

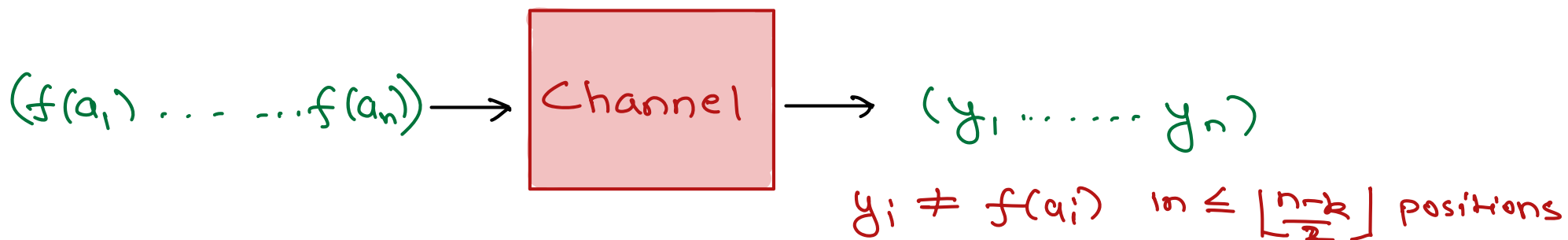
Recap

Reed-Solomon Codes

$$C = \{ (f(a_1), \dots, f(a_n)) \mid f \in \mathbb{F}_q^{\leq (k-1)}[x] \} \quad (\text{fixed } a_1, \dots, a_n)$$

$$\text{Rate} = \frac{k}{n}, \quad \Delta(C) = n - k + 1 \quad (\text{achieves Singleton bound})$$

Unique Decoding



- Find $g, e \in \mathbb{F}_q[x]$ s.t.
 $\deg(e) \leq t, \deg(g) \leq k-1+t$

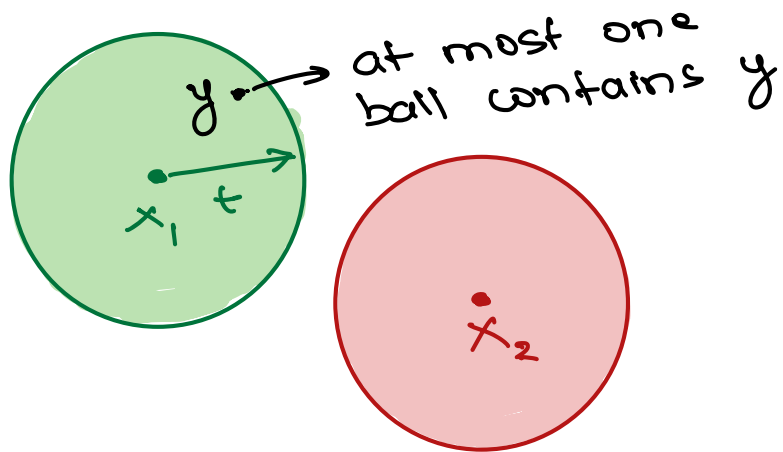
$$\forall i \quad g(a_i) = e(a_i) \cdot y_i$$

► for all solutions $\frac{g}{e} = f$

- Output $\frac{g}{e}$

Beyond Unique decoding

Unique decoding

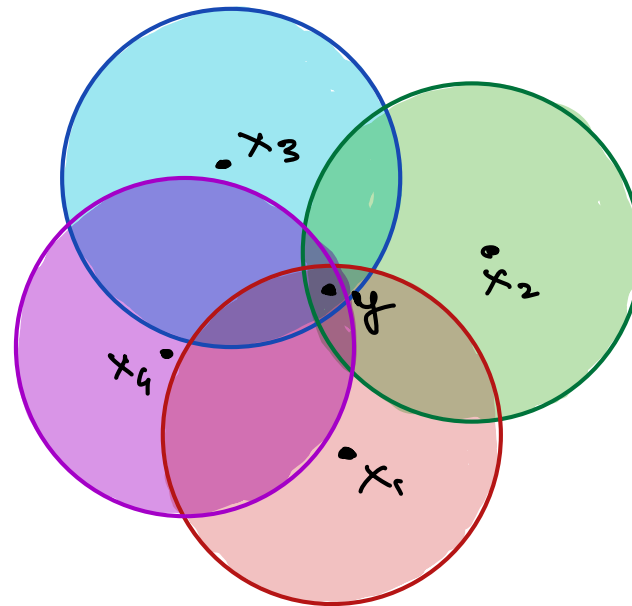


$$2t + 1 \leq \Delta(c)$$

$$t \leq \left\lfloor \frac{\Delta(c) - 1}{2} \right\rfloor$$

$$t \leq \left\lfloor \frac{n - k}{2} \right\rfloor$$

List decoding



Return list $\{x_1, x_2, x_3, x_4\}$

$$t = ?$$

$$t \leq n - 2\sqrt{nk}$$

List decoding Reed-Solomon Codes

[Sudan '97]

Unique decoding: Find g, e s.t.

$$y_i: e(a_i) - g(a_i) = 0 \quad \forall (a_i, y_i)$$

$$h(a_i, y_i) = 0 \quad \text{for } h(x, y) \equiv y \cdot e(x) - g(x)$$

$$h(x, y) = e(x) \cdot \left(y - \frac{g(x)}{e(x)} \right)$$

$f(x)$

List decoding: - Find $h(x, y)$ passing through all points

$$h(a_i, y_i) = 0 \quad \forall i \in [n]$$

- Find **factors** $y - f_j(x)$ of $h(x, y)$

List decoding

- Find $h \in \mathbb{F}_q[x, y]$ s.t.

- $\deg_x(h) \leq d_x$

- $\deg_y(h) \leq d_y$

- $h(a_i, y_i) = 0 \quad \forall i \in [n]$

- Output all f s.t.

- $(y - f(x))$ is a factor of $h(x, y)$ ($\deg f \leq k-1$)

- $|\{i \mid f(a_i) \neq y_i\}| \leq t$

$$h(x, y) = \sum_{\substack{x \leq d_x \\ s \leq d_y}} c_{xs} \cdot x^x y^s$$

$$\begin{bmatrix} \dots & a_i^x y_i^s & \dots \end{bmatrix} \begin{bmatrix} c_{00} \\ \vdots \\ c_{xs} \\ \vdots \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{bmatrix}$$

$$\# \text{ vars} = (d_x + 1) \cdot (d_y + 1)$$

$$\# \text{ eqns} = n$$

$$n < (d_x + 1) \cdot (d_y + 1)$$

Correctness

▶ Let $f(x) \in \mathbb{F}_q^{\leq k-1}[x]$ satisfy $|\{i \mid f(a_i) \neq y_i\}| \leq t$

If $n - t > d_x + (k-1) \cdot d_y$, then $(y - f(x)) \mid h(x, y)$ for any soln. h

Proof.

$$h(x, y) = y^{d_y} \cdot g_{d_y}(x) + y^{d_y-1} \cdot g_{d_y-1}(x) + \dots + y^0 \cdot g_0(x)$$

$$h(x, y) = (y - f(x)) \cdot A(x, y) + B(x)$$

$$h(x, f(x)) = B(x)$$

$h(x, f(x)) = 0$ at $\geq n - t$ points

$$\underbrace{\hspace{10em}}_{\text{deg}} \leq d_x + (k-1)d_y$$

Choosing parameters

$$1) (d_x + 1) \cdot (d_y + 1) > n$$

$$(d_x + 1)(d_y + 1) > d_x \cdot d_y = n$$

$$2) d_x + (k-1) \cdot d_y < n - t$$

$$\text{e.g. } d_x = \sqrt{nk} \quad d_y = \sqrt{\frac{n}{k}}$$

$$t < n - d_x - (k-1)d_y \leq n - 2\sqrt{nk}$$

$$k = \epsilon n$$

$$t < (1 - 2\sqrt{\epsilon}) \cdot n$$

$$|k| + 1 \leq \sqrt{\frac{n}{k}} = \sqrt{\frac{1}{\epsilon}}$$

Reducing q : Reed-Muller codes

Reed-Solomon

$$S = \{a_1, \dots, a_n\} \subseteq \mathbb{F}_q \quad q > n$$

$$H = \{a_1, \dots, a_k\}$$

For any b_1, \dots, b_k

$$C(b_1, \dots, b_k) = \left\{ \begin{array}{l} f \in \mathbb{F}_q^{\leq k-1}[x] \\ f(a_i) = b_i \quad \forall a_i \in H \end{array} \right.$$

$$= \sum_{i=1}^k b_i \cdot \prod_{j \neq i} \frac{x - a_j}{a_i - a_j}$$

$$= \begin{cases} 1 & x = a_i \\ 0 & x = a_j \\ & a_j \neq a_i \end{cases}$$

Reed-Muller

$$S = \mathbb{F}_q$$

$$H \subseteq \mathbb{F}_q, |H| = k$$

For any $h: H^m \rightarrow \mathbb{F}_q$

$$C(h) = \left\{ \begin{array}{l} f \in \mathbb{F}_q[x_1, \dots, x_m] \\ \text{s.t. } \forall a_1, \dots, a_m \in H \\ f(a_1, \dots, a_m) = h(a_1, \dots, a_m) \end{array} \right.$$

$$\forall x_i, \deg_{x_i}(f) \leq k-1$$

Lagrange on steroids

For $a_1, \dots, a_m \in H$ define

$$\delta_{a_1, \dots, a_m}(x_1, \dots, x_m) = \prod_{i=1}^m \left(\prod_{u \in H \setminus \{a_i\}} \frac{x - u}{a_i - u} \right)$$

$\left. \begin{array}{l} \lambda_1 = a_1 \\ \lambda_2 = a_2 \\ \vdots \\ \lambda_m = a_m \end{array} \right\} 0$

For $h: H^m \rightarrow \mathbb{F}_q$

$$f(x_1, \dots, x_m) = \sum_{a_1, \dots, a_m \in H} h(a_1, \dots, a_m) \cdot \delta_{a_1, \dots, a_m}(x_1, \dots, x_m)$$

$$\text{Rate} = \frac{|H|^m \cdot \log q}{q^m \cdot \log q} = \left(\frac{|H|}{q} \right)^m$$

Ex: Check linearity

Distance : Polynomial Identity Lemma (subcase)

$$wt(f) = \left| \left\{ a_1, \dots, a_m \in \mathbb{F}_q \mid f(a_1, \dots, a_m) \neq 0 \right\} \right|$$

Ore '22, Muller '54
Reed '55, Schmidt '76
Demillo - Lipton '78
Zippel '79, Schwartz '80

▶ Let $f \in \mathbb{F}_q[x_1, \dots, x_m]$ with $\deg_{x_i}(f) \leq d_i$. Then

$$q^m \cdot \mathbb{P}_{a_1, \dots, a_m \in \mathbb{F}_q} [f(a_1, \dots, a_m) \neq 0] \geq \prod_{i=1}^m \left(1 - \frac{d_i}{q}\right) \cdot q^m$$

Proof: $f(x_1, \dots, x_m) = \underbrace{x_m^{d_m} \cdot g_{d_m}(x_1, \dots, x_{m-1})}_{\neq 0} + \dots + x_m^0 \cdot g_0(x_1, \dots, x_{m-1})$

$$\mathbb{P}(f(x_1, \dots, x_m) \neq 0) \geq \underbrace{\mathbb{P}(g_{d_m}(x_1, \dots, x_{m-1}) \neq 0)}_{\prod_{i=1}^{m-1} \left(1 - \frac{d_i}{q}\right)} \cdot \underbrace{\mathbb{P}(f \neq 0 \mid g_{d_m} \neq 0)}_{\left(1 - \frac{d_m}{q}\right)}$$

$$\prod_{i=1}^{m-1} \left(1 - \frac{d_i}{q}\right)$$

$$\left(1 - \frac{d_m}{q}\right)$$

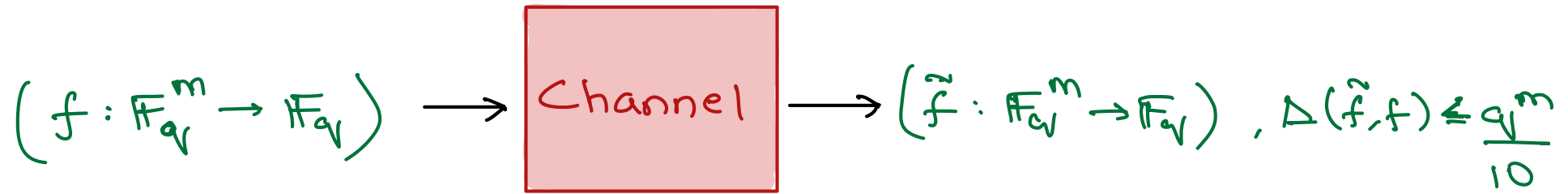
Local Decoding

- Can recover $h(a_1, \dots, a_m)$ in time $\text{poly}(q, m)$

with (say) $t = \frac{1}{10} \cdot q^m$ errors.

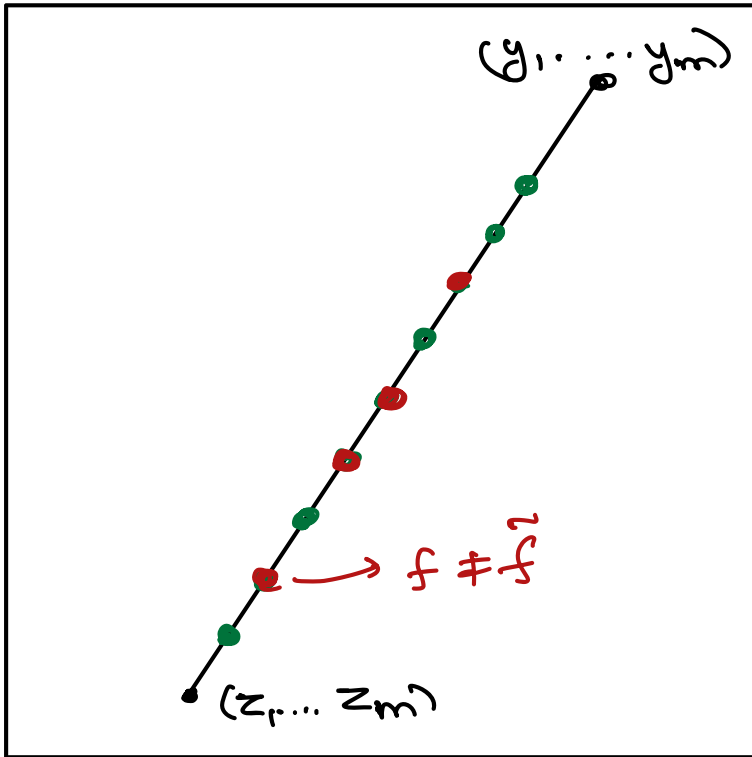
Even reading codeword
takes time q^m !

- Algorithm must be randomized.



$\deg_{x_i} f \leq k-1$
 $q \geq 5km$

\exists randomized A s.t. $\mathbb{P}[A(z_1, \dots, z_m) = f(z_1, \dots, z_m)] \geq \frac{1}{4}$
 $(\forall z_1, \dots, z_m)$



$\mathcal{L}_y = \{ (z_1, \dots, z_m) + u \cdot (y_1, \dots, y_m) \mid u \in \mathbb{F}_q \}$

$f(\mathcal{L}_y(u)) = f((z_1, \dots, z_m) + u \cdot (y_1, \dots, y_m))$

polynomial in one variable u .

$$\mathbb{P}_{y_1, \dots, y_m} [f(y_1, \dots, y_m) \neq \hat{f}(y_1, \dots, y_m)] \leq \frac{1}{5}$$

$$\mathbb{P}_{\vec{y} \in \mathbb{F}_q^m} \mathbb{P}_{u \in \mathbb{F}_q} [f(\vec{z} + u \cdot \vec{y}) \neq \hat{f}(\vec{z} + u \cdot \vec{y})] \leq \frac{1}{5}$$

$$\mathbb{P}_{\vec{y} \in \mathbb{F}_q^m} \left[\mathbb{P}_{u \in \mathbb{F}_q} [f(\vec{z} + u \cdot \vec{y}) \neq \hat{f}(\vec{z} + u \cdot \vec{y})] \geq \frac{2}{5} \right] \leq \frac{1}{4}$$

- Find f on line $l_{\vec{y}}(u) \equiv g(u)$

- Output $g(0)$