Today (+ Next Lecture)

- [Parvaresh - Vardy '05]
+ [Guruswami - Rudra '06]

"Rate-Optimal, Polychim-list-decodable Codes (over large alphabets)"

---

What

- Reed-Solomon codes + list-decoder, gives codes of rate \((1-p)^2\) correcting \(p\) fraction errors, over alphabet of size \(q(n) = n\).
(How? Set $k = (1-p)^2 n$; RS decoder corrects $1 - \sqrt{\frac{k}{n}}$ fraction errors. 

$1 - \sqrt{\frac{k}{n}} = 1 - \sqrt{(1-p)^2} = p$.)

• But is this the best we can do?

• Existentially: There exist codes of rate $1-p-\epsilon$ over alphabet of size $f(\epsilon)$, that are $(p,\text{poly})$-list-decodable

• Constructively: No “explicit” codes known till 2006.

• [PV+GR] Explicit codes + polytime list decoder, with $q = q(n, \epsilon) = n^{t(\epsilon)}$. 
Folded Reed-Solomon Codes [GR '06]

- Let \( n+1 = q^e \) prime power
- Let \( c = c(n) \) be a constant (incl. of \( n \))
- Let \( \alpha \in \mathbb{F}_q^* \) be a primitive element
  (i.e. \( \mathbb{F}_q^* = \{ \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2^{e-1}} \} \))
- \( \text{FRS}_{n,k,6} \subseteq \subseteq \subseteq \)
  where \( n' = \frac{n}{c} \); \( k' = \frac{k}{c} \); \( \subseteq = \mathbb{F}_q^c \)
  given \( m = m_1, \ldots, m_{k'} \in \mathbb{F}_q^c \)
  view \( m \) as deg. \( k-1 \) poly \( M \in \mathbb{F}_q[x] \)

Encode \( M \rightarrow \)

\[
M(\alpha), M(\alpha^2), \ldots, M(\alpha^c), M(\alpha'^1), \ldots, M(\alpha'^e), \ldots, M(\alpha^n)
\]
(yields \( n' \) elements of \( \subseteq \)!)
Theorem [Gir ’06]: An algorithm of [AV05] can be used to list-decode this code from
\[(1 - \frac{k}{n'} - \varepsilon)\] fraction errors !!!

Rest of these lectures

- Development of these codes/decoders
- Decoding Algorithm
- Analysis
Accidental Discoveries

- [Kiyias + Yunä]: Reed-Solomon decoding from more than $1 - \sqrt{\frac{k}{n}} + \epsilon$ fraction errors appears hard. Maybe can build some cryptographic primitives from this hard problem?

- Example (not from [KY] but useful for us):
  - Suppose $A$ and $B$ share secret $S \subseteq [n]$ which is not known to $E$
  - Then to send $p$ to $B$, $A$ sends $y_1...y_n$ to $B$, where $y_i = p(x_i)$, i.e.
    $$y_i = \text{random o.w.}$$
- B knows $S$, so finding $p$ is just interpolation.
- $E$ does not know $S$, so has to recover message from $1 - \frac{|S|}{n}$ errors... hard (by assumption)!

• **Weakness**: Useful for one-time key exchange, but what happens when $A$ & $B$ use same $S$ to exchange $p_1$ & $p_2$?

• Leads to new code + decoding problem

```
"Interleaved Message"
RS code" (p_1, p_2) \rightarrow \{ (p_1(\alpha), p_2(\alpha)) \}_{\alpha \in \mathbb{F}}
```
- Maps $((\mathbb{F}_q^*)^k)^2$ to $(\mathbb{F}_q^2)^n$

- Error Model: Some symbols in $\mathbb{F}_q^2$ received OK

- Others corrupted at random.

- Is it still hard to recover from $1 - \sqrt{\frac{k}{n}} + \epsilon$ errors?

- [Bleichenschloesser Kiayias Yang]

  Can recover from $1 - \frac{2k+n}{3n}$ random errors!

- [Coppersmith + S.]

  Can recover from $1 - O((\frac{k}{n})^{2/3})$ random errors!
Algorithm

Idea: Now we have triples \( \{(x_i, y_i, z_i)\}_{i=1}^{n} \) and we want to find \( p_1, p_2 \) s.t. for many \( i \in [n] \), \( y_i = p_1(x_i) \), \( z_i = p_2(x_i) \).

Maybe should fit 3-variate poly?

\[ \text{deg.} = 3n^{1/3} \ldots \text{very good!} \]

1st Attempt:

- Find coefficients of \( Q \) by solving some big linear system \( A \cdot v_q = 0 \)

- Stare at \( v_q \).

Conclusion of [CS]: Eyes get tired 😞
2nd Attempt:
- Solve $A^T \cdot w = 0$ where $A$ as before
- $w_i = 0 \Rightarrow$ Erase $(X_i, y_i, Z_i)$.

**Theorem:** [CS]: Comets $1 - O\left(\frac{k}{n}\right)^{2/3}$ random errors, if $q \gg n$.

Motivating questions for [PV]

- Is $\mathcal{O}$-Oh in $1 - O\left(\frac{k}{n}\right)^{2/3}$ necessary?
- Is random errors, the best we can deal with
- Can we stare at 1st Attempt any better?
Some Obstacles

1. Can't correct more worst-case errors unless one can decode more errors in RS codes. (else, just pad RS decoding instance with $Z_i = 0, orall i$)

2. Problem with $A \cdot v_q = 0$ approach.
If lucky we find $Q$ st.

$$Q(x, y, z) = A(x, y, z) \cdot (y - p_1(x)) + B(x, y, z) \cdot (z - p_2(x))$$

Viewing $Q \in \mathbb{F}[x][y, z]$ and plotting all its zeroes, we get a picture like the following
- We are trying to find this point.

- Only information about it we have (if we throw away data) is this...
  
  ... $(x_1, x_2)$ is somewhere on this curve.
Ingenious Idea

Impose a relation on \((p_1, p_2)\) a priori!

\[ Q_{x}(\alpha, \beta) = 0 \]

\[ R(\alpha, \beta) = 0 \]

- Specifically treat \(P_2\) as a message of bit
  \(P_2\) be such that \(R(p_1, p_2) = 0\).

- Now have only few points that could be \((p_1, p_2)\).

  Good News: list-decodable ....

  Bad News: host in rate ... rate = \(\frac{K'}{2n'}\).
Some issues

- For arbitrary $R_x(y, z)$, given $p_1$, finding $p_2$ s.t. $R(p_1, p_2) = 0$ could be non-trivial.

- Even if we find it $p_2$ may have large degree.

- [PV’05] Idea (only “clever” compared to their other idea of introducing $R(y, z)$)
  - Reduce $F[x]$ mod $h(x)$ of deg. $k$.
  - Reduces degree of $p_2$!
  - Make coefficient ring nice (a field if $h(x)$ reducible).
  - $R(y, z) = 2 - y^d$ works!!
[PV ’05]: Code + Decoding
\(L = F_{q^2}^2; \ n = q; \)

- Given message \(p_i(x) \in F_q[x]\) of \(\deg < k\).

- Let \(p_2(x) = p_i(x)^D \mod h(x)\)

* Encoding

\[p_i \mapsto \left\{ (p_i(x), p_2(x)) \right\}_{x \in F_q^2}\]

- Rate \(= \frac{k}{2n}\)
Decoding Problem

Given: \( \{(x_i, y_i, z_i)\}_{i=1}^{n} \)

Find: A list of all deg < \( k \) polys \( y_i \)

such that:
\[
\left| \{ i \mid y_i = f_1(a_i) \} \right| \geq \ell
\]
\[
y_i = y_2(x)
\]

for \( y_2(x) = f_1(x) \mod h(x) \).
**Decoding Algorithm**

**Step 1:** Find $Q$ of degree $\leq k^{\frac{2}{3}} n^{\frac{1}{3}}$ in $x$

$$\leq \left(\frac{n}{k}\right)^{\frac{1}{3}}$$ in $y$

$$\leq \left(\frac{n}{k}\right)^{\frac{1}{3}}$$ in $z$

$s.t.$ $Q(x_i, y_i, z_i) = 0 \quad \forall i$

[if $h(x) \mid Q(x, y, z)$, use $Q/h_i$ instead;]

since $h(x) \neq 0$, $Q_{h_i}(x_i, y_i, z_i) = 0 \ldots$

(Can/Should throw in multiplicities as well.)

**Step 2:** Let $Q_x(y, z) = Q(x, y, z) \mod h(x)$

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

Report all “roots” $p_i(x)$ in $E = \mathbb{F}[x]/h(x)$ satisfying $P_x(p_i(x)) = 0$
Claim 1: Such a poly \( Q \) exists & can be found (Step 1).

Claim 2: If \( P_1 = P_2 = P_i \mod h(x) \)
satisfy \( |\{i \mid \beta_i = P_i(a_i), \alpha_i = P_2(a_i)^3\}| > 3k^{2/3} n^{1/3} \)

then \( Q_x(P_1, P_2) = 0 \mod h(x) \)

Proof: Let \( g(x) = Q(x, P_1(x), P_2(x)) \)

Then \( \deg(g) \leq 3 \cdot k^{2/3} n^{1/3} \)

But \( g(a_i) = 0 \) \( \forall i \in S \)

\( \Rightarrow g = 0 \Rightarrow g \mod h(x) = 0 \)

\( \Rightarrow Q_x(P_1, P_2) = 0 \mod h(x) \).

[Note: \( Q_x(y, z) \neq 0 \).]
Claim 3: $p_i$ is a root of $p_x(y)$  
(Immediate from Claim 3)

Claim 4: $\#$ roots of $p_x$ is bounded by ... 
provided $D > \ldots \left(\left(\frac{n}{k}\right)^{1/3}\right)$

Proof: • First, $Q \neq 0$ - by constraint on Step 1.
  • Next, $Q_x = Q \mod h(x) \neq 0$ since we divided out by $h$.
  • Note $y$-degree of $Q_x \leq \left(\frac{n}{k}\right)^{1/3}$,
    so if $D > \left(\frac{n}{k}\right)^{1/3}$ then $p_x(y) \neq 0$
    (since no pair of monomials cancel each other).
  • But $\deg p_x \leq D \cdot \left(\frac{n}{k}\right)^{1/3}$
  \[\Rightarrow \#\text{roots} \leq D \left(\frac{n}{k}\right)^{1/3} - \left(\frac{n}{k}\right)^{2/3}\]
Conclusions

- Can correct $n - O(k^{2/3} n^{1/3})$ errors.
- With multiplicities $n - R^{2/3} n^{1/3}$ errors.
- But $R = \frac{1}{2} \cdot \frac{k}{n}$

- So only getting codes of rate 
  \[ \frac{1}{2} (1-p)^{3/2} \] correcting $p$ fraction errors.

- CS perspective: Exponent of $1-p$ more important than constant in front. (so this is important)

- Proved formally in [GR '06]: Next lecture!