

ST08 LECTURE 16

Note Title

4/7/2008

TODAY

Conclude: [PARVARESH - VARDY]

[GURUSWAMI + KOORA]

Rate-optimal list-decoding over large alphabets.

————— x —————

Review of last lecture

PARVARESH-VARDY CODES: Correlated RS Codes.

Message: Degree $< k$ poly P_1 over \mathbb{F}_q

Alphabet: \mathbb{F}_q^2

Encoding: let $P_2 = P_1^D \pmod{h(x)}$

Transmit $\{ (P_1(\alpha_i), P_2(\alpha_i)) \}_{i=1 \dots n}$

Code Specs: $\mathbb{F}_q, \alpha_1, \dots, \alpha_n, k, \leftarrow$ RS stuff
 $D > \binom{n}{k}^{1/3}, h(x), \text{monic, } \hat{\text{irred.}}, \text{deg. } k$ New stuff

Decoding Problem:

Given: Code Specs + $\{(\alpha_i, \beta_i, \gamma_i)\}_{i=1}^n$

Find: All poly P_i s.t.

$$|\{i \mid P_1(\alpha_i) = \beta_i \text{ \& } P_2(\alpha_i) = \gamma_i\}| > t$$

for $P_2 = P_1^D \text{ mod } h(x)$

Algorithm

Step 1: find $Q(x, y, z) \neq 0$ s.t.

- $Q(\alpha_i, \beta_i, \gamma_i) = 0 \quad \forall i$

- $\deg_x Q \leq k^{2/3} n^{1/3}$

- $\deg_y Q, \deg_z Q \leq \left(\frac{n}{k}\right)^{1/3}$

Step 1.5 - while $h(x)$ divides $Q(x, y, z)$

$$Q \leftarrow Q/h;$$

Step 2: let $Q_x^{(y, z)} = Q(x, y, z) \bmod h(x)$

let $P_x(y) = Q_x(y, y^0)$

Output all roots of P_x in

$$E = \mathbb{F}_q[x]/h(x)$$

Analysis: (Won't repeat):

- P_i has agreement $t > 3k^{2/3}n^{1/3}$
 $\Rightarrow P_i$ root of $P_x(y)$.
- $P_x \neq 0$, $\deg P_x$ not too large

Conclude:

- Get code of rate $R = \frac{k}{2n}$
- Corrects $\frac{n - 3k^{2/3}n^{1/3}}{n} = 1 - O(R^{2/3})$
fraction errors.
- Beats $1 - \sqrt{R}$ as $R \rightarrow 0$

Two Improvements

1. Multiplicities: Can use multiplicities trick to get rid of the '3' in $3 \cdot R^{2/3} n^{1/3}$

More precise result:

$$\text{Code of rate } R = \frac{R'}{2}$$

Correcting $1 - (R')^{2/3}$ errors

$$= 1 - (2R)^{2/3} \text{ errors.}$$

2. m -Correlated Polynomials

• Can have $P_1 \dots P_m$

$$P_{i+n} = P_i^D \pmod{h(x)}$$

- Get code of rate R
Correcting $1 - (mR)^{m/(m+1)}$ fraction errors
- Converges to $1 - O(R \log \frac{1}{R})$ fraction errors.

• Great for small rate!

Big rate = ?

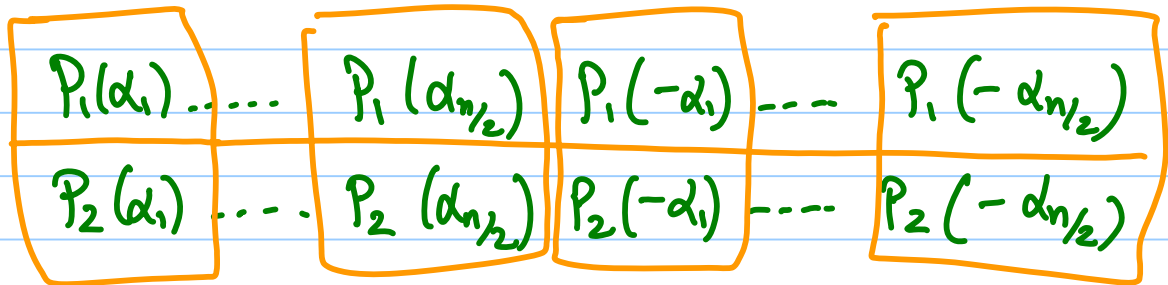
- [GURUSWAMI - RUDRA] Get rid of m
in $1 - (m \cdot R)^{m/(m+1)}$ by Algebraic
Magic.

Idea: (Back in 2 polynomial setting)

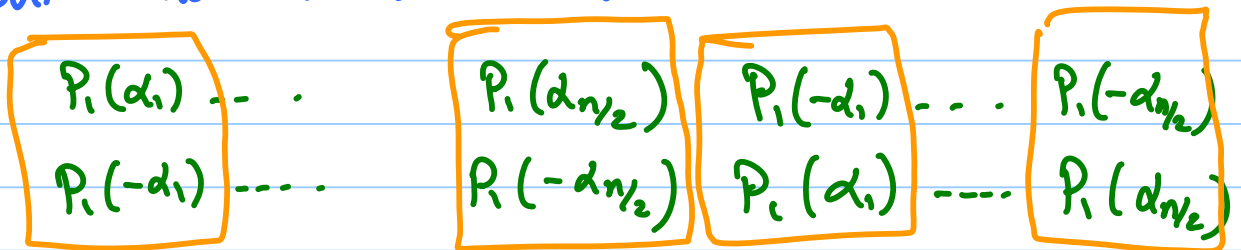
- We're losing factor 2 in rate by using $P_1(x)$, & then $P_2(x)$.

- Could recover this if $P_2(x) = P_1(-x)$ for instance!

- Then we'd be transmitting



- But this is same as



Where i^{th} symbol has same info as $(\frac{n}{2} + i)^{\text{th}}$ symbol.

- Don't need to send second half!
- Recover 2 in rate !!
- Can we implement our wish

$$P_2(x) \triangleq P_1(x)^D \pmod{h(x)} = P_1(-x) \pmod{h(x)}$$

for every P_1 ?

- Parameters under our control:

$h(x)$, D : can choose them as we please.

Some Basic Magic

Issue: How can we guarantee some identity of the form

$$P_i(x)^D = P_i(-x) \text{ for all } P_i?$$

Insight: Using $D = q$ simplifies the quest...

$$\begin{aligned} P_i(x)^D &= \left(\sum c_i x^i \right)^D \\ &= \sum c_i^D x^{iD} \\ &= \sum c_i x^{iD} \\ &= P_i(x^D) \end{aligned}$$

So suffices to have

$$x^D \equiv -x \pmod{h(x)}$$

\Rightarrow need $h(x) \mid x^D + x$

BAD NEWS

Unfortunately ... this ties our hands.

$x^2 + x$ is fixed. Can't have an
irred. factor for most \mathbb{R} .

[GIR] Recovery:

① Let's consider $x^2 - \eta \cdot x$ for some

$$\eta \neq -1.$$

② Don't have to insist $h(x)$ of degree
 \mathbb{R} ; Magic takes care of degrees.

FACT: Let $\alpha \in \mathbb{F}_q^*$ be primitive.

- Then $X^{q-1} - \alpha$ is irreducible.

- Furthermore, $\forall P_i$

$$P_i(x)^q \equiv P_i(\alpha x) \pmod{X^{q-1} - \alpha}$$



• But we no longer have

$$\{P_1(x), P_2(x)\} \equiv \{P_1(\alpha x), P_2(\alpha x)\}$$

• Fix: Imperfect covers

GIR Code :

in our example

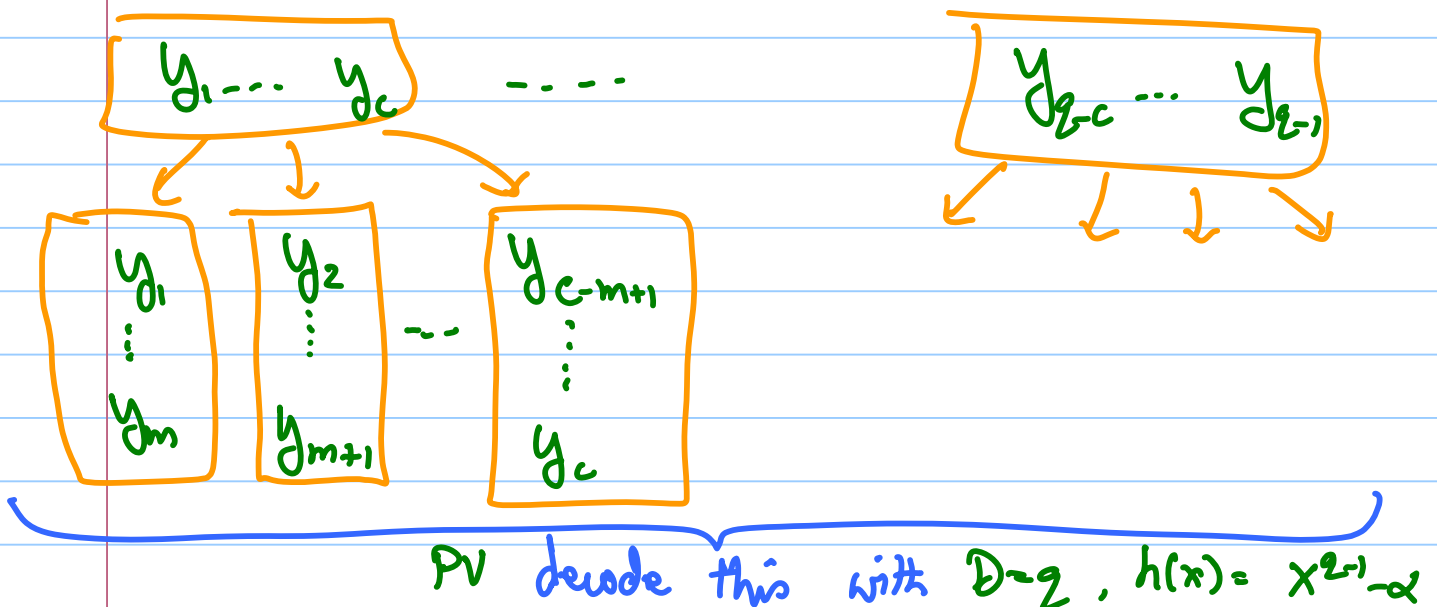
Specs : $\mathbb{F}_2, k, \alpha, (m=2), C=3$

Message : P_i of $\text{deg} < k$

Encoding :



Decoding



Performance

$$\text{Rate } R = \frac{k}{q-1}$$

Error correction: suppose t out of $\frac{q-1}{c}$ agreements

- transfers to $(c-m+1)t = t'$ out of

$n' = (c-m+1) \left(\frac{q-1}{c}\right)$ symbols of PV code in agreement.

- PV decoder needs

$$t' > n' \cdot \left(\frac{k}{n'}\right)^{\frac{m}{m+1}} \text{ agreements}$$

$$- R = \frac{R}{q-1} ; \quad q-1 = \frac{c \cdot n'}{C^{-m+1}}$$

$$\Rightarrow \frac{R}{n'} = \frac{(q-1) \cdot R}{n'} = \frac{c \cdot R}{C^{-m+1}}$$

- [GR] Code is decodable from

$$\left(\left(\frac{c}{C^{-m+1}} \right) \cdot R \right)^{\frac{m}{m+1}} \text{ fraction agreements}$$

$$- \text{let } m = \frac{1}{\epsilon} \quad \& \quad C = \frac{1}{\epsilon^2}$$

$$\text{Then error} = 1 - (1+\epsilon) \cdot R^{(1-\epsilon)}$$

$$\rightarrow 1 - R - f(\epsilon)$$

Conclusions:

- Have found essentially best possible code + decoder over large alphabets.
- Downsides: Runtime = $\text{poly}(n^{1/\epsilon})$... not so nice. Can we do better?
- Questions :- Can RS codes be decoded better?
 - What other forms of folding would work well?