TI-Lecture-14-4-2020

14 April, 2020 13:45

k bit message m

$x = E(m) \rightsquigarrow y \Rightarrow dec(y) = m$

error prob p

$r = \frac{k}{n}$ $\quad r < 1 - H(p)$

$\frac{1}{1 - H(p)}$

Shannon

n bit $\quad$ np errors

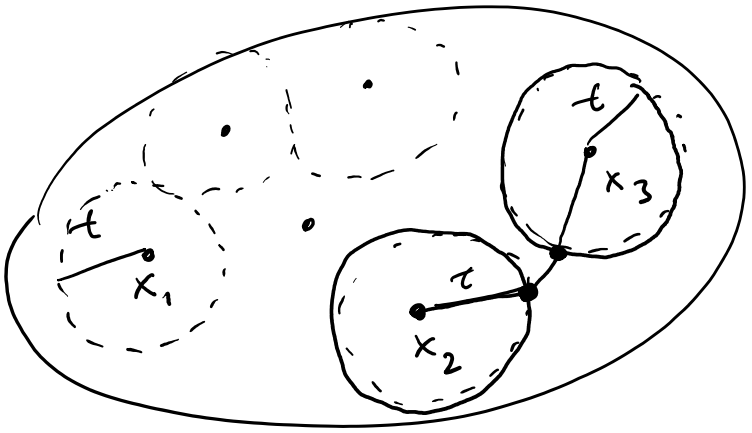
Hamming

n bit $\quad$ want to be able to correct t errors

$\approx np$

$\Rightarrow$ design a code able to correct t errors

$\{0,1\}^n$



$\{0,1\}^n$

D_x

distance between any two codewords has to be at least $2t+1$

$C \subseteq \{0,1\}^n$

~~$\min(C)$~~ ↑ minimal

distance of C = $\min_{\substack{x,y \in C \\ x \neq y}} d_{Ham}(x,y)$

Claim: ~~if~~ minimal distance of $C \geq 2t+1$ if then C can correct t errors.

$(n, k, d)_2$ ← alphabet size

k ↑ $\log|C|$

d ↖ minimal distance of C

Shannon $k = (1 - H(p))n$
$d \approx pn$

Want: efficient encoding $k \to n$
efficient decoding $n \to k$

Hamming code (binary)

$x_1 \dots x_k$

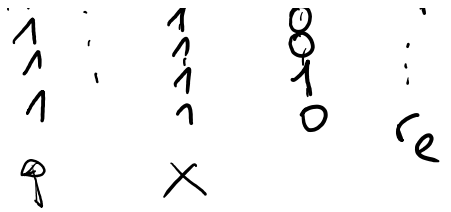
$r = \sum x_i \pmod 2$

$\to x_1 \dots x_k r$ $\quad (k+1, k, 2)$

cannot correct any error
can detect one error.

x_1	$\dots$	x_i	$\dots$	x_k	
1	$\dots$	1	$\dots$	0	r_1
1	$\dots$	1	$\dots$	0	$\vdots$
1	$\dots$	1	$\dots$	1	$\vdots$
1	$\dots$	1	$\dots$	1	

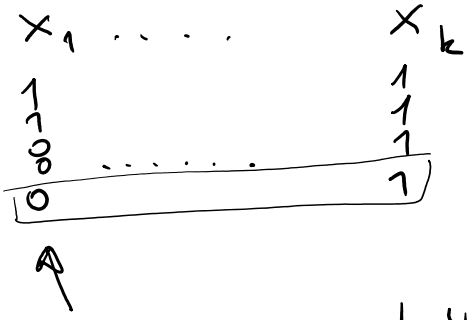
$\to x_1 \dots x_k r_1 \dots r_e$



$\rightarrow x_1 \dots x_k r_1 \dots r_\ell$

1) all characteristic vectors of parities need to be distinct

2) each char. vector has to contain at least two ones.



$k = 2^\ell - \ell - 1$

$\rightarrow x_1 \dots x_k r_1 \dots r_\ell$

each message bit labelled by a distinct vector of parity bits $\in \{0,1\}^\ell$ having at least two ones.

$\rightarrow \left[2^\ell - 1, 2^\ell - \ell - 1, 3\right]_2$ → needs to be argued

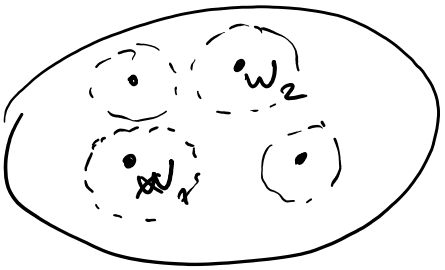
decoding:

1) error in parities – exactly one parity wrong

2) error in the message → at least two parities wrong

the wrong parities exactly reveal the flipped bit.

- corrects one error ⇒ distance ≥ 3.



balls of radius 1 around each codeword cover precisely the whole $\{0,1\}^n$.

... "perfect code".

- linear code $GF[2]$ $+, \cdot \pmod 2$

$[7,4,3]_2$

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

G generating matrix for C

$x \in \{0,1\}^4 \qquad xG = xr$

encoding message $x \in \{0,1\}^k \rightarrow xG$

$G \in \{0,1\}^{k \times n}$ ... generating matrix

parity check matrix: $H \in \{0,1\}^{n \times n-k}$

$\forall y \in \{0,1\}^n \qquad yH = 0 \Leftrightarrow \exists x \text{ s.t. } xG = y \in \{0,1\}^k$

G H is a basis of the orthogonal complement of G.

$G h_i = 0$ ⇄ $H = (h_1 | h_2 | \dots | h_{n-k})$

$G = \begin{pmatrix} g_1 \\ \vdots \\ g_k \end{pmatrix}$ $\quad g_j H = 0$

H is a basis of solution space for the system of lin. eq..

dim G = k (o/w two msg. are mapped to the same codeword)

Ex: $[7,4,3]_2$ ... proj check matrix

$$H = \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \\ 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix} \quad G = \begin{pmatrix} 1&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{pmatrix}$$

identity matrix k×k ; $n-k$

$x \in \{0,1\}^n$ $\quad xG = y$ $\quad y + e_i = y'$

↳ (000…1…0) ↑ i-th position

$\rightarrow$ $y'H = (y+e_i)H = yH + e_iH =$

$= 0 + e_iH = e_iH$ ... i-th row of H.

$y' = y + e$ ↳ error vector with ones at positions of errors

$y'H = (y+e)H = 0 + eH = eH$ ... "syndrom"

if we want to decode t errors then it must be the case that for all $e \in \{0,1\}^n$ with at most t ones, eH are all distinct. [If $e'H = eH \Rightarrow \underbrace{(e'-e)}_{\leq 2t \text{ ones}} H = 0$

$(y + (e'-e))H = 0$

$\Rightarrow y + (e'-e) \in C \Rightarrow$ distance of $C \leq 2t$.]

"syndrom decoding": calculate $y'H$ & look-up the error in a table. (syndrom)

Claim: C ... $[n, k, d]_q$ ... linear code

$x, y \in C \Rightarrow x + y \in C$

$\alpha \in GF[q] \quad \alpha x \in C \subseteq (GF[q])^n$

$\alpha(x_1 \dots x_n) = (\alpha x_1, \alpha x_2, \dots, \alpha x_n)$

$(x_1 \dots x_n) + (y_1 \dots y_n) = (x_1 + y_1, x_2 + y_2, \dots x_n + y_n)$

$x, y \in C$ $\quad x - y \ldots$ # non-zeros $= \Delta_{Ham}(x, y)$

$x, y \qquad 0^n \in C$

$d = \min_{\substack{x \in C \\ x \neq 0}} \Delta_{Ham}(x, 0^n) = |\{ i ; x_i \neq 0 \}|.$

$\Rightarrow$ Reed-Solomon codes