TSKS01 Digital Communication
Lecture 9

Error Control Codes: Decoding and examples

Emil Björnson

Department of Electrical Engineering (ISY)

Division of Communication Systems

COMMUNICATION SYSTEMS

LINKÖPING UNIVERSITY

Outline of this Lecture

- Summary of last lecture
- Syndrome decoding
- Specific structure of error control codes
  - Dual codes
  - Cyclic codes
- Specific codes
  - Repetition codes
  - Parity check codes
  - Hamming codes
  - Product codes

Weights and Distances

Hamming weight: $w_{\mathrm{H}}(\bar{a})$ # positions where $\bar{a}$ is 1 (non-zero).

Hamming distance: $d_{\mathrm{H}}(\bar{a},\bar{b})$ # positions where $\bar{a}$ and $\bar{b}$ differ.

Relation: $d_{\mathrm{H}}(\bar{a},\bar{b}) = w_{\mathrm{H}}(\bar{a}+\bar{b})$

Linear code

Minimum distance: $$d = \min_{i\neq j} d_{\mathrm{H}}(\bar{c}_i,\bar{c}_j) = \min_{i\neq j} w_{\mathrm{H}}(\bar{c}_i+\bar{c}_j) = \min_{\substack{\bar{c}\in\mathcal{C}\\ \bar{c}\neq\bar{0}}} w_{\mathrm{H}}(\bar{c})$$

Also: d is the smallest number of linearly dependent columns in H (since $H\bar{c}^T = \bar{0}$)

Example Hamming [7,4]:

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

No column $= \bar{0} \Rightarrow d > 1$

No two columns equal

$\bar{h}_1 + \bar{h}_6 + \bar{h}_7 = \bar{0}$

$\Rightarrow d > 2 \Rightarrow d = 3$

Last time – Binary Linear Codes $[n, k, d]$

A vector space expressed in a basis

$$\mathcal{C} = \{\bar{m}G \;\; \forall \bar{m} \in \mathbb{F}_2^k\}$$

Generator matrix $(k \times n)$, linearly independent rows.

… the nullspace of a matrix

$$\mathcal{C} = \{\bar{c} \in \mathbb{F}_2^n : H\bar{c}^T = \bar{0}\}$$

Parity check matrix $((n - k) \times n)$, linearly independent rows.

$$HG^{\mathrm{T}} = 0$$

Length: n, # columns in G or H

Dimension: k, # rows in G.

Minimum distance, d

Smallest Hamming distance between different codewords.

Smallest Hamming weight of non-zero codewords.

Smallest number of linearly dependent columns in H.

Syndrome Decoding

Received vector: $\bar{x} = \bar{c} + \bar{e} = (x_1, \ldots, x_n)$

Sent codeword $(c_1, \ldots, c_n)$ — Error vector $(e_1, \ldots, e_n)$

We know: $H\bar{c}^{\mathrm{T}} = \bar{0}$

Test that!

Syndrome: $\bar{s} = H\bar{x}^{\mathrm{T}} = H \cdot (\bar{c} + \bar{e})^{\mathrm{T}} = \underbrace{H\bar{c}^{\mathrm{T}}}_{=\bar{0}} + H\bar{e}^{\mathrm{T}} = H\bar{e}^{\mathrm{T}}$

Notation: $H = \begin{pmatrix} \vdots & & \vdots \\ \bar{h}_1 & \cdots & \bar{h}_n \\ \vdots & & \vdots \end{pmatrix} \Rightarrow \bar{s} = \sum_{i=1}^{n} x_i \bar{h}_i = \sum_{i=1}^{n} e_i \bar{h}_i$

One error in position i $\Rightarrow$ $\bar{s} = \bar{h}_i$

Two errors in positions i & j $\Rightarrow$ $\bar{s} = \bar{h}_i + \bar{h}_j$

Find closest codeword

$\Leftrightarrow$

Syndrome decoding: Find smallest set of columns in H that sum up to the syndrome

Example: Repetition Codes

Definition: A *repetition code* sends one information bit by repeating it n times.

Simplest error control code!

Generator matrix:

$$G = (1 \;\; 1 \;\; \ldots \;\; 1)$$

Parity check matrix:

$$H = \begin{pmatrix} I_{n-1} & \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \end{pmatrix}$$

Minimum distance: $d = n$

Short form: $[n, k, d\,] = [n, 1, n]$

Decoding: Majority vote!

Error Correction and Detection Capability

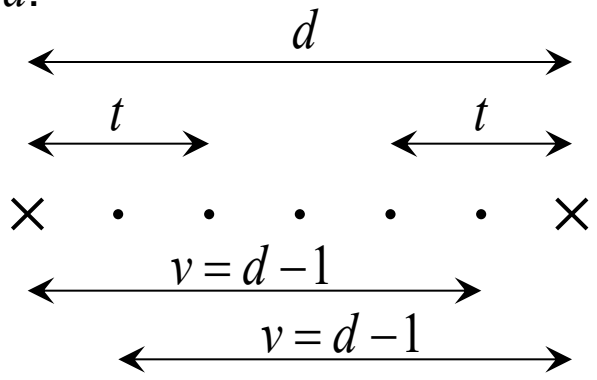
Error correction capability: $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

The code can correct every w-bit error if $w \leq t$.

Error detection capability: $v = d - 1$

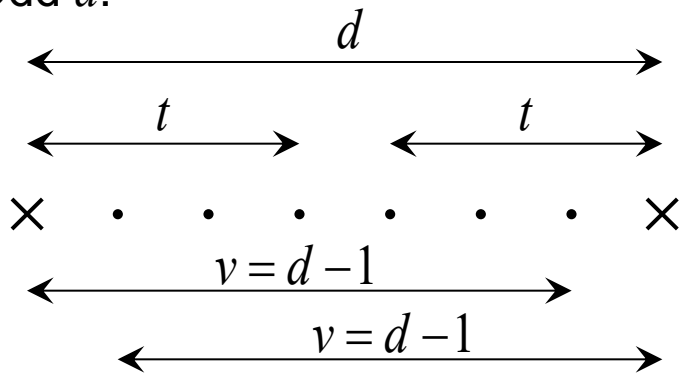
The code can detect every w-bit error if $w \leq v$.

Even d:



$$t = \frac{d-2}{2}$$

Odd d:



$$t = \frac{d-1}{2}$$

Example: Parity Check Codes

Definition: A *parity check code* sends k information bits by adding one parity-check bit that is the sum of the information bits ($k = n - 1$)

Generator matrix:

$$G = \begin{pmatrix} & 1 \\ I_{n-1} & \vdots \\ & 1 \end{pmatrix}$$

Parity check matrix:

$$H = (1 \;\; 1 \;\; \ldots \;\; 1)$$

Minimum distance: $d = 2$

Short form: $[n, k, d\,] = [n, n-1, 2]$

Detects odd-weight errors:
In particular one error

Example: Hamming Codes

Definition: A *Hamming code* is defined by one parameter $m \geq 2$. The parity check matrix contains all non-zero binary vectors of length m.

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

$n = 2^m - 1$

All columns of H are different: $d > 2$

All non-zero binary vectors in H: $d = 3$

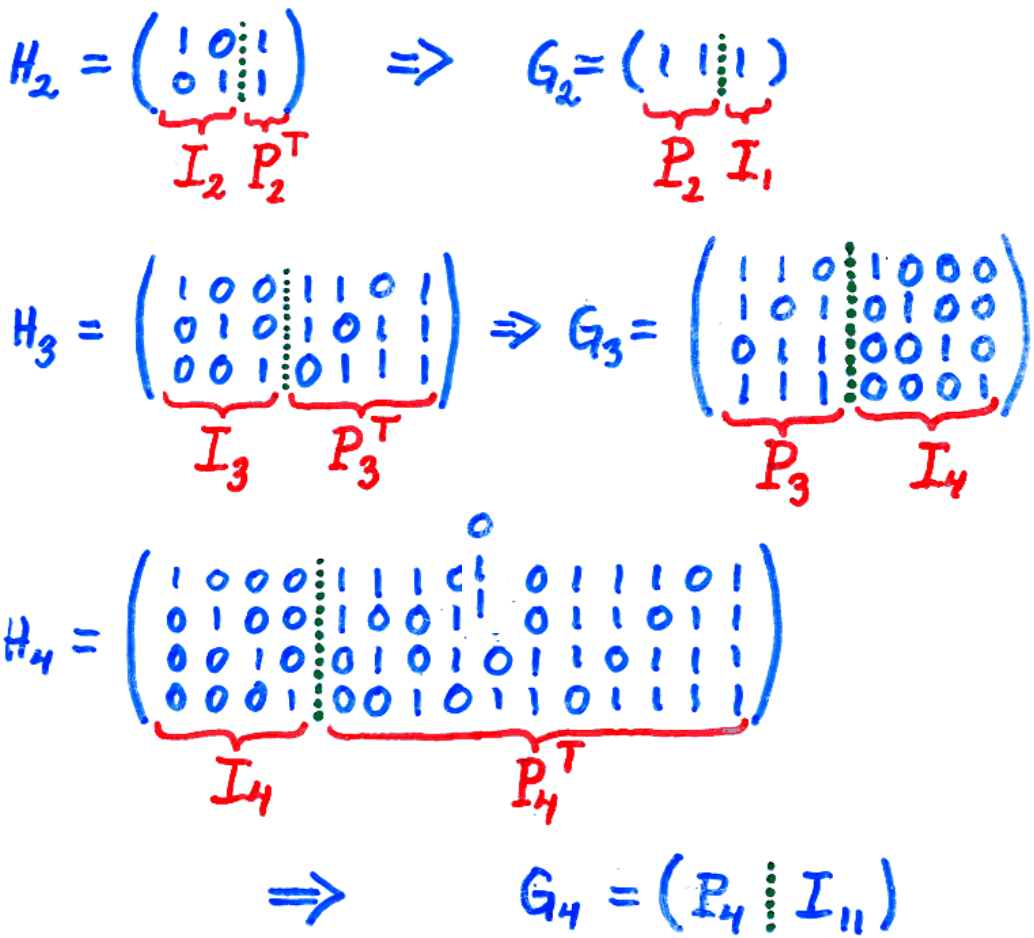
Short form: $[n, k, d] = [2^m - 1, 2^m - m - 1, 3]$

Example: Hamming Codes, cont.

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

$n = 2^m - 1$

m	n	k
2	3	1
3	7	4
4	15	11
5	31	26
6	63	57
7	127	120
⋮	⋮	⋮



Dual Codes

$\mathcal{C}$: A binary linear code with generator matrix G and parity check matrix H.

$\mathcal{C}^{\perp}$: Its dual, a bin. linear code with gen. matrix H and parity check matrix G.

Note: $G^{\perp} = H, \quad H^{\perp} = G$ and $\mathcal{C} : [n, k] \leftrightarrow \mathcal{C}^{\perp} : [n, n-k]$

Example: $\mathcal{C}$ is Hamming [7,4,3]

$$H = \begin{pmatrix} 0111 & 100 \\ 1011 & 010 \\ 1101 & 001 \end{pmatrix} = G^{\perp}$$

$$G = \begin{pmatrix} 1000 & 011 \\ 0100 & 101 \\ 0010 & 110 \\ 0001 & 111 \end{pmatrix} = H^{\perp}$$

$\mathcal{C}^{\perp}$:

Info $\overline{m}$	Codeword $\overline{m}G^{\perp}$	Weight
000	0000000	0
001	1101001	4
010	1011010	4
011	0110011	4
100	0111100	4
101	1010101	4
110	1100110	4
111	0001111	4

$d^{\perp} = 4$

$\mathcal{C}^{\perp}$ is [7,3,4]

Example: Cyclic Codes

Definition: A *cyclic code* is a linear code for which all cyclic shifts of codewords are also codewords.

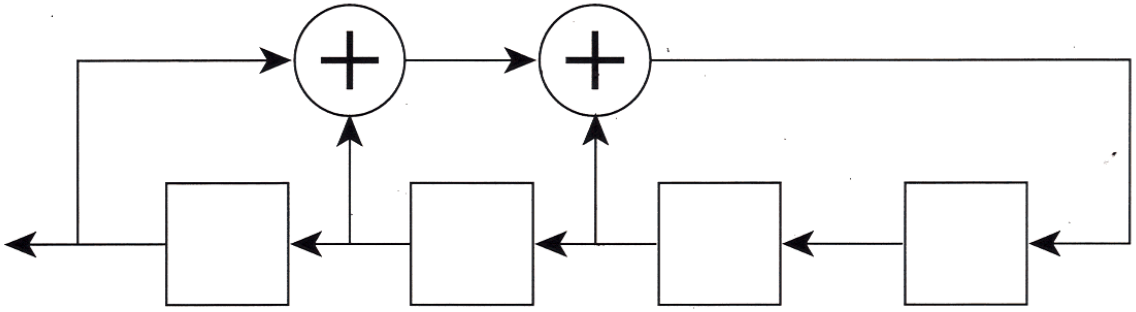
Cyclic shifts of $\bar{c}_k = (1\ 0\ 0\ 1)$ are $(1\ 1\ 0\ 0)$, $(0\ 1\ 1\ 0)$, $(0\ 0\ 1\ 1)$

(Note: Two codewords need to be cyclic shifts of each other)

Example: Cyclic [7,4,3] Hamming Code

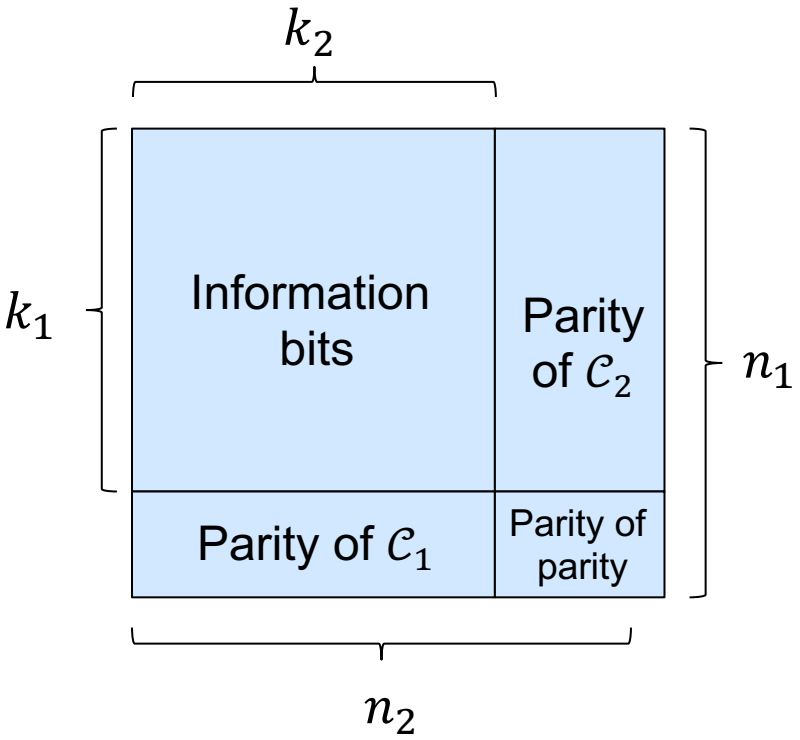
$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

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



$$\begin{array}{cccc} c_1 & c_2 & c_3 & c_4 \\ c_2 & c_3 & c_4 & c_5 \\ c_3 & c_4 & c_5 & c_6 \\ c_4 & c_5 & c_6 & c_7 \end{array}$$

Product Codes (2-dimensional code)



$\mathcal{C}_1$: One code for columns $[n_1, k_1, d_1]$

$\mathcal{C}_2$: One code for rows $[n_2, k_2, d_2]$

Result:

$$n = n_1 n_2$$
$$k = k_1 k_2$$
$$d = d_1 d_2$$

Simple implementation: First $\mathcal{C}_1$ and then $\mathcal{C}_2$, then iterate…

Good performance using two short codes instead of one long code


LINKÖPING
UNIVERSITY
www.liu.se