COMS 6998: Unconditional Lower Bounds and Derandomization **Spring 2024**

Lecture 6: February 20, 2024

Lecturer: Rocco Servedio *Scribes: Yizhi Huang*

1 Introduction

In this class we discuss average-case lower bounds against polynomials over $\mathbb{F}_2$, that is, to construct an explicit function f such that f has low correlation with any $\mathbb{F}_2$-polynomials with bounded degree. We want an explicit function since otherwise an easy counting argument suffices.

The following is an open problem we dream to but are unable to solve.

Open problem. Construct some function $f : \{0,1\}^n \to \{0,1\}$ such that $f \in \mathsf{NP}$ and f is $(1/n)$-hard for any degree-$(\log n)$ polynomials for some distribution $\mathcal{D}$ over $\{0,1\}^n$.

Nevertheless, we introduce two results that are not satisfiable enough.

Theorem 1 says that there is an explicit function f such that any degree-$((1/4)\sqrt{n})$ polynomial over $\mathbb{F}_2$ has at most 3/4 correlation with f. The degree here is actually higher than in our dream, but the bound on correlation is quite weak.

Theorem 1 ([Smo87])**.** *Define* $\mathrm{mod}_3 : \{0,1\}^n \to \{0,1\}$ *as*

$$\mathrm{mod}_3(x) := \begin{cases} 1 & x_1 + x_2 + \cdots + x_n \equiv 1 \pmod 3 \\ 0 & \textit{otherwise} \end{cases}$$

Then, for any degree-$((1/4)\sqrt{n})$ *polynomial* $p : \mathbb{F}_2^n \to \mathbb{F}_2$*,*

$$\Pr_{\mathbf{x}\sim\mathbb{F}_2^n}[\mathrm{mod}_3(\mathbf{x}) = p(\mathbf{x})] \le 7/8.$$

(Here we naturally identify $\{0,1\}$ *with* $\mathbb{F}_2$*.)*

Theorem 2 says that there is an explicit function f such that any degree-d polynomial over $\mathbb{F}_2$ has at most $2^{-\Omega(n/(d2^d))}$ with f. Note that this result is only interesting if $d2^d \ll n$, which requires $d = o(\log n)$. Thus, we achieve a strong bound on correlation, but the degree is lower than our dream.

Theorem 2 ([BNS92])**.** *For any degree-d polynomial p over $\mathbb{F}_2$,*

$$\Pr_{\mathbf{x}\sim\mathbb{F}_2^n}[\mathrm{GIP}_{d+1}(\mathbf{x}) = p(\mathbf{x})] \le \frac{1}{2} + 2^{-\Omega(n/(d2^d))}.$$

For a recent survey on this topic, see [Vio22, Section 1].

2 High degree but weak bound on correlation

In this section, we prove a correlation bound for degree-$O(\sqrt{n})$ polynomials, but the bound itself is only constant.

Theorem 1 ([Smo87])**.** *Define* $\mathrm{mod}_3 : \{0,1\}^n \to \{0,1\}$ *as*

$$\mathrm{mod}_3(x) := \begin{cases} 1 & x_1 + x_2 + \cdots + x_n \equiv 1 \pmod 3 \\ 0 & \textit{otherwise} \end{cases}$$

Then, for any degree-$((1/4)\sqrt{n})$ polynomial $p : \mathbb{F}_2^n \to \mathbb{F}_2$,

$$\Pr_{\mathbf{x}\sim\mathbb{F}_2^n}[\mathrm{mod}_3(\mathbf{x}) = p(\mathbf{x})] \le 7/8.$$

(Here we naturally identify $\{0,1\}$ with $\mathbb{F}_2$.)

Example 3. $\mathrm{mod}_3(1000) = \mathrm{mod}_3(1111) = 1$, $\mathrm{mod}_3(1010) = \mathrm{mod}_3(0111) = 0$.

The high-level idea of the proof is as follows. Define

$$X := \{x \in \{0,1\}^n : p(x) = \mathrm{mod}_3(x)\},$$

then the goal is to prove that $|X| \le (7/8)\cdot 2^n$. Intuitively, mod_3 should have a high degree as an $\mathbb{F}_2$-polynomial, which might mean mod_3 can be used to "simulate" high-degree polynomials over $\{0,1\}^n$. Since $p(x) = \mathrm{mod}_3(x)$ for $x \in X$, this means maybe p can be used to "simulate" high-degree $\mathbb{F}_2$-polynomials over X. However, p has a low degree, which might mean X cannot be too big.

For the proof, we use $\mathbb{F}_4$, an extension field of $\mathbb{F}_2$, defined as follows.

Definition 4. *Let $\mathbb{F}_4 = \mathbb{F}_2[t]/(t^2+t+1)$, that is, the field of all $\mathbb{F}_2$-polynomials over t modulo t^2+t+1.*

Fact 5. *$\mathbb{F}_4$ has 4 elements, namely $0, 1, t, t+1$. Any $\mathbb{F}_2$-polynomials of degree at least 2 is equal to one of $0, 1, t, t+1$ modulo t^2+t+1.*

Intuitively, to calculate sum or product over $\mathbb{F}_4$, we first do the usual calculation for polynomials over $\mathbb{F}_2$, but we will change any t^{k+2} to $t^k(t+1)$ until there is no monomial of degree at least 2.

Example 6. $t^3 = t \cdot t^2 = t \cdot (t+1) = t^2 + t = 1$.

Now we start with the proof of Theorem 1.

Proof of Theorem 1. Without loss of generality, we assume n is a multiple of 3. Then for $x_1, x_2, \ldots, x_n \in \{0,1\}$,

$$\mathrm{mod}_3(1+x_1, 1+x_2, \ldots, 1+x_n) = 1 \text{ iff } x_1 + x_2 + \cdots + x_n \equiv 2 \pmod 3. \tag{1}$$

Define $h : \{1, t\} \to \mathbb{F}_2, \alpha \mapsto t(\alpha+1)$. Therefore, $h(1) = 0$ and $h(t) = t^2 + t = 1$.

Claim 7. *For any $y \in \{1, t\}^n$,*

$$y_1 y_2 \cdots y_n = 1 + (t+1)\mathrm{mod}_3(h(y_1), \ldots, h(y_n)) + (t^2+1)\mathrm{mod}_3(1 + h(y_1), \ldots, 1 + h(y_n)). \tag{2}$$

Proof of claim. Note that

$$\begin{aligned}\mathrm{mod}_3(h(y_1), \ldots, h(y_n)) &= \begin{cases} 1 & h(y_1) + \cdots + h(y_n) \equiv 1 \pmod 3 \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} 1 & (\#\{i \in [n] : y_i = t\}) \equiv 1 \pmod 3 \\ 0 & \text{otherwise} \end{cases}\end{aligned}$$

and by eq. (1),

$$\begin{aligned}\mathrm{mod}_3(1 + h(y_1), \ldots, 1 + h(y_n)) &= \begin{cases} 1 & h(y_1) + \cdots + h(y_n) \equiv 2 \pmod 3 \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} 1 & (\#\{i \in [n] : y_i = t\}) \equiv 2 \pmod 3 \\ 0 & \text{otherwise} \end{cases}.\end{aligned}$$

Therefore,

- When $(\#\{i \in [n] : y_i = t\}) \equiv 0 \pmod 3$, the left-hand side of eq. (2) equals $t^{3k} = 1$ (since $t^3 = 1$), and the right-hand side equals $1 + 0 + 0 = 1$.

- When $(\#\{i \in [n] : y_i = t\}) \equiv 1 \pmod 3$, the left-hand side equals $t^{3k+1} = t$, and the right-hand side equals $1 + (t+1) + 0 = t$.
- When $(\#\{i \in [n] : y_i = t\}) \equiv 2 \pmod 3$, the left-hand side equals $t^{3k+2} = t^2$, and the right-hand side equals $1 + 0 + (t^2 + 1) = t^2$.

■

Now we get back to the proof of Theorem 1. We fix p to be any polynomial $\mathbb{F}_2^n \to \mathbb{F}_2$ of degree at most $d := \varepsilon\sqrt{n}$ where $\varepsilon = 1/4$, and let

$$\delta = \Pr_{\mathbf{x}\sim\mathbb{F}_2^n}[p(\mathbf{x}) \neq \mathrm{mod}_3(\mathbf{x})],$$

then the goal is to prove $\delta \geq 1/8$.

Let $p' : \{1,t\}^n \to \mathbb{F}_4$ be

$$p'(y_1,\dots,y_n) := 1 + (t+1)p(h(y_1),\dots,h(y_n)) + (t^2+1)p(1+h(y_1),\dots,1+h(y_n)).$$

We observe that if $p(x) = \mathrm{mod}_3(x)$ for both $x = (h(y_1),\dots,h(y_n))$ and $x = (1 + h(y_1),\dots,1+h(y_n))$, then $p'(y_1,\dots,y_n) = y_1\cdots y_n$ by Claim 7. Note in addition that both $(h(\mathbf{y}_1),\dots,h(\mathbf{y}_n))$ and $(1+h(\mathbf{y}_1),\dots,1+h(\mathbf{y}_n))$ are uniformly random in $\{1,t\}^n$ when $\mathbf{y}$ is uniformly sampled in $\mathbb{F}_2^n$, so by union bound,

$$\begin{aligned}
&\Pr_{\mathbf{y}\sim\{1,t\}^n}[p'(\mathbf{y}_1,\dots,\mathbf{y}_n) = \mathbf{y}_1\cdots\mathbf{y}_n]\\
&\geq 1 - \Pr_{\mathbf{y}\sim\{1,t\}^n}[p(h(\mathbf{y}_1),\dots,h(\mathbf{y}_n)) = \mathrm{mod}_3(h(\mathbf{y}_1),\dots,h(\mathbf{y}_n))]\\
&\quad - \Pr_{\mathbf{y}\sim\{1,t\}^n}[p(1+h(\mathbf{y}_1),\dots,1+h(\mathbf{y}_n)) = \mathrm{mod}_3(1+h(\mathbf{y}_1),\dots,1+h(\mathbf{y}_n))]\\
&\geq 1 - 2\delta.
\end{aligned}$$

Define $S = \{y \in \{1,t\}^n : y_1\cdots y_n = p'(y_1,\dots,y_n)\}$. We have just showed $|S| \geq 2^n(1-2\delta)$.

Consider any $f : S \to \mathbb{F}_4$. We can always write f as a multilinear polynomial as the following:

$$f(y_1,\dots,y_n) = \sum_{(a_1,\dots,a_n)\in\{1,t\}^n} f(a_1,\dots,a_n)\prod_{i=1}^{n}(1 + h(y_i) + h(a_i)).$$

This is because

$$1 + h(y_i) + h(a_i) = \begin{cases} 1 & y_i = a_i \\ 0 & \text{otherwise} \end{cases}$$

and thus $\prod_{i=1}^{n}(1+h(y_i)+h(a_i))=1$ iff $y_i=a_i$ for all i.

We now make the following claim.

Claim 8. *For any multilinear monomial $M=y_{j_1}\cdots y_{j_k}$ over $y_1,\ldots,y_n\in\mathbb{F}_4$ of degree at least $n/2$, there exists a polynomial Q over $\mathbb{F}_4$ of degree $n/2+d$ such that $M(y)=Q(y)$ for any $y\in S$.*

Proof of claim. Let

$$Q(y)=p'(y_1,\ldots,y_n)\prod_{i\notin\{j_1,\ldots,j_k\}}(y_it+y_i+t).$$

Since $\deg h=1$ and $\deg p\le d$, we have $\deg p'\le d$ and thus $\deg Q\le n/2+d$.

Note that if $y_i=1$, then $y_i(y_it+y_i+t)=1(1+t+t)=1$, and if $y_i=t$, then $y_i(y_it+y_i+t)=t(t^2+2t)=t^3=1$. Therefore, for any $y\in S\subset\{1,t\}^n$,

$$\begin{aligned}
M(y) &= \prod_{i\in\{y_{j_1},\ldots,y_{j_k}\}} y_i \\
&= y_1\cdots y_n\cdot\prod_{i\notin\{y_{j_1},\ldots,y_{j_k}\}}(y_it+y_i+t) \\
&= p'(y_1,\ldots,y_n)\cdot\prod_{i\notin\{y_{j_1},\ldots,y_{j_k}\}}(y_it+y_i+t) \\
&= Q(y).
\end{aligned}$$

■

Now we apply the above claim to every monomial in f and obtain $f':S\to\mathbb{F}_4$ that is a polynomial over $\mathbb{F}_4$ of degree $n/2+d$ such that $f'(y)=f(y)$ for all $y\in S$. There are $|\mathbb{F}_4|^{|S|}$ functions $f:S\to\mathbb{F}_4$, where as the number of possible f' is at most the number of degree-$(n/2+d)$ polynomials over $\mathbb{F}$, which is $|\mathbb{F}_4|^{\sum_{i=0}^{n/2+d}\binom{n}{i}}$. Therefore,

$$\begin{aligned} 2^n(1-2\delta) &\leq |S| \\ &\leq \sum_{i=0}^{n/2+d}\binom{n}{i} \\ &\leq 2^{n-1} + (d+1)\cdot\binom{n}{n/2} \\ &\leq 2^n\left(\frac{1}{2}+\frac{d}{\sqrt{n}}\right) \\ &\leq 2^n\left(\frac{1}{2}+\varepsilon\right). \quad (\text{recall } d=\varepsilon\sqrt{n}) \end{aligned}$$

It follows that $1-2\delta \leq 1/2+\varepsilon$, so when $\varepsilon = 1/4$, we have $\delta \geq 1/8$. ■

3 Stronger bound on correlation but for low degree

In this section, we prove a non-trivial correlation bound which only works for $\mathbb{F}_2$-polynomials of degree at most slightly less than $\log n$.

Let IP be the polynomial over $\mathbb{F}_2$ such that $\mathrm{IP}(x) := x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$. It can be shown that for any degree-1 polynomial p over $\mathbb{F}_2$,

$$\Pr_{\mathbf{x}\sim\mathbb{F}_2^n}[\mathrm{IP}(\mathbf{x}) = p(\mathbf{x})] = \frac{1}{2} + \frac{1}{2^{n/2}}.$$

This motivates defining

$$\mathrm{GIP}_{d+1}(x) = x_1x_2\cdots x_{d+1} + x_{d+2}\cdots x_{2d+2} + \cdots + x_{n-d}\cdots x_n,$$

and trying to show a correlation bound between $\mathrm{GIP}_{d+1}(x)$ and any degree-d polynomial. Actually, this is true.

Theorem 2 ([BNS92]). *For any degree-d polynomial p over $\mathbb{F}_2$,*

$$\Pr_{\mathbf{x}\sim\mathbb{F}_2^n}[\mathrm{GIP}_{d+1}(\mathbf{x}) = p(\mathbf{x})] \leq \frac{1}{2} + 2^{-\Omega(n/(d2^d))}.$$

In the following, sometimes it will be more convenient to consider $\{1,-1\}$ instead of $\{0,1\}$. For given $f : \mathbb{F}_2^n \to \{0,1\}$, we will use the notation $e(f) := (-1)^f$. Moreover, we will use capital letter F to denote $e(f)$, G for $e(g)$, etc.

We also denote by $\deg_k$ the set of all degree-k polynomials $\mathbb{F}_2^n \to \mathbb{F}_2$, and $\mathrm{Deg}_k := \{e(p) : p \in \deg_k\}$.

For $F, G : \mathbb{F}_2^n \to \{1, -1\}$, we define $\mathrm{Cor}[F, G] := |\mathbb{E}_{\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x}) \cdot G(\mathbf{x})]|$. Our goal is to analyse $\mathrm{Cor}[F, \mathrm{Deg}_d] := \max_{P\in\mathrm{Deg}_d}[F, P]$. We would like to relate this to $\mathrm{Cor}[Q, \mathrm{Deg}_{d-1}]$ for some function $Q : \mathbb{F}_2^n \to \{1, -1\}$, so that we could do an induction in some sense.

It turns out that it is useful to consider $\mathrm{Cor}^2[\cdot, \cdot]$. Actually, we have the following.

Claim 9. *Let $F : \mathbb{F}_2^n \to \{1, -1\}$ be an arbitrary function, $p : \mathbb{F}_2^n \to \{0, 1\}$ be a degree-d polynomial and let $P := e(p)$, then*

$$\mathrm{Cor}[F, P]^2 = \mathop{\mathbb{E}}_{\mathbf{h}\sim\mathbb{F}_2^n}[\mathrm{Cor}[F(x)F(x + \mathbf{h}), P(x)P(x + \mathbf{h})]]$$

Proof. We have

$$\mathrm{Cor}[F, P] = |\mathop{\mathbb{E}}_{\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})P(\mathbf{x})]|.$$

Taking squares on both side, we have

$$\begin{aligned}
\mathrm{Cor}[F, P]^2 &= \mathop{\mathbb{E}}_{\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})P(\mathbf{x})]^2 \\
&= \mathop{\mathbb{E}}_{\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})P(\mathbf{x})] \mathop{\mathbb{E}}_{\mathbf{y}\sim\mathbb{F}_2^n}[F(\mathbf{y})P(\mathbf{y})] \\
&= \mathop{\mathbb{E}}_{\mathbf{x},\mathbf{y}\sim\mathbb{F}_2^n}[F(\mathbf{x})F(\mathbf{y})P(\mathbf{x})P(\mathbf{y})] \\
&= \mathop{\mathbb{E}}_{\mathbf{h}\sim\mathbb{F}_2^n}[\mathop{\mathbb{E}}_{\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})F(\mathbf{x} + \mathbf{h})P(\mathbf{x})P(\mathbf{x} + \mathbf{h})]]. \quad \text{(substituting } \mathbf{h} = \mathbf{x} - \mathbf{y}\text{)}
\end{aligned}$$

Here

$$P(x)P(x + h) = e(p(x)) \cdot e(p(x + h)) = e(p(x) + p(x + h)).$$

A key observation is, for any fixed h, for any polynomial p of degree at most d, $p(x) + p(x + h)$ has degree at most $d - 1$. This can be easily proved by considering every monomial of maximal degree in p. For example, the only monomial of degree d in $(x_1 + h_1) \cdots (x_d + h_d)$ is $x_1 \cdots x_d$, so $x_1x_2 \cdots x_d + (x_1 + h_1) \cdots (x_d + h_d)$ has degree $d - 1$. Actually, $p(x) + p(x + h) = p(x + h) - p(x)$ can be viewed as a discrete derivative, also called finite difference, of p, and as in the case of derivatives, after taking the difference, the degree of the polynomial decreases by 1.

Therefore,

$$\mathrm{Cor}[F, P]^2 = \mathop{\mathbb{E}}_{\mathbf{h}\sim\mathbb{F}_2^n}[\mathrm{Cor}[F(x)F(x + \mathbf{h}), P(x)P(x + \mathbf{h})]].$$

∎

In the following we will use the notation $F^{+y}(x)$ for $F(x+y)$.

Now we define Gowers uniformity.

Definition 10 (Gowers uniformity). *Let $F : \mathbb{F}_2^n \to \{1,-1\}$, let $k \in \mathbb{Z}_{\geq 0}$. The k-uniformity of f is defined as*

$$U_k(F) = \mathop{\mathbb{E}}_{\mathbf{h}_1,\ldots,\mathbf{h}_k,\mathbf{x}\sim\mathbb{F}_2^n}\left[\prod_{S\subset[k]} F^{+\sum_{j\in S} h_j}(x)\right].$$

Note that any fixed $h_1,\ldots,h_k$ define a k-dimensional parallelepiped. So $U_k(F)$ can be viewed as the average of the product of F across all of points in a random parallelepiped "based" at x.

Example 11. *Some small k:*

- *When $k=0$, $U_0(F) = \mathbb{E}_{\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})]$.*
- *When $k=1$,*

$$U_1(F) = \mathop{\mathbb{E}}_{\mathbf{h}_1,\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})F^{+\mathbf{h}_1}(x)] = \mathop{\mathbb{E}}_{\mathbf{x},\mathbf{y}\sim\mathbb{F}_2^n}[F(\mathbf{x})F(\mathbf{y})] = \mathop{\mathbb{E}}_{\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})]^2 \geq 0.$$

- *When $k=2$,*

$$\mathop{\mathbb{E}}_{\mathbf{h}_1,\mathbf{h}_2,\mathbf{x}\sim\mathbb{F}_2^n}[F(\mathbf{x})F^{+\mathbf{h}_1}(\mathbf{x})F^{+\mathbf{h}_2}(\mathbf{x})F^{+\mathbf{h}_1+\mathbf{h}_2}(\mathbf{x})] = \mathop{\mathbb{E}}_{\mathbf{h}_2\sim\mathbb{F}_2^n}[U_1[F\cdot F^{+\mathbf{h}_2}]] \geq 0.$$

It is easy to see from definition that for any $k \in \mathbb{Z}_{\geq 0}$,

$$U_{k+1}[F] = \mathop{\mathbb{E}}_{\mathbf{h}_{k+1}\sim\mathbb{E}_2^n}[U_k[F\cdot F^{+\mathbf{h}_{k+1}}]],$$

so by induction we also have $U_{k+1}[F] \geq 0$.

Below as an example that is also useful later, we consider k-uniformity of the function AND.

Lemma 12 ($(d+1)$-uniformity of AND). *Let f be the* AND *function, that is,*

$$f : \mathbb{F}_2^{d+1} \to \mathbb{F}_2, (x_1,\ldots,x_{d+1}) \mapsto \begin{cases} 1 & x_1 = \cdots = x_{d+1} = 1 \\ 0 & \textit{otherwise} \end{cases}.$$

Let $F = e(f)$, then $U_{d+1}(F) \approx 0.6$.

Proof. It is easy to see that $U_{d+1} = 1 - 2p$, where

$$p := \Pr_{\mathbf{h}_1,\ldots,\mathbf{h}_{d+1},\mathbf{x}\sim\mathbb{F}_2^{d+1}} \left[\prod_{S\subset[d+1]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x}) = -1 \right].$$

If $h_1, \ldots, h_{d+1}$ form a basis of $\mathbb{F}_2^{d+1}$, then for any fixed x, $x + \sum_{j\in S} h_j$ varies over all of $\mathbb{F}_2^{d+1}$. Therefore,

$$\prod_{S\subset[d+1]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x}) = -1$$

as there is exactly one $S \subset [d+1]$ such that $F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x}) = -1$.

On the other hand, if $h_1, \ldots, h_{d+1}$ does not form a basis of $\mathbb{F}_2^{d+1}$, then for any $x, y \in \mathbb{F}_2^{d+1}$, the number of S such that $y = x + \sum_{j\in S} h_j$ is even, since either there is no such S, or all such S form an affine subspace of dimension at least 1. Therefore,

$$\prod_{S\subset[d+1]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x}) = 1.$$

It follows that

$$\begin{aligned} p &= \Pr_{\mathbf{h}_1,\ldots,\mathbf{h}_{d+1}\sim\mathbb{F}_2^{d+1}}[\mathbf{h}_1, \ldots, \mathbf{h}_{d+1} \text{ form a basis of } \mathbb{F}_2^{d+1}] \\ &= \left(1 - \frac{1}{2^{d+1}}\right) \cdot \left(1 - \frac{2}{2^{d+1}}\right) \cdot \left(1 - \frac{4}{2^{d+1}}\right) \cdots \left(1 - \frac{2^d}{2^{d+1}}\right) \\ &= \frac{1}{2} \cdot \frac{3}{4} \cdot \frac{7}{8} \cdots \left(1 - \frac{1}{2^{d+1}}\right) \\ &\approx 0.2. \end{aligned}$$

■

Also note that k-uniformity is multiplicative, which we can prove immediately from definition.

Fact 13. *Let $F_1, F_2 : \mathbb{F}_2^n \to \{1, -1\}$, and define $G(x, y) := F_1(x) \cdot F_2(y)$. Then,*

$$U_k(G) = F_1(x) \cdot F_2(y).$$

We have the following lemma.

Lemma 14. *Let $F : \mathbb{F}_2^n \to \{1,-1\}$ be any function, let $p : \mathbb{F}_2^n \to \mathbb{F}_2$ be a degree d polynomial, and let $P = e(p)$. Then,*

$$\mathrm{Cor}[F,P] \le U_{d+1}(F)^{1/2^{d+1}}.$$

To prove this lemma we need the following two facts.

Fact 15. *For any function $F : \mathbb{F}_2^n \to \{1,-1\}$, $U_k[F] \le U_{k+1}[F]^{1/2}$.*

Proof.

$$\begin{aligned}
U_{k+1}[F] &= \mathop{\mathbb{E}}_{\mathbf{h}_1,\ldots,\mathbf{h}_k \sim \mathbb{F}_2^n}\left[\mathop{\mathbb{E}}_{\mathbf{h}_{k+1},\mathbf{x} \sim \mathbb{F}_2^n}\left[\prod_{S\subset[k]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x})F^{+\sum_{j\in S}\mathbf{h}_j+\mathbf{h}_{k+1}}(\mathbf{x})\right]\right] \\
&= \mathop{\mathbb{E}}_{\mathbf{h}_1,\ldots,\mathbf{h}_k \sim \mathbb{F}_2^n}\left[\mathop{\mathbb{E}}_{\mathbf{x} \sim \mathbb{F}_2^n}\left[\prod_{S\subset[k]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x})\right]\cdot \mathop{\mathbb{E}}_{\mathbf{y} \sim \mathbb{F}_2^n}\left[\prod_{S\subset[k]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{y})\right]\right] \qquad (\mathbf{y} := \mathbf{x}+\mathbf{h}_{k+1}) \\
&= \mathop{\mathbb{E}}_{\mathbf{h}_1,\ldots,\mathbf{h}_k \sim \mathbb{F}_2^n}\left[\mathop{\mathbb{E}}_{\mathbf{x} \sim \mathbb{F}_2^n}\left[\prod_{S\subset[k]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x})\right]^2\right] \\
&\ge \mathop{\mathbb{E}}_{\mathbf{h}_1,\ldots,\mathbf{h}_k \sim \mathbb{F}_2^n}\left[\mathop{\mathbb{E}}_{\mathbf{x} \sim \mathbb{F}_2^n}\left[\prod_{S\subset[k]} F^{+\sum_{j\in S}\mathbf{h}_j}(\mathbf{x})\right]\right] \\
&= U_k[F]^2.
\end{aligned}$$

■

The next fact uses the idea in Claim 9.

Fact 16. *Let $F : \mathbb{F}_2^n \to \{1,-1\}$ be any function, let $p : \mathbb{F}_2^n \to \mathbb{F}_2$ be a degree d polynomial, and let $P = e(p)$. Then,*

$$U_{d+1}[F\cdot P] = U_{d+1}[F].$$

Proof. From definition, we have

$$U_{d+1}[F\cdot P] = \mathop{\mathbb{E}}_{\mathbf{h}_1,\ldots,\mathbf{h}_{k+1},\mathbf{x} \sim \mathbb{F}_2^n}\left[\prod_{S\subset[d+1]} F^{+\sum_{j\subset S}\mathbf{h}_j}(\mathbf{x}) \prod_{S\subset[d+1]} P^{+\sum_{j\subset S}\mathbf{h}_j}(\mathbf{x})\right].$$

Define $p_k(x) := \sum_{S\subset[k]} p(x + \sum_{j\subset S} h_j)$, then $p_{k+1}(x) = p_k(x) + p_k(x + h_{k+1})$ and

$$\prod_{S\subset[d+1]} P^{+\sum_{j\subset S}\mathbf{h}_j}(\mathbf{x}) = e(p_{k+1}(x)).$$

As we have observed in Claim 9, for every k we have $\deg p_{k+1} \le \deg p_k - 1$. Since $p_0 = p$ and thus $\deg p_0 = d$, we have $\deg p_d = 0$ and thus $p_{d+1}(x) = 0$. Therefore,

$$\prod_{S\subset[d+1]} P^{+\sum_{j\subset S}\mathbf{h}_j}(\mathbf{x}) = 0,$$

and thus

$$U_{d+1}[F\cdot P] = \mathop{\mathbb{E}}_{\mathbf{h}_1,\ldots,\mathbf{h}_{k+1},\mathbf{x}\sim\mathbb{F}_2^n}\left[\prod_{S\subset[d+1]} F^{+\sum_{j\subset S}\mathbf{h}_j}(\mathbf{x})\right] = U_{d+1}[F].$$

■

Now we prove Lemma 14.

Proof of Lemma 14. We have observed in Example 11 that for any function $G : \mathbb{F}_2^n \to \{1,-1\}$, $U_1[G] = \mathbb{E}_{\mathbf{x}\sim\mathbb{E}_2^n}[G(\mathbf{x})]$. Therefore, using the above two facts,

$$|\mathrm{Cor}[F,P]| = \left|\mathop{\mathbb{E}}_{\mathbf{x}\sim\mathbb{E}_2^n}[(F\cdot P)(\mathbf{x})]\right| = U_1[F\cdot P]^{1/2} \le U_2[F\cdot P]^{1/4} \le \cdots \le U_{d+1}[F\cdot P]^{1/2^{d+1}} = U_{d+1}[F]^{1/2^{d+1}}.$$

■

Now we prove Theorem 2.

Proof of Theorem 2. For any degree-d polynomial p over $\mathbb{F}_2$, we have

$$\begin{aligned}\mathrm{Cor}[\mathrm{GIP}_{d+1}, p] &\le U_{d+1}(\mathrm{GIP}_{d+1})^{1/2^{d+1}} \quad \text{(Lemma 14)}\\ &= U_{d+1}(e(\textsc{and}_{d+1}))^{n/((d+1)2^{d+1})} \quad \text{(there are } n/(d+1)\text{monomials in } \mathrm{GIP}_{d+1})\\ &\le (0.6)^{m/2^{d+1}}.\end{aligned}$$

■

References

[BNS92] László Babai, Noam Nisan, and Mario Szegedy. Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs. *J. Comput. Syst. Sci.*, 45(2):204–232, 1992. 2, 2

[Smo87] Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *STOC*, pages 77–82. ACM, 1987. 1, 1

[Vio22] Emanuele Viola. Correlation bounds against polynomials. *Electron. Colloquium Comput. Complex.*, TR22-142, 2022. 1