i + q_i \text{Maj}_i, \quad \deg(p_i), \deg(q_i) \leq m,$$

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

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

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

Given $S \subseteq [n]$, let

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

with $j(S) = \infty$ if $L(S) = \emptyset$. 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

$$\mathcal{B}^* := \{x^S \text{Maj}^I \in \mathcal{B} : j(S) \notin I\}.$$

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 $x^S \text{Maj}^I \in \mathcal{B} \setminus \mathcal{B}^*$, we have $j := j(S) \in I$, and we replace Maj_j using

$$\text{Maj}_j = P + \sum_{i \neq j} \text{Maj}_i \quad \text{on } \mathcal{T}, \quad (1)$$

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 $x^{S'} \text{Maj}^{I'}$ is either in $\mathcal{B}^*$ or satisfies $w(S') < w(S)$, where the *potential* w is defined as

$$w(S) := 2|S| + (2d+1)|L(S)|, \quad (2)$$

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 $x^S \text{Maj}^I \in \mathcal{B}$ 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

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

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

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

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 $x^{S \cup U} \text{Maj}^{I \setminus \{j\}}$ 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

$$x^{S_i \cup U_i} = p_i + q_i \text{Maj}_i, \quad \deg(p_i), \deg(q_i) \leq m.$$

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

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

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

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

(b) **If $j(S') \in I'$, then $w(S') < w(S)$:** 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:

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

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

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:

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

References

- [BNS92] László Babai, Noam Nisan, and Mária 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.
- [Vio06] Emanuele Viola, *New correlation bounds for GF(2) polynomials using Gowers uniformity*, Tech. Report TR06-097, Electronic Colloquium on Computational Complexity, 2006.
- [Vio09] ———, *Correlation bounds for polynomials over $\{0, 1\}$* , SIGACT News **40** (2009), no. 1, 27–44.