Lecture 7

Note Title 1/16/2008

→ G, H

→ d: minimum distance

→ Syndrome decoder

Ex:

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

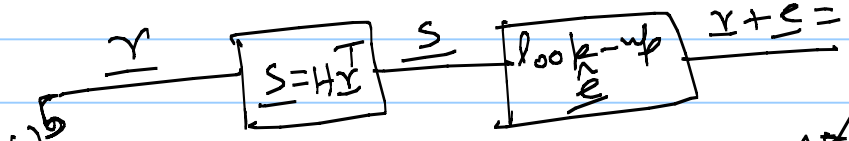
$\underline{s} = H \underline{e}^T$

↓

3-bit vector $\Rightarrow$ 8 possibilities

$\underline{s}$	$\hat{\underline{e}}$	
000	000000	$(1-p)^6$
001	000001	
010	000010	
100	000100	
011	001000	$p(1-p)^5$
101	100000	
110	010000	
111	001100	

correctable errors.



$$Pr(\hat{\underline{c}} \neq \underline{c}) = Pr(\underline{e} \neq \hat{\underline{e}})$$

$\hat{\underline{e}}$ from table

$$= 1 - Pr(\underline{e} = \hat{\underline{e}} \text{ from table})$$

if $\underline{e} = [100001]$, $\hat{\underline{e}} = 000100$ ✗

$$Pr(\hat{\underline{c}} \neq \underline{c}) = 1 - (1-p)^6 - 6p(1-p)^5 - 2p^2(1-p)^4$$

→ Extension: add an overall parity, rate ↓

→ Puncturing: drop parities, rate ↑

→ Shortening:

(n, k, d) Code C: G, H $\quad G = [I \; P]$

$$\underline{c} = [m_0 \; m_1 \; \cdots \; m_{k-1}] \, G$$

$$= [m_0 \; m_1 \; \cdots \; m_{k-1} \; \underline{m}P]$$

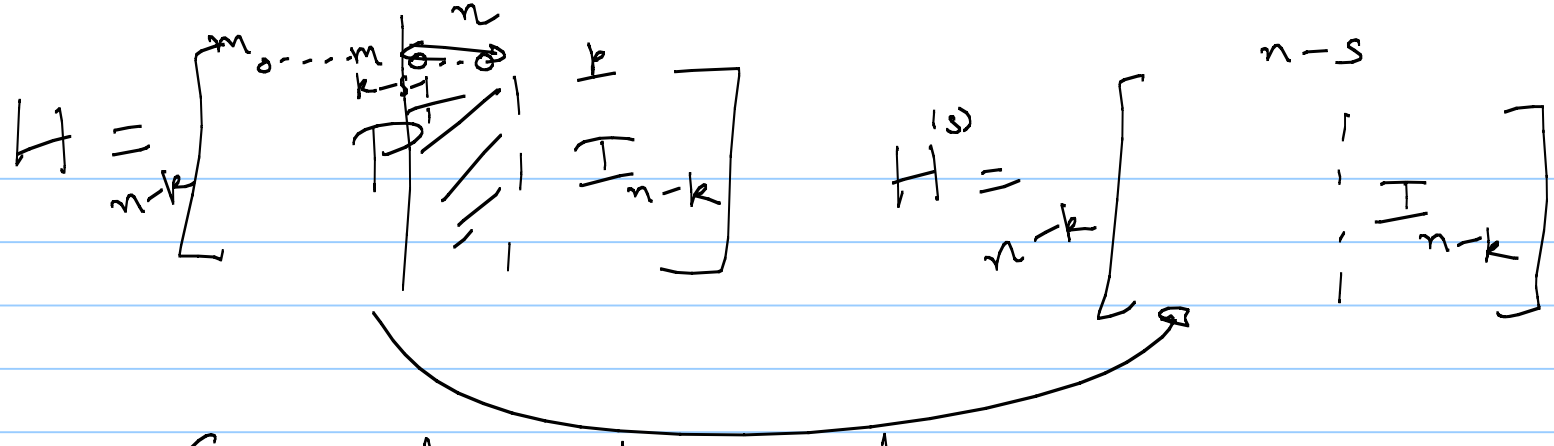
Shortened code $(n-s, k-s)$ C_s: $\quad \underline{m} = [m_0 \cdots m_{k-s-1} \; 0 \cdots 0]$

Codewords $[m_0 \; m_1 \; \cdots \; m_{k-s-1} \; \underline{m}P]$

$k-s$ bits are message

last s bits are set to zero

$$G = \left[\begin{array}{c|c} I_{k} & P \\ \hline & \end{array}\right] \quad \begin{array}{l} \leftarrow s \text{ cols become } 0 \\ \updownarrow \text{ last } s \text{ rows are removed} \end{array} \quad \Rightarrow \quad G^{(s)} = \left[I_{k-s} \;\; P_{1 \text{ to } k-s} \right]$$



Crucial: $d_{(s)} \geq d$.

$\longrightarrow$ rate $\downarrow$

$\longrightarrow$ $G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

Ex: $n = 31$, $d \geq 4$, maximize k

$n' = 30$, $d = 3$

$H' = 5\Big[$ $\Big]$ (30 columns)

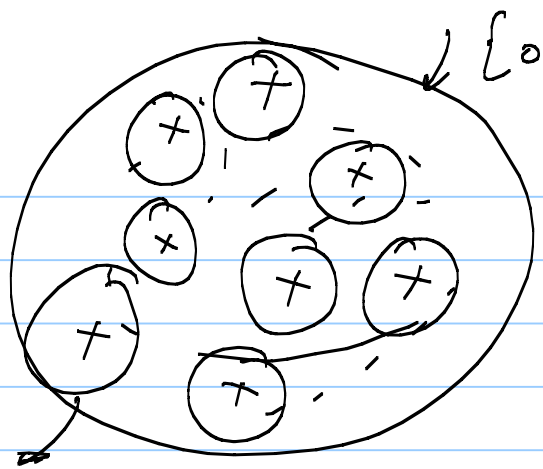
$(30, 25, 3)$ Code

$\downarrow$ extend

$(31, 25, 4)$

Bounds:

Hamming bound:



$x \to$ Codewords of a (n,k,d) code

# of vectors in each sphere

$$\left(1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t}\right) 2^k \leq 2^n$$

$n = 31,\ d = 4,\ t = 1 \Rightarrow k \leq 26$

Singleton bound:

(n,k,d) code

look at $k-1$ columns

$$\underline{c}_1 = [c_{10}\ c_{11}\ \cdots\ c_{1n-1}]$$
$$\underline{c}_2 = [c_{20}\ c_{21}\ \cdots\ c_{2n-1}]$$
$$\vdots$$
$$\underline{c}_{2^k} = [c_{2^k 0}\ c_{2^k 1}\ \cdots\ c_{2^k n-1}]$$

2^k rows, but only 2^{k-1} vectors

$\Rightarrow \underline{c}_i$ & $\underline{c}_j$ agree in first $k-1$ positions

$$d \leq d_H(\underline{c}_i, \underline{c}_j) \leq n-k+1$$

$$d \leq n-k+1 \text{ or } k \leq n-d+1$$

$\longrightarrow$ MDS codes satisfy $d = n-k+1$

Max. Distance separable

Ex: $(n, 1, n) \longrightarrow$ MDS

$(n, n-1, 2) \longrightarrow$ MDS

Dual of repetition code

"even-weight code"

$(n, n, 1) \longrightarrow$ MDS

$(31, 25, 4) \longrightarrow k \leq 28$

Gilbert-Varshamov Bound: target $d_{min} = d$

$H =$ r rows $\begin{bmatrix} \cdots & \cdots & \cdots \end{bmatrix}$

$n-1$ columns already added.

when can an n^{th} column be added?

$$1 + \binom{n-1}{1} + \binom{n-1}{2} + \binom{n-1}{3} + \cdots + \binom{n-1}{d-2} \leq 2^r$$

- 1: all-zero
- $\binom{n-1}{1}$: each column
- $\binom{n-1}{2}$: sum of two columns
- $\binom{n-1}{3}$: 3 cols

Ex: $n = 31$, $d = 4$

GV bound: $r \geq 9 \Rightarrow k \leq 23$

Recap

- Binary linear codes
- Block length, Dimension & d_{min}
- Encoding : $\underline{m}\,G$
- Decoding : syndrome decoding
  - Solving $\underline{s} = H\underline{e}^T$
- k/n versus d/n

Finite fields

field : set of elements that can be added/subtracted, multiplied/divided.

Ex: Rational numbers $\mathbb{Q}$ — not finite
Real numbers $\mathbb{R}$ —

finite ← $F_2 = \{0, 1\}$ $+, \cdot \bmod 2$

$1 + 1 = 0$

$F_3 = \{0, 1, 2\}$ $+, \cdot \bmod 3$

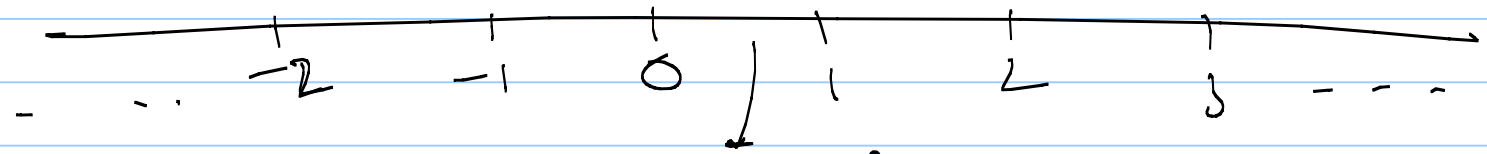
$1/2 = 1 \cdot 2^{-1}$?

$1 - 2 = ?$

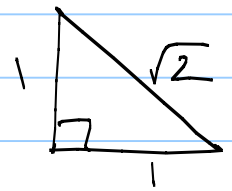
History: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

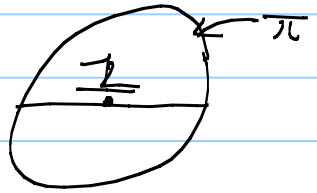
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

?



rational numbers





Abstract fields: → ruler-compass
→ solutions for poly. eqns