20SK – Signals and Codes

Lecture 11 – Hamming code (2018/12/10)

Topics discussed:

- Hamming sphere for correcting t errors.
- Hamming bound. Hamming bound for binary code that corrects t erros.
- Perfect codes.
- Hamming code: definition, parity-check matrix properties, construction of generator matrix.
- Syndrome decoding of Hamming code.
- Hamming code examples, construction of the code from parity-check matrix, direct construction of generator matrix.

The relevant literature is [1, chapter 3], [2, chapters 10 and 12] and [3, chapter 4].

Resources

[1] Morelos-Zaragoza, R. H.: The Art of Error-Correcting Coding. 2nd edition, John Wiley & Sons, 2006, 263pp.

[2] Adámek, J: Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory. Wiley Interscience, 1991, 352 pp.

[3] Moon, T. K.: Error Correction Coding – Mathematical Methods and Algorithms. Wiley Interscience, 2005, 756 pp.

Note: Due to your no-show at the lecture I consider this topic to be fully explained and I will not consult this under any circumstances.

„PERFECT" CODES

- the shortest possible code for given detection & correction capabilities (it does not always exist for given n and k)

→ Hamming bound: For every single-error correction code it holds

$$n \le 2^{n-k} - 1$$

and for a perfect code

$$n = 2^{\boxed{n-k}} - 1$$

added redundancy

Ex. (3,1)-code

$n = 3$

$k = 1$

$3 \le 2^2 - 1 = 3$

⇒ perfect single-error-corr. code

(4,3)-code

$n = 4$

$k = 3$

$4 \le 2 - 1$

⇒ does not correct any error

(4,2)-code

$n = 4$

$k = 2$

$4 \le 2^2 - 1 = 3$

→ does not correct single.

(7,4)-code

$7 \le 2^3 - 1 = 7$

→ perfect code

(8,4)

$8 \le 2^4 - 1 = 15$

→ corrects single err. not perfect

(4,2)-code

$n = 4$

$k = 2$

$4 \leq 2^2 - 1 = 3$

→ does not correct anyth.

(7,4)-code

$7 \leq 2^3 - 1 = 7$

→ perfect code

(8,4)

$8 \leq 2^4 - 1 = 15$

→ corrects single err.
not perfect

„PERFECT" CODES

$n = 2^m - 1$

m	n	k
1	1	∅
2	3	1
3	7	4
4	15	11
5	31	26

and so on...

(3,1), (5,2), (6,3), (7,4),
(9,5), (10,6), (11,7), ... (15,11) → (16,12) does not correct a single err.

⇒ we need (17,12)

⇓

Hamming codes = perfect codes for correcting single errors
for m bits of redundancy

$n = 2^m - 1$ $d_{min} = 3$

$k = 2^m - m - 1$

Ex. (3,1)-code

$n = 3$

$k = 1$

$3 \leq 2^2 - 1 = 3$

⇒ perfect single-error-corr. code

(4,3)-code

$n = 4$

$k = 3$

$4 \leq 2 - 1$

⇒ does not correct any error

Ex:

$$\mathbb{H}=\begin{pmatrix}0&1&1\\1&0&1\end{pmatrix}$$ repetition code $n=3$ $(3,1)$

$$\mathbb{H}=\begin{pmatrix}0&0&1&1\\1&0&0&1\\0&1&1&1\end{pmatrix}$$ $(4,1)$ code

$$\mathbb{H}=\left.\underbrace{\begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix}}_{n=7}\right\}\begin{array}{l}n-k\\-3\end{array}$$ $(7,4)$

→ non-systematic!

HAMMING CODES

- „perfect codes" for single error correction
- for $\underline{m}$ redundancy symb.

$$n=2^m-1$$

$$k=2^m-m-1$$

$$\boxed{d=3}$$

Definition: Binary lin. code $\mathbb{K}$ corrects single errors <u>iff</u> its partity check matrix $\mathbb{H}$ has (i) nonzero and (ii) pairwise distinct columns.

Hamming code:

- matrix $\mathbb{H}$ has 2^m-1 columns
- $\mathbb{H}$ can be constructed by listing all numbers from $1 \ldots n$ in binary form as columns

$$\vec{v}=\vec{u}\cdot G$$

$$\vec{v}\cdot H^T=0$$

$$\hookrightarrow H\cdot\vec{v}=0$$

Ex:

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

$$\mathbb{H} = \underbrace{\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}}_{n=7} \quad (7,4)$$

→ non-systematic!

systematic code: $\mathbb{G} = \left[\mathbb{I}_{k \times k} \,\vdots\, \mathbb{P}_{k \times (n-k)} \right]$

$\mathbb{H} = \left[\mathbb{P}^T_{(n-k) \times k} \,\vdots\, \mathbb{I}_{(n-k) \times (n-k)} \right]$

$$\mathbb{H}_{sys} = \left(\begin{array}{cccc:ccc} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \rightarrow \mathbb{P}^T = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \rightarrow \mathbb{P} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

$$\rightarrow \mathbb{G}_{sys} = \left(\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

alternative $\mathbb{H} \cdot \vec{v} = 0$ (using non-sys)

$v_3 \oplus v_4 \oplus v_5 \oplus v_6 = 0$ row 1 of $\mathbb{H}$

$v_1 \oplus v_2 \oplus v_5 \oplus v_6 = 0$ row 2

$v_0 \oplus v_2 \oplus v_4 \oplus v_6 = 0$ row 3

$$\downarrow \qquad \mathbb{G} \cdot \mathbb{H}^T = 0$$

$$\downarrow$$

$$\boxed{\begin{array}{l} v_3 \\ v_1 \\ v_0 \end{array}} \begin{array}{l} = \underbrace{v_4 \oplus v_5 \oplus v_6 \\ = v_2 \oplus v_5 \oplus v_6 \\ = v_2 \oplus v_4 \oplus v_6}_{\text{information bits}} \end{array}$$

→ parity bits

non-systematic generator matrix:

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

$$\vec{v} = \vec{u} \cdot \mathbb{G}$$

Ex:

$\vec{u} = (1011)$

$\vec{v} = (1,0,1,1) \cdot G_{sys}$

$= (1011010)$

$H_{sys} \cdot \vec{v}^T = (0\,0\,0) \Rightarrow$ $\vec{v}$ is a code-word

$$\vec{w} = (101\overset{\text{error}}{\boxed{0}}010)$$

$H_{sys} \cdot \vec{w}^T = (1\,1\,1) \rightarrow$ $\vec{w}$ is not a code-word

↳ corresponds to the 4th column of H_{sys}

$\vec{w}$ has 4th bit flipped

$\Rightarrow \vec{v} = (101\boxed{1}010)$

$$H_{sys} = \left(\begin{array}{cccc|ccc} 0 & 1 & 1 & \boxed{1} & 1 & 0 & 0 \\ 1 & 0 & 1 & \boxed{1} & 0 & 1 & 0 \\ 1 & 1 & 0 & \boxed{1} & 0 & 0 & 1 \end{array}\right)$$

$$\rightarrow G_{sys} = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

$$(1011)\begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = 0$$

Decoding:

$\vec{v} \cdot H^T = H \cdot \vec{v}^T = 0$ ← syndrome

$$\text{syndrome is} \begin{cases} = 0 & \text{... code word} \\ \neq 0 & \text{... error} \end{cases}$$

For single errors, syndrome points to the erratic bit!

$\vec{w} = (\vec{v} + \vec{e})$ ← error vector single bit set

$\vec{w} \cdot H^T = (\vec{v} + \vec{e}) \cdot H^T =$

$= \underbrace{\vec{v} \cdot H^T}_{0} + \vec{e} \cdot H^T = \vec{e} \cdot H^T$

$\Rightarrow \vec{e}$ copies out the column of H where the error occured

H_{sys} needs another LUT to map syndrome to corresponding bit in the code-word; non-systematic coding does not need that.

HAMMING CODES

- perfect codes for correcting single errors
  - ↪ minimum possible redundancy
- defined for m bits of redundancy as (n,k) codes where

$d_{min} = 3$

$$n = 2^m - 1$$
$$k = 2^m - k - 1$$

Ex: Hamming codes

(3,1) ... (7,4) ... (15,11)

Def: A perfect binary code to correct single errors iff all columns of parity check matrix $\mathbb{H}$ are (a) nonzero (b) different

Ex: (3,1) Hamming code

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

Ex: (7,4) Hamming code

$$\mathbb{H} = \begin{array}{c} \begin{array}{ccccccc} 7 & 6 & 1 & 5 & 2 & 3 & 4 \end{array} \\ \underbrace{\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}}_{n} \end{array} \left.\vphantom{\begin{matrix} 0 \\ 0 \\ 0 \end{matrix}}\right\} n-k$$

$\mathbb{H} \rightarrow \mathbb{G}$ possible for systematic codes:

$$H_{sys} = \left(\mathbb{P}^T \,\middle|\, \mathbb{I} \right)$$
$$\Downarrow$$
$$G_{sys} = \left(\mathbb{I} \,\middle|\, \mathbb{P} \right)$$

For (7,4)-code we have

$$H_{sys} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

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

Decoding:

input $\vec{u}$; code-word $\vec{v} = \vec{u} \cdot \mathbb{G}$

$\rightsquigarrow$ (transmission)

$\vec{w}$ received $\quad \vec{w} \cdot H^T = \vec{0}$

a) $\vec{u} = (0101) \longrightarrow \vec{v} = (0101\,010)$

$\vec{v} \cdot \mathbb{H}^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ $\vec{v}$ is a code-word !!

b) single error: $\vec{v} = (0101010) \rightarrow$

$\rightarrow \vec{w} = (010\boxed{0}010)$

$\vec{w} \cdot \mathbb{H}^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \vec{s}$ $\vec{w}$ is <u>not</u> a code word, $\vec{s}$ corresponds to the column in $\mathbb{H}$ where the error occured

<u>Ex:</u> Why is this possible?

$\vec{w} = \vec{v} + \vec{e}$

<u>Note:</u> vector $\vec{e}$ has all-but-one bits 0

$$\vec{w} \cdot \mathbb{H}^T = (\vec{v} + \vec{e}) \cdot \mathbb{H}^T = \underbrace{\vec{v} \cdot \mathbb{H}^T}_{\vec{0}} + \underbrace{\vec{e} \cdot \mathbb{H}^T}_{\text{copies out the } \underline{i}\text{-th column of } \mathbb{H}}$$

c) double error: $\vec{w} = (0\boxed{0}0\boxed{0}010)$

$\vec{w} \cdot \mathbb{H}^T = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ $\vec{w}$ is not a code word, but incorrectly estimates $\vec{v} = (0000000)$

$\Rightarrow d_{min} = 3$, cannot correct double errors!

$\mathbb{H} \rightarrow \mathbb{G}$ possible for systematic codes:

$$\mathbb{H}_{sys} = (\mathbb{P}^T \mid \mathbb{I}) \quad \Downarrow \quad \mathbb{G}_{sys} = (\mathbb{I} \mid \mathbb{P})$$

For (7,4)-code we have

$$\mathbb{H}_{sys} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

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

Decoding:

input $\vec{u}$; code-word $\vec{v} = \vec{u} \cdot G$

(transmission)

$\vec{w}$ received $\qquad \vec{w} \cdot H^T = \vec{0}$

a) $\vec{u} = (0101) \rightarrow \vec{v} = (0101\,010)$

$\vec{v} \cdot H^T = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ $\vec{v}$ is a code-word !!

b) single error: $\vec{v} = (0101010) \rightarrow$

$\rightarrow \vec{w} = (010\boxed{0}010)$

$\vec{w} \cdot H^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \vec{s}$ $\vec{w}$ is not a code word, $\vec{s}$ corresponds to the column in H where the error occured

Ex: Why is this possible?

$\vec{w} = \vec{v} + \vec{e}$

Note: vector $\vec{e}$ has all-but-one bits 0

$\vec{w} \cdot H^T = (\vec{v} + \vec{e}) \cdot H^T = \underbrace{\vec{v} \cdot H^T}_{\vec{0}} + \underbrace{\vec{e} \cdot H^T}_{\text{copies out the } i\text{-th column of } H}$

c) double error: $\vec{w} = (0\boxed{0}0\boxed{0}010)$

$\vec{w} \cdot H^T = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ $\vec{w}$ is not a code word, but incorrectly estimated $\vec{v} = (0000000)$

$\Rightarrow d_{min} = 3$, cannot correct double errors!

$H \rightarrow G$ possible for systematic codes:

$H_{sys} = (P^T \mid I)$

$\Downarrow$

$G_{sys} = (I \mid P)$

For (7,4)-code we have

$$H_{sys} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$$G_{sys} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Ex: Hamming (3,1) ... repetition code

$$G_{sys} = [1\ 1\ 1]$$

$$P = [1\ 1] \Rightarrow P^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$H_{sys} = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

$$\left.\begin{matrix} \vec{x} = (000) \\ \hat{e} = (001) \end{matrix}\right\} x' = (001)$$

$$x' H^T = (001) \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$x' \cdot H^T = (101) \cdot \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$n = 2^m - 1$$

HAMMING CODES

Construction:

a) from H (7,4)

$$H = \underbrace{\left[\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right]}_{n \text{ columns}} \Big\} m \text{ rows}$$

- columns are distinct
- represent numbers from 1 to n

$$H_{sys} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

b) using parity bit assignment
non-systematic code
construct a parity bit assignment and
copy it to systematic G afterwards

		p_2 p_1 p_0
1	...	001
2	...	010
3	...	011
4	...	100
5	...	101
6	...	110
7	...	111

	1	2	3	4	5	6	7	
	p_0	p_1	d_0	p_2	d_1	d_2	d_3	
p_0	▨		X		X		X	position 1 ⇒ ...1 (2^1)
p_1		▨	X			X	X	position 2 ⇒ .1. (2^2)
p_2				▨	X	X	X	position 4 ⇒ 1.. (2^3)

$$G = \underbrace{\begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}}_{n} \Big\} k$$

$$\vec{u} \cdot \vec{G} = \vec{x}$$

$$\Rightarrow \begin{aligned} p_0 &= d_0 \oplus d_1 \oplus d_3 \\ p_1 &= d_0 \oplus d_2 \oplus d_3 \\ p_2 &= d_1 \oplus d_2 \oplus d_3 \end{aligned}$$