TSKS02 Telecommunication

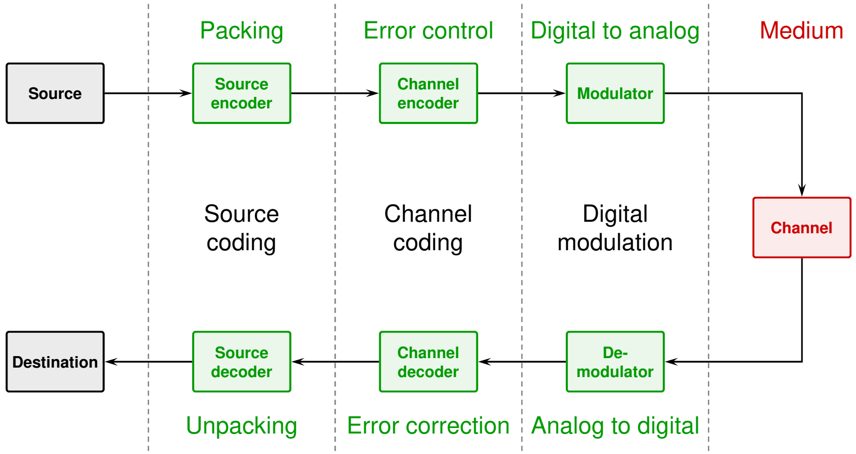
Lecture 9

Error Control Codes – Introduction

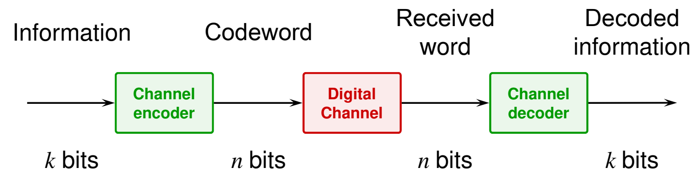
Mikael Olofsson
Department of EE (ISY)
Div. of Communication Systems

LINKÖPINGS UNIVERSITET

A One-way Telecommunication System



Block Codes – Basic Idea



Calculate r parity bits from the k information bits.

Send $n = k + r$ codeword bits.

Received: n possibly corrupted bits.

Decode to the most likely sent codeword given the received bits.

More general:
Map k information bits on $n = k + r$ codeword bits.

If the codewords are well chosen, then we will be able to correct errors.

Block Code – Set of Binary Vectors

Code: $\mathscr{C} = \left\{ \bar{c}_i \in \{0,1\}^n \right\}_{i=1}^{2^k}$

Codeword: $\bar{c}_i = \left(c_{i,1}, \ldots, c_{i,n} \right)$, $\in \{0,1\}$

Rate: $R = \dfrac{k}{n}$

Example code:

Information	Codeword
00	10101010
01	11010000
10	01100111
11	00011101
$k = 2$	$n = 8$

Decoding principles:

Assume that all errors are equally serious. $\Rightarrow$

Choose the most likely codeword given the received vector.

Decoding

Stochastic variables: Sent codeword: $\overline{C}$

Received word: $\overline{X}$

MAP decoding:

Decoding rule 1: Set $\hat{c} = \overline{c}_i$ if $\Pr\{\overline{C} = \overline{c}_j \mid \overline{X} = \overline{x}\}$ is maximized for $j = i$.

Bayes rule $\Rightarrow$

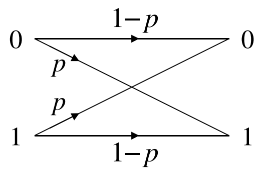
Decoding rule 2: Set $\hat{c} = \overline{c}_i$ if $\Pr\{\overline{C} = \overline{c}_j\}\Pr\{\overline{X} = \overline{x} \mid \overline{C} = \overline{c}_j\}$ is max for $j = i$.

ML decoding $\left(\Pr\{\overline{C} = \overline{c}_j\} = 1/2^k\right)$:

Decoding rule 3: Set $\hat{c} = \overline{c}_i$ if $\Pr\{\overline{X} = \overline{x} \mid \overline{C} = \overline{c}_j\}$ is maximized for $j = i$.

The Binary Symmetric Channel (BSC)

Input



Output

Consecutive uses of the channel are independent.

Hamming distance: $d_H(\overline{a},\overline{b})$ # positions where $\overline{a}$ and $\overline{b}$ differ.

Properties: $d_H(\overline{a},\overline{a}) = 0$ $\quad d_H(\overline{a},\overline{b}) \geq 0$ $\quad d_H(\overline{a},\overline{c}) \leq d_H(\overline{a},\overline{b}) + d_H(\overline{b},\overline{c})$

We get: $\Pr\{\overline{X} = \overline{x} \mid \overline{C} = \overline{c}_j\} = p^{d_H(\overline{x},\overline{c}_j)}(1-p)^{n-d_H(\overline{x},\overline{c}_j)}$

ML decoding for BSC with error probability p (assuming $0 < p < 0.5$):

Decoding rule 4: Set $\hat{c} = \overline{c}_i$ if $d_H(\overline{x},\overline{c}_j)$ is minimized for $j = i$.

Example of Decoding

Information	Codeword
00	10101010
01	11010000
10	01100111
11	00011101
$k = 2$	$n = 8$

$d_H(10101010, 11010000) = 5$

$d_H(10101010, 01100111) = 5$

$d_H(10101010, 00011101) = 6$

$d_H(11010000, 01100111) = 6$

$d_H(11010000, 00011101) = 5$

$d_H(01100111, 00011101) = 5$

Minimum distance $d = 5$

Decoding: Choose closest codeword.

(10111010) is decoded to (10101010)

(11110111) is decoded to (01100111)

(00111000) is on distance 3 from both (10101010) & (00011101)

Error correction capability

$t = \left\lfloor \frac{d-1}{2} \right\rfloor$ Here $t = 2$

Error detection capability

$v = d - 1$ Here $v = 4$

The Binary Field, GF(2)

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Integer arithmetic reduced modulo 2.

Associative law: $(a + b) + c = a + (b + c) \quad \forall\, a, b, c \in \mathrm{GF}(2)$

$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall\, a, b, c \in \mathrm{GF}(2)$

Commutative law: $a + b = b + a \quad \forall\, a, b \in \mathrm{GF}(2)$

$a \cdot b = b \cdot a \quad \forall\, a, b \in \mathrm{GF}(2)$

Unit elements: $\exists\, 0 \in \mathrm{GF}(2)\colon\ a + 0 = a \quad \forall\, a \in \mathrm{GF}(2)$

$\exists\, 1 \in \mathrm{GF}(2)\colon\ a \cdot 1 = a \quad \forall\, a \in \mathrm{GF}(2)$

Inverses: $\exists\, -a \in \mathrm{GF}(2)\colon\ a + (-a) = 0 \quad \forall\, a \in \mathrm{GF}(2)$

$\exists\, a^{-1} \in \mathrm{GF}(2)\colon\ a \cdot a^{-1} = 1 \quad \forall\, a \in \mathrm{GF}(2),\ a \neq 0$

Distributive law: $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall\, a, b, c \in \mathrm{GF}(2)$

Binary Linear Codes

Definition:
A binary linear code is a linear subspace of the full vector space $\mathrm{GF}(2)^n$.

Equivalent definition:
The binary code $\mathscr{C}$ is called linear if $\bar{c}_1 + \bar{c}_2 \in \mathscr{C}$ holds for all $\bar{c}_1, \bar{c}_2 \in \mathscr{C}$.

Generator matrix G:

$$\mathscr{C} = \left\{ \bar{m} G \ \forall\, \bar{m} \in \mathrm{GF}(2)^k \right\}$$

Generator matrix, $k \times n$

Information vector, k bits

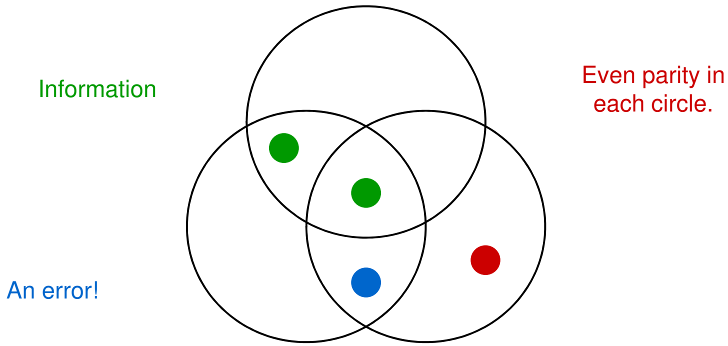
Example:

$$G = \begin{pmatrix} 1100 \\ 0111 \end{pmatrix}$$

$\bar{m}$	$\bar{c} = \bar{m}G$
00	0000
01	0111
10	1100
11	1011

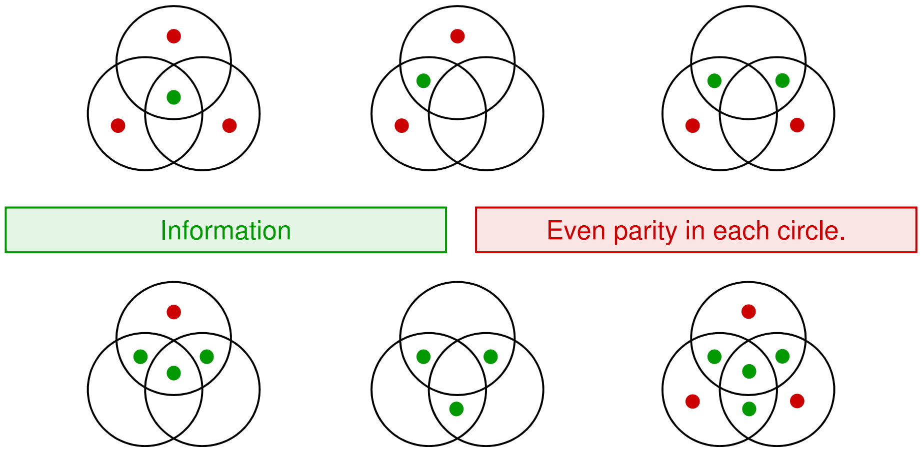
We can use everything from linear algebra!!

The [7,4] Hamming Code – Example

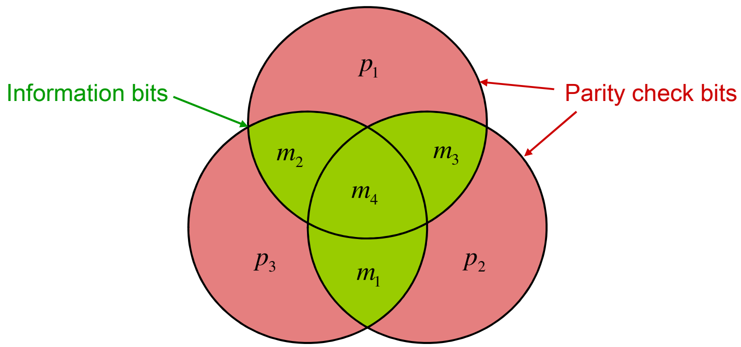


Result: Even parity in the upper circle, odd parity in the two lower circles.
Only one position can explain that – the actual error.

The [7,4] Hamming Code – More Examples



The [7,4] Hamming Code



Even parity in each circle. $\Rightarrow$

$$\begin{cases} p_1 + m_2 + m_3 + m_4 = 0 \pmod 2 \\ p_2 + m_1 + m_3 + m_4 = 0 \pmod 2 \\ p_3 + m_1 + m_2 + m_4 = 0 \pmod 2 \end{cases}$$

[7,4] Hamming Code – Generator Matrix

$$\begin{cases} p_1+m_2+m_3+m_4=0 \pmod 2 \\ p_2+m_1+m_3+m_4=0 \pmod 2 \\ p_3+m_1+m_2+m_4=0 \pmod 2 \end{cases} \Rightarrow \begin{cases} p_1=m_2+m_3+m_4 \pmod 2 \\ p_2=m_1+m_3+m_4 \pmod 2 \\ p_3=m_1+m_2+m_4 \pmod 2 \end{cases}$$

Codeword:

$$\bar{c}=(m_1,m_2,m_3,m_4,p_1,p_2,p_3)=(m_1,m_2,m_3,m_4)\left(\begin{array}{cccc|ccc} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{array}\right)$$

Generator matrix, G, on systematic form

$$G=(I_k,P) \quad \text{with} \quad P=\begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix}$$

Code:

$$\mathscr{C}=\left\{\bar{c}=\bar{m}G \;\forall\; \bar{m}\in \mathrm{GF}(2)^4\right\}$$

Dimension:
k = # rows in G. Here 4.

Length:
n = # columns in G. Here 7.

Nullspaces and Parity Check Matrices

A vector space (code) expressed in a basis:

$$\mathscr{C}=\left\{\bar{m}G \;\forall\; \bar{m}\in \mathrm{GF}(2)^k\right\}$$

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

A vector space (code) expressed as the nullspace of a matrix:

$$\mathscr{C}=\left\{\bar{c}\in \mathrm{GF}(2)^n : H\bar{c}^{\mathrm{T}}=\bar{0}\right\}$$

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

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

[7,4] Hamming Code – Parity Check Matrix

$$\begin{cases} m_2+m_3+m_4+p_1=0 \\ m_1+m_3+m_4+p_2=0 \\ m_1+m_2+m_4+p_3=0 \end{cases} \Rightarrow \left(\begin{array}{cccc|ccc} 0&1&1&1&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{array}\right)\begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ p_1 \\ p_2 \\ p_3 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Parity check matrix, H, on systematic form

Compare to the generator matrix:

$$G=\left(\begin{array}{cccc|ccc} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{array}\right)=(I_4,P)$$

$$H=(P^{\mathrm{T}},I_3)$$

In general:

$$\begin{cases} G=(I_k,P) \\ H=(P^{\mathrm{T}},I_{n-k}) \end{cases} \quad \text{or} \quad \begin{cases} G=(P,I_k) \\ H=(I_{n-k},P^{\mathrm{T}}) \end{cases}$$

Codes may have non-systematic generator and/or parity check matrices.

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

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

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

Example Hamming [7,4]:

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

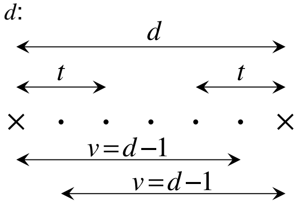
No column $=\bar{0}$ $\Rightarrow d>1$
No 2 columns equal
$\Rightarrow d>2$
$\bar{h}_1+\bar{h}_6+\bar{h}_7=\bar{0}$
$\Rightarrow d=3$

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 $w \le t$.

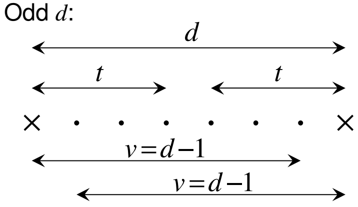
Error detection capability: $v = d-1$ — The code can detect every w-bit error if $w \le v$.

Even d:



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

Odd d:



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

Overview – Binary Linear Codes $[n,k,d]$

A vector space expressed in a basis

$$\mathscr{C} = \left\{ \overline{m}G \ \forall\ \overline{m} \in \mathrm{GF}(2)^k \right\}$$

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

… the nullspace of a matrix

$$\mathscr{C} = \left\{ \overline{c} \in \mathrm{GF}(2)^n : H\overline{c}^{\mathrm{T}} = \overline{0} \right\}$$

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.

Mikael Olofsson
ISY/CommSys

www.liu.se

LINKÖPINGS UNIVERSITET