The List Decoding Radius of RM codes

Abhishek Bhowmick, UT Austin

Joint work with
Shachar Lovett, UCSD

FOCS 2014, Higher order Fourier Analysis Workshop October, 2014

Organization

- Coding theory preliminaries
- The main results, Thm 1 and Thm 2
- Proof outline of Thm 1
- Higher order Fourier analysis

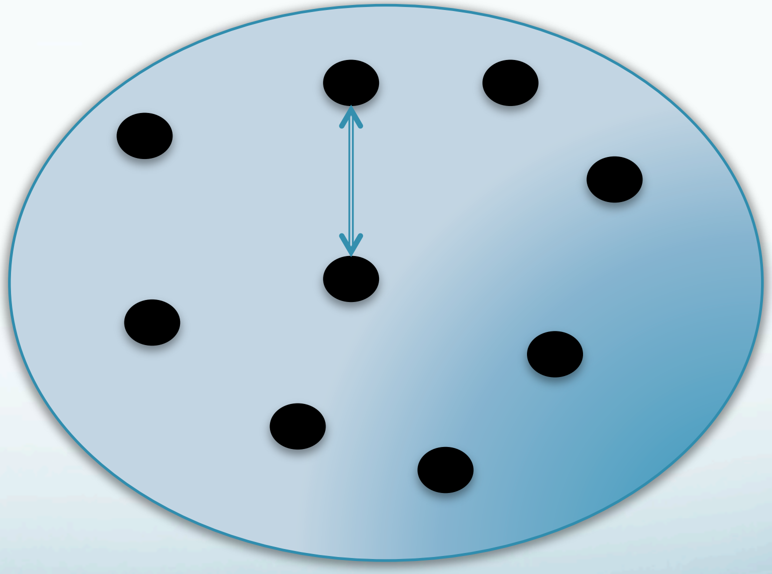
Codes

- Rate

  How many codewords?

- Min distance

  Minimum pairwise distance

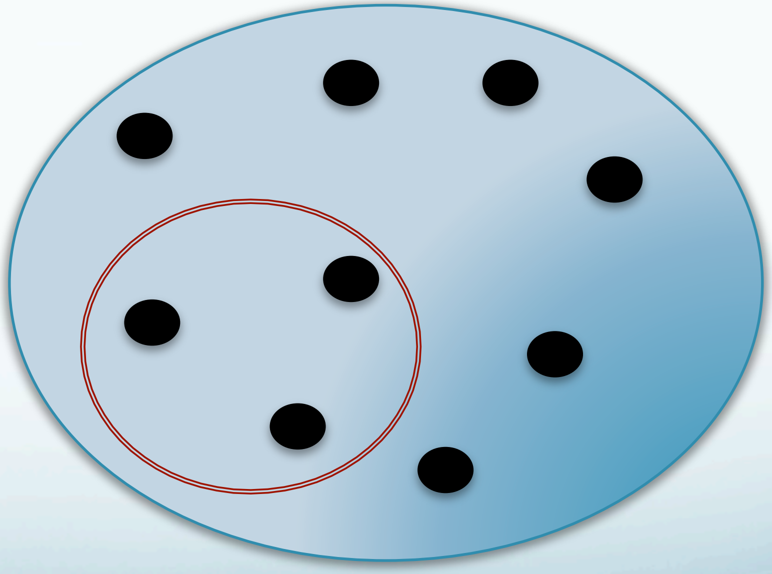


List Decodability

- Number of codewords... **[Elias'57, Wozencraft'58]**

  in ball of radius r?

  bounded?



RM Code

$F = F_p$
$d < p$

[Muller'54, Reed'54]

$$g : F^n \to F$$

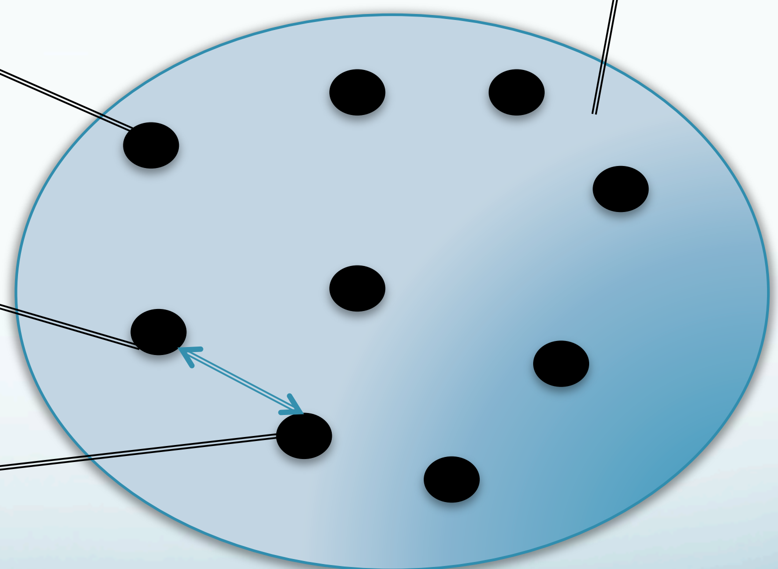
$$P : F^n \to F$$

$$\deg(P) \le d$$

$$(P_1(x) : x \in F^n)$$

$\delta(d,p) = 1 - d/p$

$$(P_2(x) : x \in F^n)$$



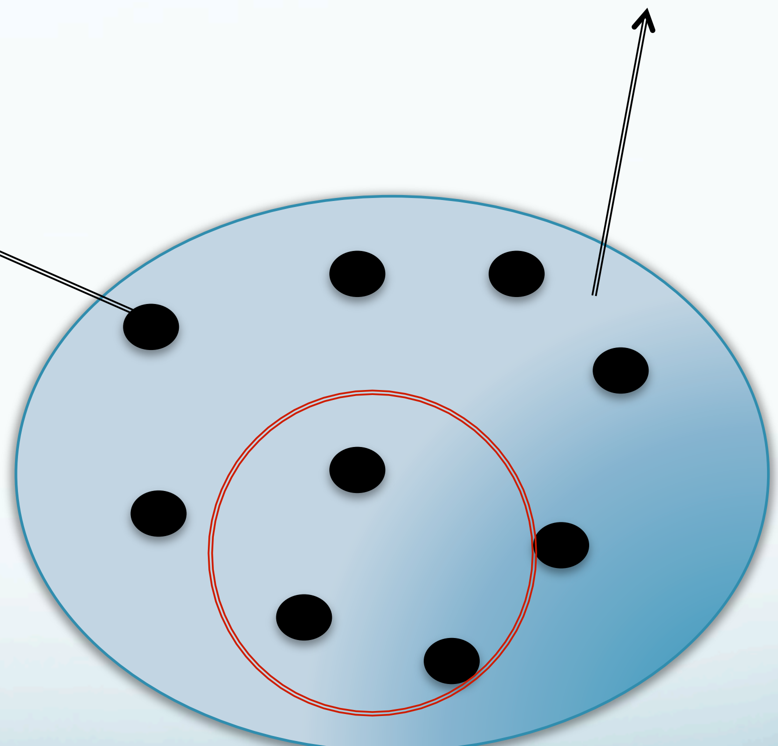
RM Code

List decoding

$P : F^n \to F$

$g : F^n \to F$

$\deg(P) \leq d$



Ball of radius r_0- ε

Number of codewords

Independent of n

List Decoding Radius=largest r_0

RM Code

$F = F_p$
$d < p$

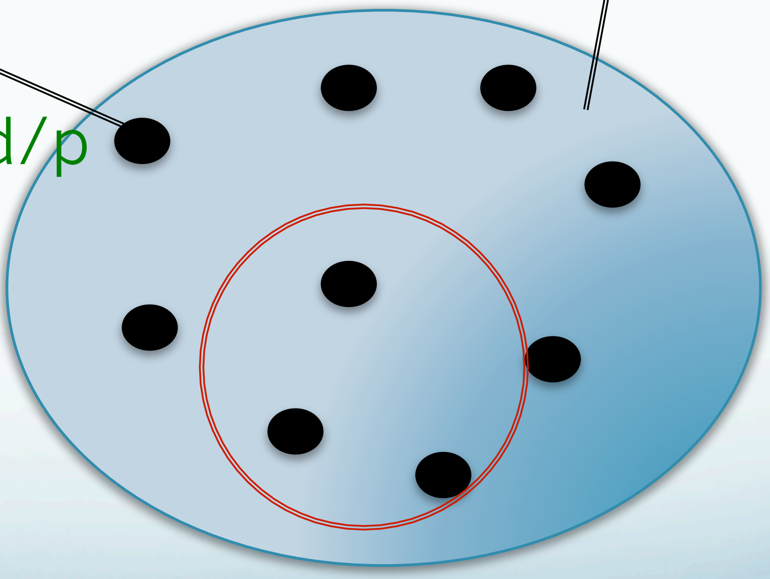
List decoding

$P : F^n \to F$

$g : F^n \to F$

$\deg(P) \le d$

Ball of radius $\delta(d,p) = 1 - d/p$



How many codewords?

$\ge p^n$

$$P(x) = (L(x) - 1)\ldots(L(x) - d)$$

RM Code

$F=F_p$
$d<p$

List decoding

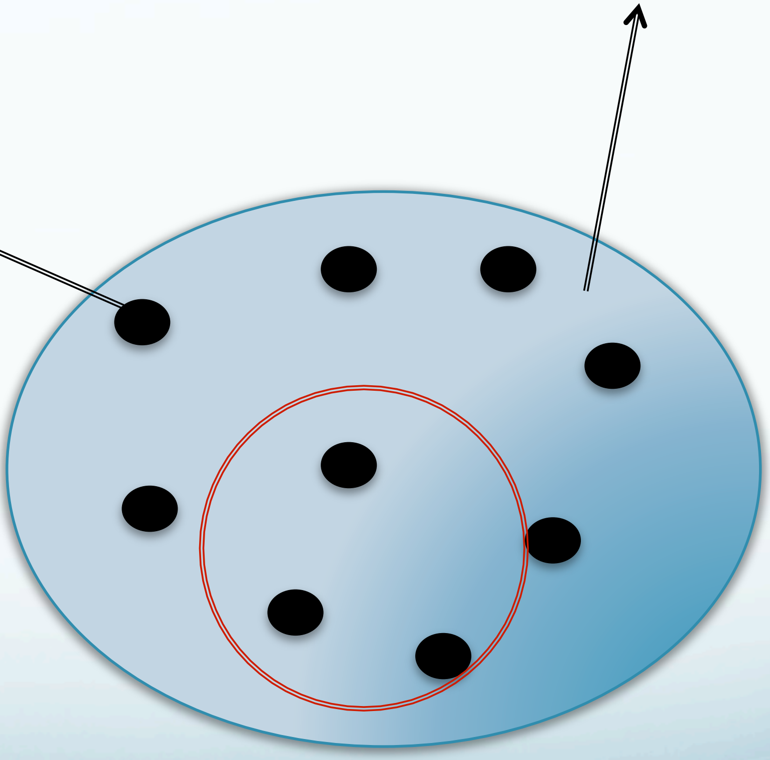
$P : F^n \to F$

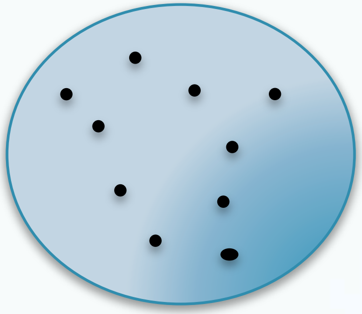
$g : F^n \to F$

$\deg(P) \le d$

Ball of radius $\delta(d,p)-\varepsilon$

How many codewords?





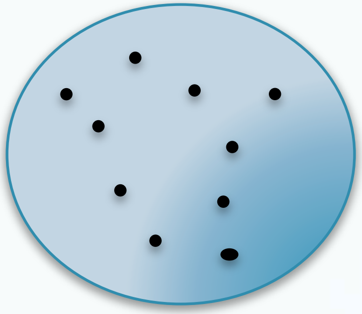
$P: F^n \to F$

$\deg(P) \leq d$

RM Code

List decoding (large fields)

- [Goldreich, Rubinfield, Sudan '95]
- [Sudan, Trevisan, Vadhan '01]
- [Arora, Sudan '03]
- [Sudan '97]
- [Guruswami, Sudan '99]



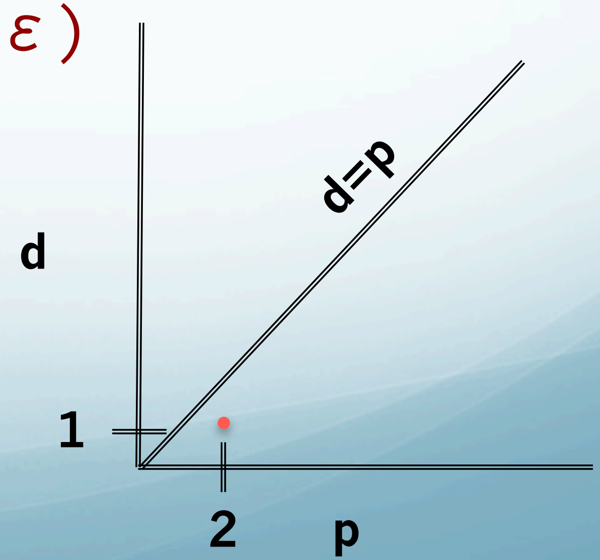
$P: F^n \to F$

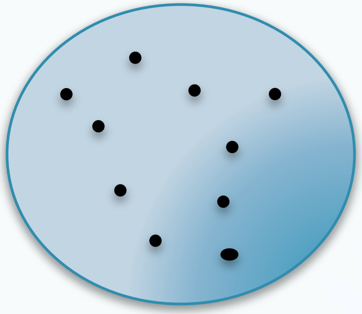
$\deg(P) \le d$

RM Code

List decoding (small fields)

- **d=1, p=2**
- Ball of radius $\delta(d,p) \cdot \varepsilon = 1/2 \cdot \varepsilon$
- No. of codewords = $c(d,p,\varepsilon)$
- **Independent of n!**
- **[Goldreich, Levin,'89]**





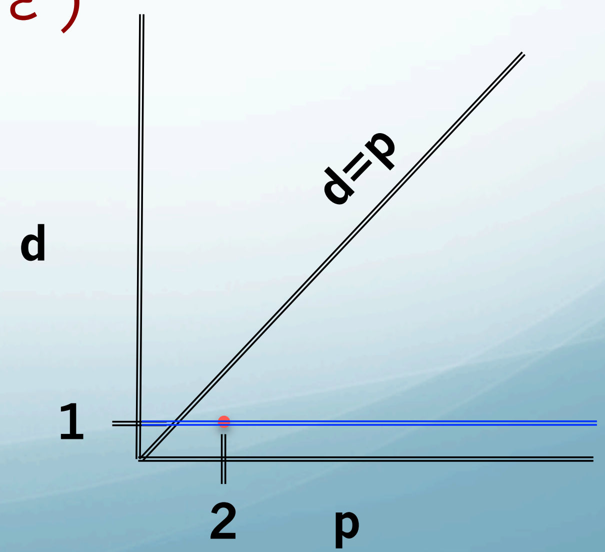
$P: F^n \to F$

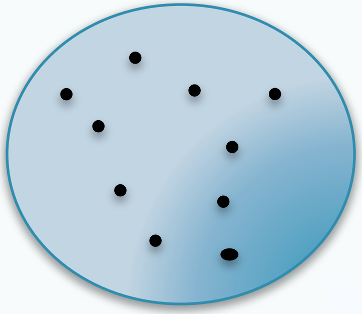
$\deg(P) \leq d$

RM Code

List decoding (small fields)

- **d=1, all p**
- Ball of radius $\delta(d,p) - \varepsilon = 1 - 1/p - \varepsilon$
- No. of codewords = $c(d,p,\varepsilon)$
- **Independent of n!**
- **[Goldreich, Rubinfield, Sudan,'00]**





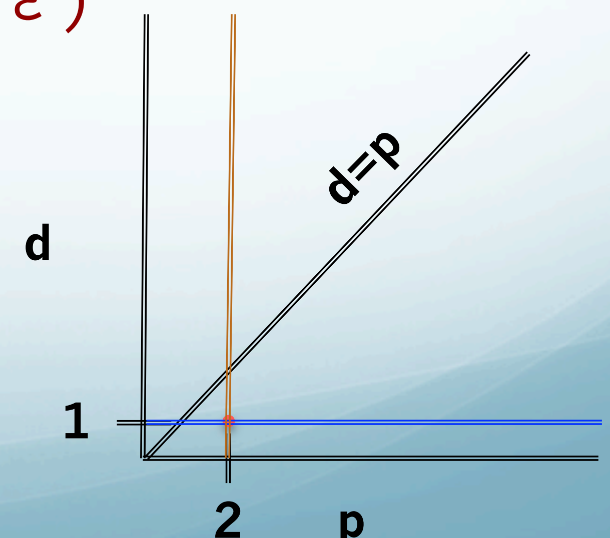
$P: F^n \to F$

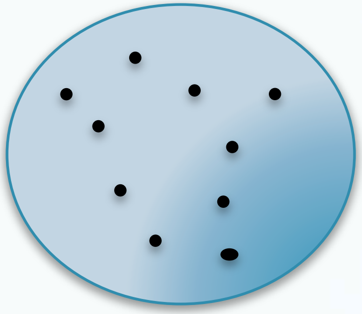
$\deg(P) \le d$

RM Code

List decoding (small fields)

- **all d, p=2**
- Ball of radius $\delta(d,p) \cdot \varepsilon = 1/2^d \cdot \varepsilon$
- No. of codewords = $c(d,p,\varepsilon)$
- **Independent of n!**
- **[Gopalan, Klivans, Zuckerman,'08]**





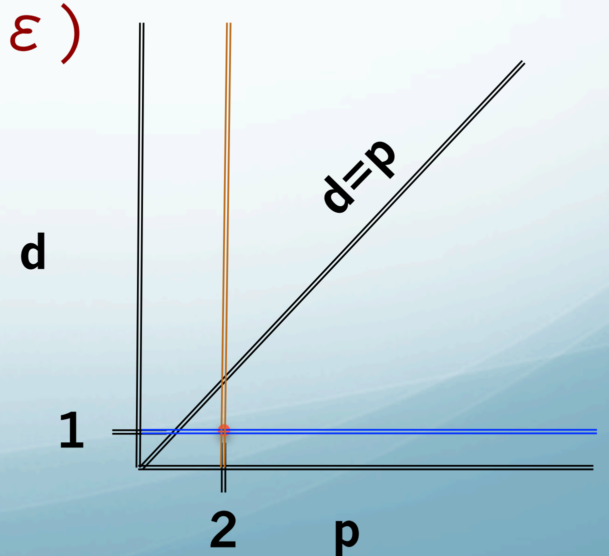
$P : F^n \to F$

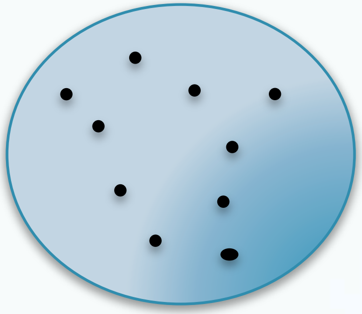
$\deg(P) \le d$

RM Code

List decoding (small fields)

- **all fixed d,p**
- Ball of radius δ(d,p)- ε
- No. of codewords = c(d,p, ε)
- **Independent of n!**
- **Conjectured in [GKZ,'08]**





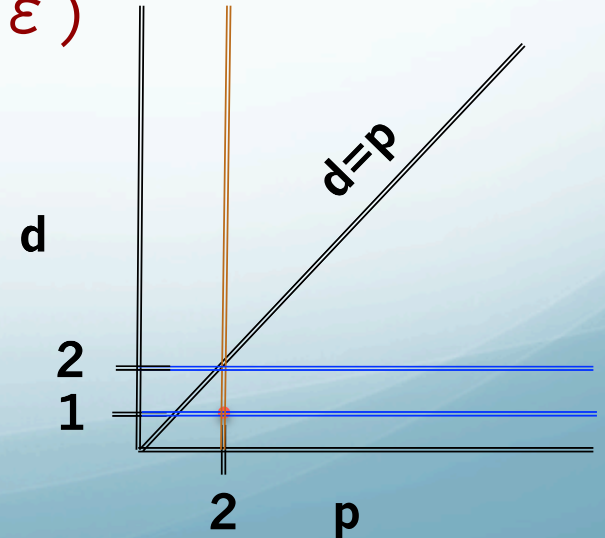
$P : F^n \to F$

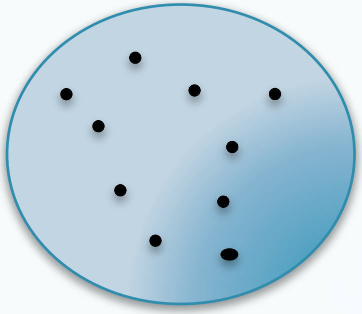
$\deg(P) \le d$

RM Code

List decoding (small fields)

- **d=2, all p**
- Ball of radius δ(d,p)- ε
- No. of codewords = c(d,p, ε)
- **Independent of n!**
- **[Gopalan '10]**





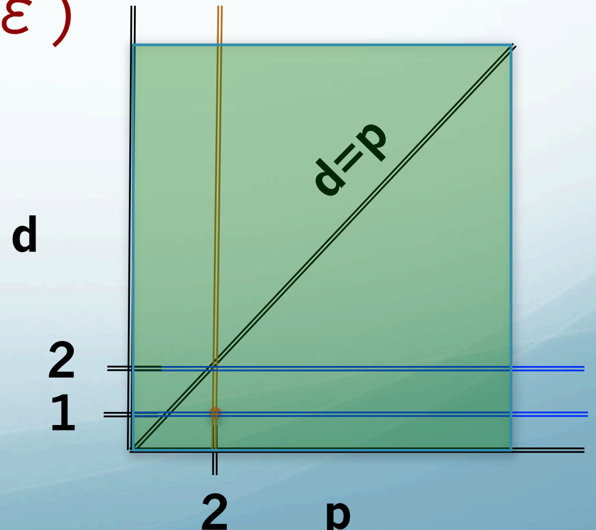
$P : F^n \rightarrow F$

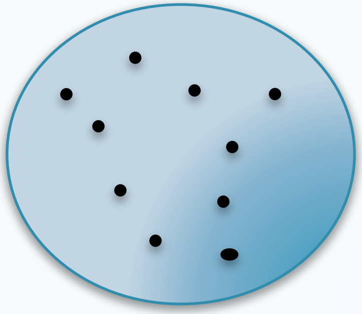
$\deg(P) \leq d$

RM Code

List decoding (small fields)

- **all fixed d,p**
- Ball of radius δ(d,p)- ε
- No. of codewords = c(d,p, ε)
- **Independent of n!**
- **Thm 1 [This work]**





$P : F^n \rightarrow F$

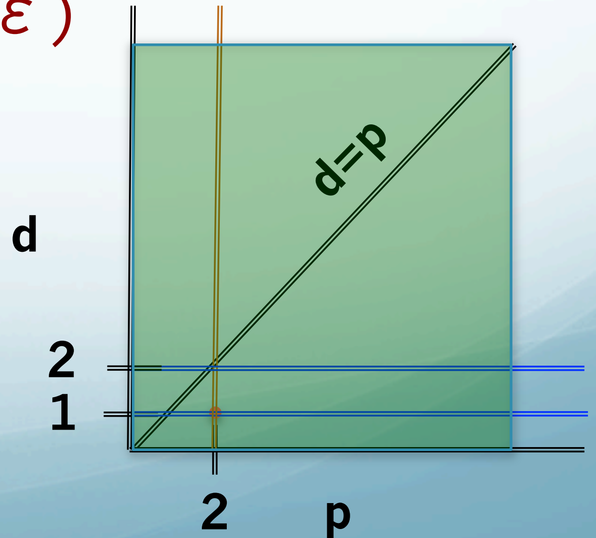
$\deg(P) \leq d$

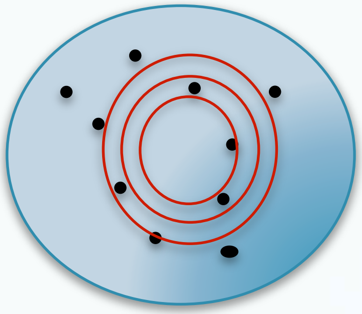
RM Code

List decoding (small fields)

- **all fixed d,p**
- Ball of radius δ(d,p)- ε
- No. of codewords = c(d,p, ε)
- **Independent of n!**
- **Thm 1 [This work]**

Algorithm [Gopalan, Klivans, Zuckerman,'08]





$P : F^n \to F$

$\deg(P) \le d$

RM Code

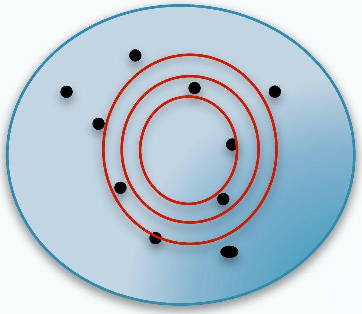
List decoding beyond δ(d,p)

- Fix e <d.
- Ball of radius δ(e,p)- ε =1-e/p- ε
- No. of codewords?

>exp(n^{d-e}) **δ(P,0)=(1-e/p)(1-1/p)**

$$P(x) = (x_1 - 1)\ldots(x_1 - e)(Q(x_3 \ldots x_n) + x_2)$$

$$\deg(Q) \le d - e$$



$P: F^n \to F$

$\deg(P) \le d$

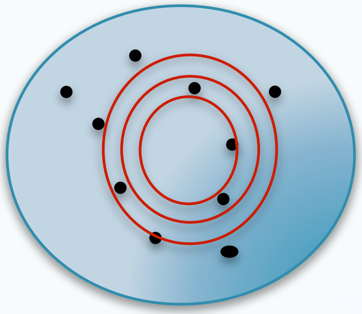
RM Code

List decoding beyond δ(d,p)

- Fix e $<$d.
- Ball of radius δ(e,p)- ε
- No. of codewords?

$< \exp(n^{d-e})$

p=2: [Kaufman, Lovett, Porat, '12]



$P : F^n \rightarrow F$

$\deg(P) \leq d$

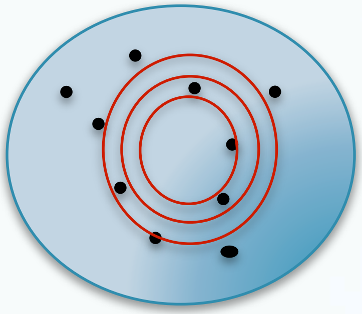
RM Code

List decoding beyond δ(d,p)

- Fix $e < d$.
- Ball of radius δ(e,p)- ε
- No. of codewords?

$$< \exp(O_{p,d,\varepsilon}(n^{d-e}))$$

All fixed p, d. Thm 2 [This work]



$P : F^n \to F$

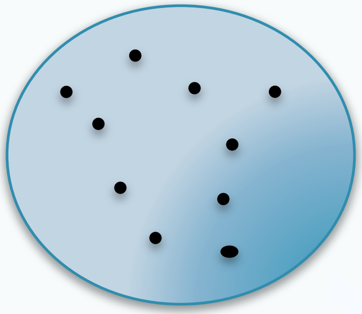
$\deg(P) \le d$

RM Code

Weight distribution

- No. of codewords
- wt(1-e/p- ε)

$$=\exp(\Theta_{p,d,\varepsilon}(n^{d-e}))$$



$P : F^n \rightarrow F$

$\deg(P) \leq d$

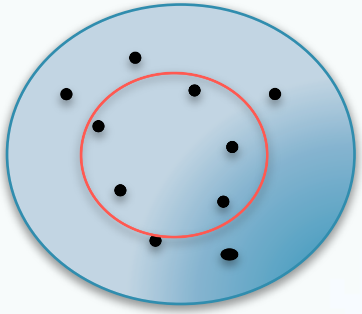
RM Code

Recall Problem ($d<p$)

- No. of codewords
- In ball of radius $1-d/p-\varepsilon$

$< c(p,d,\varepsilon)$

Thm 1



$P: F^n \to F$

$\deg(P) \leq d$

Thm 1

Proof Outline

- Given $g: F^n \longrightarrow F$
- **STEP 1. Weak regularity lemma** – Get low complexity proxy **g'** for **g** made of 'few' low degree polynomials (generalize **Frieze-Kannan '99** weak regularity)
- **STEP 2.** Any **f** close to **g (g')** is a composition of the 'few' low degree polynomials

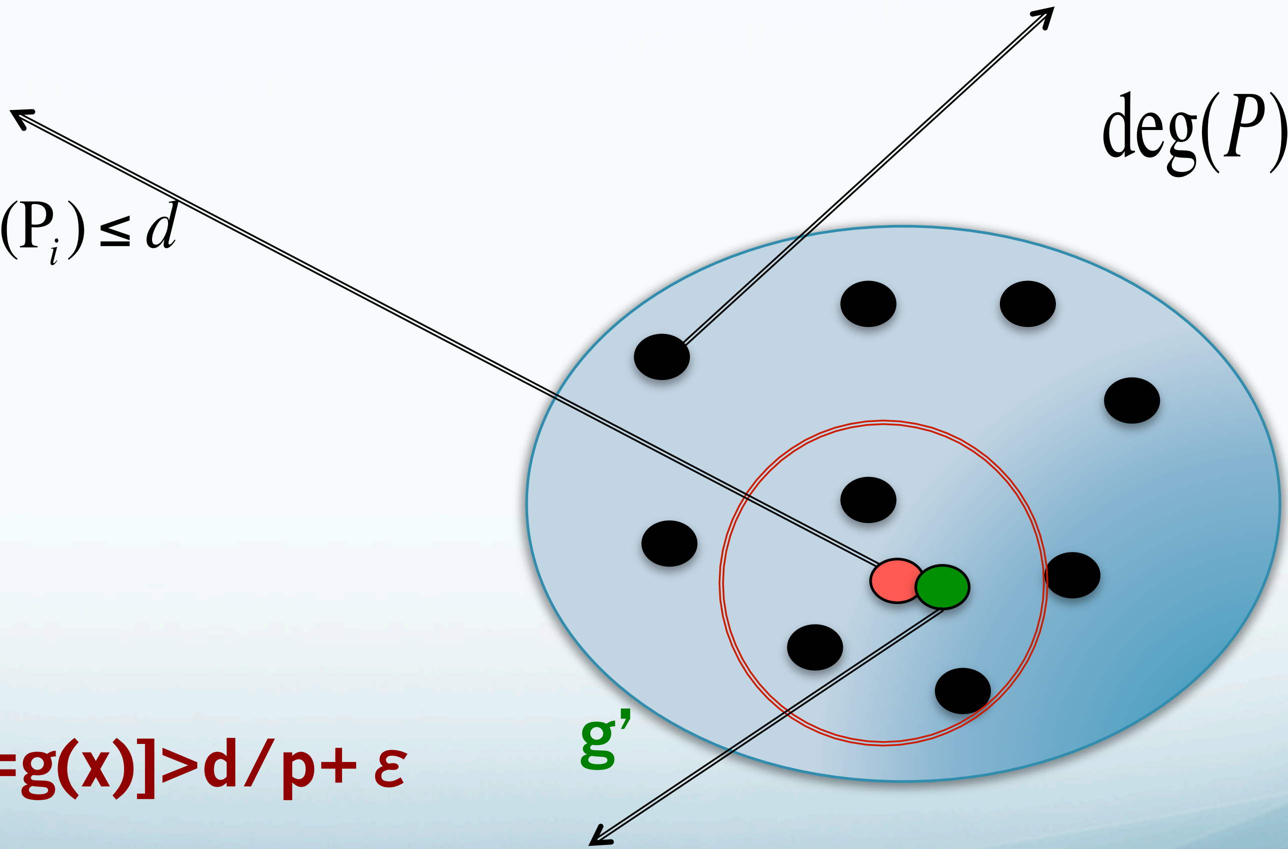
Thm 1
(STEP 1)

$P : F^n \rightarrow F$

$g : F^n \rightarrow F$

$\deg(P) \leq d$

$\exists P_1, \ldots, P_c, \ \deg(P_i) \leq d$



Pr[P(x)=g(x)]>d/p+ ε

⟹ **Pr[P(x)=$T_P(P_1,\ldots,P_c)$)]>d/p+ ε /2**

Thm 1
(STEP 1)

Generalized Weak Regularity Lemma

X,Y arbitrary finite spaces, $\varepsilon > 0$ $\mathcal{F}$ collection of functions from X to Y

Given g:X → Y there exist $f_1, \ldots, f_c$ in $\mathcal{F}$, $c < 1/\varepsilon^2$

such that

For any f in $\mathcal{F}$, there exists $T: Y^c \to Y$

satisfying g'

$$\Pr[f(x) = T(f_1, \ldots, f_c)] > \Pr[f(x) = g(x)] - \varepsilon$$

Thm 1

(STEP 2)

P_i's need to be regular

$g : F^n \to F$

Higher order Fourier Analysis

$\exists P_1, \ldots, P_c, \ \deg(P_i) \le d$

$P(x)=T(P_1,\ldots,P_c)$

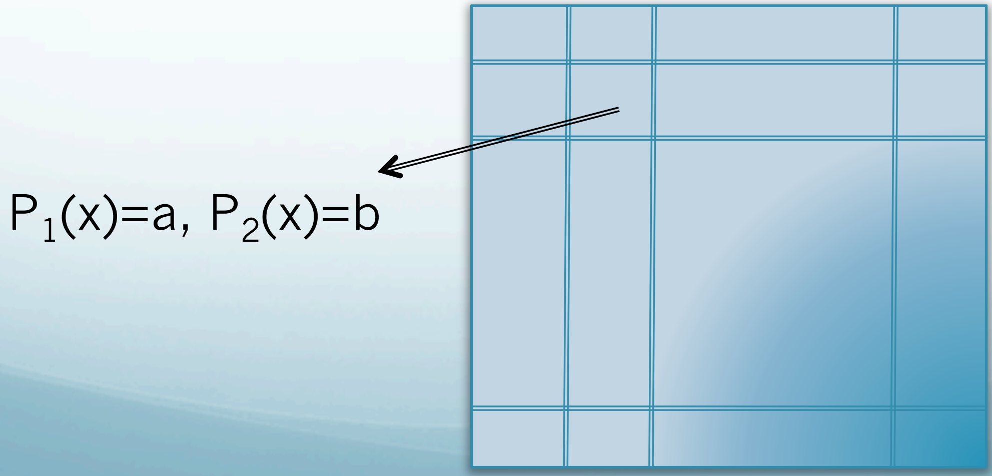
No. of P's < $c(p,d,\varepsilon)$

$\Pr[P(x)=g(x)]>d/p+\varepsilon$

⟹ $\Pr[P(x)=T_P(P_1,\ldots,P_c)]>d/p+\varepsilon/2$

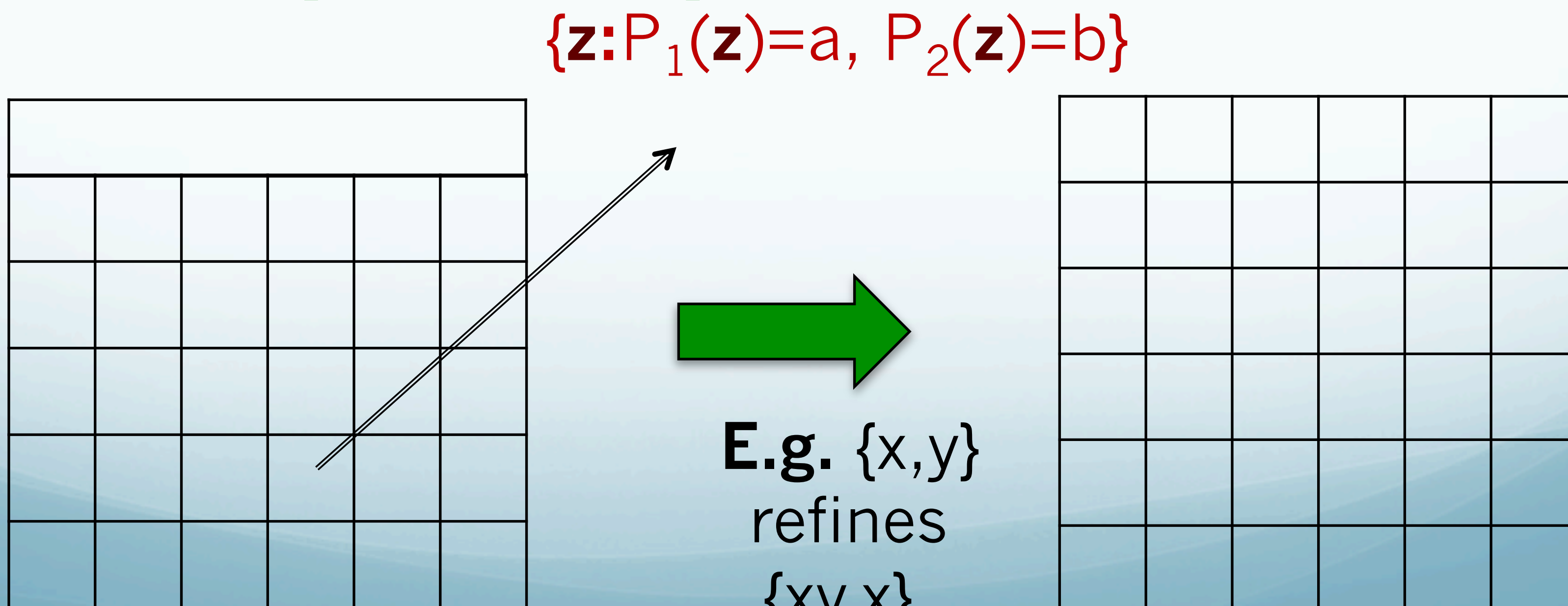
Higher order Fourier Analysis

- **$Rank_d(f)$.** Smallest r s.t. $f=T(f_1,...,f_r)$ where $deg(f_i) \leq d-1$, E.g. $Rank_2(L_1(x).L_2(x)) \leq 2$, $Rank_3(xyzt) \leq 2$ as $xyzt=(xy)(zt)$
- **Factor.** Partition of F^n
- **Polynomial Factor.** Partition of F^n based on collection of polynomials



Higher order Fourier Analysis

- **Rank of Polynomial Factor[Green, Tao '07].** Min **(over nonzero $a=(a_1,a_2)$)** r s.t. $\mathrm{rank}_d(a_1P_1+a_2P_2)=r$, $d=\max_i(\deg(a_iP_i))$
- **Refinement of Factor.** R_1,… is a refinement of Q_1… if fixing $R_1(x)$… fixes $Q_1(x)$….



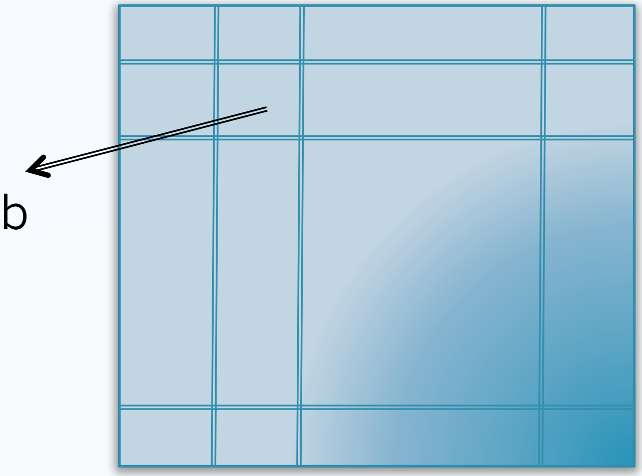
Higher order Fourier Analysis

- **Rank of Polynomial Factor.** Min **(over nonzero $a=(a_1,a_2)$)** r s.t. $\mathrm{rank}_d(a_1P_1+a_2P_2)=r$, $d=\max_i(\deg(a_iP_i))$
- **Refinement of Factor.** $R_1,\ldots$ is a refinement of $Q_1\ldots$ if fixing $R_1(x)\ldots$ fixes $Q_1(x)\ldots$.

High rank polynomial factors essential in analysis

All linear combinations of polynomials have high rank

Higher order Fourier Analysis



$P_1(x)=a,\ P_2(x)=b$

All squares ≈ same size

[Green, Tao'07, Kaufman, Lovett '08]

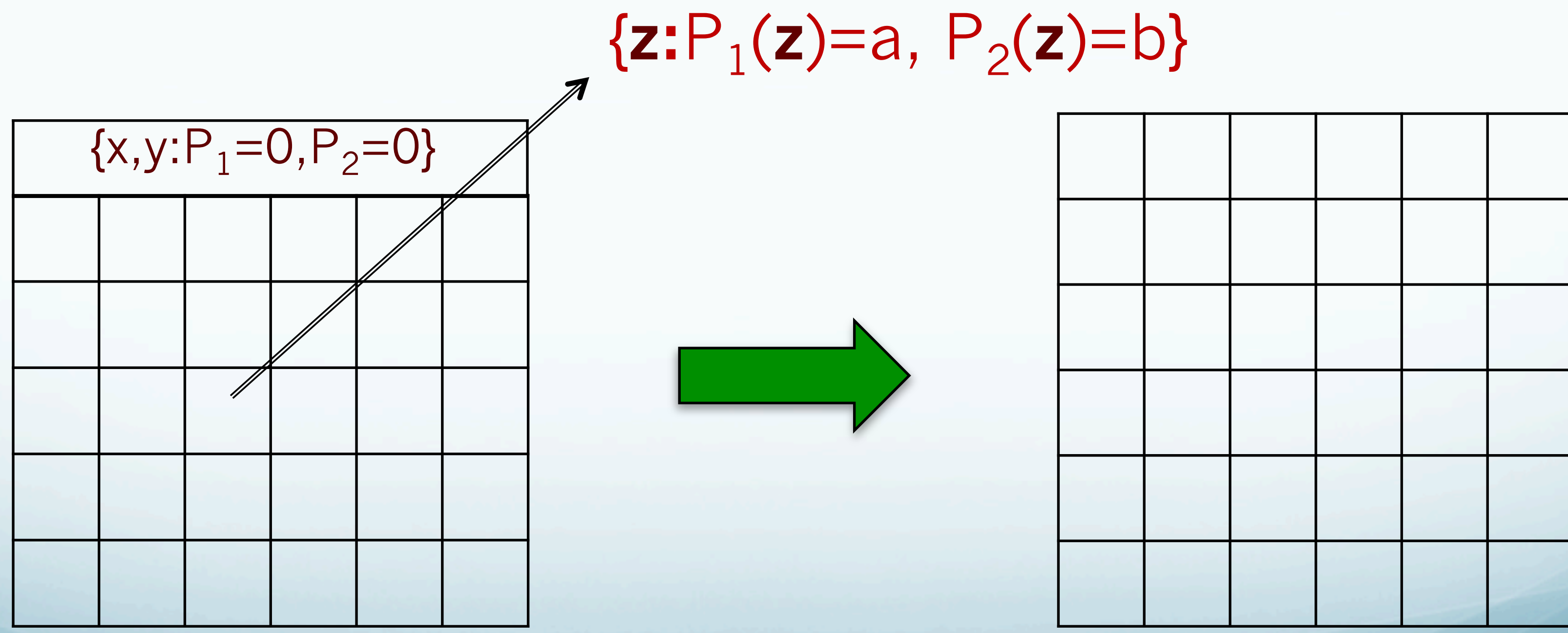
High rank polynomial factors essential in analysis

All linear combinations of polynomials have high rank

Higher order Fourier Analysis

Regularization [Green, Tao'07, Kaufman, Lovett '08, Tao, Ziegler'11]

Refinement that turns



P_1=xy, P_2=x

Q_1=x, Q_2=y

Thm 1
(STEP 2)

P_i's need to be regular

$g : F^n \to F$

Higher order Fourier Analysis

$\exists P_1,\ldots,P_c,\ \deg(P_i) \le d$

$P(x)=T(P_1,\ldots,P_c)$

No. of P's < c(p,d, ε)

$\Pr[P(x)=g(x)]>d/p+\varepsilon$

→ **$\Pr[P(x)=T_P(P_1,\ldots,P_c)]>d/p+\varepsilon/2$**

Thm 1
(STEP 2)

$Pr[P(x)=T_P(P_1,\ldots,P_c)]>d/p$

$\longrightarrow$ $P(x)=T(P_1,\ldots,P_c)$

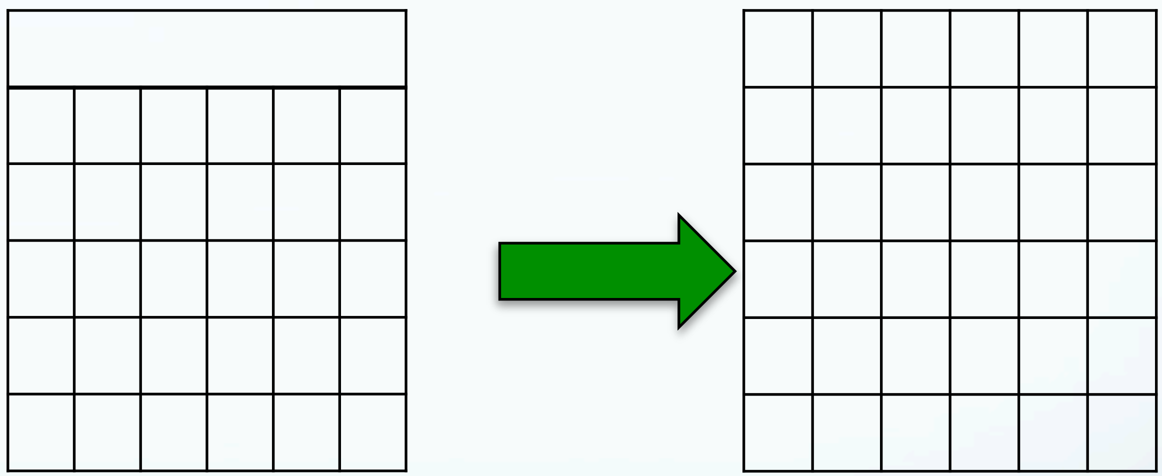
Thm 1
(STEP 2)

$\Pr[P(x)=T_P(P_1,\ldots,P_c)]>d/p$

$P_1,\ldots,P_c$

↓ regularize

$Q_1,\ldots,Q_{c'}$



$\Pr[P(x)=T'_P(Q_1,\ldots,Q_{c'})]>d/p \rightarrow P(x)=T(Q_1,\ldots,Q_{c'})$

Thm 1

(STEP 2)

$\Pr[P(x)=T'_P(Q_1,\ldots,Q_{c'})]>d/p$ → $P(x)=T(Q_1,\ldots,Q_{c'})$

$Q_1,\ldots,Q_{c'},P$

↓ Weakly regularize

$Q_1,\ldots,Q_{c'},R_1,\ldots,R_{c''}$

$P=U(Q_1,\ldots,Q_{c'},R_1,\ldots,R_{c''})$

$\Pr[U(Q_1,\ldots,Q_{c'},R_1,\ldots,R_{c''})=T'_P(Q_1,\ldots,Q_{c'})]>d/p$

Thm 1
(STEP 2)

$\Pr[U(Q_1,\ldots,Q_{c'},R_1,\ldots,R_{c''})=T'_P(Q_1,\ldots,Q_{c'})]>d/p$

More higher order Fourier analysis

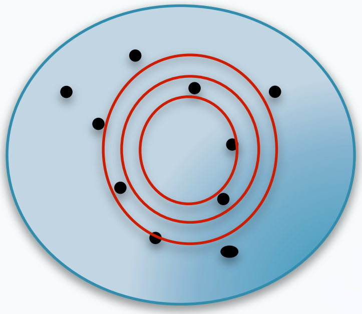
Generalization of
Schwartz-Zippel-DeMillo-Lipton lemma

U does not depend on any R_j

$P(x)=U'(Q_1,\ldots,Q_{c'})$

Thm 1
(General)

- Proof outline for $d<p$ case
- $d \geq p$ case needs introduction of **non classical polynomials [Tao, Ziegler '11]**

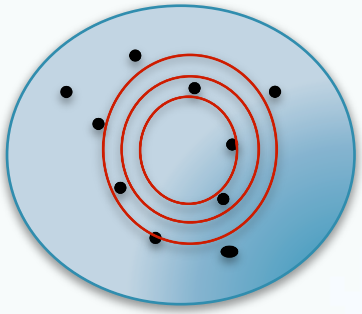


$P : F^n \rightarrow F$

$\deg(P) \leq d$

Thm 2

- Build on the steps of Thm 1
- Develop additional techniques
- esp, in the setting of **non classical polynomials**



$P : F^n \to F$

$\deg(P) \le d$

Conclusion

- **$e \le d$**
- **No. of codewords in ball of radius $\delta(e,p) - \varepsilon$**
- **$< \exp(c_{p,d,\varepsilon}\ n^{d-e})$**

Open Problems

- Improve bounds
- Extend to nonprime fields

Thanks!