Electronic Colloquium on Computational Complexity, Report No. 175 (2019)

Matching Smolensky's correlation bound with majority

Emanuele Viola[*]

December 4, 2019

Abstract

We show that there are degree-d polynomials over $\mathbb{F}_2$ with correlation $\Omega(d/\sqrt{n})$ with the majority function on n bits. This matches the $O(d/\sqrt{n})$ bound by Smolensky.

The "correlation" between two boolean functions $f, g : \{0,1\}^n \to \{0,1\}$, when one function is balanced, can be defined as

$$2^{-n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}(-1)^{g(x)}.$$

The study of correlation between explicit functions and low-degree polynomials $p(x_0, x_1, \dots, x_{n-1})$ over $\mathbb{F}_2 = \{0,1\}$ is the subject of intense study also because it is linked to many long-standing questions in complexity theory. For a survey see [Vio09].

Building on Razborov [Raz87], Smolensky proved [Smo87, Smo93] that the correlation between majority and degree-d polynomials is at most $O(d/\sqrt{n})$. In this paper $O(.)$ and $\Omega(.)$ denote absolute constants. Here we define the majority function Maj on n bits to output 0 if the input Hamming weight is $\geq n/2$ (note $(-1)^0 = 1$ and $(-1)^1 = -1$).

Smolensky's bound was known to be tight up to constant factors for $d = \Omega(\sqrt{n})$, see [Vio09]. It can also be verified to be tight for $d = O(1)$ by considering the polynomial $1 - x_0$. But apparently it was not known to be tight for other values of d. Here we prove a matching construction for any d, also recovering both previous constructions.

Theorem 1. *There are degree-d polynomials over $\mathbb{F}_2$ with correlation $\Omega(d/\sqrt{n})$ with the majority function, for any n, d.*

The rest of this paper is devoted to the proof of this theorem. The main proof is for odd n. If n is even we can use the polynomial $p'(x_0, x_1, \dots, x_{n-1}) := p(x_0, x_1, \dots, x_{n-2})(1 - x_{n-1})$ where p is the polynomial with the highest correlation γ with majority on input length $n-1$. The correlation of p' 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 $f_w : \{0,1,\dots,n\} \to \{0,1\}$ for $f(x) = f_w(|x|)$

[*]Supported by NSF CCF award 1813930.

ISSN 1433-8092

where $|x|$ is the Hamming weight of x. The correlation between a symmetric polynomial p and Majority 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 for $\ell = \log_2(2d)$ the following result which is Theorem 2.4 in [BGL06] and follows from Lucas' theorem.

Claim 2. Let $f_w : \{0, 1, \ldots, n\} \to \{0, 1\}$ depend 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 Hamming weights starting from the biggest one $i = 0$. The term $(-1)^{p_w((n+1)/2+i)}$ will be $+1$ on the first $t + (d - t) = d$ Hamming weights, then -1 on the next d, then again $+1$ on the next d, and so on. We group the Hamming weights 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 Hamming weights 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 3. *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

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

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.

References

[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.

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

[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.

[Smo93] Roman Smolensky. On representations by low-degree polynomials. In *34th IEEE IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 130–138, 1993.

[Vio09] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il