Matrix Rigidity

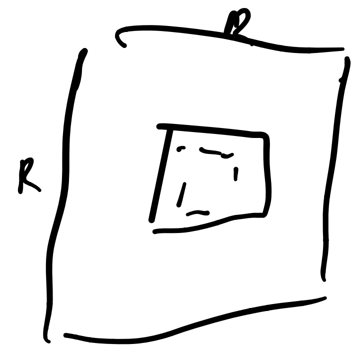
Rigidity of $M(x, y) = f(x + y)$

Sasha Golovnev

November 9, 2020

Limitations

- Limits of Untouched Minor method



Limitations

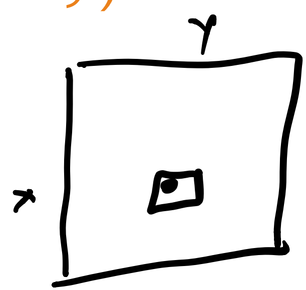
- Limits of Untouched Minor method
- Upper bound on rigidity of super regular matrices

Limitations

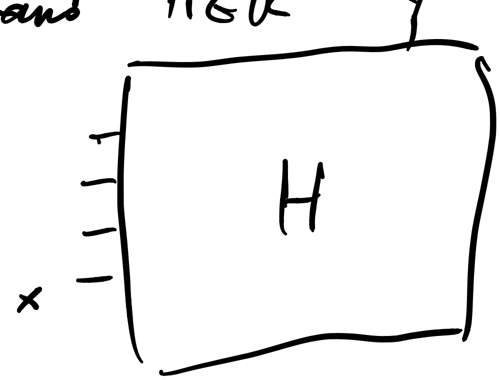
- Limits of Untouched Minor method
- Upper bound on rigidity of super regular matrices
- Upper bounds for ECCs
- Upper bound for Hadamard

Limitations

- Limits of Untouched Minor method
- Upper bound on rigidity of super regular matrices
- Upper bound for Hadamard
- Upper bound for $M(x, y) = f(x + y)$



Hadamard $H \in \mathbb{R}^{2^n \times 2^n}$



$x \in \{0,1\}^n$ $\quad y \in \{0,1\}^n$ $\quad H_{x,y} = (-1)^{\langle x,y \rangle}$

$$= (-1)^{\sum_{i=1}^{n} x_i y_i} = (-1)^{\|x\|_0/2} (-1)^{\|y\|_0/2} (-1)^{\|x \oplus y\|_0/2}$$

If you multiply every row by $(-1)^{\|x\|_0/2}$

every col by $(-1)^{\|y\|_0/2}$

Rigidity stays the same, but your matrix now

$$\tilde{H}_{x,y} = (-1)^{\|x \oplus y\|_0/2}$$

$F : \boxed{\mathbb{F}_2^n} \to \boxed{\mathbb{R}}$ $\quad F(z) = (-1)^{\|z\|_0/2}$

$$\tilde{H}_{x,y} = F(x + y)$$

xor / over $\mathbb{F}_2^n$

$$x \quad [0\,0\,1\,0\,1\,0\,0\,1\,1]$$

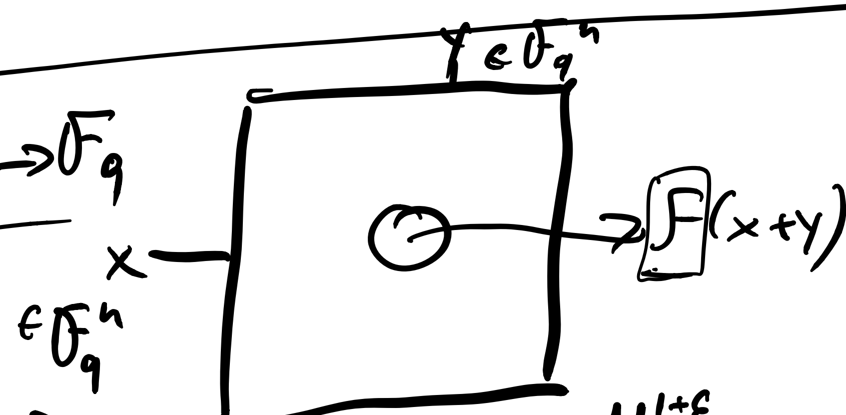
$$y \quad [1\,0\,0\,1\,0\,0\,0\,1\,0]$$

$$H_{x,y} = (-1)^{\langle x,y\rangle} = (-1)^{(x^2+y^2+(x\oplus y)^2)/2} =$$

$$= (-1)^{\|x\|_0^2/2} \cdot (-1)^{\|y\|_0^2/2} \cdot (-1)^{\|x\oplus y\|_0^2/2} =$$

$$= (-1)^{\|x\|_0/2} \cdot (-1)^{\|y\|_0/2} \cdot (-1)^{\|x\oplus y\|_0/2}$$

Any $F : \mathbb{F}_q^n \to \mathbb{F}_q$



Non-rigid: if you want rigidity $N^{1+\varepsilon} \Rightarrow$ then you have it only for rank $N^{1-\varepsilon}$.

Main Result

Theorem (DE17)

Let $\mathbb{F}_q$ be a fixed finite field, and let $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ be an arbitrary function. Let $M \in \mathbb{F}_q^{N\times N}$ for $N = q^n$ be the matrix where the (x, y) entry of M equals $f(x + y)$ for every $x, y \in \mathbb{F}_q^n$.

For any $\varepsilon > 0$, there exists $\varepsilon' > 0$ such that $\mathcal{R}_M^{\mathbb{F}_q}(N^{1-\varepsilon'}) \leq N^{1+\varepsilon}$ for every large enough n.

Proof Outline

over $\mathbb{F}_2$ $x^2 = x$
over $\mathbb{F}_p$ $x^p = x$

$f(z)$

- Step 1: Any n-variate function over $\mathbb{F}_q$ can be approximated by a polynomial of degree $(1-\delta)(q-1)n$ for some constant δ

Max degree $\boxed{(q-1) \cdot n}$ exactly

Proof Outline

- Step 1: Any n-variate function over $\mathbb{F}_q$ can be approximated by a polynomial of degree $(1-\delta)(q-1)n$
- Step 2: $P_{x,y} = p(x+y)$ for a polynomial p has rank upper bounded by the number of monomials of degree at most $\mathbf{deg}(p)/2$

Proof Outline

- Step 1: Any n-variate function over $\mathbb{F}_q$ can be approximated by a polynomial of degree $(1-\delta)(q-1)n$
- Step 2: $P_{x,y} = p(x+y)$ for a polynomial p has rank upper bounded by the number of monomials of degree at most $\deg(p)/2$

  $= f(x+y)$
- Conclude: M is close to P, P has low-rank. M is non-rigid

Monomials over Finite Fields

$m_d(q, n)$ denotes the number of distinct n-variate monomial over $\mathbb{F}_q$ of degree at most d.

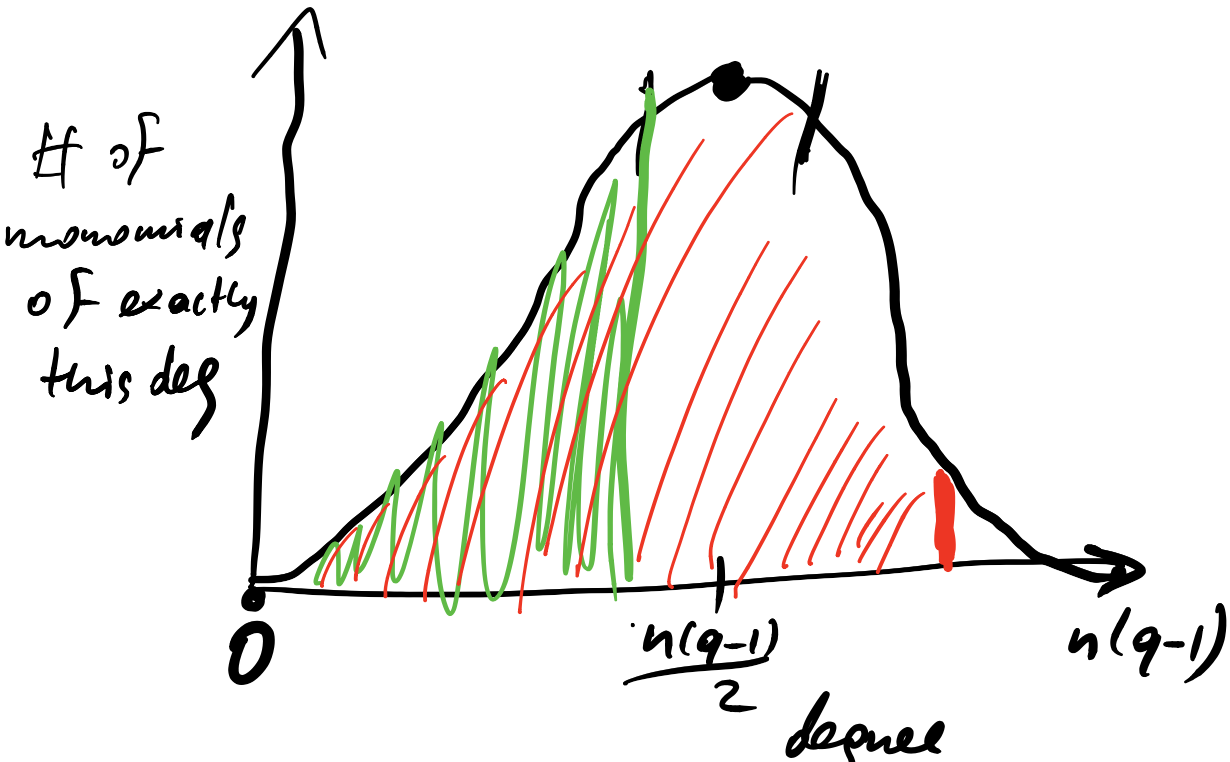
Every monomial wlog has x_i deg $0, 1, 2, \ldots, q-1$

Max degree : $n \cdot (q-1)$.

$$x_1^{\boxed{\cdot}} \; x_2^{\boxed{\cdot}} \cdots \; x_n^{\boxed{\cdot}}$$

$$\boxed{} \in \{0, \ldots, q-1\}$$

$m_d(q, n)$ — # monomials ~~deg~~ $\leq d$



# of monomials q^n

Monomials over Finite Fields

$m_d(q,n)$ denotes the number of distinct n-variate monomial over $\mathbb{F}_q$ of degree at most d.

Proposition

For every $\delta > 0$ there exists $\varepsilon' > 0$ s.t.

$$m_{(1-\delta)\boxed{\frac{(q-1)n}{2}}}(q,n) \leq \boxed{q^{(1-\varepsilon')n}}.$$

Chernoff: sample random monomial, av degree is $\frac{(q-1)n}{2}$ $\Longrightarrow$

$$\Pr\left[\deg < (1-\delta)\frac{(q-1)n}{2}\right] = e^{-\Omega(n\delta^2)}$$

Monomials over Finite Fields

$m_d(q,n)$ denotes the number of distinct n-variate monomial over $\mathbb{F}_q$ of degree at most d.

Proposition

For every $\delta > 0$ there exists $\varepsilon' > 0$ s.t.

$$m_{(1-\delta)\frac{(q-1)n}{2}}(q,n) \leq q^{(1-\varepsilon')n}.$$

Proposition

For any $q \geq 2$ and $\varepsilon > 0$, there exists $\delta > 0$ s.t.

$$m_{(1-\delta)(q-1)n}(q,n) \geq q^n - q^{\varepsilon n}.$$

✓✓

Step 1

$M_{x,y} = f(x,y)$

Step 1: approximated by low-deg poly

Step 2: low-deg poly matrix has low-rank

Lemma

For any $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and $\varepsilon > 0$, there exists $\delta > 0$ and a polynomial p of degree at most $\boxed{(1-\delta)(q-1)n}$ such that f and p disagree on at most $\cancel{q^{\varepsilon n}}$ points.

✓

$\boxed{q^{\varepsilon n}}$

By lin alg: $\boxed{d'} \le d$

any function of degree d
can be turned into a fn of deg d'
by changing

$$\underline{\boxed{m_d}(n,q) - \boxed{m_{d'}}(n,q)}$$

points.

<u>Sketch</u> $f : \mathbb{F}_q^n \to \mathbb{F}_q$

$\downarrow$

$N = \boxed{q^n}$ $\quad \boxed{v_f} \in \mathbb{F}_q^N$

v_f - truth table of f.

$f : \mathbb{F}_2^2 \to \mathbb{F}_2$

x	y	$f(x,y)$
0	0	0
0	1	1
1	0	1
1	1	0

v_f.

For original fn of deg d, it leaves in a space of dim $\underline{m_d(n,q)}$

fns of deg d' live a space of dim $\underbrace{m_{d'}(n,q)}$

$m_d(n,q) - m_{d'}(n,q)$ changes will take you from the first space to the second one $\square$

$$f \quad d = (q-1)n$$

$$\Downarrow$$

$$p \quad d' = (1-\delta)(q-1)n$$

$f \neq p$ at

$$\boxed{m_{(q-1)n}}(q,n) -$$

$$- \underline{m_{(1-\delta)(q-1)n}}(q-n) \text{ points}$$

$$= q^n - (q^n - q^{\epsilon n}) = q^{\epsilon n} \quad \square$$

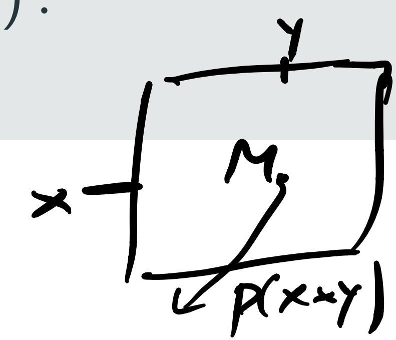
Step 2

$\deg p = (1-\delta)(q-1)n$

Lemma (CLP17)

Let p be an n-variate polynomial over $\mathbb{F}_q$ of degree at most d, and $M \in \mathbb{F}_q^{N \times N}$ for $N = q^n$ be a matrix defined as $M_{x,y} = p(x+y)$ for every $x, y \in \mathbb{F}_q^n$. Then

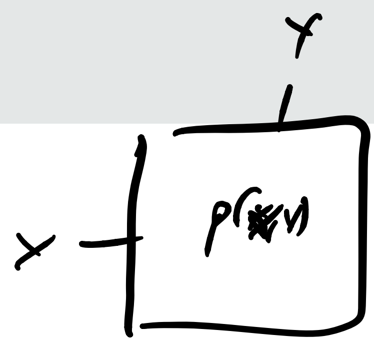
$$\operatorname{rank}(M) \leq 2m_{\lfloor \frac{d}{2} \rfloor}(q, n)\,.$$



Lemma

Let $p(x, y)$ for $x, y \in \mathbb{F}^n$ be a $(2n)$-variate polynomial with m monomials. Let $P \in \mathbb{F}^{2^n \times 2^n}$ be a matrix defined as $P_{x,y} = p(x, y)$ for every $x, y \in \{0, 1\}^n$.

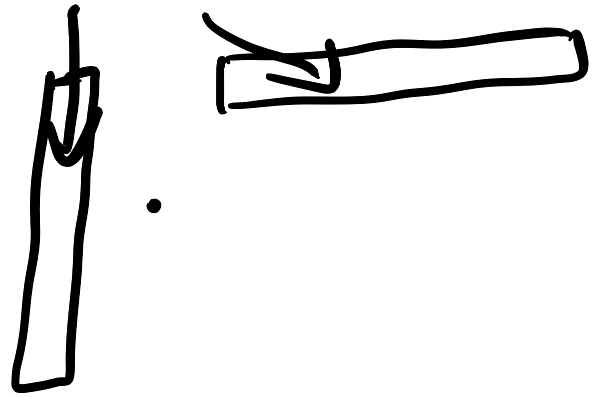
$$\mathrm{rank}(P) \le m\,.$$



$$p(x,y) = \sum_{i\in[m]} c_i (x_1 x_3 x_4)(y_2 y_n)$$

$$P = \sum_{i\in[m]} c_i P_i$$

matrix $P_i =$



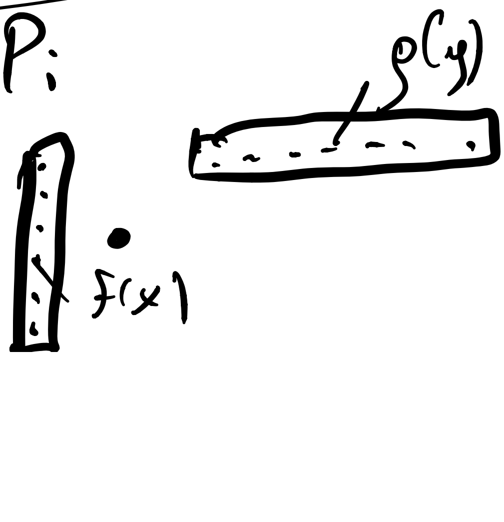
rank $(P) \le m$.

Same holds if

$$\boxed{p(x,y) = \sum_{i\in[m]} c_i \cdot f(x) \cdot g(y)}$$

$$P = \sum_{i\in[m]} c_i P_i$$

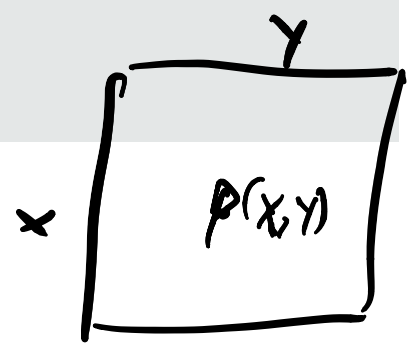
$\boxed{P_i} =$



Lemma

Let $p(x, y)$ for $x, y \in \mathbb{F}^n$ be a $(2n)$-variate polynomial that can be written as $p(x, y) = \sum_{i \in [m]} c_i f_i(x) g_i(y)$. Let $P \in \mathbb{F}^{2^n \times 2^n}$ be a matrix defined as $P_{x,y} = p(x, y)$ for every $x, y \in \{0, 1\}^n$.

$$\mathrm{rank}(P) \leq m\,.$$



Lemma (CLP17)

Let p be an n-variate polynomial over $\mathbb{F}_q$ of degree at most d, and $M \in \mathbb{F}_q^{N \times N}$ for $N = q^n$ be a matrix defined as $M_{x,y} = p(x+y)$ for every $x, y \in \mathbb{F}_q^n$. Then

$$\operatorname{rank}(M) \le \boxed{2 m_{\lfloor \frac{d}{2} \rfloor}}(q,n)\,. \ll q^n = N^{1-\varepsilon}$$

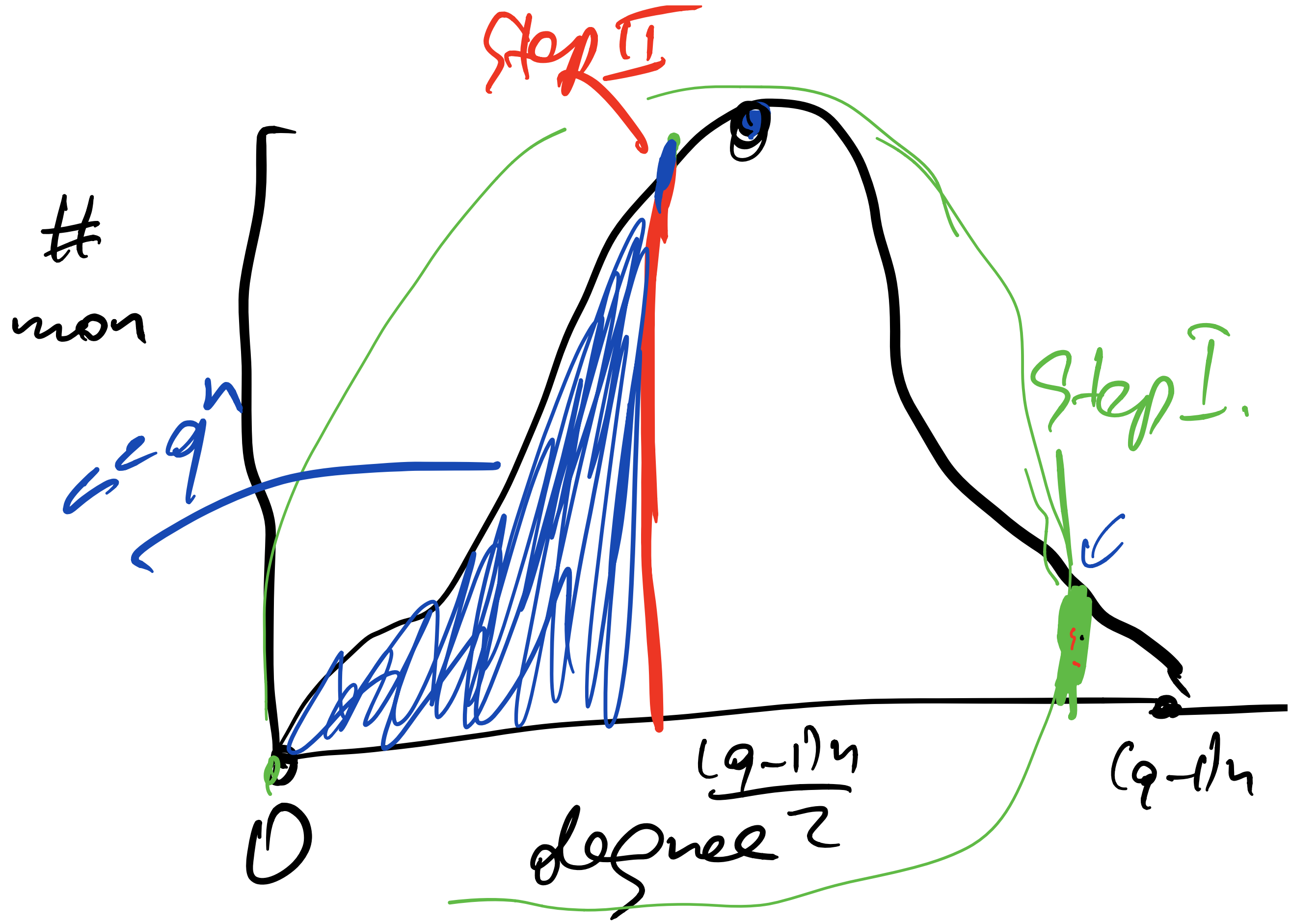
size of the matrix

$p(x+y)$ – poly of degree $\le d$

$\Rightarrow \ \le m_d(q,n)$ monomials

$M = \sum m_d(q,n)$ matrices of rank 1

$\Rightarrow \operatorname{rank}(M) \le m_{\boxed{d}}(q,n)$

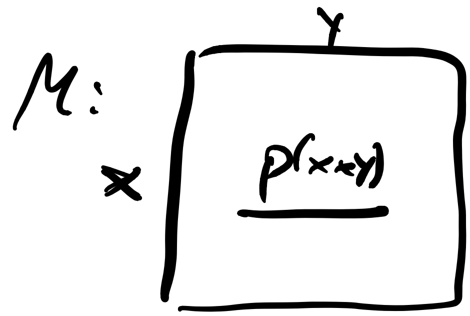


#
mon
$\leq q^n$
Step II
Step I.
0
$\frac{(q-1)n}{2}$
$(q-1)n$
degree

Lemma (CLP17)

Let p be an n-variate polynomial over $\mathbb{F}_q$ of degree at most d, and $M \in \mathbb{F}_q^{N\times N}$ for $N = q^n$ be a matrix defined as $M_{x,y} = p(x+y)$ for every $x, y \in \mathbb{F}_q^n$. Then

$$\operatorname{rank}(M) \le 2m_{\lfloor \frac{d}{2} \rfloor}(q,n)\,.$$



$x = (x_1 \ldots x_n)$ ✓

$y = (y_1 \ldots y_n)$ ✓

$z = (z_1, \ldots, z_n)$

$\text{Rank} \le m_{\lfloor d/2 \rfloor}(q,n) \cdot 2$

$$p(z) = \sum_{\alpha \in M_d(q,n)} z^{\alpha} \cdot c_\alpha$$

$$p(x+y) = \sum_{\alpha \in M_d(q,n)} c_\alpha \cdot (x+y)^{\alpha}$$

Every mon has y-deg + x-deg $\le d$.

In particular, either x-deg or y-deg of each monomial $\le \lfloor d/2 \rfloor$

$$= \sum_{\beta \in M_{\lfloor d/2 \rfloor}(q,n)} c_\alpha \cdot \boxed{x^{\alpha}} \cdot \boxed{F_\beta(y)} +$$

some function

$$+ \sum_{\gamma \in M_{\lfloor d/2 \rfloor}(q,n)} c_\gamma \cdot \boxed{y^{\gamma}} \cdot \boxed{G_\gamma(x)}$$

Total # of terms is $2 \cdot m_{\lfloor d/2 \rfloor}(q,n)$

$$p(z) = 3z^2$$

$$p(x+y) = 3(x+y)^2$$

rank $p \leq$ # of monomials of deg 2

Instead, rank ≤ 2(# of monomials of deg 1)

$$p(x+y) = 3(x^2 + y^2 + 2xy) =$$

$$= \boxed{3x^2 + 2xy} + \boxed{3y^2}$$

low y-degree

low x-degree

$$= \boxed{y^0 \cdot 3x^2 + y^1 \cdot 2x} + \boxed{x^0 \cdot 3y^2}$$

# of monomials (in x, y) of degree ≤ 1

$\boxed{\text{\# of deg up to 1}}$

$\delta \in m[\frac{q}{2}]$

Main Result

Theorem (DE17)

Let $\mathbb{F}_q$ be a fixed finite field, and let $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ be an arbitrary function. Let $M \in \mathbb{F}_q^{N\times N}$ for $N = q^n$ be the matrix where the (x, y) entry of M equals $f(x + y)$ for every $x, y \in \mathbb{F}_q^n$.

For any $\varepsilon > 0$, there exists $\varepsilon' > 0$ such that $\mathcal{R}_M^{\mathbb{F}_q}(N^{1-\varepsilon'}) \leq N^{1+\varepsilon}$ for every large enough n.