A ROBUST VERSION OF HEGEDUS'S LEMMA

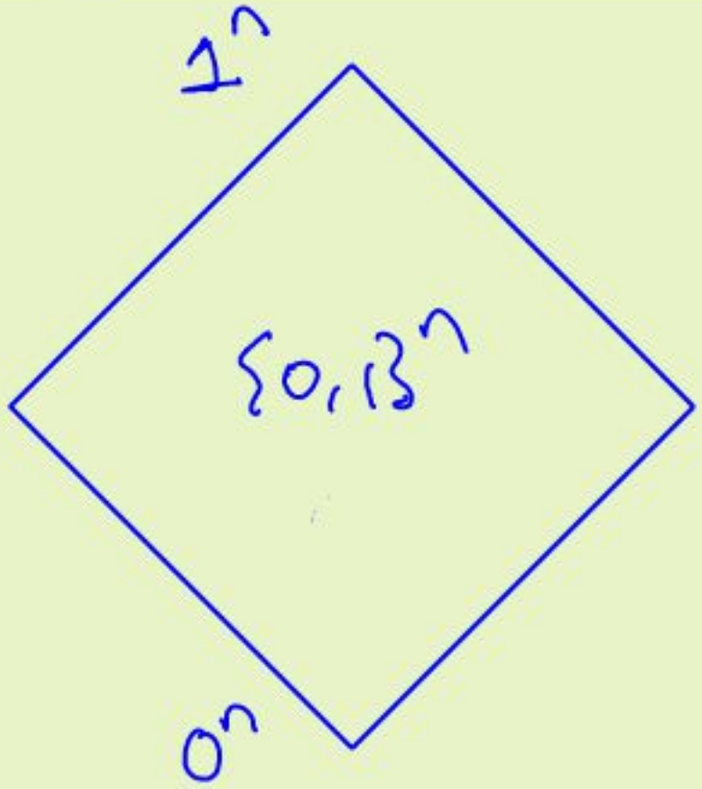
WITH APPLICATIONS

SRIKANTH SRINIVASAN

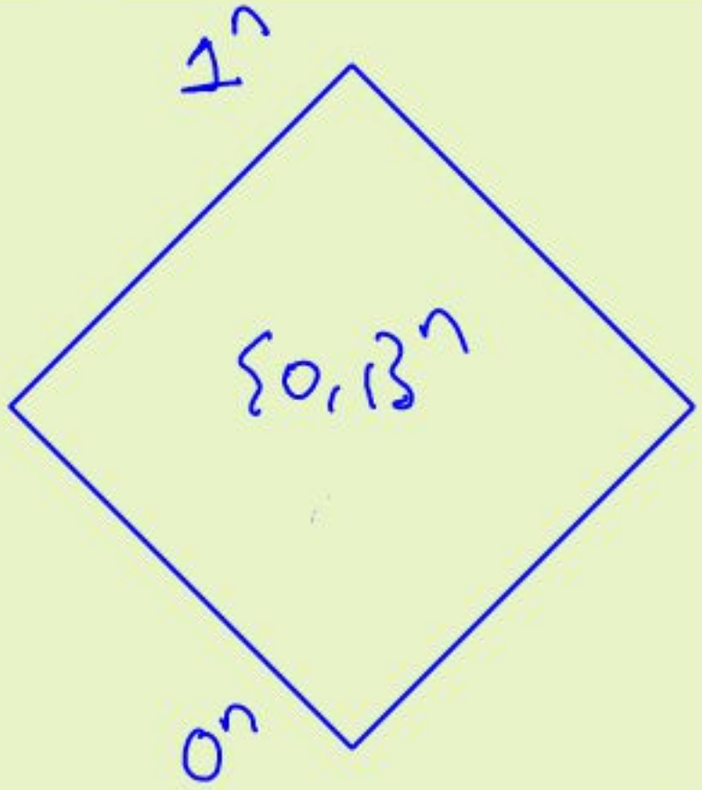
(DEPT. OF MATH., IIT BOMBAY)

OXFORD - WARWICK COMPLEXITY MEETINGS

Polynomials over the hypercube



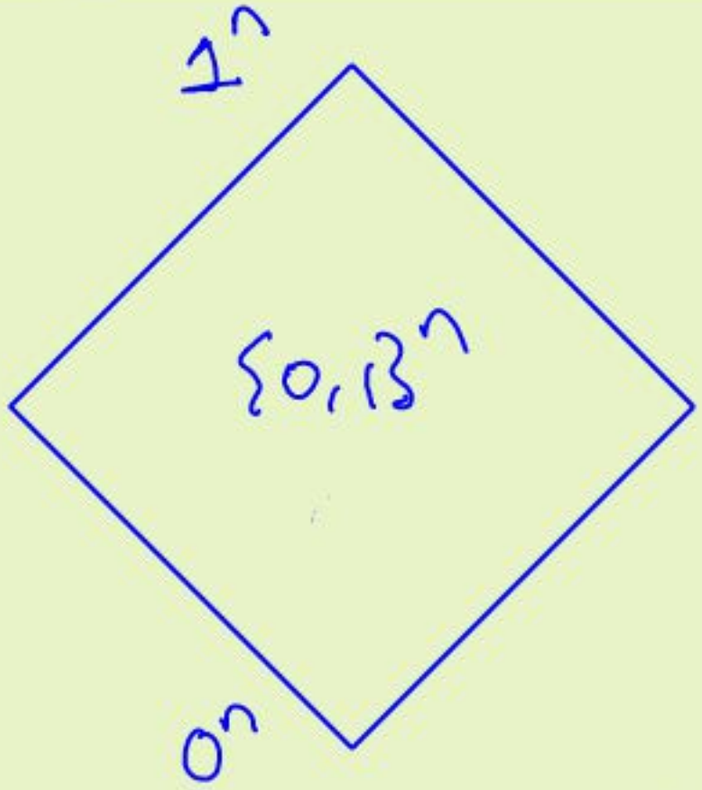
Polynomials over the hypercube



Combinatorial/algebraic properties of low degree polynomials over $\{0,1\}^n$

$R \in \mathbb{F}[x_1, \ldots, x_n]$

Polynomials over the hypercube

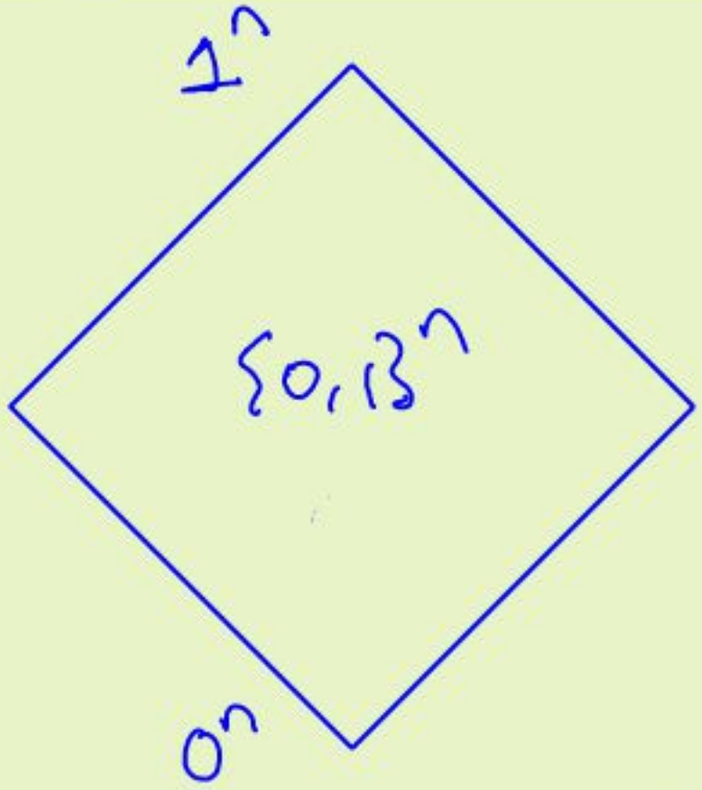


Useful in

Combinatorial/algebraic properties of low degree polynomials over $\{0,1\}^n$

$R \in \mathbb{F}[x_1, \ldots, x_n]$

Polynomials over the hypercube



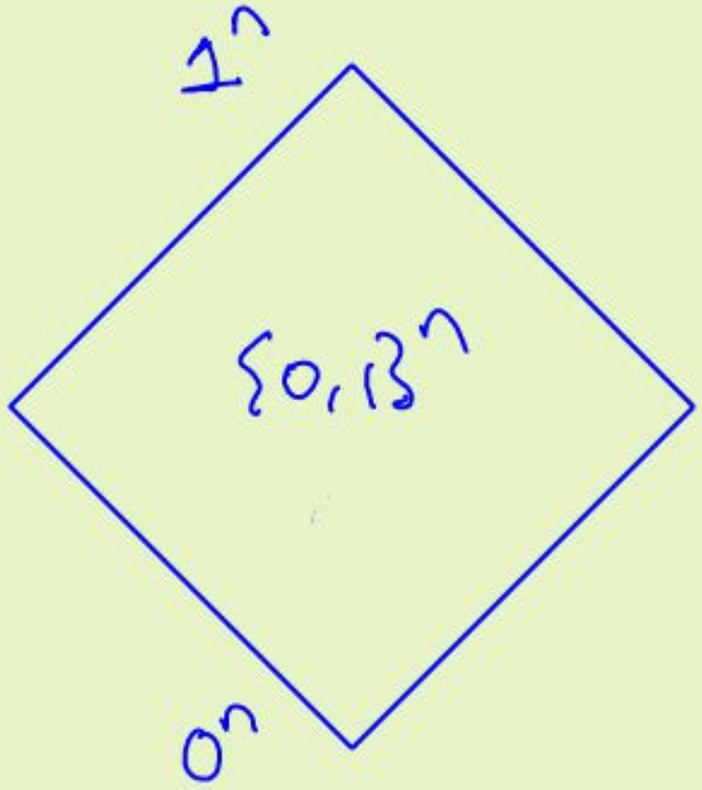
Useful in

1. Complexity theory
   - → Circuit complexity [Razborov '87]
   - → Derandomization [Braverman '10]

Combinatorial/algebraic properties of low degree polynomials over $\{0,1\}^n$

$R \in \mathbb{F}[x_1, \ldots, x_n]$

Polynomials over the hypercube



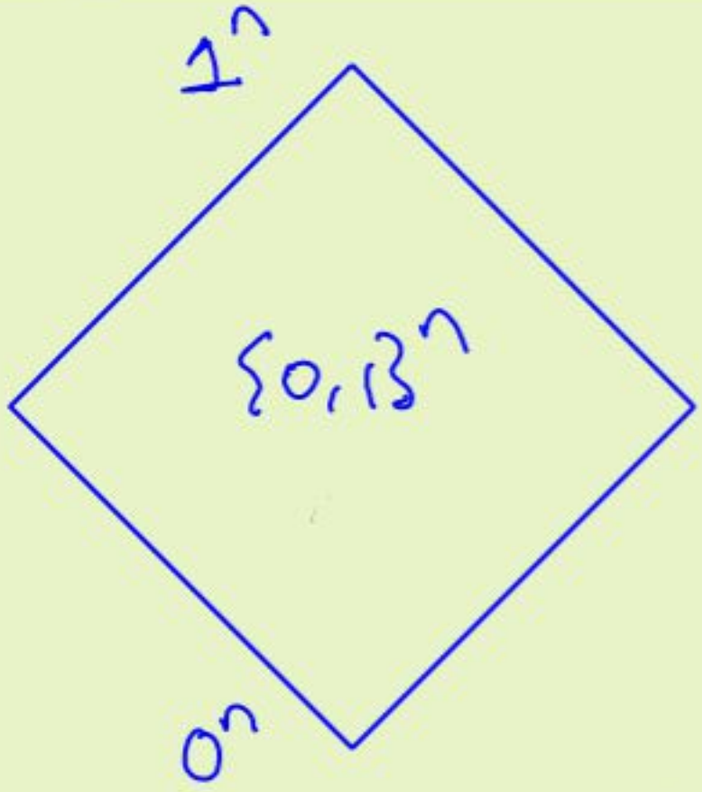
Combinatorial/algebraic properties of low degree polynomials over $\{0,1\}^n$

$R \in \mathbb{F}[x_1, \ldots, x_n]$

Useful in

1. Complexity theory
   - → Circuit complexity [Razborov '87]
   - → Derandomization [Braverman '10]
2. Learning theory [Klivans-Servedio '01]

Polynomials over the hypercube



Combinatorial/algebraic properties of low degree polynomials over $\{0,1\}^n$

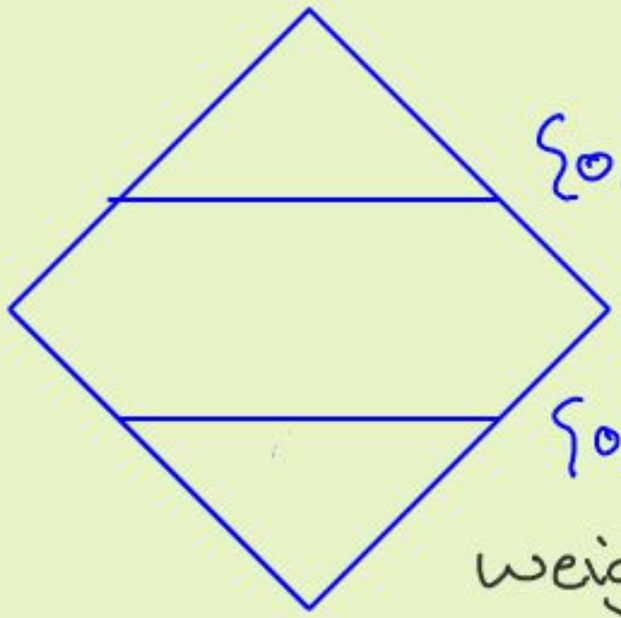
$R \in \mathbb{F}[x_1, \ldots, x_n]$

Useful in

1. Complexity theory
   → Circuit complexity [Razborov '87]
   → Derandomization [Braverman '10]
2. Learning theory [Klivans-Servedio '01]
3. Combinatorial algos [Williams '14]

Hegedüs's lemma

Hegedüs's lemma



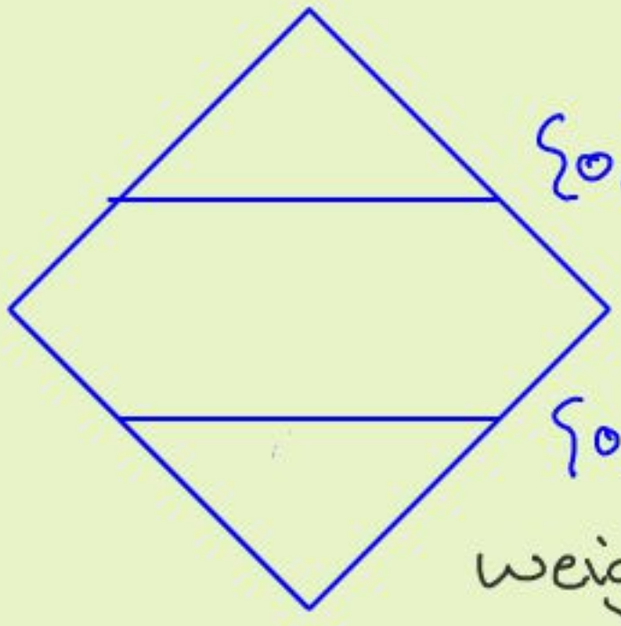
$\{0,1\}^n_{k+q}$

$\{0,1\}^n_k$

weight k

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



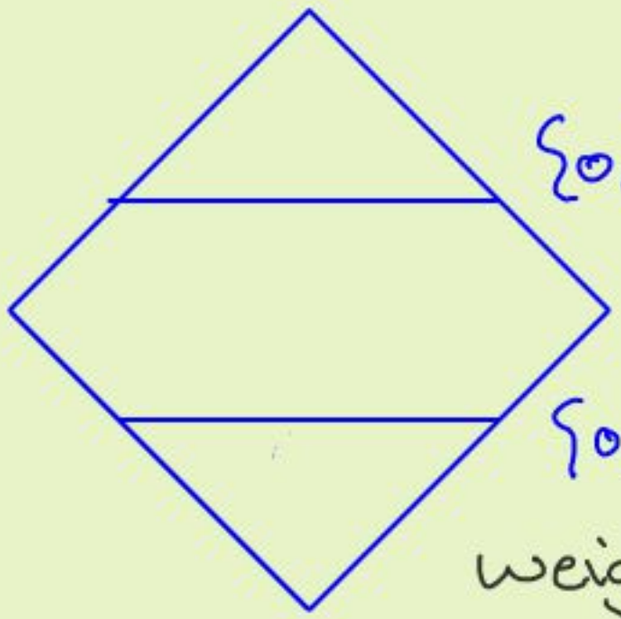
Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $|b| = k+q \Rightarrow R(b) \neq 0$

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

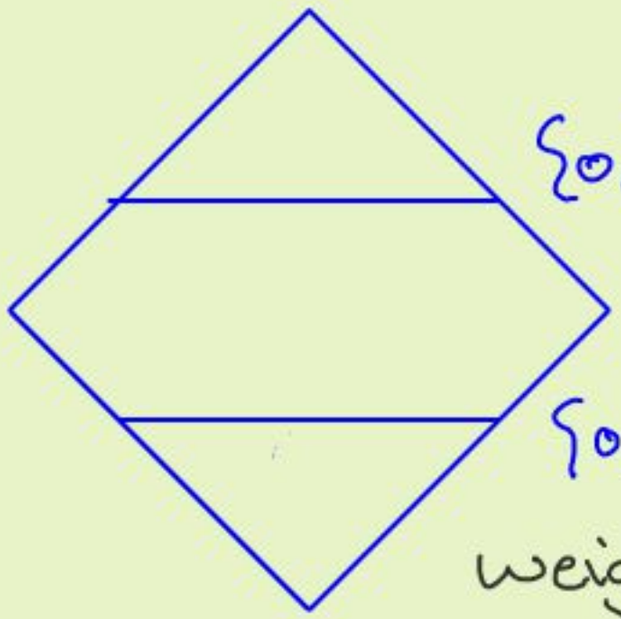
(I) $|a| = k \Rightarrow R(a) = 0$

(II) $|b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

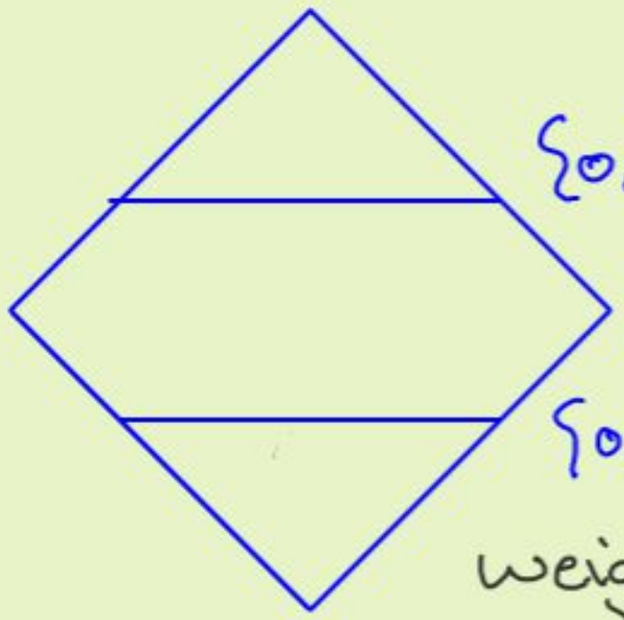
(II) $|b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$

$\mathbb{F} = \mathbb{R}$: $R(x_1, \dots, x_n) = \left(\sum_i x_i - k\right)$

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $|b| = k+q \Rightarrow R(b) \neq 0$

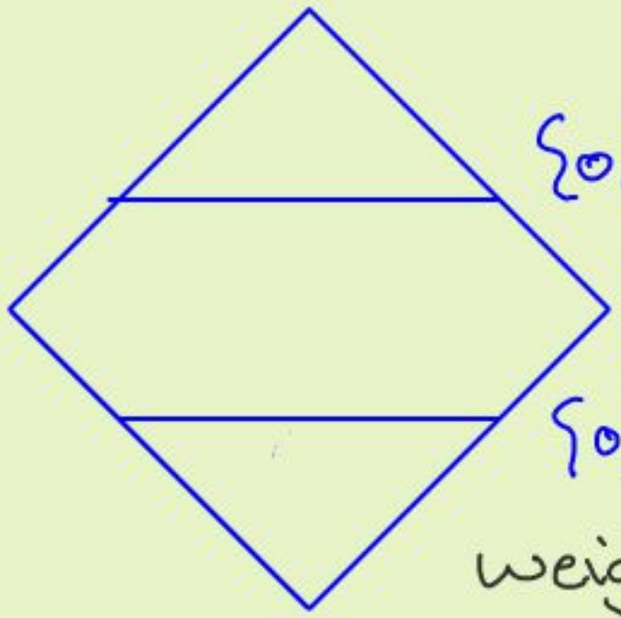
A: Depends on $\mathbb{F}$

$\mathbb{F} = \mathbb{Q}$: $R(x_1, \dots, x_n) = \left(\sum_i x_i - k\right)$

$\mathrm{char}(\mathbb{F}) = p$: Same construction if $p \nmid q$.

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

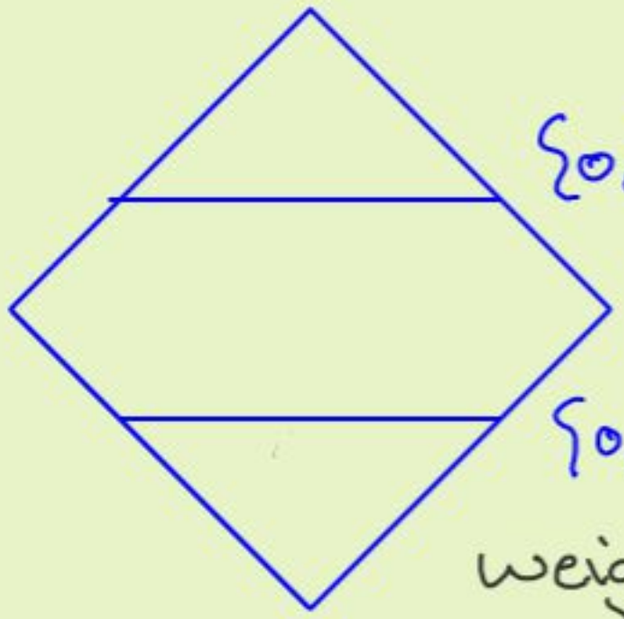
(II) $|b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$

$\mathrm{char}(\mathbb{F}) = p$, $q = p^s$:

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $|b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$

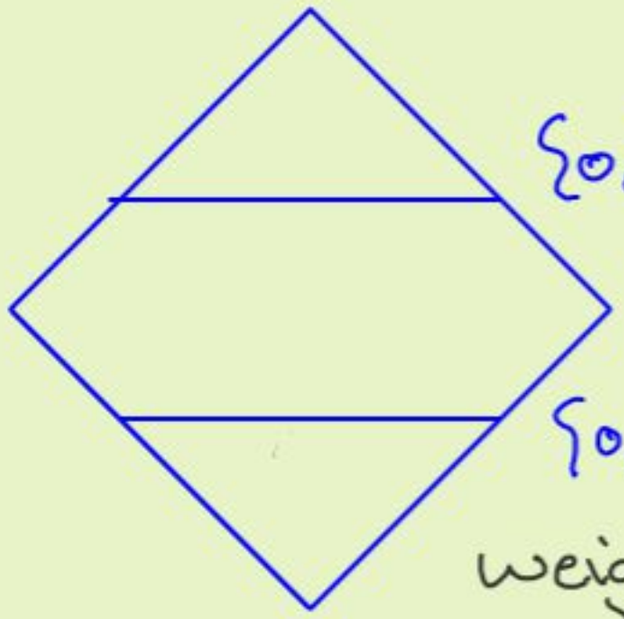
$\mathrm{char}(\mathbb{F}) = p$, $q = p^s$:

Elementary symm. poly. of deg. q

$$R(x_1, \dots, x_n) = \sum_{|I| = q} x^I$$

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$

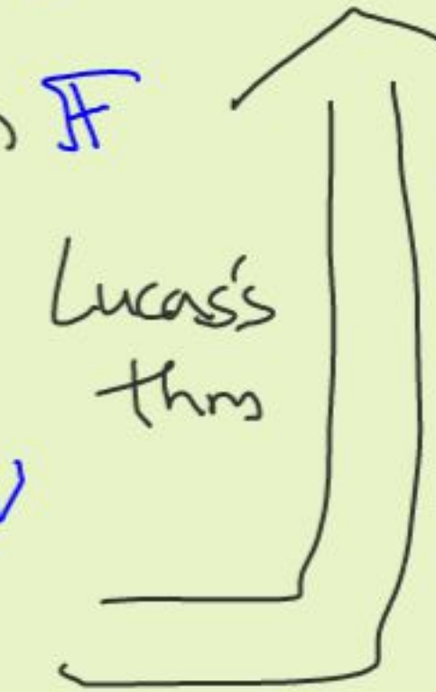


Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $|b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$



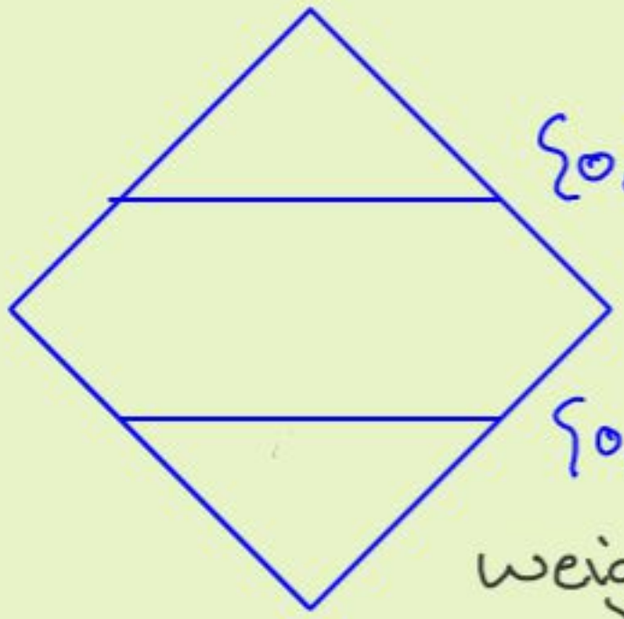
$\mathrm{char}(\mathbb{F}) = p$, $q = p^s$:

Elementary symm. poly. of deg. q

$$R(x_1, \dots, x_n) = \sum_{|I|=q} x^I$$

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$

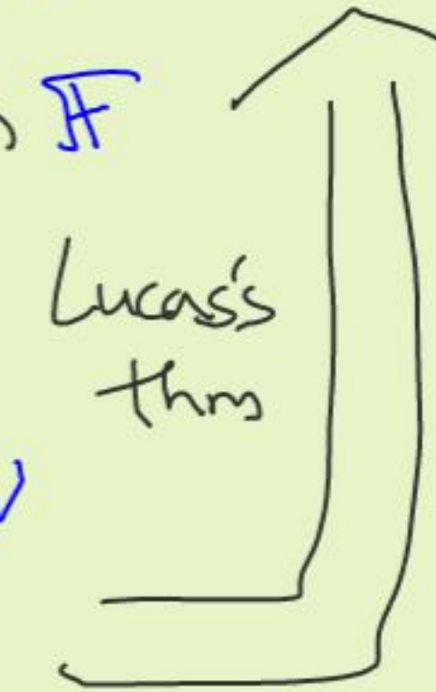


Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $|b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$



$\mathrm{char}(\mathbb{F}) = p$, $q = p^s$:

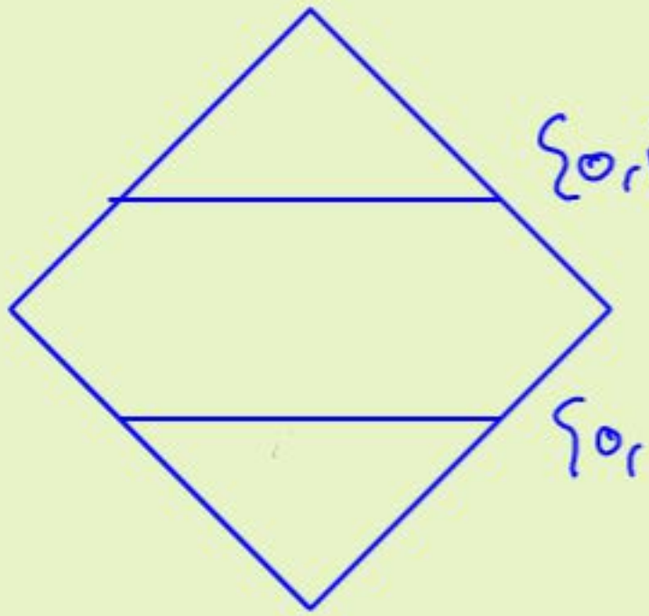
Elementary symm. poly. of deg. q

$$R(x_1, \dots, x_n) = \sum_{|I|=q} x^I$$

Hegedüs's lemma: This is tight.

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

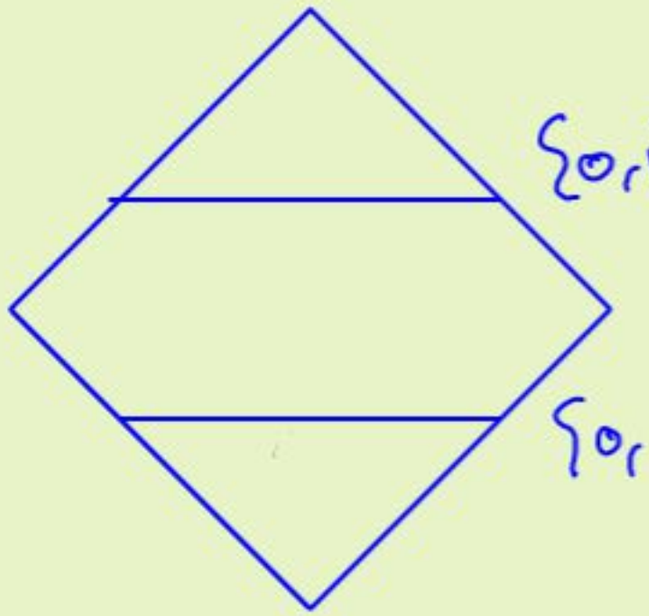
(II) $\exists b. |b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$

Hegedüs's lemma: $\mathrm{char}(\mathbb{F}) = p$, $q = p^s$, $q \leq k \leq n-q$

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $\exists b. |b| = k+q \Rightarrow R(b) \neq 0$

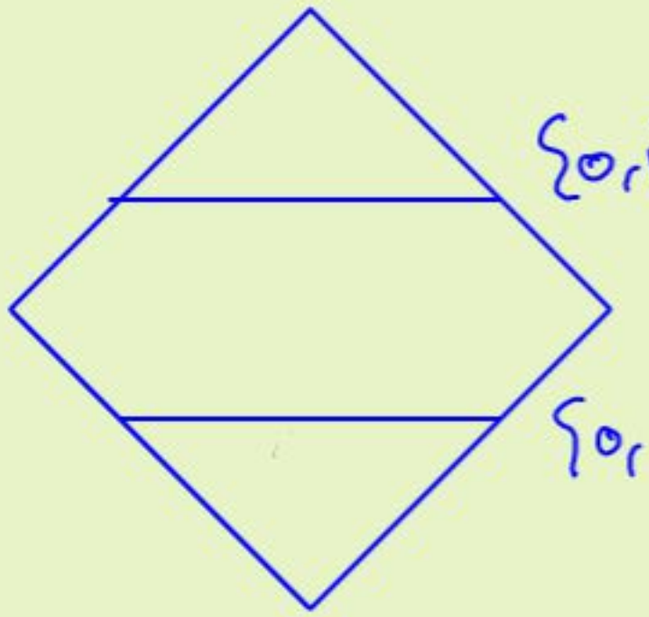
A: Depends on $\mathbb{F}$

Hegedüs's lemma: $\mathrm{char}(\mathbb{F}) = p$, $q = p^s$, $q \le k \le n-q$

$\deg(R) \geq q$.

Hegedüs's lemma

$\mathbb{F}[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $\exists b. |b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$

Hegedüs's lemma: $\mathrm{char}(\mathbb{F}) = p$, $q = p^s$, $q \le k \le n-q$

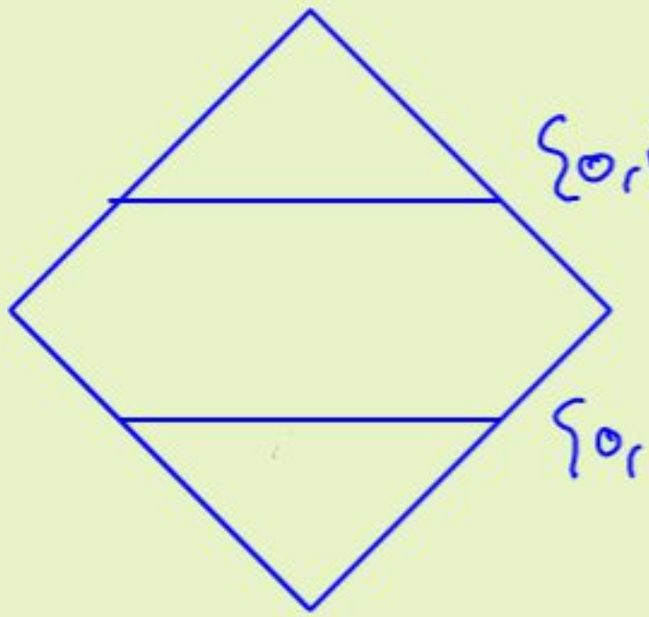
$\deg(R) \geq q$.

[Hegedüs '10] - Gröbner bases

[S'18, Alon'19] - Elementary

Hegedüs's lemma

$\mathbb{F}[x_1, \ldots, x_n]$



Q: lowest deg. $R(x_1, \ldots, x_n)$ s.t.

(I) $|a| = k \Rightarrow R(a) = 0$

(II) $\exists b. |b| = k+q \Rightarrow R(b) \neq 0$

A: Depends on $\mathbb{F}$

Hegedüs's lemma: $\text{char}(\mathbb{F}) = p$, $q = p^s$, $q \leq k \leq n-q$

$\deg(R) \geq q$.

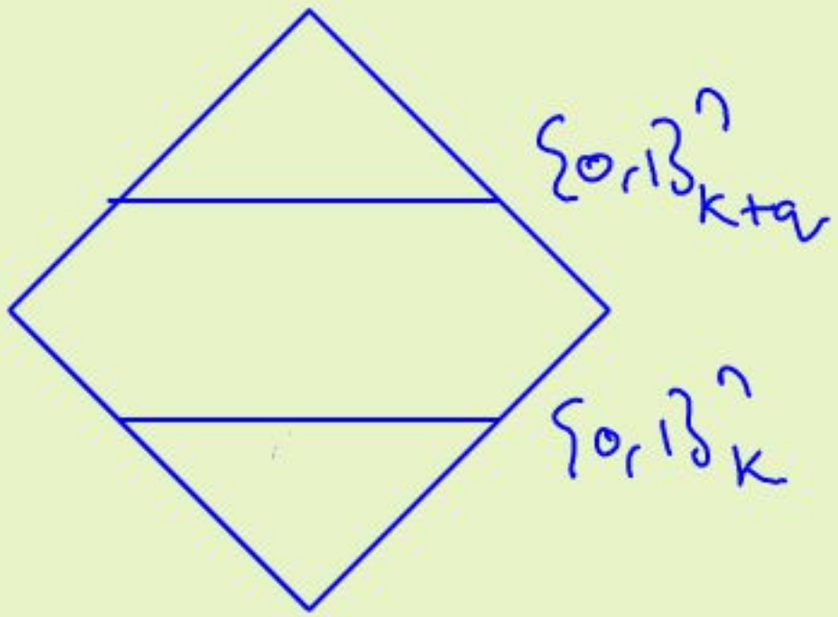
[Hegedüs '10] - Gröbner bases

[S'18, Alon'19] - Elementary

Applications

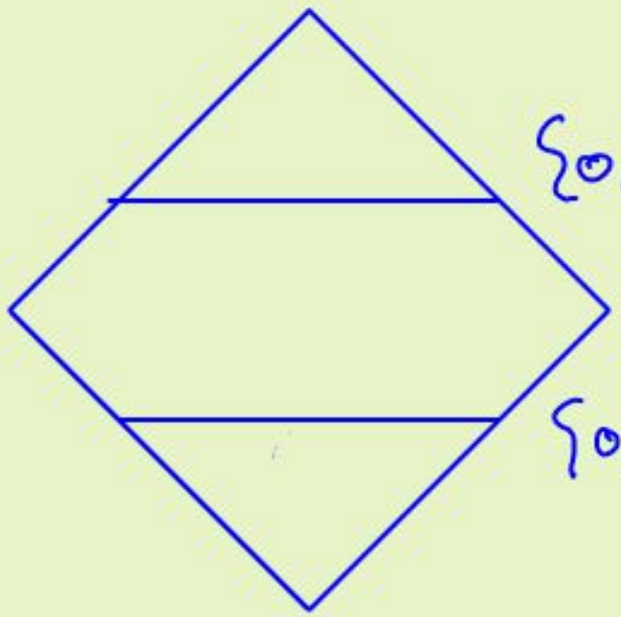
- Algebraic ckts [Alon-Kumar-Volk'18]
- Threshold ckts [Hrubeš et al. '19]

Robust Hegedüs



Robust Hegedüs

$F[x_1, \dots, x_n]$



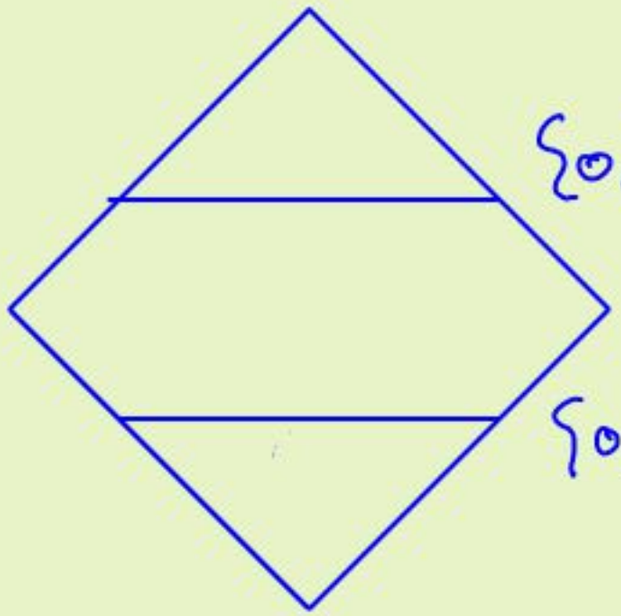
Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

Robust Hegedüs

$F[x_1, \dots, x_n]$



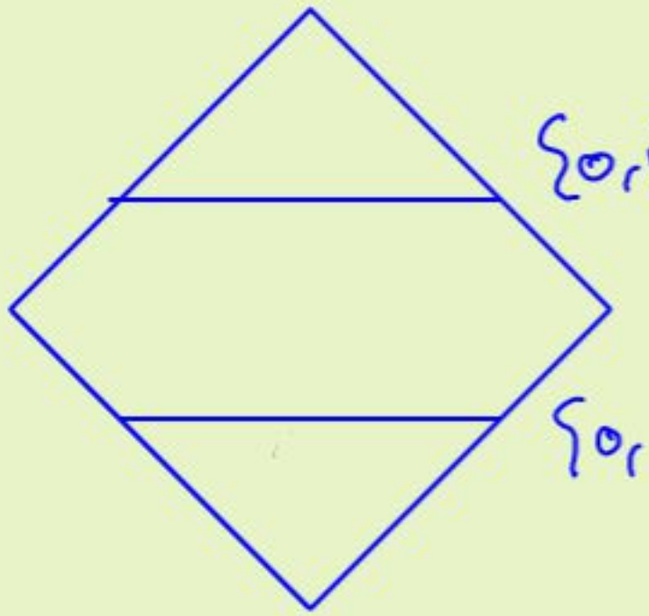
Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\mathrm{char}(F) = p$, $q = p^s$

Robust Hegedüs



$\mathbb{F}[x_1, \dots, x_n]$

Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

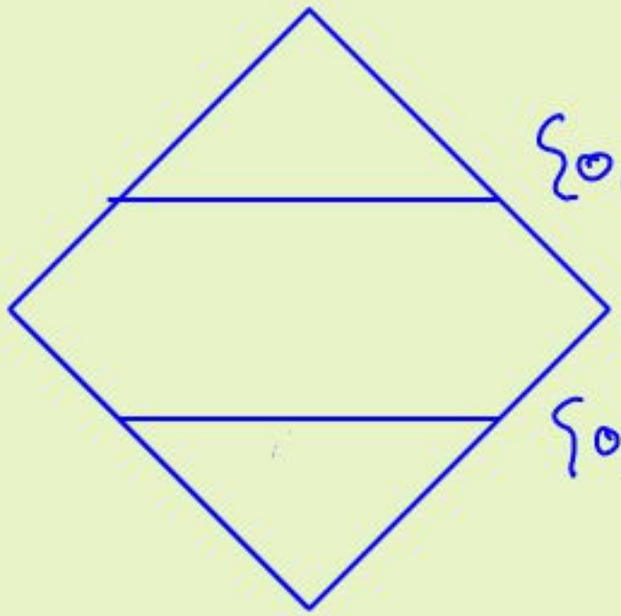
$\mathrm{char}(\mathbb{F}) = p$, $q = p^s$

Same lower bound (i.e. q)?

No!

Sampling construction

$F[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

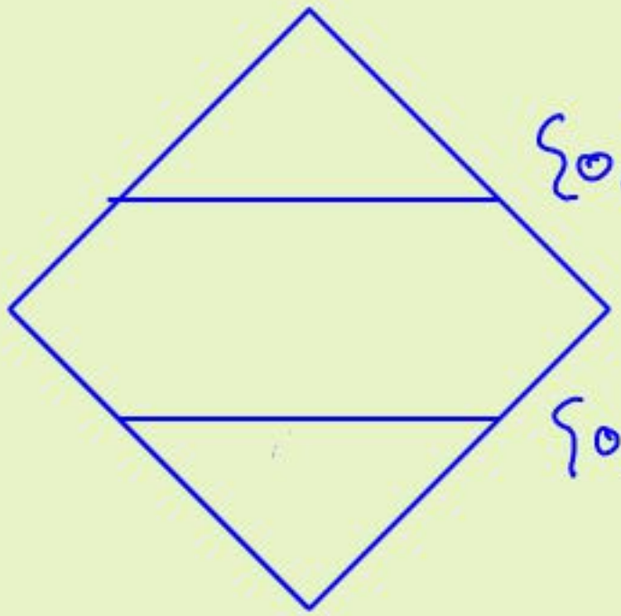
(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\text{char}(F) = p$, $q = p^s$

Say $k = 0.49n$, $k+q = 0.51n$.

Sampling construction

$F[x_1, \dots, x_n]$



Q: lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

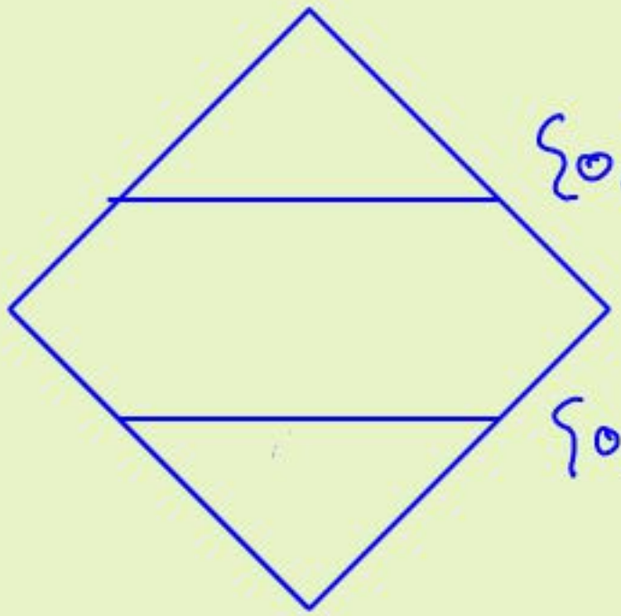
$\text{char}(F) = p$, $q = p^s$

Say $k = 0.49n$, $k+q = 0.51n$.

$R(x_1, \dots, x_n) = \text{Maj}_t(x_1, \dots, x_t)$

Sampling construction

$F[x_1, \dots, x_n]$



Q: Lowest deg. $R(x_1, \dots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\text{char}(F) = p$, $q = p^s$

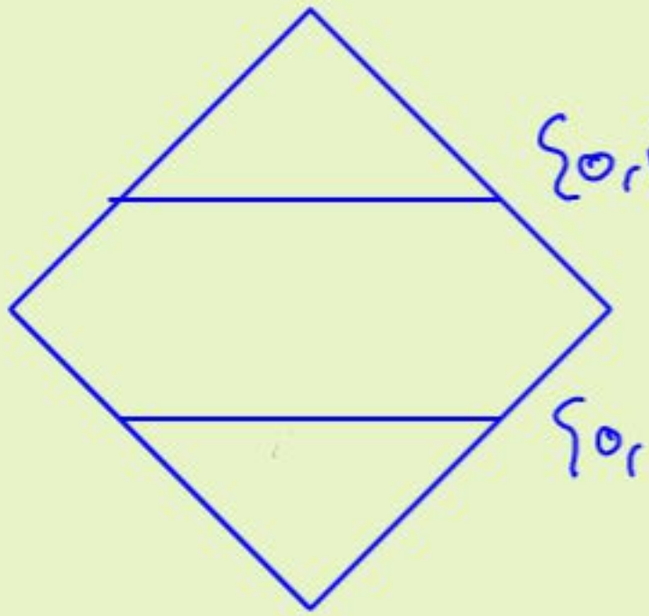
Say $k = 0.49n$, $k+q = 0.51n$.

$R(x_1, \dots, x_n) = \text{Maj}_t(x_1, \dots, x_t)$

(A) Satisfies above when $t = \Theta(\log 1/\varepsilon)$.

Sampling construction

$\mathbb{F}[x_1, \cdots, x_n]$



Q: lowest deg. $R(x_1, \cdots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\text{char}(\mathbb{F}) = p$, $q = p^s$

Say $k = 0.49n$, $k+q = 0.51n$.

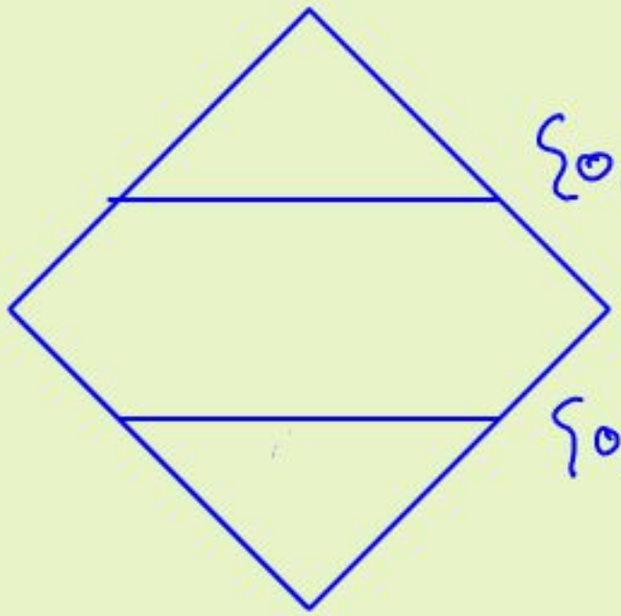
$R(x_1, \cdots, x_n) = \text{Maj}_t(x_1, \cdots, x_t)$

(A) Satisfies above when $t = \Theta(\log 1/\varepsilon)$.

(B) deg $t = \Theta(\log 1/\varepsilon)$.

Main lemma

$\mathbb{F}[x_1, \cdots, x_n]$



Q: lowest deg. $R(x_1, \cdots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

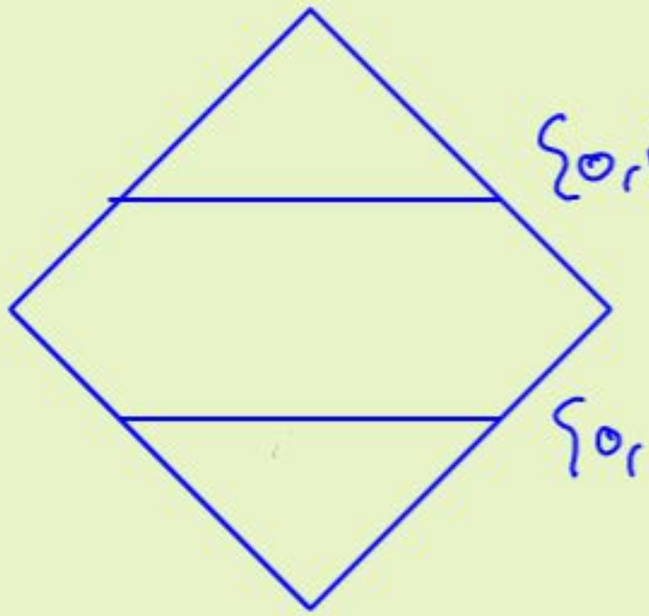
(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\mathrm{char}(\mathbb{F}) = p, \; q = p^s$

Main Result: $\deg(R) = \Omega(\min\{\text{sampling bound}, q\})$

Main lemma

$\mathbb{F}[x_1, \cdots, x_n]$



Q: lowest deg. $R(x_1, \cdots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\text{char}(\mathbb{F}) = p, \; q = p^s$

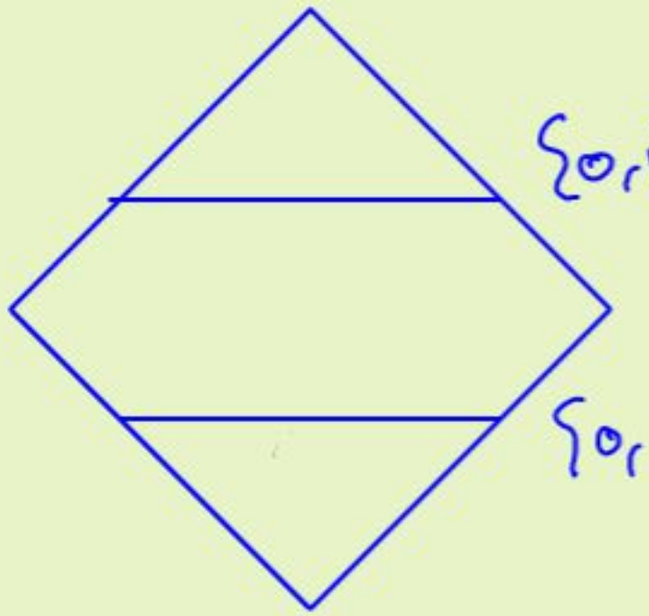
Main Result: $\deg(R) = \Omega(\min\{\text{sampling bound}, q\})$

Eg: $k = n/2 - \sqrt{n \log 1/\varepsilon}$

$k+q = n/2$

Main lemma

$\mathbb{F}[x_1, \cdots, x_n]$



Q: lowest deg. $R(x_1, \cdots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\text{char}(\mathbb{F}) = p, \; q = p^s$

Main Result: $\deg(R) = \Omega(\min\{\text{sampling bound}, q\})$

Eg: $k = n/2 - \sqrt{n \log 1/\varepsilon} \Rightarrow \deg(R) = \Omega(\sqrt{n \log 1/\varepsilon})$

$k+q = n/2$

Applications

Applications

1. Optimal degree lower bounds for the Coin Problem.

Applications

1. Optimal degree lower bounds for the Coin Problem.
2. Optimal probabilistic degree lower bounds for all symmetric functions.

Applications

1. Optimal degree lower bounds for the Coin Problem.
2. Optimal probabilistic degree lower bounds for all symmetric functions.
3. Robust version of Galvin's problem.

Applications

1. Optimal degree lower bounds for the Coin Problem.

2. Optimal probabilistic degree lower bounds for all symmetric functions.

3. Robust version of Galvin's problem.

Probabilistic polynomials

Probabilistic polynomials

$f : \{0,1\}^n \to \{0,1\}$

$\mathcal{P} = \{P_1, \ldots, P_r\}$ – polys of deg. $\leq d$

Probabilistic polynomials

$$f : \{0,1\}^n \to \{0,1\}$$

$\mathcal{P} = \{P_1, \ldots, P_r\}$ – polys of deg. $\leq d$

Def: $\mathcal{P}$ an ε-error probabilistic poly. for f if:

$$\forall x : \Pr_{P \sim \mathcal{P}}[P(x) \neq f(x)] \leq \varepsilon$$

Probabilistic polynomials

$f : \{0,1\}^n \to \{0,1\}$

$\mathbb{P} = \{P_1, \ldots, P_r\}$ - polys of deg. $\leq d$

Def: $\mathbb{P}$ an ε-error probabilistic poly. for f if:

$\forall x : \Pr_{P \sim \mathbb{P}}[P(x) \neq f(x)] \leq \varepsilon \Rightarrow \mathrm{pdeg}_{\varepsilon}(f) \leq d$

Probabilistic polynomials

$f : \{0,1\}^n \to \{0,1\}$

$\mathbb{P} = \{P_1, \ldots, P_r\}$ - polys of deg. $\leq d$

Def: $\mathbb{P}$ an ε-error probabilistic poly. for f if:

$\forall x : \Pr_{P \sim \mathbb{P}}[P(x) \neq f(x)] \leq \varepsilon \Rightarrow \mathrm{pdeg}_{\varepsilon}(f) \leq d$

→ Introduced by Razborov (1987)

Probabilistic polynomials

$f : \{0,1\}^n \to \{0,1\}$

$\mathbb{P} = \{P_1, \ldots, P_r\}$ – polys of deg. $\leq d$

Def: $\mathbb{P}$ an ε-error probabilistic poly. for f if:

$\forall x : \Pr_{P \sim \mathbb{P}}[P(x) \neq f(x)] \leq \varepsilon \Rightarrow \text{pdeg}_\varepsilon(f) \leq d$

→ Introduced by Razborov (1987)

→ Used to prove lower bounds for $AC^0[MOD_p]$ ckts.

Upper & lower bounds on pdeg

→ Razborov '87: $\mathrm{pdeg}_{1/10}(OR_n) = O(1)$

$\mathrm{pdeg}_{1/10}(\text{a symmetric } f) = \Omega(\sqrt{n})$.

Upper & lower bounds on pdeg

→ Razborov '87: $\mathrm{pdeg}_{1/10}(OR_n) = O(1)$

$\mathrm{pdeg}_{1/10}(\text{a symmetric } f) = \Omega(\sqrt{n})$.

→ Smolensky '87: $\mathrm{pdeg}_{1/10}(Maj_n)$, $\mathrm{pdeg}_{1/10}(MOD_n^q) = \Omega(\sqrt{n})$

Upper & lower bounds on pdeg

→ Razborov '87: $\mathrm{pdeg}_{1/10}(OR_n) = O(1)$

$\mathrm{pdeg}_{1/10}(\text{a symmetric } f) = \Omega(\sqrt{n})$.

→ Smolensky '87: $\mathrm{pdeg}_{1/10}(Maj_n)$, $\mathrm{pdeg}_{1/10}(MOD_n^q) = \Omega(\sqrt{n})$

→ S. '13: $\mathrm{pdeg}_{1/10}(\text{any symmetric } f) = \widetilde{O}(\sqrt{n})$

Upper & lower bounds on pdeg

→ Razborov '87: $\mathrm{pdeg}_{1/10}(OR_n) = O(1)$

$\mathrm{pdeg}_{1/10}(\text{a symmetric } f) = \Omega(\sqrt{n})$.

→ Smolensky '87: $\mathrm{pdeg}_{1/10}(Maj_n)$, $\mathrm{pdeg}_{1/10}(MOD_n^q) = \Omega(\sqrt{n})$

→ S. '13: $\mathrm{pdeg}_{1/10}(\text{any symmetric } f) = \tilde{O}(\sqrt{n})$

→ Aaronson- '15: $\mathrm{pdeg}_{1/10}(\text{any symmetric } f) = O(\sqrt{n})$
Williams

Upper & lower bounds on pdeg

→ Razborov '87: $\mathrm{pdeg}_{1/10}(OR_n) = O(1)$

$\mathrm{pdeg}_{1/10}(\text{a symmetric } f) = \Omega(\sqrt{n})$.

→ Smolensky '87: $\mathrm{pdeg}_{1/10}(Maj_n)$, $\mathrm{pdeg}_{1/10}(MOD_n^q) = \Omega(\sqrt{n})$

→ S. '13: $\mathrm{pdeg}_{1/10}(\text{any symmetric } f) = \tilde{O}(\sqrt{n})$

→ Aaronson- '15: $\mathrm{pdeg}_{1/10}(\text{any symmetric } f) = O(\sqrt{n})$
Williams

→ Algorithmic applications

Tight bounds on pdeg of any symmetric f?

Tight bounds on pdeg of any symmetric f?

S.-Tripathi-Venkitesh'19: Upper bounds for any symmetric f

Theorem 8 (Known upper bounds on probabilistic degree of symmetric functions [STV19]). *Let $\mathbb{F}$ be a field of constant characteristic $p > 0$ and $n \in \mathbb{N}$ be a growing parameter. Let $f \in s\mathcal{B}_n$ be arbitrary and let (g, h) be a standard decomposition of f. Then we have the following for any $\varepsilon > 0$.*

1. *If* $\mathrm{per}(g) = 1$, *then* $\mathrm{pdeg}_\varepsilon(g) = 0$.
   If $\mathrm{per}(g)$ *is a power of* p, *then* $\mathrm{pdeg}^{\mathbb{F}}_\varepsilon(g) \leq \mathrm{per}(g)$,
2. $\mathrm{pdeg}_\varepsilon(h) = O(\sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon))$ *if* $B(h) \geq 1$ *and* 0 *otherwise, and*
3. $$\mathrm{pdeg}_\varepsilon(f) = \begin{cases} O(\sqrt{n\log(1/\varepsilon)}) & \text{if } \mathrm{per}(g) > 1 \text{ and not a power of } p, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g)\}) & \text{if } \mathrm{per}(g) \text{ a power of } p \text{ and } B(h) = 0, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g) + \\ \quad \sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon)\}) & \text{otherwise.} \end{cases}$$

Tight bounds on pdeg of any symmetric f?

S.-Tripathi-Venkitesh'19: Upper bounds for any symmetric f

Theorem 8 (Known upper bounds on probabilistic degree of symmetric functions [STV19]). *Let $\mathbb{F}$ be a field of constant characteristic $p > 0$ and $n \in \mathbb{N}$ be a growing parameter. Let $f \in s\mathcal{B}_n$ be arbitrary and let (g, h) be a standard decomposition of f. Then we have the following for any $\varepsilon > 0$.*

1. *If* $\mathrm{per}(g) = 1$, *then* $\mathrm{pdeg}_\varepsilon(g) = 0$.
   If $\mathrm{per}(g)$ *is a power of* p, *then* $\mathrm{pdeg}^{\mathbb{F}}_\varepsilon(g) \leq \mathrm{per}(g)$,
2. $\mathrm{pdeg}_\varepsilon(h) = O(\sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon))$ *if* $B(h) \geq 1$ *and* 0 *otherwise, and*
3. $$\mathrm{pdeg}_\varepsilon(f) = \begin{cases} O(\sqrt{n\log(1/\varepsilon)}) & \text{if } \mathrm{per}(g) > 1 \text{ and not a power of } p, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g)\}) & \text{if } \mathrm{per}(g) \text{ a power of } p \text{ and } B(h) = 0, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g) + \\ \quad \sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon)\}) & \text{otherwise.} \end{cases}$$

Also: nearly matching lower bounds.

Tight bounds on pdeg of any symmetric f?

S.-Tripathi-Venkitesh'19: Upper bounds for any symmetric f

Theorem 8 (Known upper bounds on probabilistic degree of symmetric functions [STV19]). *Let $\mathbb{F}$ be a field of constant characteristic $p > 0$ and $n \in \mathbb{N}$ be a growing parameter. Let $f \in s\mathcal{B}_n$ be arbitrary and let (g, h) be a standard decomposition of f. Then we have the following for any $\varepsilon > 0$.*

1. *If* $\mathrm{per}(g) = 1$, *then* $\mathrm{pdeg}_\varepsilon(g) = 0$.
   If $\mathrm{per}(g)$ *is a power of* p, *then* $\mathrm{pdeg}^{\mathbb{F}}_\varepsilon(g) \leq \mathrm{per}(g)$,
2. $\mathrm{pdeg}_\varepsilon(h) = O(\sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon))$ *if* $B(h) \geq 1$ *and* 0 *otherwise, and*
3. $$\mathrm{pdeg}_\varepsilon(f) = \begin{cases} O(\sqrt{n\log(1/\varepsilon)}) & \text{if } \mathrm{per}(g) > 1 \text{ and not a power of } p, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g)\}) & \text{if } \mathrm{per}(g) \text{ a power of } p \text{ and } B(h) = 0, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g) + \\ \quad \sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon)\}) & \text{otherwise.} \end{cases}$$

Also: nearly matching lower bounds.
↳ off by poly log. factors.

Tight bounds on pdeg of any symmetric f?

S.-Tripathi-Venkitesh'19: Upper bounds for any symmetric f

Theorem 8 (Known upper bounds on probabilistic degree of symmetric functions [STV19]). *Let $\mathbb{F}$ be a field of constant characteristic $p > 0$ and $n \in \mathbb{N}$ be a growing parameter. Let $f \in s\mathcal{B}_n$ be arbitrary and let (g, h) be a standard decomposition of f. Then we have the following for any $\varepsilon > 0$.*

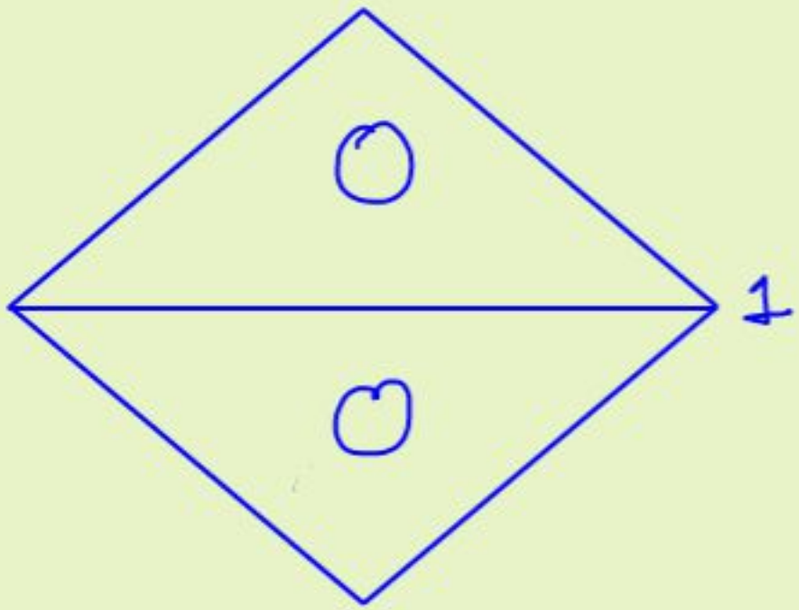
1. *If* $\mathrm{per}(g) = 1$, *then* $\mathrm{pdeg}_\varepsilon(g) = 0$.
   If $\mathrm{per}(g)$ *is a power of* p, *then* $\mathrm{pdeg}^{\mathbb{F}}_\varepsilon(g) \leq \mathrm{per}(g)$,
2. $\mathrm{pdeg}_\varepsilon(h) = O(\sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon))$ *if* $B(h) \geq 1$ *and* 0 *otherwise, and*
3. $$\mathrm{pdeg}_\varepsilon(f) = \begin{cases} O(\sqrt{n\log(1/\varepsilon)}) & \text{if } \mathrm{per}(g) > 1 \text{ and not a power of } p, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g)\}) & \text{if } \mathrm{per}(g) \text{ a power of } p \text{ and } B(h) = 0, \\ O(\min\{\sqrt{n\log(1/\varepsilon)}, \mathrm{per}(g) + \sqrt{B(h)\log(1/\varepsilon)} + \log(1/\varepsilon)\}) & \text{otherwise.} \end{cases}$$

Also: nearly matching lower bounds.

↳ off by poly log. factors.

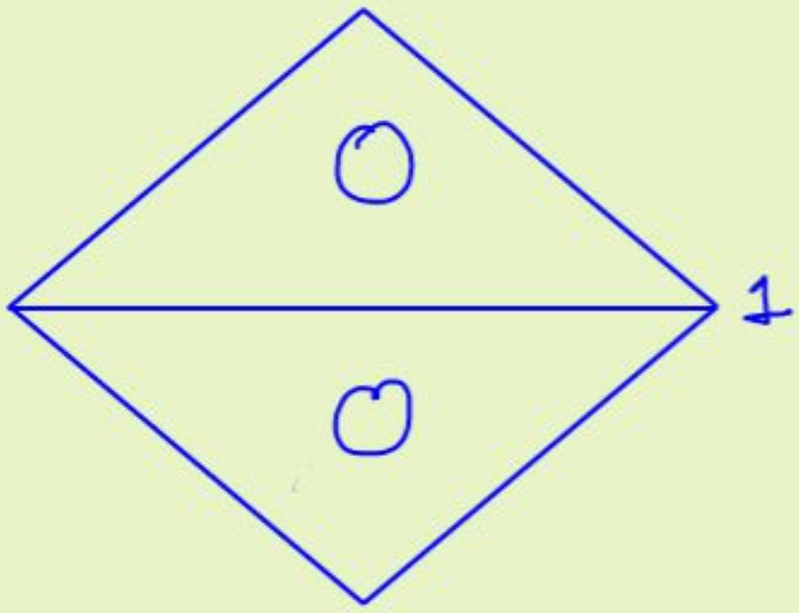
This paper: Tight bounds for all symmetric fns

Example: $ETHR_n^{n/2}$



$pdeg_\varepsilon(ETHR_n^{n/2}) = ?$

Example: $ETHR_n^{n/2}$

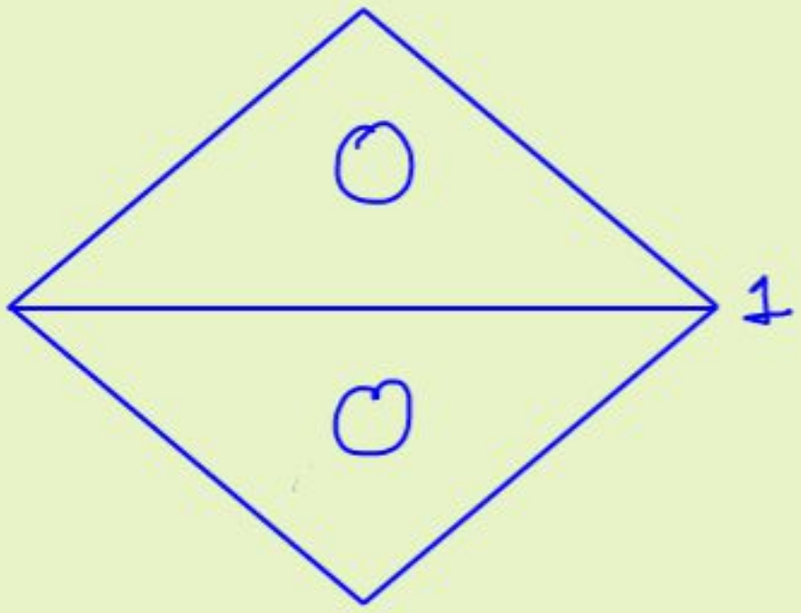


$$pdeg_{\varepsilon}(ETHR_n^{n/2}) = ?$$

[STV'19]:

$$Maj_{n/2}(x) = \sum_{i=0}^{n/4-1} ETHR_n^{n/2}(x 1^i 0^{n/2-i})$$

Example: $ETHR_n^{n/2}$



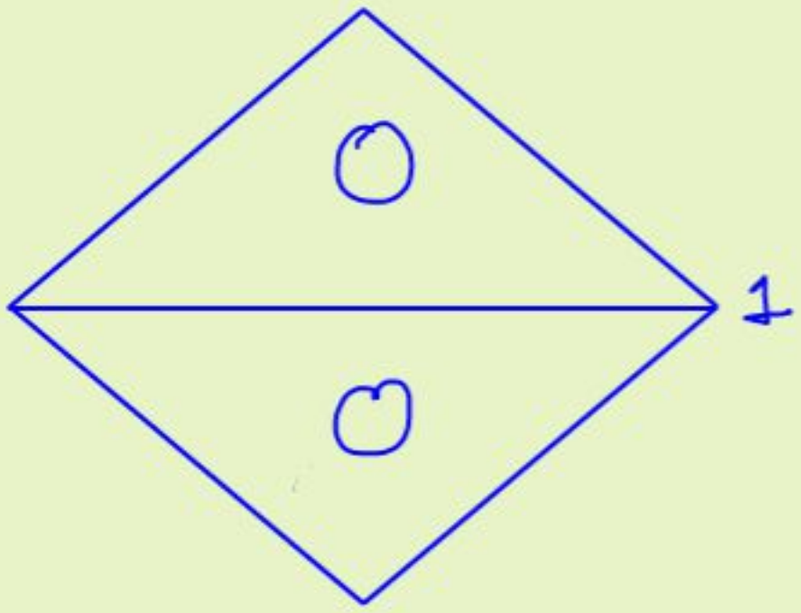
$pdeg_\varepsilon(ETHR_n^{n/2}) = ?$

[STV'19]:

$$Maj_{n/2}(x) = \sum_{i=0}^{n/4-1} ETHR_n^{n/2}(x 1^i 0^{n/2-i})$$

$$\Rightarrow pdeg_\varepsilon(Maj_{n/2}(x)) \leq pdeg_{\varepsilon/n}(ETHR_n^{n/2})$$
$$\leq pdeg_\varepsilon(ETHR_n^{n/2}) \cdot \log n$$

Example: $ETHR_n^{n/2}$



$pdeg_\varepsilon(ETHR_n^{n/2}) = ?$

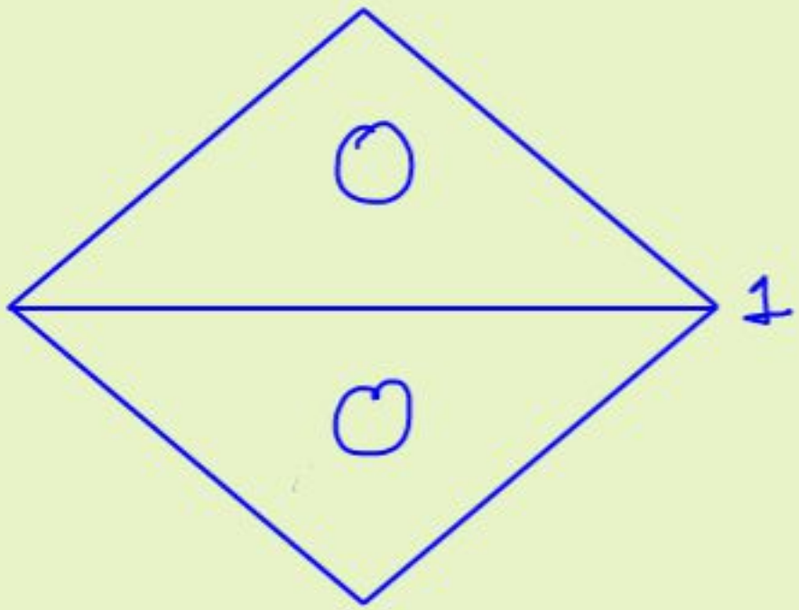
[STV'19]:

$$Maj_{n/2}(x) = \sum_{i=0}^{n/4-1} ETHR_n^{n/2}(x 1^i 0^{n/2-i})$$

$$\Rightarrow pdeg_\varepsilon(Maj_{n/2}(x)) \leq pdeg_{\varepsilon/n}(ETHR_n^{n/2}) \leq pdeg_\varepsilon(ETHR_n^{n/2}) \cdot \log n$$

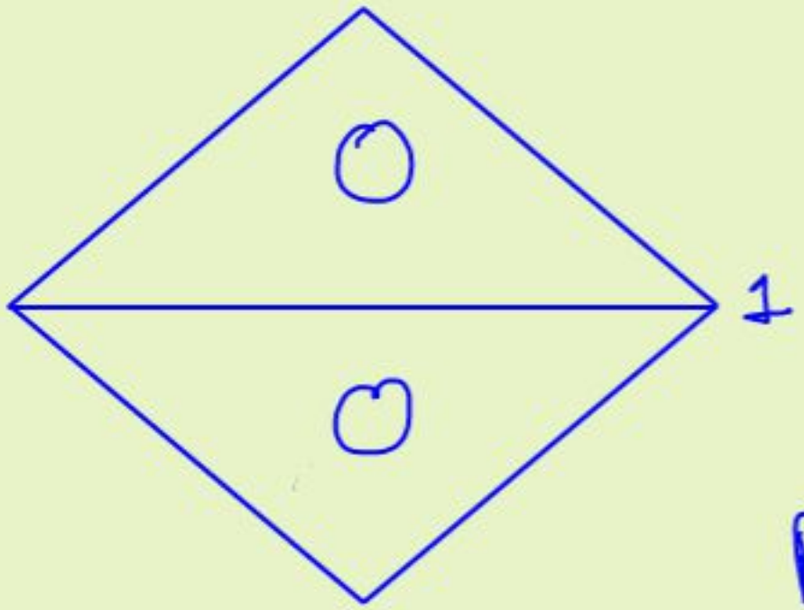
$$\Rightarrow pdeg_\varepsilon(ETHR_n^{n/2}) = \widetilde{\Omega}(\sqrt{n})$$

Example: $ETHR_n^{n/2}$



$pdeg_\varepsilon(ETHR_n^{n/2}) = ?$

Example: $ETHR_n^{n/2}$

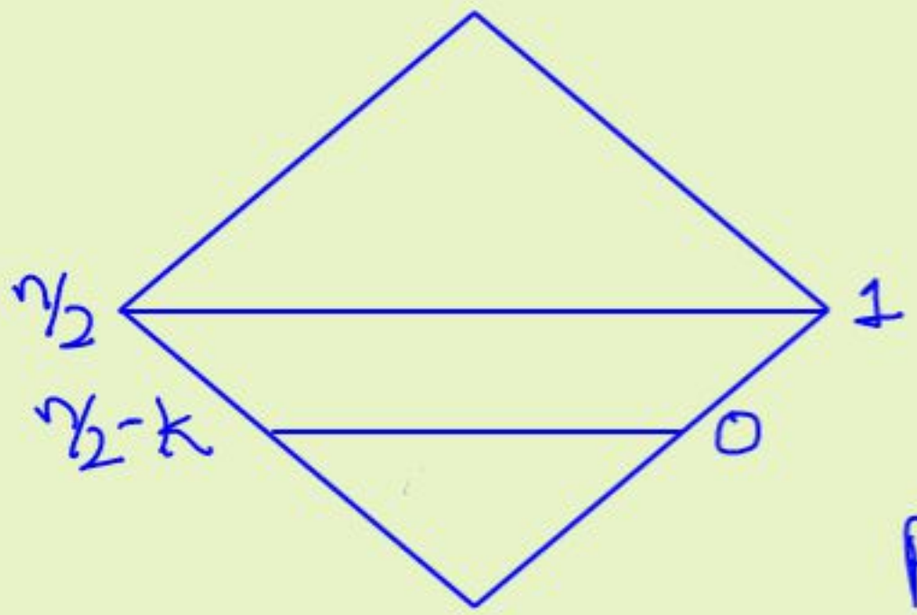


$pdeg_\varepsilon(ETHR_n^{n/2}) = ?$

$\mathbb{P} = \{P_1, \ldots, P_r\}$

$P \sim \mathbb{P}$ $\quad Pr\left[P(x) \neq ETHR_n^{n/2}(x)\right] \leq \varepsilon$

Example: $ETHR_n^{n/2}$

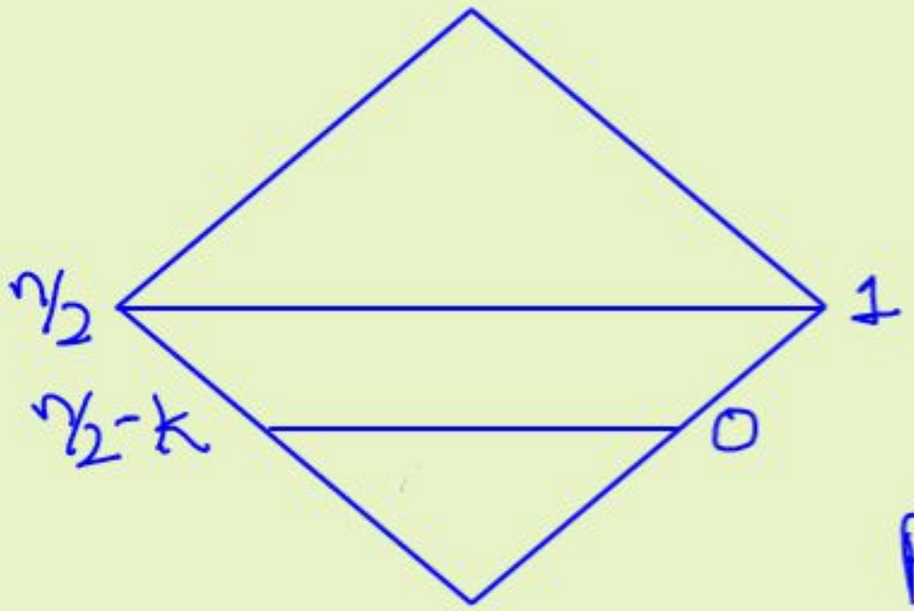


$$pdeg_{\varepsilon}(ETHR_n^{n/2}) = ?$$

$$\mathbb{P} = \{P_1, \ldots, P_r\}$$

$$Pr_{P \sim \mathbb{P}}[P(x) \neq ETHR_n^{n/2}(x)] \leq \varepsilon$$

Example: $ETHR_n^{n/2}$



$$pdeg_\varepsilon(ETHR_n^{n/2}) = ?$$

$$\mathbb{P} = \{P_1, \ldots, P_r\}$$

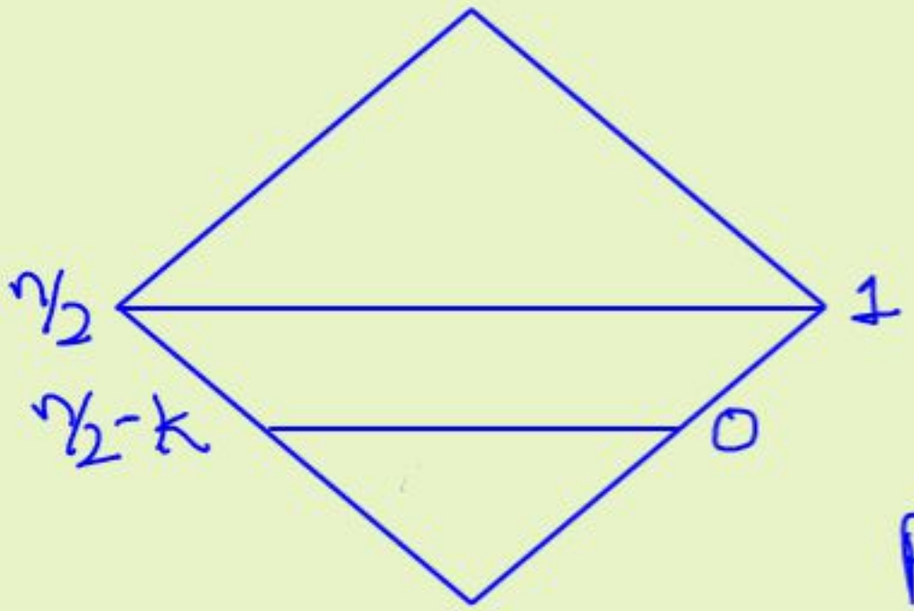
$$Pr_{P \sim \mathbb{P}}\left[P(x) \neq ETHR_n^{n/2}(x)\right] \leq \varepsilon$$

By averaging, $\exists P \in \mathbb{P}$ such that

$$Pr_{x \sim \{0,1\}^n_{n/2}}\left[P(x) \neq 1\right] < 2\varepsilon$$

$$Pr_{x \sim \{0,1\}^n_{n/2-k}}\left[P(x) \neq 0\right] < 2\varepsilon$$

Example: $ETHR_n^{n/2}$



$pdeg_\varepsilon(ETHR_n^{n/2}) = ?$

$\mathbb{P} = \{P_1, \dots, P_r\}$

$\Pr_{P \sim \mathbb{P}}[P(x) \neq ETHR_n^{n/2}(x)] \leq \varepsilon$

By averaging, $\exists P \in \mathbb{P}$ such that

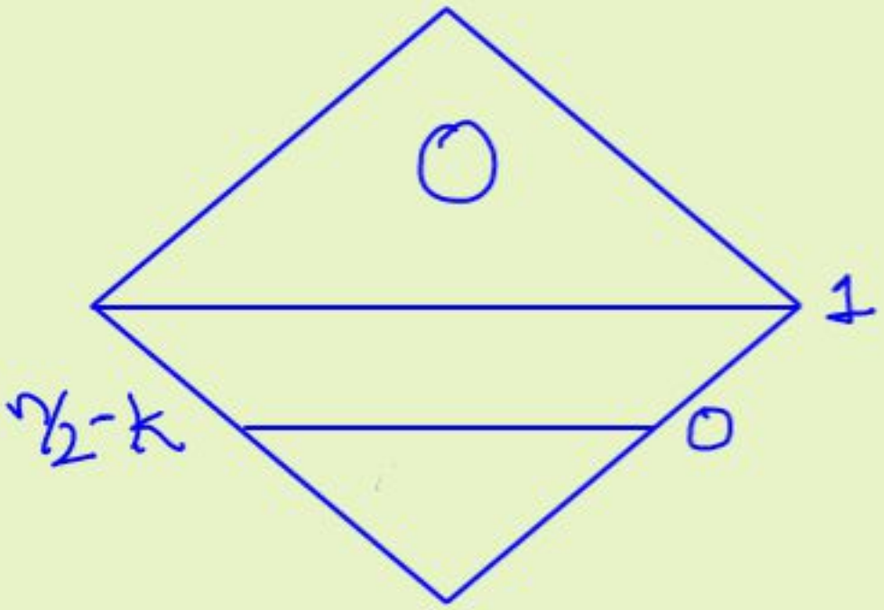
$\Pr_{x \sim \{0,1\}^n_{n/2}}[P(x) \neq 1] < 2\varepsilon$

$\Pr_{x \sim \{0,1\}^n_{n/2-k}}[P(x) \neq 0] < 2\varepsilon$

$k := p^3 = \Theta(\sqrt{n})$ ⟹ $deg(P) = \Omega(\sqrt{n})$

Robust Hegedüs

Example: $ETHR_n^{n/2}$



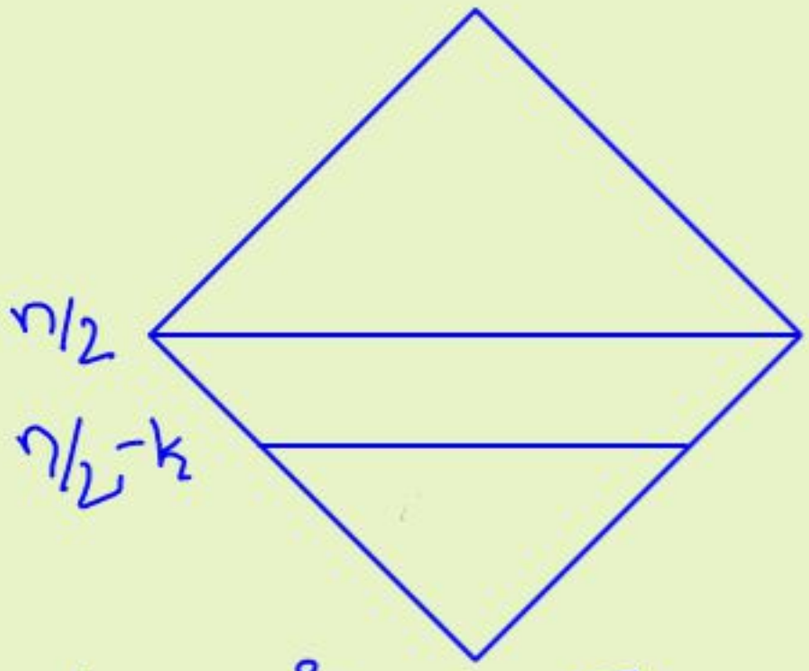
Message:

→ Robust Megedüs ⇒ lbds on pdeg of simple promise symmetric fns.

→ Easier to reduce to other symmetric functions.

Proof of Robust Hegedüs lemma

Proof of Robust Hegedüs lemma



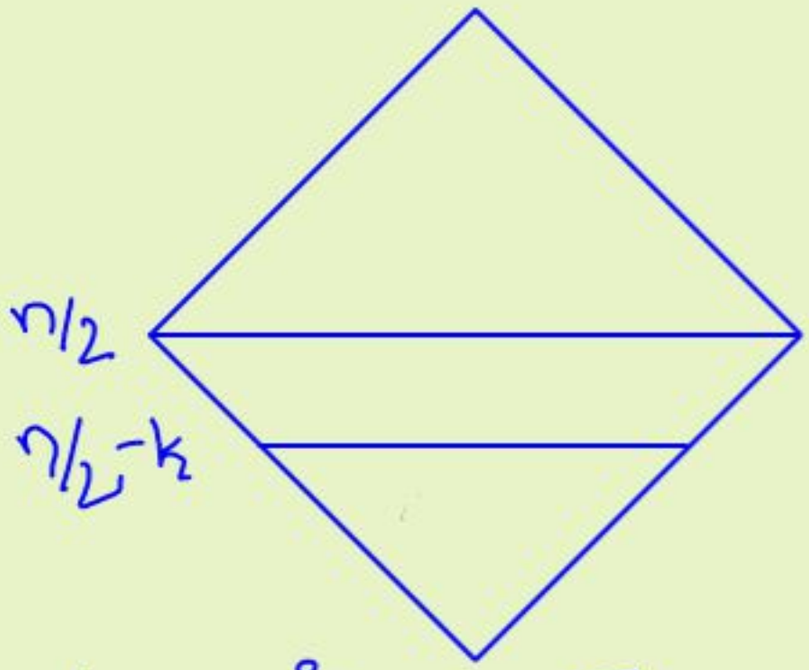
$R(x_1,\dots,x_n) \in \mathbb{F}_p[x_1,\dots,x_n]$ s.t.

(A) $\Pr_{a \sim \{0,1\}^n_{n/2}}[R(a) = 0] \leq \varepsilon$

(B) $\Pr_{b \sim \{0,1\}^n_{n/2}}[R(b) \neq 0] \leq \varepsilon \Rightarrow \deg(R) = \Omega(\sqrt{n})$

$k = p^3 = C \cdot \sqrt{n}$

Proof of Robust Hegedüs lemma

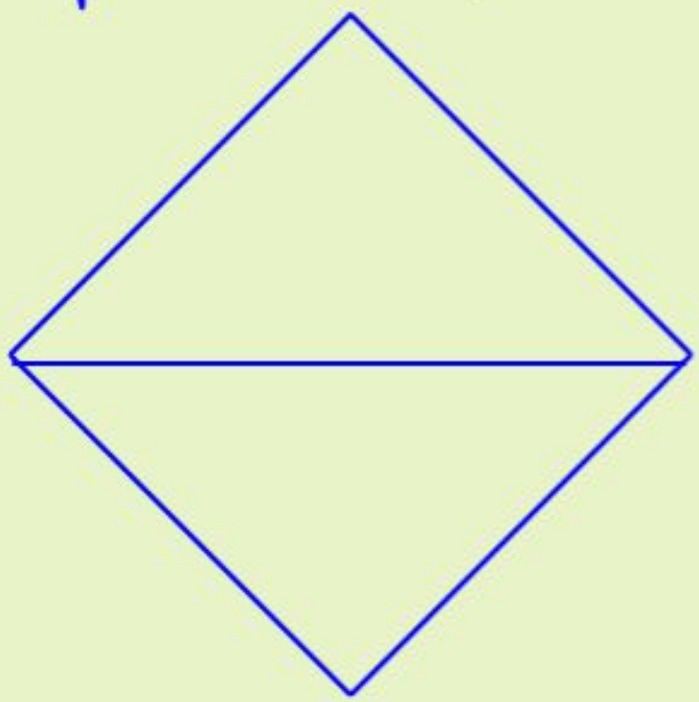


$R(x_1,\dots,x_n) \in \mathbb{F}_p[x_1,\dots,x_n]$ s.t.

(A) $\Pr_{a\sim\{0,1\}^n_{n/2}}[R(a)=0] \le \varepsilon$

(B) $\Pr_{b\sim\{0,1\}^n_{n/2}}[R(b)\neq 0] \le \varepsilon \Rightarrow \deg(R)=\Omega(\sqrt{n})$

$K=p^3=C\cdot\sqrt{n}$



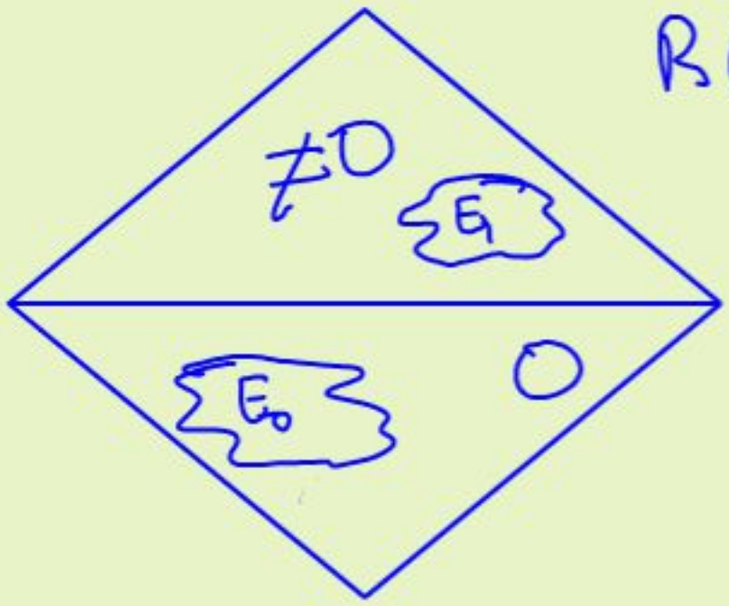
Smolensky's thm:

(A) $\Pr_{a\sim\{0,1\}^n_{\le n/2}}[R(a)=0] \le \varepsilon$

(B) $\Pr_{b\sim\{0,1\}^n_{<n/2}}[R(a)\neq 0] \le \varepsilon$

$\Rightarrow \deg(R)=\Omega(\sqrt{n})$.

Proof of Smolensky's thm

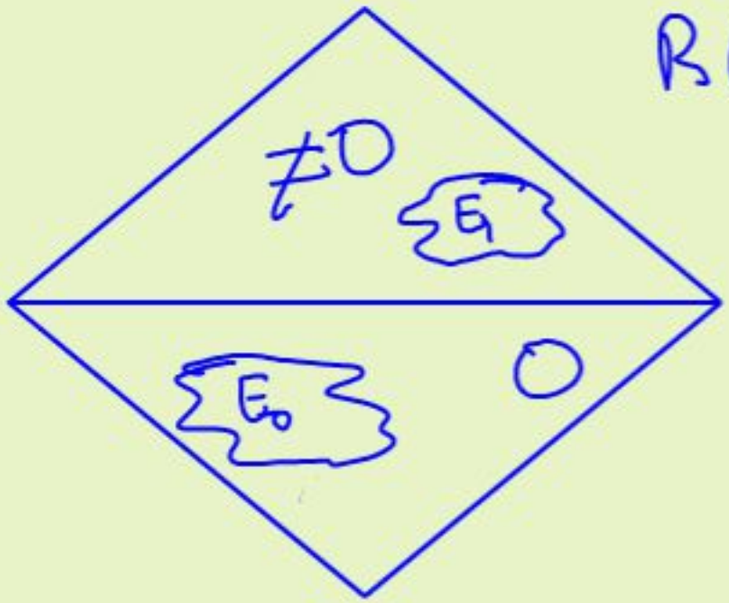


$R(x_1, \dots, x_n)$

$|E_0|, |E_1| \leq \varepsilon \cdot 2^n.$

$\Rightarrow \deg(R) = \Omega(\sqrt{n})$

Proof of Smolensky's thm



$R(x_1, \dots, x_n)$

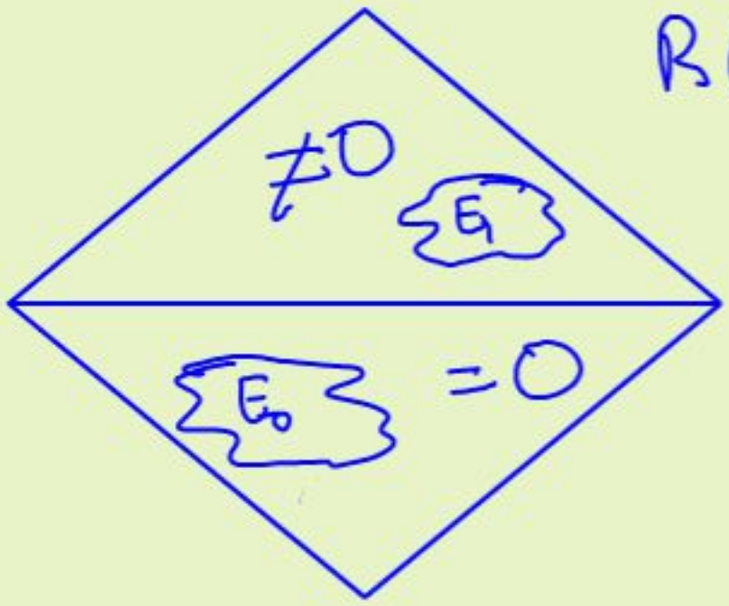
$|E_0|, |E_1| \leq \varepsilon \cdot 2^n$.

$\Rightarrow \deg(R) = \Omega(\sqrt{n})$

Clm 1: $\exists Q$, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$ s.t.

$Q|_{E_0 \cup E_1} \equiv 0$ & $Q \cdot R \not\equiv 0$

Proof of Smolensky's thm



$R(x_1, \dots, x_n)$

$|E_0|, |E_1| \leq \varepsilon \cdot 2^n$.

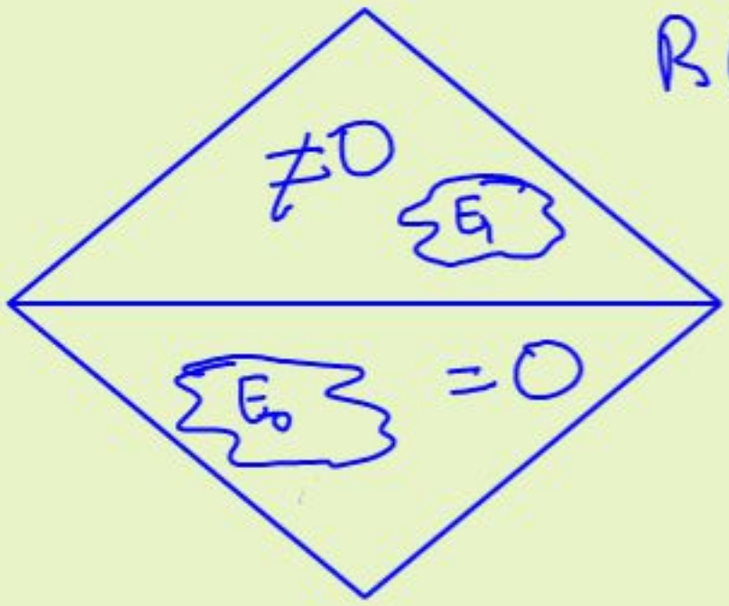
$\Rightarrow \deg(R) = \Omega(\sqrt{n})$

Clm 1: $\exists Q$, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$ s.t.

$Q|_{E_0 \cup E_1} \equiv 0$ & $Q \cdot R \not\equiv 0$

Clm 2: $P \not\equiv 0$ & $P|_{\Sigma^0_{\leq n/2} \cup \Sigma^1_{\leq n/2}} \equiv 0 \Rightarrow \deg(P) \geq n/2$.

Proof of Smolensky's thm



$R(x_1, \dots, x_n)$

$|E_0|, |E_1| \leq \varepsilon \cdot 2^n$.

$\Rightarrow \deg(R) = \Omega(\sqrt{n})$

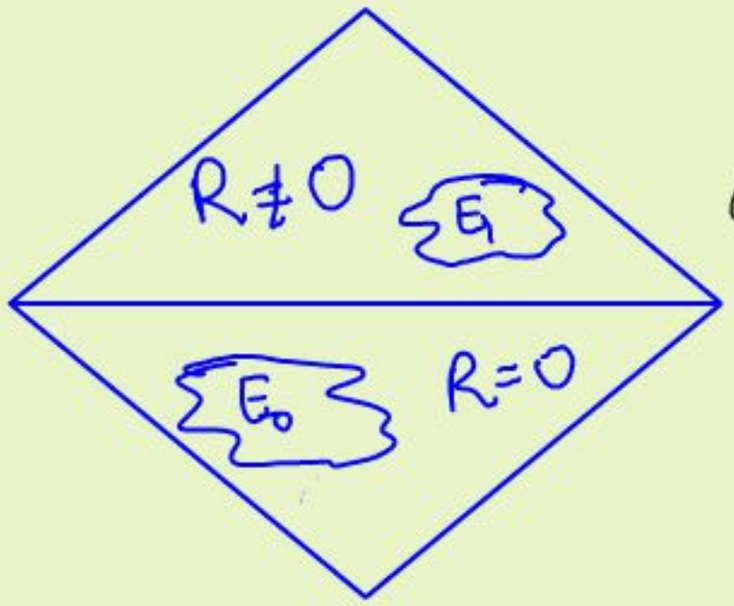
Clm 1: $\exists Q$, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$ s.t.

$$Q|_{E_0 \cup E_1} \equiv 0 \quad \& \quad Q \cdot R \not\equiv 0$$

Clm 2: $P \not\equiv 0$ & $P|_{\Sigma^n_{0,1} \leq n/2} \equiv 0 \Rightarrow \deg(P) \geq n/2$.

Pf of Smolensky: $P = Q \cdot R \Rightarrow \deg(P) \geq n/2$. $\square$

Proof of Smolensky's thm

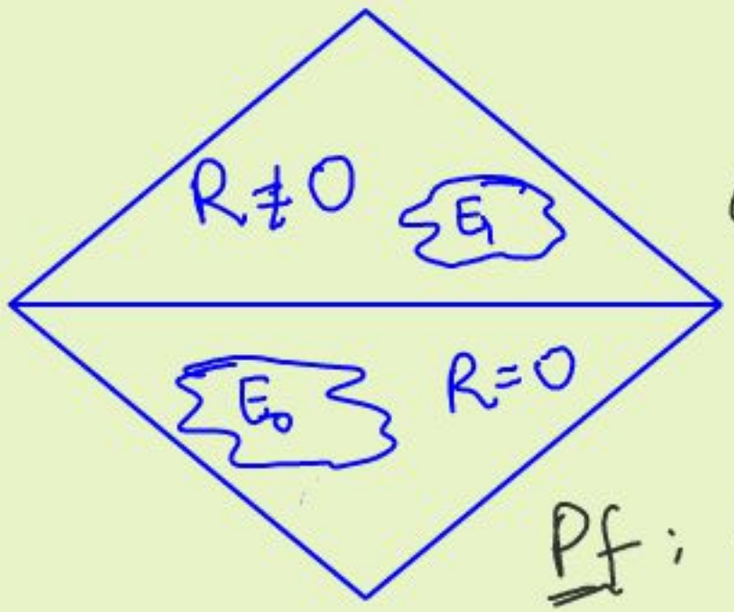


$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$

s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Proof of Smolensky's thm



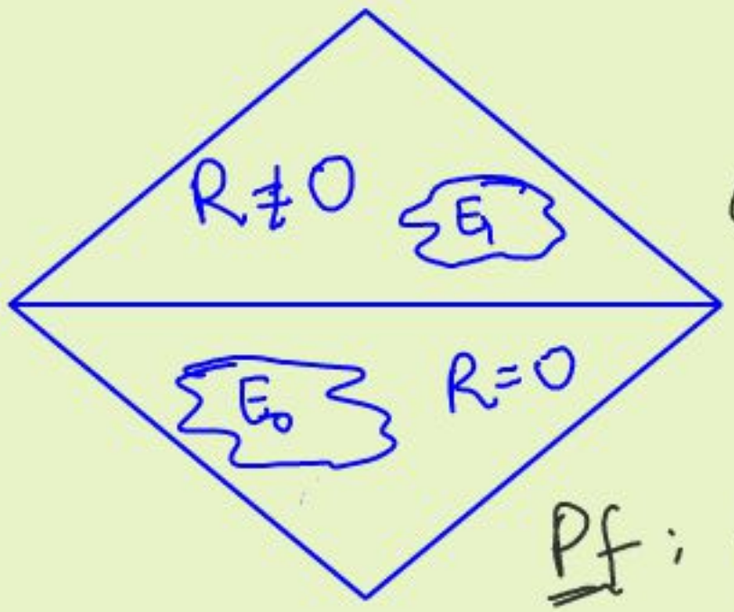
$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$ s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Pf: Assume Q of deg $\le D$.

$$Q(x_1, \dots, x_n) = \sum_{I \subseteq [n] : |I| \le D} \alpha_I x^I$$

Proof of Smolensky's thm



$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$

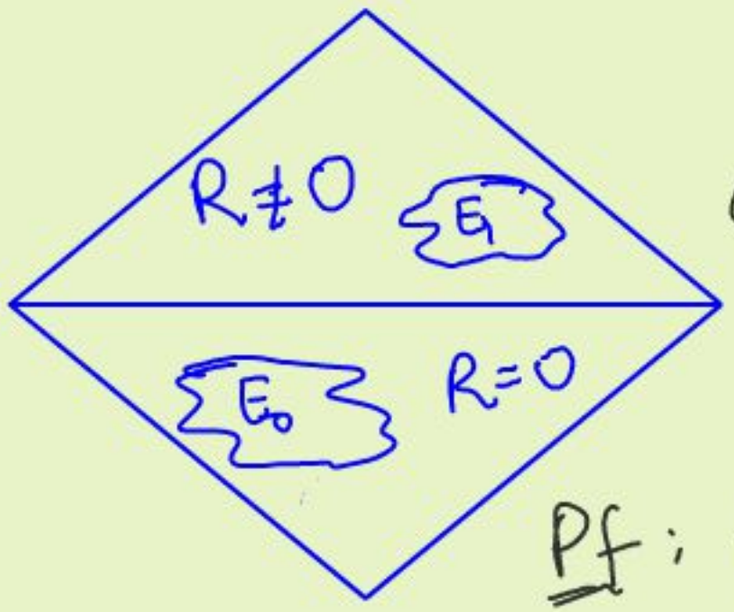
s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Pf: Assume Q of deg $\le D$.

$$Q(x_1, \dots, x_n) = \sum_{I \subseteq [n] : |I| \le D} \alpha_I x^I$$

Need $Q(a) \equiv 0 \quad \forall a \in E$

Proof of Smolensky's thm



$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$

s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Pf: Assume Q of deg $\le D$.

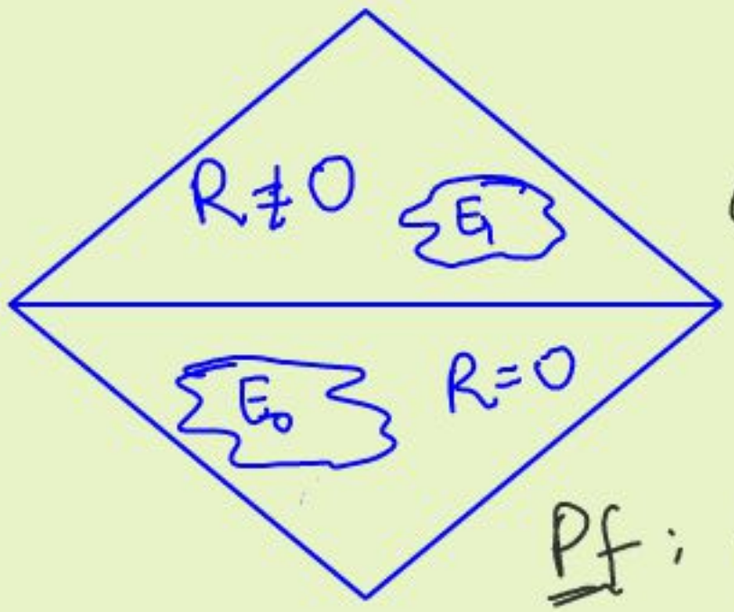
$$Q(x_1, \dots, x_n) = \sum_{I \subseteq [n] : |I| \le D} \alpha_I x^I$$

Need $Q(a) = 0 \quad \forall a \in E$

# of constraints $= |E| \le 2\varepsilon \cdot 2^n$

# of variables $= \binom{n}{\le D}$

Proof of Smolensky's thm



$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$

s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Pf: Assume Q of deg $\le D$.

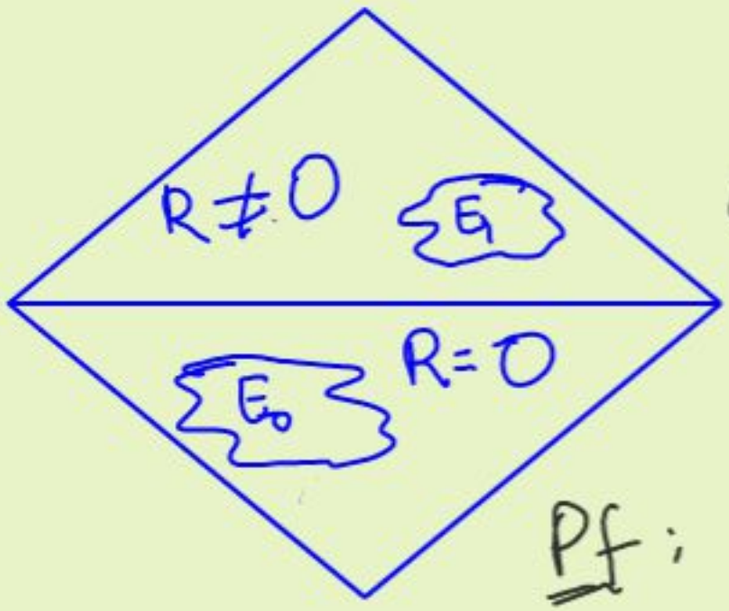
$$Q(x_1, \dots, x_n) = \sum_{I \subseteq [n] : |I| \le D} \alpha_I x^I$$

Need $Q(a) = 0 \quad \forall a \in E$

# of constraints $= |E| \le 2\varepsilon \cdot 2^n$

# of variables $= \binom{n}{\le D} > 2\varepsilon \cdot 2^n$ if $D \ge \frac{n}{2} - \Omega(\sqrt{n})$.

Proof of Smolensky's thm



$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

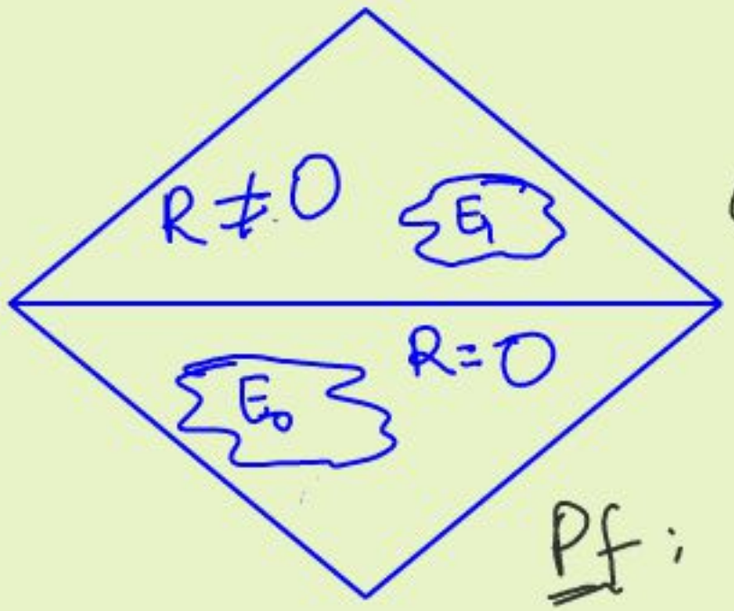
Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$

s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Pf: Q of deg $\le n/2 - \Omega(\sqrt{n})$.

$Q \not\equiv 0$, $Q|_E \equiv 0$

Proof of Smolensky's thm



$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

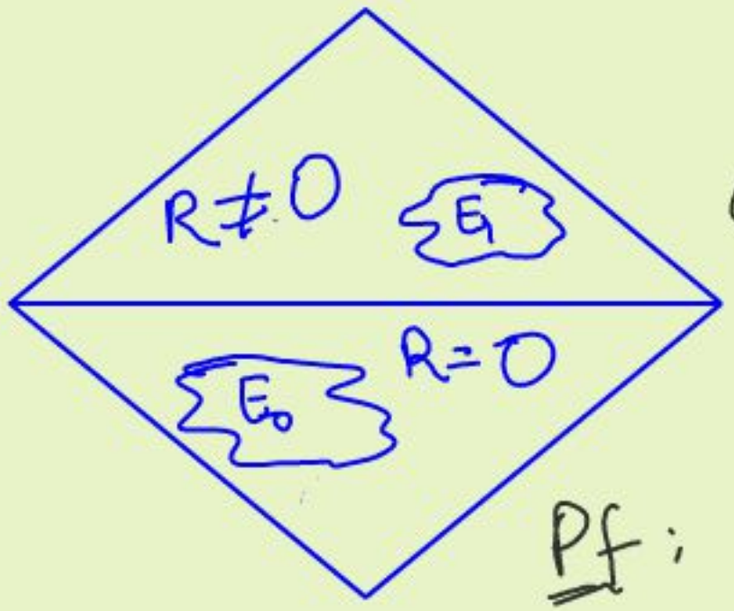
Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$
s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Pf: Q of deg $\le n/2 - \Omega(\sqrt{n})$.

$Q \not\equiv 0$, $Q|_E \equiv 0$

$\deg(Q) < n/2 \Rightarrow Q|_{\{0,1\}^n} \not\equiv 0$

Proof of Smolensky's thm



$E = E_0 \cup E_1$, $|E| \le 2\varepsilon \cdot 2^n$.

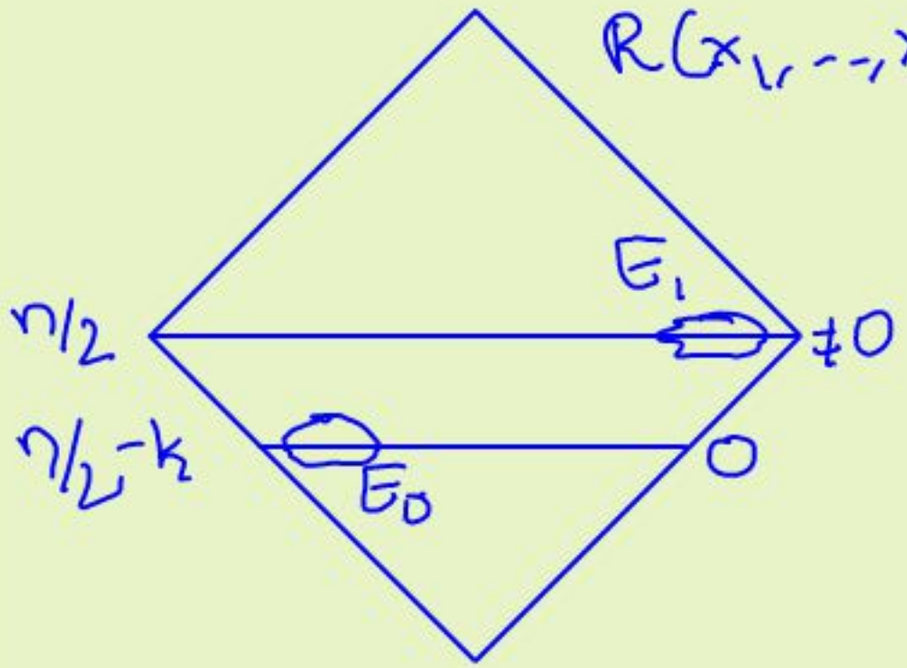
Clm 1: $\exists Q$, $\deg(Q) \le n/2 - \Omega(\sqrt{n})$ s.t $Q|_E \equiv 0$ & $Q \cdot R \not\equiv 0$.

Pf: Q of deg $\le n/2 - \Omega(\sqrt{n})$.

$Q \not\equiv 0$, $Q|_E \equiv 0$

$\deg(Q) < n/2 \Rightarrow Q|_{\{0,1\}^n} \not\equiv 0 \Rightarrow Q \cdot R \not\equiv 0$. □

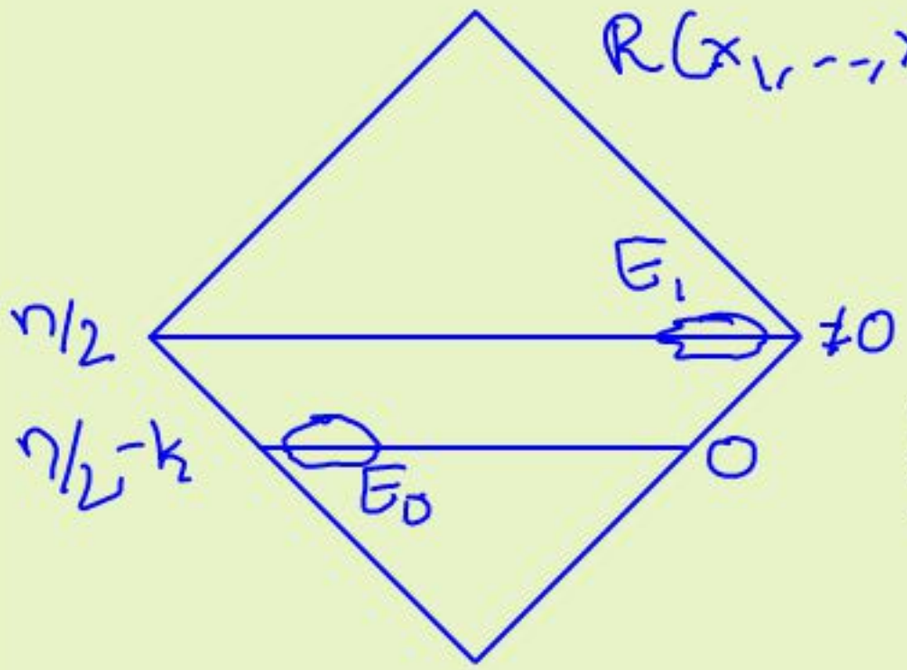
Proof of Robust Hegedüs lemma



$$k=\rho^3 \geq C\cdot\sqrt{n},\ C\to\infty$$

$$|E| = |E_0 \cup E_1| \leq \varepsilon\cdot\binom{n}{n/2},\ \varepsilon\to 0$$

Proof of Robust Hegedüs lemma



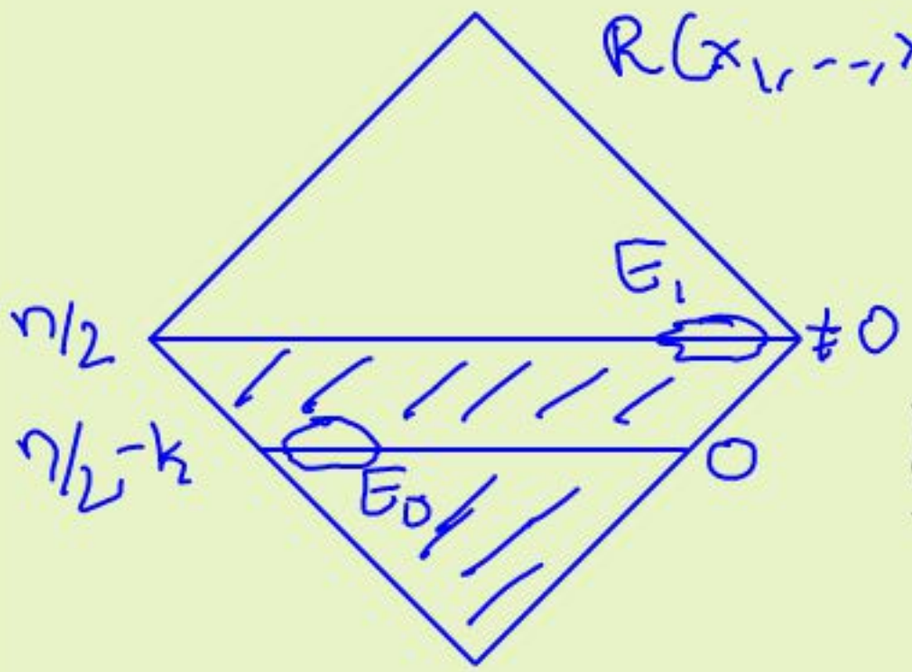
$k = p^3 \approx C \cdot \sqrt{n}$, $C \to \infty$

$|E| = |E_0 \cup E_1| \le \varepsilon \cdot \binom{n}{n/2}$, $\varepsilon \to 0$

Easy: $\exists Q$: $\deg(Q) \le n/2 - \Omega(\sqrt{n})$

$Q|_E \equiv 0$, $Q \not\equiv 0$.

Proof of Robust Hegedüs lemma



$k = \rho^3 \geq C\cdot\sqrt{n}$, $C\to\infty$

$|E| = |E_0 \cup E_1| \leq \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

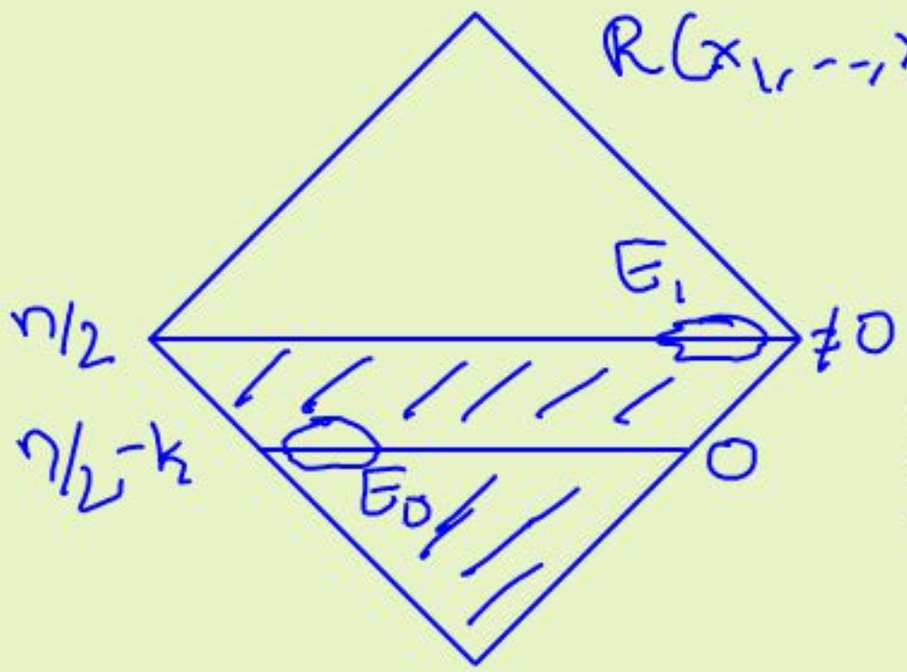
Easy: $\exists Q$: $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q|_E \equiv 0$, $Q \not\equiv 0$.

Issues:

(1) Other points in $\{0,1\}^n_{<n/2}$?

Proof of Robust Hegedüs lemma



$k = \rho^3 \geq C \cdot \sqrt{n}$, $C \to \infty$

$|E| = |E_0 \cup E_1| \leq \varepsilon \cdot \binom{n}{n/2}$, $\varepsilon \to 0$

Easy: $\exists Q$: $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

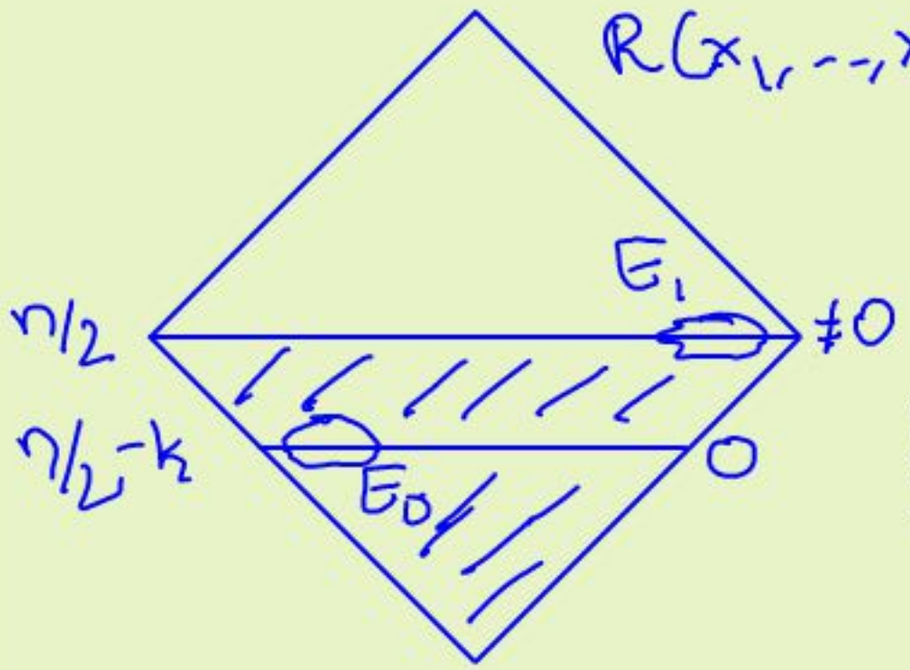
$Q|_E \equiv 0$, $Q \not\equiv 0$.

Issues:

(1) Other points in $\{0,1\}^n_{<n/2}$?

(2) Why is $Q \cdot R \not\equiv 0$?

Proof of Robust Hegedüs lemma



$k = \rho^3 \geq C\cdot\sqrt{n}$, $C\to\infty$

$|E| = |E_0 \cup E_1| \leq \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

Easy: $\exists Q$: $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q|_E \equiv 0$, $Q \not\equiv 0$.

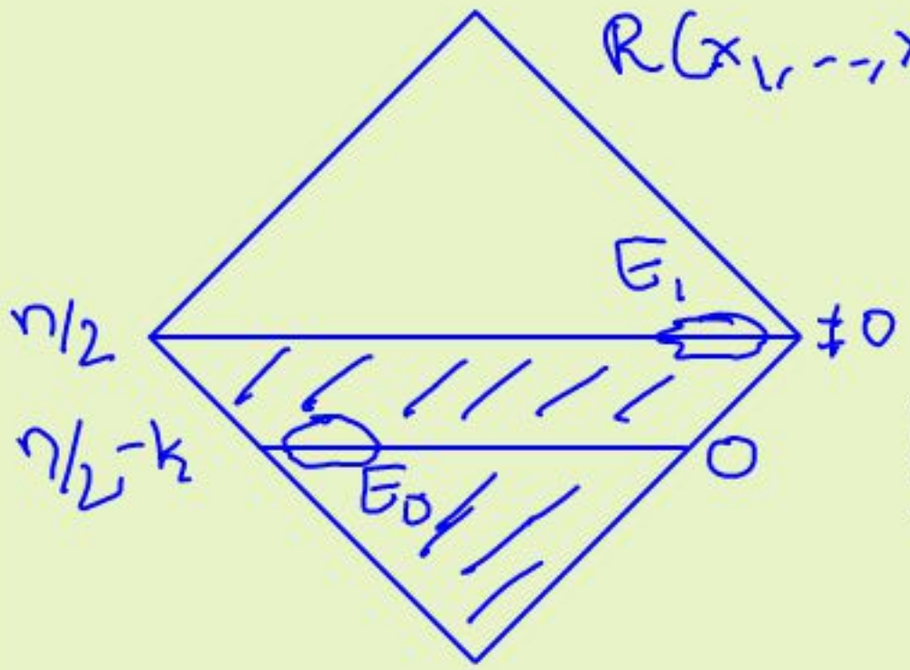
Issues:

(1) Other points in $\{0,1\}^n_{<n/2}$?

(2) Why is $Q\cdot R \not\equiv 0$?

Fixes: $Q = Q_1 \cdot Q_2$

Proof of Robust Hegedüs lemma



$k = \rho^3 \approx C\cdot\sqrt{n}$, $C\to\infty$

$|E| = |E_0 \cup E_1| \le \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

Easy: $\exists Q$: $\deg(Q) \le n/2 - \Omega(\sqrt{n})$

$Q|_E \equiv 0$, $Q \not\equiv 0$.

Issues:

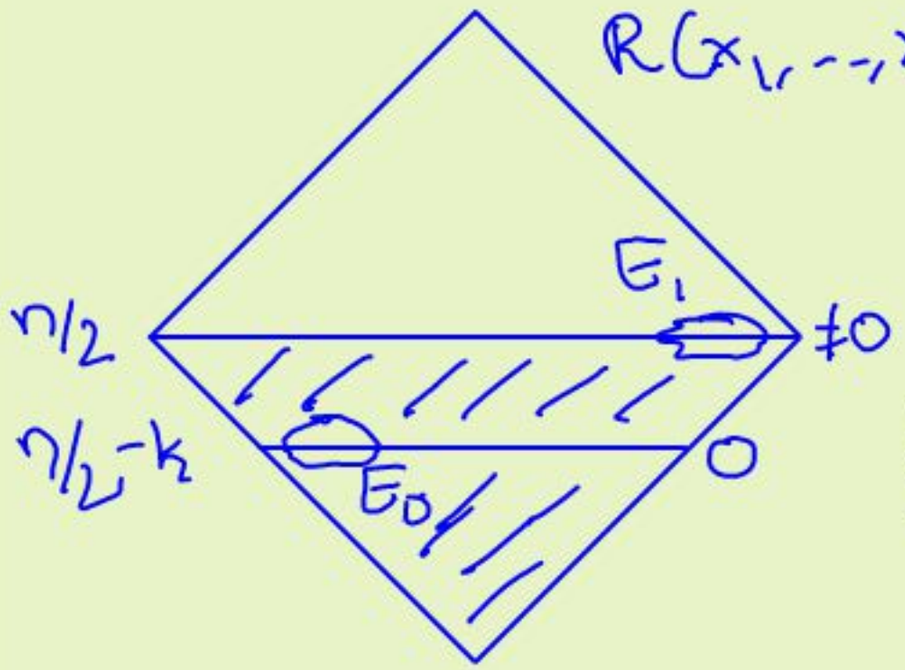
① Other points in $\{0,1\}^n_{<n/2}$?

② Why is $Q\cdot R \not\equiv 0$?

Fixes: $Q = Q_1\cdot Q_2$

① $\deg(Q_1) \le k$ & $Q_1|_{\boxtimes} \equiv 0$

Proof of Robust Hegedüs lemma



$k = \rho^3 \geq C\cdot\sqrt{n}$, $C\to\infty$

$|E| = |E_0 \cup E_1| \leq \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

Easy: $\exists Q$: $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q|_E \equiv 0$, $Q \not\equiv 0$.

Issues:

① Other points in $\{0,1\}^n_{<n/2}$?

② Why is $Q\cdot R \not\equiv 0$?

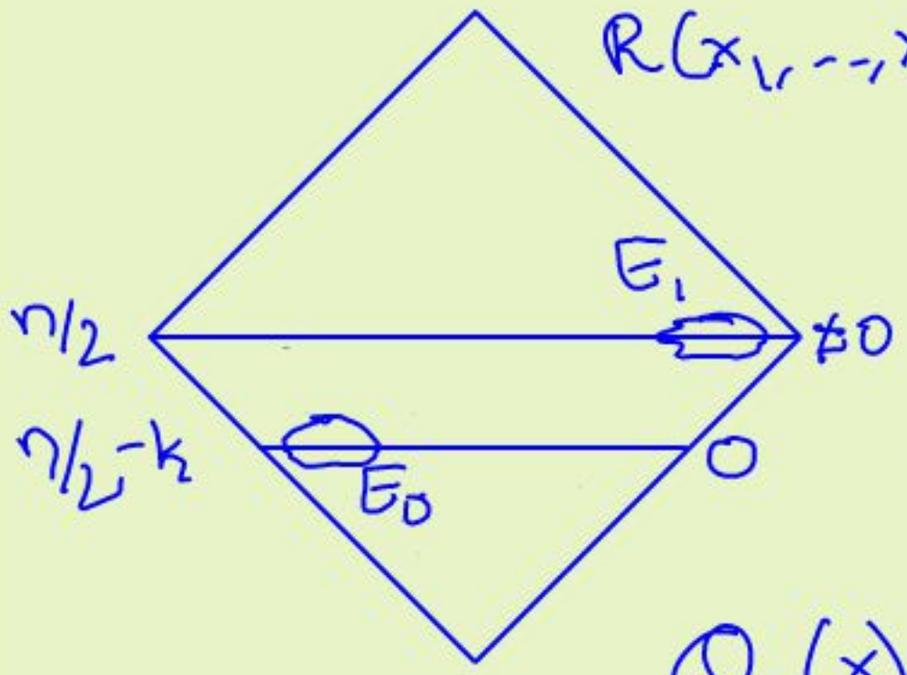
Fixes: $Q = Q_1\cdot Q_2$

① $\deg(Q_1) \leq k$ & $Q_1|_{\boxtimes E} \equiv 0$

② $\deg(Q_2) \leq n/2 - k - \Omega(k)$ &

$Q_2|_E \equiv 0$, $Q_2|_{\{0,1\}^n_{n/2}} \not\equiv 0$.

Proof of Robust Hegedüs lemma



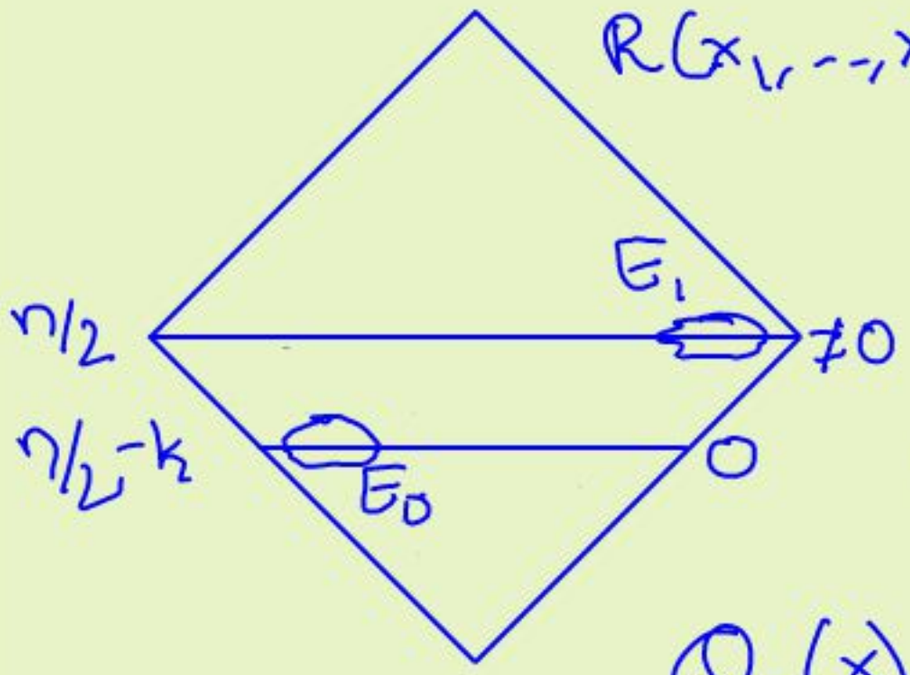
$k=p^3 \simeq C\cdot\sqrt{n}$, $C\to\infty$

$|E| = |E_0 \cup E_1| \leq \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

Constructing Q_1:

$$Q_1(x) = \prod_{j=1}^{s-1}\left(\left(\sum_{|I|=p} x^I\right)^{p-1} - 1\right)$$

Proof of Robust Hegedüs lemma



$k=p^s \simeq C\cdot\sqrt{n}$, $C\to\infty$

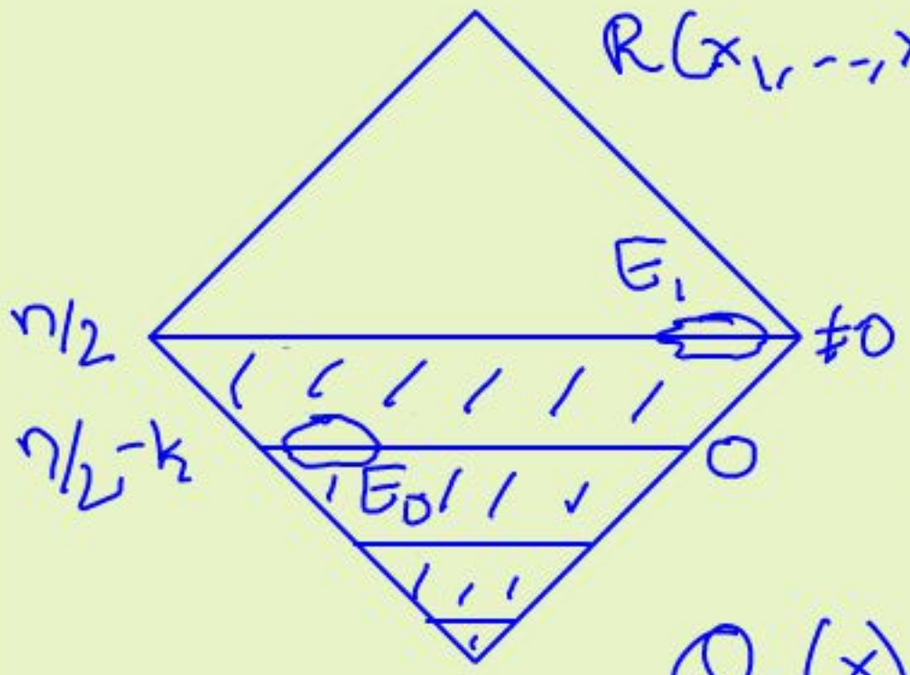
$|E| = |E_0 \cup E_1| \le \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

Constructing Q_1:

$$Q_1(x) = \prod_{j=1}^{s-1}\left(\left(\sum_{|I|=p} x^I\right)^{p-1} - 1\right)$$

Lucas's thm $\Rightarrow$ $Q_1(a)\neq 0 \iff |a| \equiv n/2 \pmod{k}$

Proof of Robust Hegedüs lemma



$k = p^s \simeq C\cdot\sqrt{n}$, $C\to\infty$

$|E| = |E_0 \cup E_1| \le \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

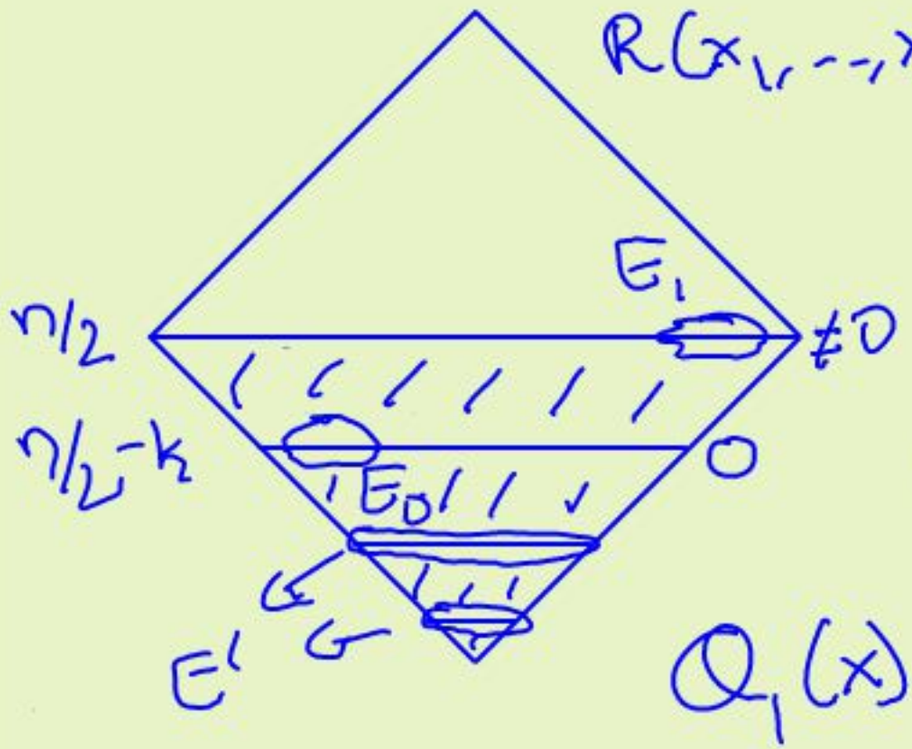
Constructing Q_1:

$$Q_1(x) = \prod_{j=1}^{s-1}\left(\left(\sum_{|I|=p} x^I\right)^{p-1} - 1\right)$$

Lucas's thm $\Rightarrow$ $Q_1(a)\neq 0 \iff |a| \equiv n/2 \pmod k$

$Q_1(a)\neq 0 \iff a \in$ ▭

Proof of Robust Hegedüs lemma



$k=p^s \simeq C\cdot\sqrt{n}$, $C\to\infty$

$|E| = |E_0 \cup E_1| \le \varepsilon\cdot\binom{n}{n/2}$, $\varepsilon\to 0$

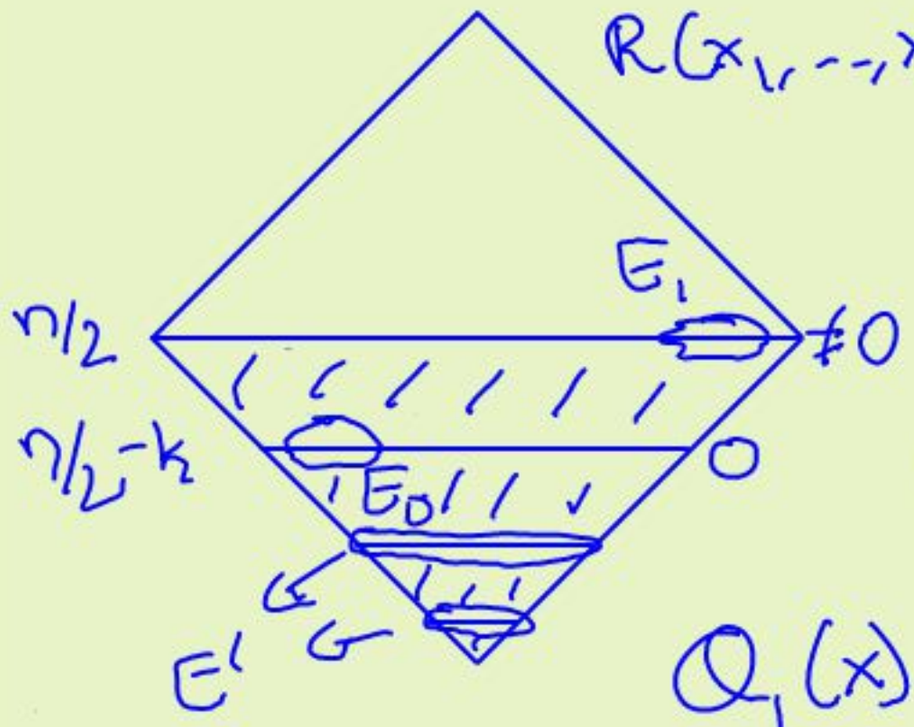
Constructing Q_1:

$$Q_1(x) = \prod_{j=1}^{s-1}\left(\left(\sum_{|I|=p} x^I\right)^{p-1} - 1\right)$$

Lucas's thm $\Rightarrow$ $Q_1(a)\neq 0 \iff |a| \equiv n/2 \pmod k$

$Q_1(a)\neq 0 \iff a \in$ ▯

Proof of Robust Hegedüs lemma



$k = p^s \approx C\cdot\sqrt{n}$, $C \to \infty$

$|E| = |E_0 \cup E_1| \le \varepsilon \cdot \binom{n}{n/2}$, $\varepsilon \to 0$

Constructing Q_1:

$$Q_1(x) = \prod_{j=1}^{s-1} \left(\left(\sum_{|I|=p} \cdot x^I \right)^{p-1} - 1 \right)$$

Lucas's thm $\Rightarrow$ $Q_1(a) \neq 0 \iff |a| \equiv n/2 \pmod{k}$

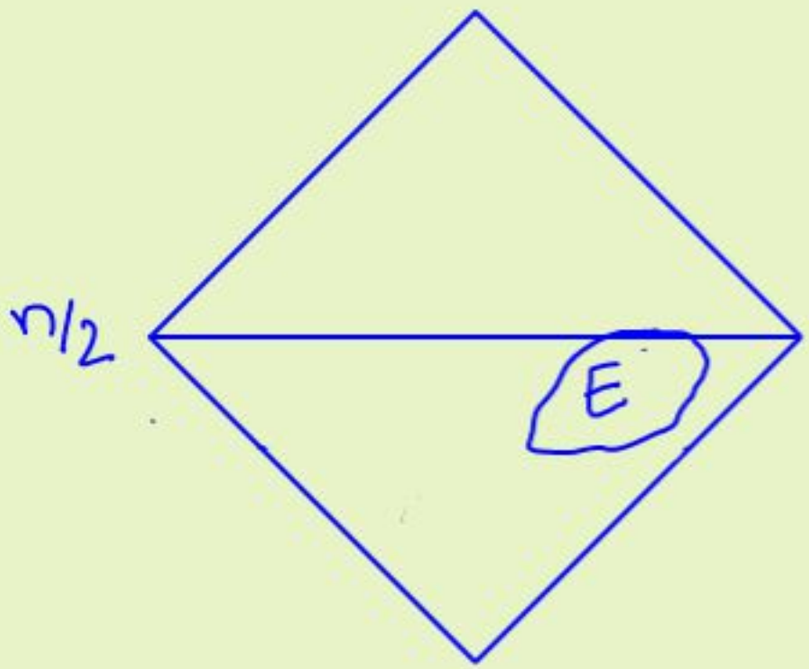
$Q_1(a) \neq 0 \iff a \in$ ▣

$E'' = E \cup E' \Rightarrow |E''| \le \varepsilon \cdot \binom{n}{n/2} + \binom{n}{n/2-2k} + \binom{n}{n/2-3k} + \cdots$

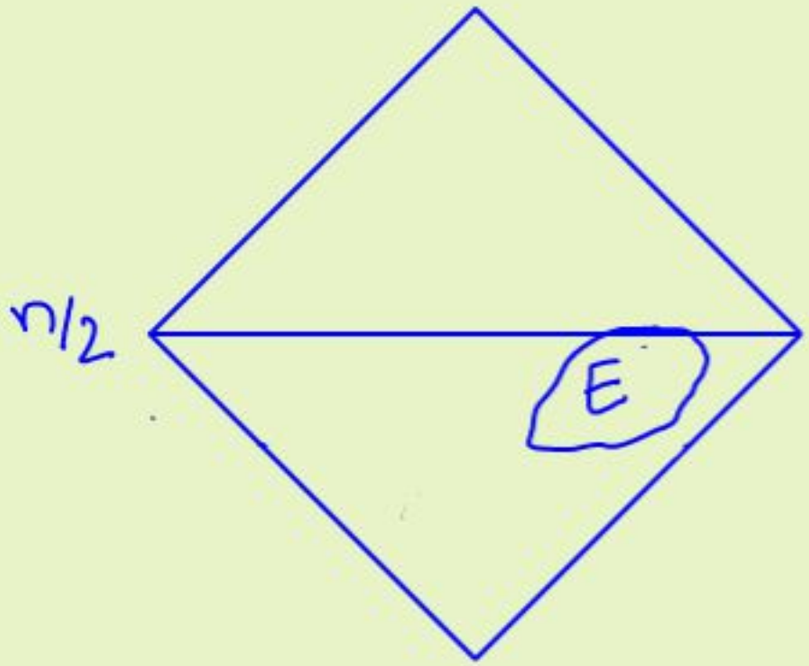
$\le 2\varepsilon \cdot \binom{n}{n/2}$

Proof of Robust Hegedüs lemma

$E \subseteq \{0,1\}^n, \ |E| \leq \varepsilon \cdot \binom{n}{n/2}$



Proof of Robust Hegedüs lemma

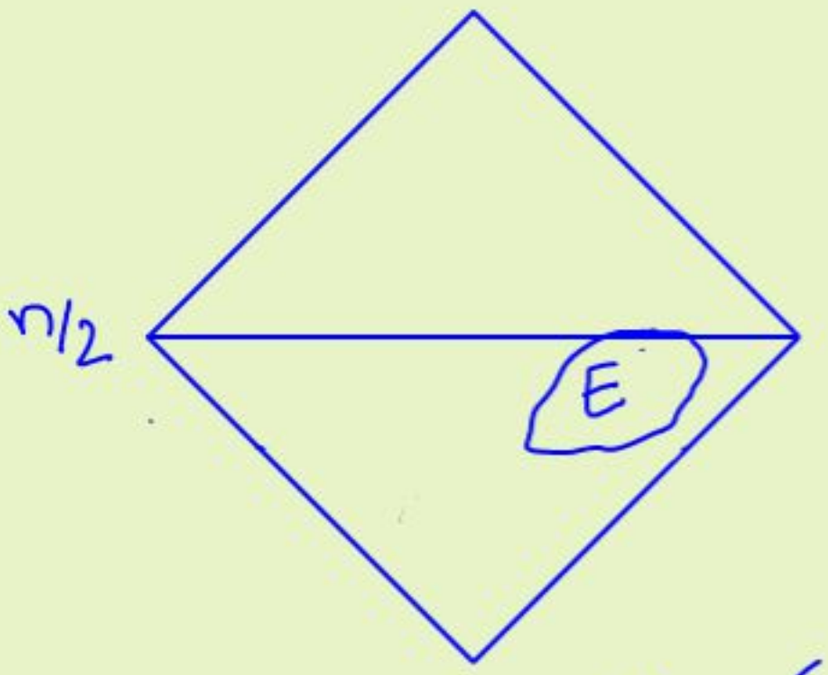


$E \subseteq \{0,1\}^n$, $|E| \leq \varepsilon \cdot \binom{n}{n/2}$

Want: Q_2, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q_2|_E \equiv 0$, $Q_2|_{\{0,1\}^n_{n/2}} \not\equiv 0$.

Proof of Robust Hegedüs lemma



$E \subseteq \{0,1\}^n$, $|E| \leq \varepsilon \cdot \binom{n}{n/2}$

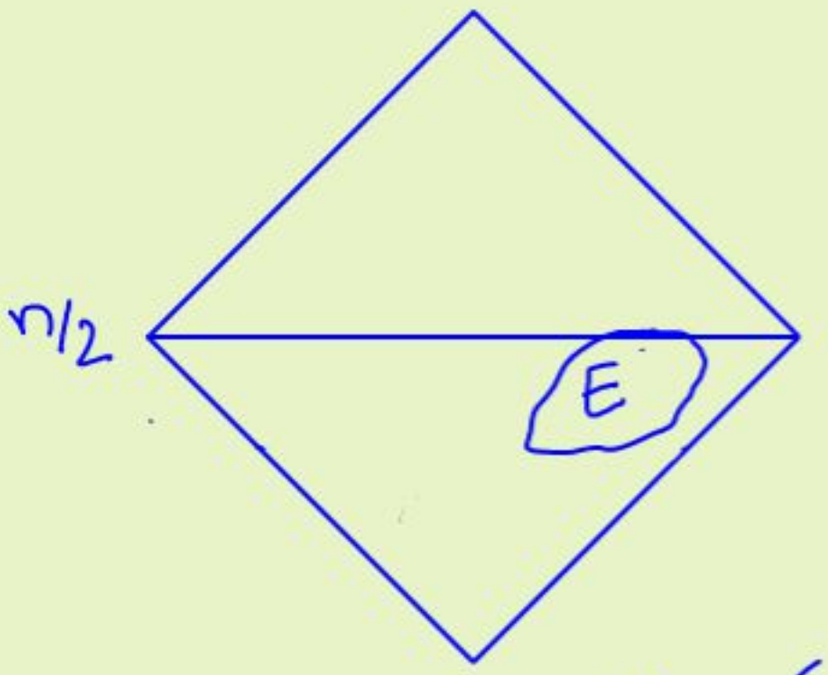
Want: Q_2, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q_2|_E \equiv 0$, $Q_2|_{\{0,1\}^n_{n/2}} \not\equiv 0$.

Defn: $Cl_D(E) = \{a \mid \forall Q_2 \atop \deg(Q_2) \leq D$, $Q_2|_E \equiv 0 \Rightarrow Q_2(a) = 0\}$

closure of E

Proof of Robust Hegedüs lemma



$E \subseteq \{0,1\}^n$, $|E| \leq \varepsilon \cdot \binom{n}{n/2}$

Want: Q_2, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q_2|_E \equiv 0$, $Q_2|_{\{0,1\}^n_{n/2}} \not\equiv 0$.

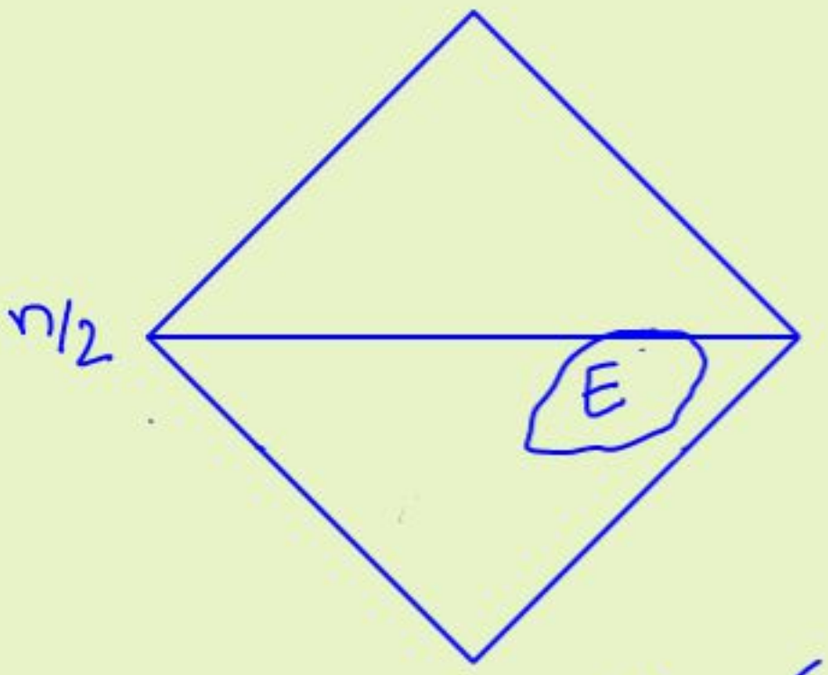
Defn: $cl_D(E) = \{a \mid \forall Q_2 \atop \deg(Q_2) \leq D$, $Q_2|_E \equiv 0 \Rightarrow Q_2(a) = 0\}$

closure of E

Thm: [Nie-Wang '14]

$$\frac{|cl_D(E)|}{2^n} \leq \frac{|E|}{\binom{n}{\leq D}}$$

Proof of Robust Hegedüs lemma



$E \subseteq \{0,1\}^n$, $|E| \leq \varepsilon \cdot \binom{n}{n/2}$

Want: Q_2, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q_2|_E \equiv 0$, $Q_2|_{\{0,1\}^n_{n/2}} \not\equiv 0$.

Defn: $cl_D(E) = \{a \mid \forall Q_2 \atop \deg(Q_2) \leq D$, $Q_2|_E \equiv 0 \Rightarrow Q_2(a) = 0\}$

closure of E

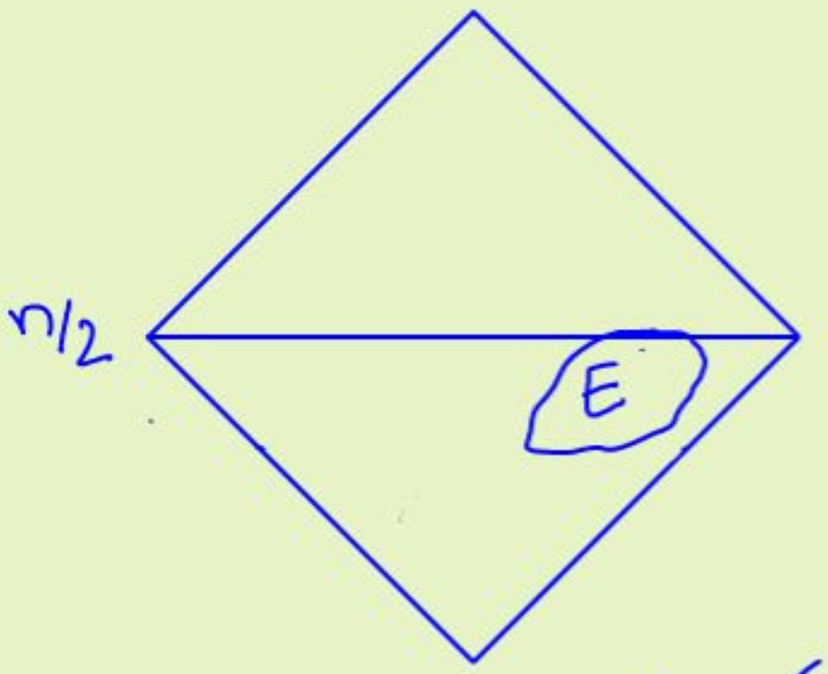
Thm: [Nie-Wang '14]

$$\frac{|cl_D(E)|}{2^n} \leq \frac{|E|}{\binom{n}{\leq D}}$$

→ # of constraints

→ # of variables

Proof of Robust Hegedüs lemma



$E \subseteq \{0,1\}^n$, $|E| \leq \varepsilon \cdot \binom{n}{n/2}$

Want: Q_2, $\deg(Q) \leq n/2 - \Omega(\sqrt{n})$

$Q_2|_E \equiv 0$, $Q_2|_{\{0,1\}^n_{n/2}} \not\equiv 0$.

Defn: $Cl_D(E) = \{a \mid \forall Q_2 \atop \deg(Q_2) \leq D$, $Q_2|_E \equiv 0 \Rightarrow Q_2(a) = 0\}$

closure of E

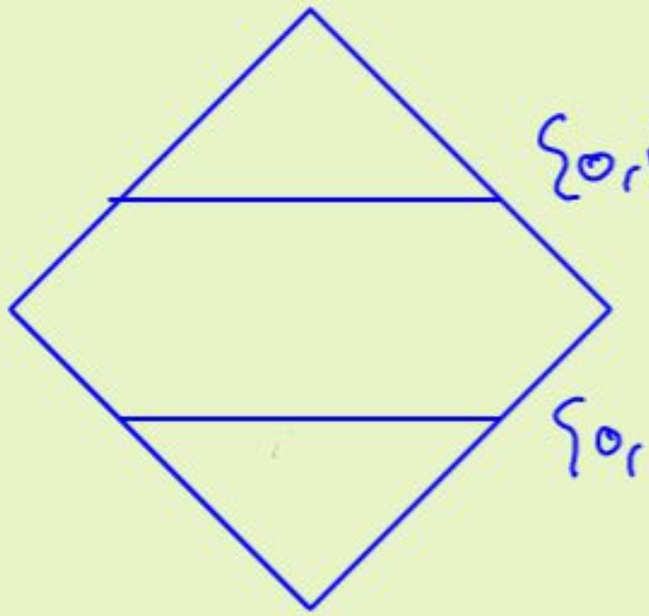
Thm: [Nie-Wang '14]

$$\frac{|Cl_D(E)|}{2^n} \leq \frac{|E|}{\binom{n}{\leq D}} \leq \frac{\varepsilon \cdot \binom{n}{n/2}}{\Omega(2^n)} \leq O(\varepsilon) \cdot \binom{n}{n/2}$$

□

Main lemma

$\mathbb{F}[x_1, \cdots, x_n]$



Q: lowest deg. $R(x_1, \cdots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

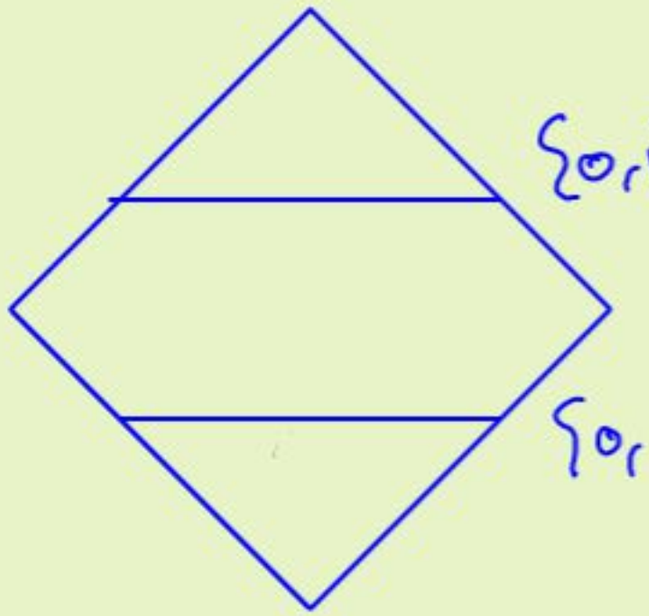
(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\mathrm{char}(\mathbb{F}) = p, \; q = p^s$

Main Result: $\deg(R) = \Omega(\min\{\text{sampling bound}, q\})$

Main lemma

$\mathbb{F}[x_1, \ldots, x_n]$



Q: lowest deg. $R(x_1, \ldots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

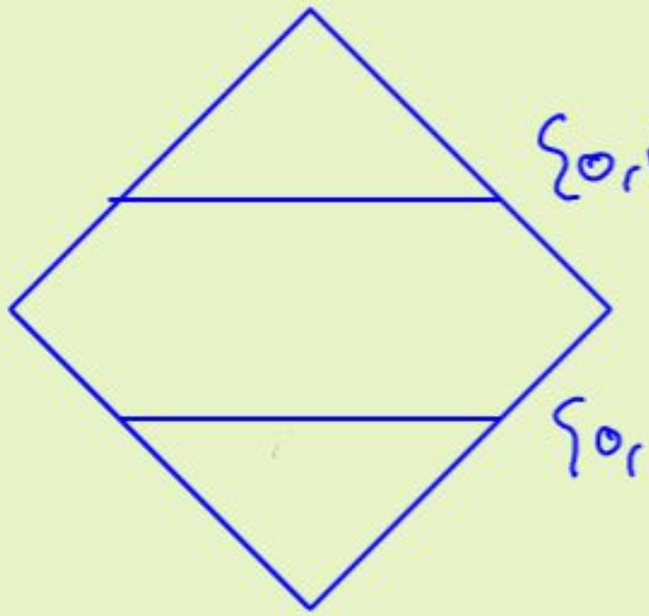
(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\mathrm{char}(\mathbb{F}) = p$, $q = p^s$

Main Result: $\deg(R) = \Omega(\min\{\text{sampling bound}, q\})$

Applications: Degree lower bds for polynomial approximations.

Main lemma



$\mathbb{F}[x_1, \cdots, x_n]$

Q: lowest deg. $R(x_1, \cdots, x_n)$ s.t.

(I) $\Pr_{|a|=k}[R(a) \neq 0] \leq \varepsilon$

(II) $\Pr_{|b|=k+q}[R(a) \neq 0] \geq 1-\varepsilon$

$\mathrm{char}(\mathbb{F}) = p$, $q = p^s$

Main Result: $\deg(R) = \Omega(\min\{\text{sampling bound}, q\})$

Applications: Degree lower bds for polynomial approximations.

Others?

Thanks!

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1,\dots,x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \le \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \le \varepsilon$$

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1, \ldots, x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \leq \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \leq \varepsilon$$

Studied in many models of computation

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1,\dots,x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \le \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \le \varepsilon$$

Studied in many models of computation

→ Circuits - [Ajtai '83, Shaltiel-Viola '08, Limaye et al. '19]

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1, \ldots, x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2}-\delta}[R(a)=1] \leq \varepsilon, \quad \Pr_{D_{1/2}+\delta}[R(a)=0] \leq \varepsilon$$

Studied in many models of computation

→ Circuits - [Ajtai '83, Shaltiel-Viola '08, Limaye et al. '19]

→ Read-once Branching Programs - [Brody-Verbin '10]

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1, \ldots, x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \leq \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \leq \varepsilon$$

Minimum degree of R?

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1,\dots,x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \le \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \le \varepsilon$$

Minimum degree of R?

Sampling: deg $O(1/\delta \log 1/\varepsilon)$.

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1, \ldots, x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \le \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \le \varepsilon$$

Minimum degree of R?

Sampling: deg $O(1/\delta \log 1/\varepsilon)$.

$\varepsilon = \Omega(1) \Rightarrow \deg(R) = \Omega(\frac{1}{\delta})$

[Limaye et al. '19] :

[Chattopadhyay et al. '19]

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1, \ldots, x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \le \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \le \varepsilon$$

Minimum degree of R?

Sampling: deg $O(1/\delta \log 1/\varepsilon)$.

[Limaye et al. '19]: $\varepsilon = \Omega(1) \Rightarrow \deg(R) = \Omega(\frac{1}{\delta})$

[Chattopadhyay et al. '19] Smaller ε?

Coin Problem

D_α^n - distribution over $\{0,1\}^n$, each bit 1 with prob. α

$R(x_1,\dots,x_n)$ solves δ-Coin Problem w/error ε if:

$$\Pr_{D_{1/2-\delta}}[R(a)=1] \le \varepsilon, \quad \Pr_{D_{1/2+\delta}}[R(a)=0] \le \varepsilon$$

Minimum degree of R?

Sampling: deg $O(1/\delta \log 1/\varepsilon)$.

Corollary to Robust Hegedüs: $\deg(R) = \Omega\left(\frac{1}{\delta}\log\frac{1}{\varepsilon}\right)$.