16548Notes9

Systematic Codes

University of Idaho

systematic codes

review:

in general $\bar{c} = \bar{m} G$

$\bar{m} = (m_0\, m_1 \ldots m_{k-1})$ $\quad m_i \in \{0,1\}$

$$G = \begin{bmatrix} \bar{g}_0 \\ \hline \bar{g}_1 \\ \hline \vdots \\ \bar{g}_{k-1} \end{bmatrix} \quad \left.\begin{matrix} 1\times n \\ 1\times n \\ \\ 1\times x \end{matrix}\right\} k\times n$$

The $\bar{g}_i$ are basis vectors

The $\bar{g}_i$ are orthogonal

if $i \neq j$ $\quad \bar{g}_i \cdot \bar{g}_j^T = 0$

For a systematic block code, G has a special form. If the code is (n, k), then

$$G = \left[P_{k \times r} \;\vdots\; I_{k \times k} \right], \quad r = n-k$$

$\bar{c} = \bar{m} G = (c_0 \, c_1 \cdots c_{r-1} \, m_0 \, m_1 \cdots m_{k-1})$

Example

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

$d_{min} \leq 3$

$d_{min} = \min_{\substack{\bar{c} \\ \bar{c} \neq \bar{0}}} w_H(\bar{c})$

$= \bar{g}_0$

$n = 4$

$\bar{m}_1 = (1000) \Rightarrow \bar{c}_1 = (1101000)$

$\bar{m}_2 = (0100) \Rightarrow \bar{c} = \bar{g}_1$

$\bar{m}_4 = (0010) \Rightarrow \bar{g}_2$

$\bar{m}_8 = (0001) \Rightarrow \bar{g}_3$

The $\bar{g}_i$ must be valid codevectors $\quad \bar{c} = \bar{0}$

University of Idaho

For This example, $d_{min} = 3 \Rightarrow t_c = 1$

Systematic Parity Check Matrix

$$H = \left[I_{r\times r} \;\vdots\; -P^T_{r\times k} \right]$$

$\left(\begin{array}{c} -1 = 1 \text{ in} \\ \text{binary} \end{array} \right)$

$1+1=0$

$\therefore 1=-1$

$-P^T_{r\times k} = P^T_{r\times k}$ in binary codes

$$\underbrace{GH^T}_{k\times r} = \left[P_{k\times r} \;\vdots\; I_{k\times k} \right] \begin{bmatrix} I_{r\times r} \\ \hdashline -P_{k\times r} \end{bmatrix} = P - P$$

$$= [\,\bar{0}\,]$$

example

$$G = \left[\;\overbrace{\begin{matrix}1 & 1 & 0\\ 1 & 0 & 1\\ 0 & 1 & 1\\ 1 & 1 & 1\end{matrix}}^{P}\;\;\begin{matrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{matrix}\;\right]$$

$k = 4$

$n = 7$

$\therefore r = 7 - 4 = 3$

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

suppose we have a system

$$\bar{v} = \bar{c} + \bar{e} \quad , \quad \bar{e} = (e_0 e_1 \cdots e_{n-1})$$

$$e_i \in \{\underbrace{0}_{\text{no error}} \; \underbrace{1}_{\text{error}}\}$$

<u>syndrome vector</u>

$$\bar{s} \triangleq \bar{v} H^T = (\bar{c} + \bar{e}) H^T$$

$$= \bar{m} G H^T + \bar{e} H^T = \bar{m}[\bar{0}] + \bar{e} H^T = \bar{e} H^T$$

First Thing:

$\bar{e}$ may or may not be the same as some codeword.

if it is the same, $\bar{e} \in C$

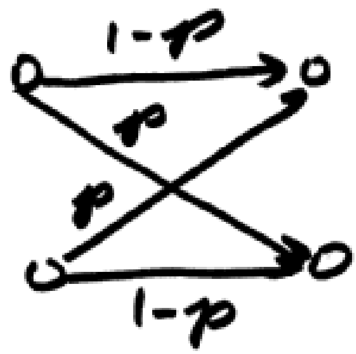
$\therefore \bar{e} = \bar{m}G$ for some $\bar{m}$

in this case, $\bar{e}H^T = \bar{0}$

These are called <u>undetectable</u> errors

if the code has Hamming distance d_{min} <u>and</u> if $w_H(\bar{e}) < d_{min} \Rightarrow \bar{e} \notin C$ <u>or</u> $\bar{e} = \bar{0}$

$$\Pr\left[w_H(\bar{e}) < d_{min}\right] = \sum_{j=0}^{d_{min}-1} \binom{n}{j} p^j (1-p)^{n-j}$$



BSC

$p < \frac{1}{2}$

University of Idaho

now suppose

$$\bar{e} \notin C$$

there $\bar{e} \neq \bar{m}G$ for any $\bar{m}$

in this case, $\bar{s} = \bar{e}H^T \neq \bar{0}$

For doing error <u>detection</u> (w/ no correction),

$\bar{s} \neq \bar{0} \Rightarrow$ error.

what about error correction?

University of Idaho

example: Same G and H matrices as before. (C had $d_{min} = 3$)

$d_{min} = 3 \Rightarrow 3 \geq 2t_c + 1 \Rightarrow t_c = 1$

For our G matrix

$$P = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \qquad G = [\, P \,\vdots\, I \,]$$

$\bar{c} = \bar{m} G \Rightarrow$ Parity bits will be $\bar{m} P$

let $\bar{m} = (0101)$

$\Rightarrow \bar{m}P = (0101)\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} = (010)$

$\therefore\ \bar{c} = (010\ 0101)$

now let $\bar{e} = (0000100)$

$w_H(\bar{e}) = t_c \quad ; \quad \bar{v} = \bar{c} + \bar{e}$

$\bar{v} = (0100001)$

$\bar{s} = \bar{v}H^T = \bar{e}H^T$

University of Idaho

our matrix H^T is

$$H^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hdashline 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{matrix} \leftarrow I \\ \\ \\ \\ \leftarrow P \\ \\ \\ \end{matrix}$$

$\bar{e} = (0000100)$; $\bar{e}H^T = (101)$

what about other $\bar{e}$ s.t. $w_H(\bar{e}) = 1$?

University of Idaho

15

$\therefore$ if $w_H(\bar{e}) = 1 = t_c$

$\bar{s}$ will be <u>unique</u> for that $\bar{e}$

The set $\{\bar{e} \mid w_H(\bar{e}) = 1\}$ is the set of all correctable errors.

Proposition: every $\bar{e} \neq 0$ such that $w_H(\bar{e}) \leq t_c$ will produce its own unique syndrome vector $\bar{s} = \bar{v} H^T$

University of Idaho

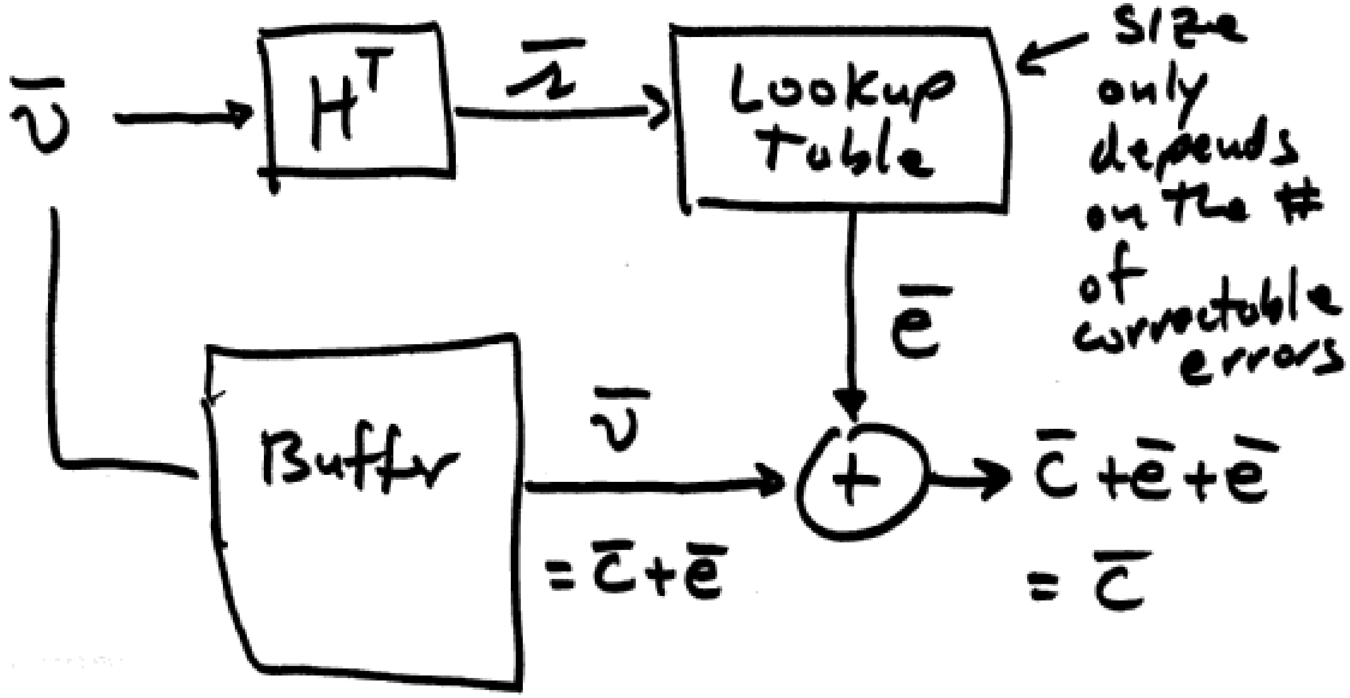
EE 455
Lec 26

From last time: we learned that $\bar{s} = \bar{v} H^T$ generates unique syndrome vectors provided $w_H(\bar{e}) \le t_c$,

If we know the set of all correctable errors, since $\bar{s} = \bar{e} H^T$ we can make a lookup table

$$\bar{s} \rightarrow \boxed{\text{Lookup Table}} \rightarrow \bar{e}$$

for binary codes, $-\bar{e} = \bar{e}$



lookup table size is a function of t_c, <u>not</u> n.

University of Idaho

3

$r = n - k$

more neat stuff.

$$G = \begin{bmatrix} \bar{g}_0 \\ \hdashline \bar{g}_1 \\ \hdashline \vdots \\ \hdashline \bar{g}_{k-1} \end{bmatrix}, \quad H = \begin{bmatrix} \bar{h}_0 \\ \hdashline \bar{h}_1 \\ \hdashline \vdots \\ \bar{h}_{r-1} \end{bmatrix}$$

We also know

$$GH^T = [\bar{0}] = \begin{bmatrix} \bar{g}_0 \\ \hdashline \bar{g}_1 \\ \hdashline \vdots \\ \bar{g}_{k-1} \end{bmatrix} \left[\bar{h}_0^T \,\vdots\, \bar{h}_1^T \,\vdots\, \cdots \,\vdots\, \bar{h}_{r-1}^T \right]$$

University of Idaho

④

as an example, let $k = 4$, $r = 3$

$(n = 7)$

Then

$$GH^T = \begin{bmatrix} \bar{g}_0 \bar{h}_0^T & \bar{g}_0 \bar{h}_1^T & \bar{g}_0 \bar{h}_2^T \\ \bar{g}_1 \bar{h}_0^T & \bar{g}_1 \bar{h}_1^T & \bar{g}_1 \bar{h}_2^T \\ \bar{g}_2 \bar{h}_0^T & \bar{g}_2 \bar{h}_1^T & \bar{g}_2 \bar{h}_2^T \\ \bar{g}_3 \bar{h}_0^T & \bar{g}_3 \bar{h}_1^T & \bar{g}_3 \bar{h}_2^T \end{bmatrix}$$

$GH^T = [\bar{0}] \Rightarrow \bar{g}_i \bar{h}_j^T = 0 \Rightarrow \bar{h}_j$ are orthogonal to the $\bar{g}_i$

University of Idaho

(5)

The set of $\bar{h}_j$ vectors are not only orthogonal to the $\bar{g}_i$'s but

1) orthogonal to each other
2) linear independent

$\therefore$

$$H = \begin{bmatrix} \bar{h}_0 \\ \bar{h}_1 \\ \vdots \\ \bar{h}_{r-1} \end{bmatrix}$$

we have r orthogonal, linearly independent vectors (basis vectors!)

defines an r-dim. linear vector space

H <u>also</u> defines a linear block code. It is called "the dual code of G"

if G generates a code C (n,k)

Then H generates a code $C^{\perp}$ (n,r)

$$C \subset V \quad ; \quad C^{\perp} \subset V$$

$$C \cap C^{\perp} = \emptyset \text{ except for } \bar{c} = \bar{0}$$

$R = \frac{4}{7} \rightarrow$ (7,4) code

$$H = \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ \underbrace{0 \quad 0 \quad 1} & & & \underbrace{0 \quad 1 \quad 1 \quad 1}_{-P^T} & & & \end{array}\right] \Longleftrightarrow G = \left[\begin{array}{ccc:cccc} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ \underbrace{1 \quad 1 \quad 1}_{P} & & & \underbrace{0 \quad 0 \quad 0 \quad 1} & & & \end{array}\right].$$

$$G^{\perp} = \left[\begin{array}{cccc:ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}\right]. \Longleftrightarrow H^{\perp} = \left[\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

(7,3) $R = \frac{3}{7}$

University of Idaho

(8)

So far: lot's of theory, not very many codes

So far, we only have 2 "base" codes

1) repetition codes

2) "2-D" code from H.W., last quiz, and some lecture awhile back

A new code: Hamming Codes

- All Hamming codes have $d_{min} = 3$ $(t_c = 1)$
- Hamming codes have $r \geq 3$
- Hamming codes have a codelength $n = 2^r - 1$
  $r=3 \Rightarrow n=7$; $r=4 \Rightarrow n=15$, $r=5 \Rightarrow n=31$

Since $k = n - r$

$$R = \frac{k}{n} = \frac{n-r}{n} = \frac{2^r - 1 - r}{2^r - 1}$$

$$\lim_{r \to \infty} R \to \frac{2^r}{2^r} = 1$$

$$t_c \geq \bar{t} + 3t_\sigma$$

r	3	4	5	6	7	8
n	7	15	31	63	127	255
k	4	11	26	57	120	247
$R \simeq$	.571	.733	.839	.905	.945	.969

Designing Hamming Codes:

1) pick r (establishes n, k)
2) write down the H matrix

example: $r = 3 \Rightarrow n = 7 \Rightarrow k = 4$

H is 3×7 and starts w/ 3×3 identity matrix

$$H = \begin{array}{c} \left[\begin{array}{ccc:cccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{array}\right] \\ \begin{array}{ccccccc} 1 & 2 & 4 & 3 & 5 & 6 & 7 \end{array} \end{array}$$

$H = [I_{r \times r} \vdots -P^T_{r \times k}]$

Systematic Code

University of Idaho

17

Construct the systematic parity check matrix for the (15, 11) Hamming code

$r=4$

$$H=\left[\begin{array}{cccc:ccccccccccc}1&0&0&0&1&1&0&1&1&0&1&0&1&0&1\\0&1&0&0&1&0&1&1&0&1&1&0&0&1&1\\0&0&1&0&0&1&1&1&0&0&0&1&1&1&1\\0&0&0&1&0&0&0&0&1&1&1&1&1&1&1\end{array}\right].$$

1 2 4 8 3 5 6 7 9 10 11 12 13 14 15

$r \geq 3$

University of Idaho

Back to (7,4) Hamming Code

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

$d_{min} = 3$

$$\bar{s} = \bar{v} H^T = \bar{e} H^T$$

and $w_H(\bar{e}) \leq 1$ for correctable errors

$\therefore$ whichever $e_i = 1$, $\bar{e} H^T$ will strip out that row of H^T

University of Idaho

$$H^T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{array}{l} \leftarrow \bar{s} \text{ for } \bar{e} = (1000000) \\ \leftarrow \bar{s} \text{ for } \bar{e} = (0100000) \\ \leftarrow \bar{s} \text{ for } \bar{e} = (0010000) \\ \\ \\ \\ \leftarrow \bar{s} \text{ for } \bar{e} = (0000001) \end{array}$$

$C^{\perp}$ for (7,4) Hamm. code is a (7,3) code

d_{min} for $C^{\perp}$ is $d_{min} = 4$