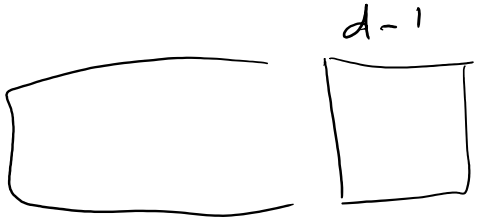
TI-Lecture-21-4-2020

21 April, 2020 13:56

Singleton bound: $(n, k, d) \Rightarrow n \geq k + d - 1$

- n: codeword length
- k: log # of words = dimension of the code
- d: minimal distance of the code



$$2^k \leq 2^{n-(d-1)}$$

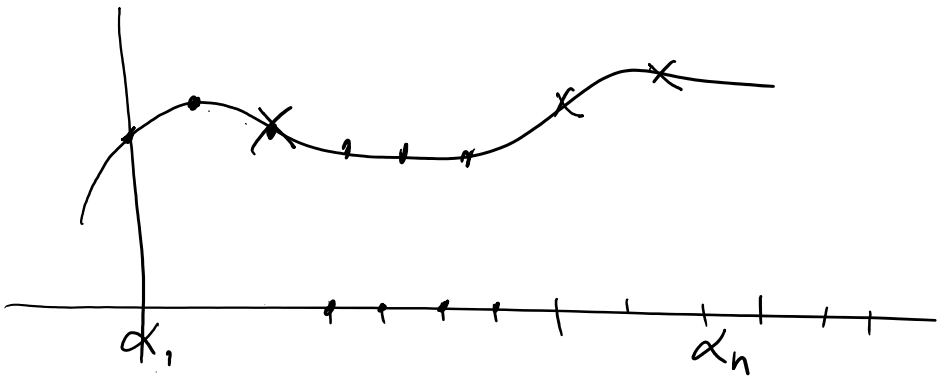
$$k \leq n - (d-1)$$

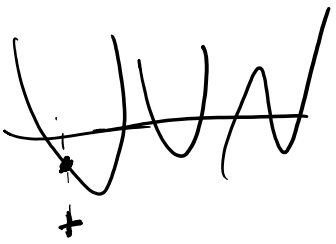
$$d - 1 + k \leq n$$

$$d \leq n + k + 1$$

Reed-Solomon codes

$\mathbb{Z}_p$, $\mathbb{R}$





- degree k polynomial has at k roots
- $k+1$ points with corresponding values determine the polynomial

Finite fields: $\mathbb{R}$, $\mathbb{C}$ ... infinite fields

finite fields: $\mathbb{R}$, $\mathbb{C}$ ... infinite fields

$x \to \frac{1}{x}$

- $(+, \cdot, 0, 1)$ $\quad \mathbb{F} \ni 0, 1$

$\frac{a}{b} = a \cdot b^{-1}$

$\frac{1}{6}$

$\mathbb{F} \setminus \{0\}$ ... group $\cdot$ / : $\quad -1$

↑ group +/-

EX: $\mathbb{Z}_p \cong (\{0, \dots, p-1\}, +_{(\mathrm{mod}\, p)}, \cdot_{(\mathrm{mod}\, p)}, 0, 1)$

$\forall a \in \{0, \dots p-1\}$

$\exists\, a^{-1} \in \{0, \dots p-1\}$ $\quad a \cdot a^{-1} = 1$

$\mathbb{Z}_p = GF[p]$ ... Galois Field of size p.

$GF[p^s]$ $\quad \dots \quad p^s$

$s \geq 1$

no other Finite fields $\Leftrightarrow$ p prime

p^2 $\quad GF[p^2] \neq \mathbb{Z}_{p^2}$ $\quad$ (EXC)

$GF[p^2] = \{\{0, \dots p^2-1\}, +_{\mathrm{mod}\, p^2}, \cdot_{\mathrm{mod}\, p^2}, 0, 1\}$

$(\{0, \dots p-1\}^s, +_{\mathrm{mod}\, p}, \cdot, \dots, (0,0,\dots 0), (0,0,\dots 0,1))$ $\quad \cdot p = 0 \pmod{p^2}$

↑ coordinate-wise

$\|$

coefficients of degree $\leq s-1$ polynomial over $GF[p]$

$(c_{s-1}, \dots, c_1, c_0)$ $\quad \sum_{i=0}^{s-1} c_i \cdot x^i = p_{c_0, \dots c_{s-1}}(x) =$

$p + q =$

$p \cdot q \pmod r$

$p \cdot g \pmod r$

degree s irreducible polynomial

not a product of lower degree polynomials

$\longrightarrow GF[2^8]$

$\longrightarrow GF[2^{32}]$

$GF[p]$ map

$GF[p^s]$ $s \geq 2$ polynomials of degrees $\leq s-1$

$\longrightarrow$ coding theory

- $\mathbb{F}$ finite field : degree s polynomial has at most s roots
  : systems of linear equations - Gauss elimination

Reed - Solomon codes

n, k

$\mathbb{F}$ ... field of size $\geq n$.

$\alpha_1, \alpha_2, \ldots \alpha_n \in \mathbb{F}$ distinct

$m \in \mathbb{F}^k$

$\| $

$(m_1, \ldots, m_k)$

$$p_m(x) = \sum_{i=0}^{k-1} m_{i+1} x^i$$

codeword For m ... $\langle p_m(\alpha_1), p_m(\alpha_2), \dots, p_m(\alpha_n) \rangle$

$[n, k, d]_{\mathbb{F}}$

- linear code: m, m' $\quad p_m, p_{m'}$

$$\begin{array}{l} \langle p_m(\alpha_1), \dots \rangle \\ + \langle p_{m'}(\alpha_1), \dots \rangle \\ \hline \langle \underbrace{p_m(\alpha_1) + p_{m'}(\alpha_1)}_{p_{m+m'}(\alpha_1)}, \dots \rangle \end{array}$$

$m + m'$ $\qquad C(m) + C(m') = C(m' + m)$

$\alpha \in \mathbb{F}$ $\qquad \alpha \cdot C(m) = C(\alpha \cdot m)$

$= (\alpha m_1, \alpha m_2, \dots, \alpha m_k)$

generating matrix G:

$$\begin{array}{c} \\ m_1 \\ m_2 \\ \\ \\ m_k \end{array} \begin{pmatrix} \overset{1}{\alpha_1^0} & \alpha_2^0 & \cdots & \overset{1}{\alpha_n^0} \\ \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_n^1 \\ & & & \\ & & & \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \cdots & \alpha_n^{k-1} \end{pmatrix}$$

$$\downarrow \qquad \downarrow \qquad\qquad \downarrow$$

$$\langle p_m(\alpha_1) \quad p_m(\alpha_2) \quad \cdots \quad p_m(\alpha_n) \rangle$$

$m \cdot G = C(m)$

$k \times n$

minimal distance d: (for linear codes C

min. distance $= \min_{x \neq 0} \omega_{Ham}(x)$.)

$x \in C$
$x \neq 0^n$

$$\left[\Delta_{Ham}(\bar{x}, \bar{y}) = \Delta_{Ham}(\bar{x} - \bar{y}) \right]$$

- How many 0's can a codeword have?

$\longrightarrow$ at most $k-1$ b/c $\deg \leq k-1$.

on non-zeros $\geq n - (k-1) = n-k+1$.

$\Rightarrow$ $d = n - k + 1$ (by Singleton bound)

RS:

$[n, k, n-k+1]_{\mathbb{F}}$ ... code

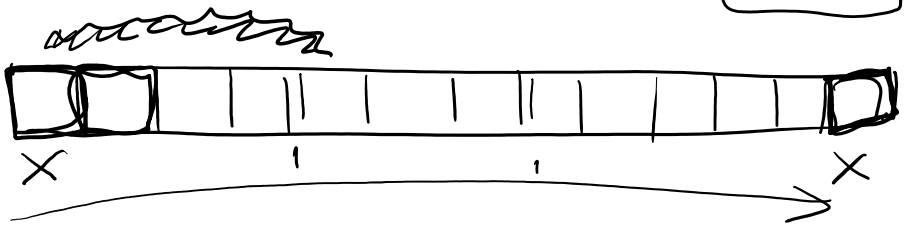
Ex: $n = 2k$ $[2k, k, k+1]_{\mathbb{F}}$

able to correct $\frac{k}{2}$ errors.

Ex.: $|\mathbb{F}| = 256$ $n = 256$ ...

able to correct $\frac{n-k}{2}$ errors

(Field elmts) $256 \cdot 8 = 2048$



Ex: $k = n-4$ $[n, k, 5]_{\mathbb{F}}$ 2 errors

as a binary code $[n \cdot \log \mathbb{F}, k \cdot \lg \mathbb{F}, 5]_2$

$GF = 2^q$ $[nq, kq, \frac{5}{2}]_2$ can correct

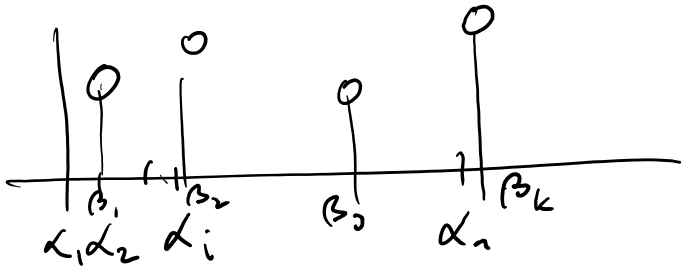
ideally $[n_2, k_2, 5_2]_2$ two bit errors.

- How do we decode?

Berlekamp - Walch (1986)

$\langle p_m(\alpha_1), p_m(\alpha_2), \dots p_m(\alpha_n) \rangle \longrightarrow$

$\langle r_1, r_2, \dots, r_n \rangle$ decode?



correct k points

Can you decode?

Lagrange interpolation

$\beta_1, \beta_2, \dots \beta_k$ distinct ~~pt's~~ pt's with known value

$$L_{i, \beta_1, \dots \beta_k}(x) = \frac{\prod_{j \neq i} (x - \beta_j)}{\prod_{j \neq i} (\beta_i - \beta_j)} = \begin{cases} 1 & x = \beta_i \\ 0 & x = \beta_j \ j \neq i \\ * & \text{o/w} \end{cases}$$

deg $= k-1$

$r_i \dots$ known values of p in β_i $\quad p(\beta_i) = r_i$

$$p(x) = \sum_{i=1}^{k} r_i \cdot L_{i, \beta_1, \dots \beta_k}(x)$$

if we know which places are correct we can recover $p(x)$ easily and read-off the message.

$\rightarrow O(n^3)$

→ How to find which places are correct?

error locating polynomial $E(x)$:

- "small" degree (but $\not\equiv 0$)
- $r_i \neq p_m(\alpha_i) \Rightarrow E(\alpha_i) = 0$

$\frac{n-k-1}{2} \simeq \frac{d}{2}$

$d_e \dots \deg E(x) \quad 1 \leq d_e \leq \#\text{errors}$

$\forall i \in \{1, \dots n\} \quad (r_i - p_m(\alpha_i)) \cdot E(\alpha_i) = 0$

$\forall i \in \{1, \dots, n\} \; r_i E(\alpha_i) = p_m(\alpha_i) \cdot E(\alpha_i)$

$p_m(x) \cdot E(x) = Q(x)$

$\deg Q(x) \leq \frac{n+k-3}{2}$

$= \quad \leq \frac{n-k-1}{2}$

$Q(x) = \sum_{i=0}^{\frac{n+k-3}{2}} c_i' x^i$

$E(x) = \sum_{i=0}^{n-k-1/2} c_i x^i$

⇒ system of linear equations in unknowns

$c'_0 \dots c'_{\frac{n+q-3}{2}}$, $c_0, \dots c_{\frac{n-k-1}{2}}$.

n eq's in n variables

→ solve it to find the coefficients.

— look for non-trivial solution.

15:55