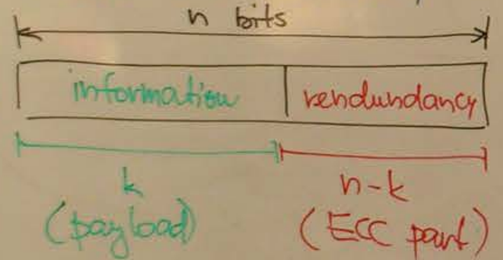
ERROR CORRECTING CODES (ECC)

- variable length codes
- block codes

① detecing an error
② correct the error, if possible

↳ add REDUNDANCY



(n,k)-code

Information rate: $\frac{k}{n}$

Minimum code distance:

$d(w_1,w_2)$ ... number of bits where w_1 and w_2 differ

$$\min_{\substack{w_1 \in \mathbb{K} \\ w_2 \in \mathbb{K} \\ w_1 \neq w_2}} d(w_1,w_2) = d_{min}$$

⇒ minimal number of bits to flip for obtaining another code word

Detection capabilities: code detects t-ary error iff $t < d_{min}$

Example:

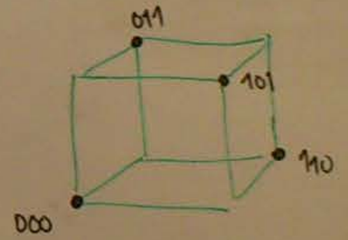
parity (3,2)

000 i.r. $= \frac{2}{3}$
011
101
110

$\mathbb{K} \subset \mathbb{V} = \{0,1\}^3$

$\mathbb{K}$ ... 8 possible words (2^3)
... 4 codewords

$d(011,110) = 2$
$d(000,110) = 2$
$d_{min} = 2$



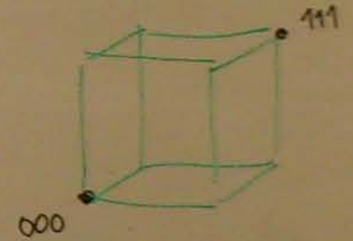
repetition code (3,1)

000 i.r. $= \frac{1}{3}$
111

2 codewords

$d(000,111) = 3$

$d_{min} = 3$



ERROR CORRECTING CODES (ECC)

Correction capabilities: code corrects t-ary error iff $\boxed{2t < d_{min}}$

↓

difficult to design by hand

↓

! use linear algebra !

→ **LINEAR CODES**

$\oplus$	0	1
0	0	1
1	1	0

XOR

$\cdot$	0	1
0	0	0
1	0	1

AND

Information rate: $\frac{k}{n}$

Minimum code distance:

$d(w_1, w_2)$ ... number of bits where w_1 and w_2 differ

$$\min_{\substack{w_1 \in \mathbb{K} \\ w_2 \in \mathbb{K} \\ w_1 \neq w_2}} d(w_1, w_2) = \boxed{d_{min}} \qquad (2^k - 1)\, 2^{k-1}$$

⇒ minimal number of bits to flip for obtaining another code word

Detection capabilities: code detects t-ary error iff $\boxed{t < d_{min}}$

Example

parity (3,2)

000
011
101
110

i.r. $= \frac{2}{3}$

$\mathbb{K} \subset \mathbb{V} = \{0,1\}^3$

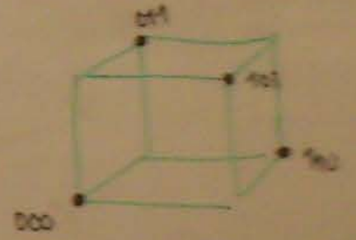
$\mathbb{K}$ ... 8 possible words (2^3)

... 4 codewords

$d(011, 110) = 2$

$d(000, 110) = 2$

$d_{min} = 2$



repetition code (3,1)

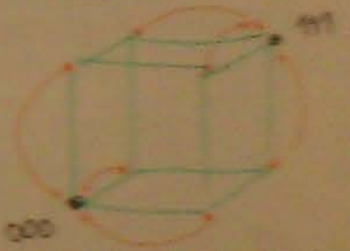
000
111

i.r. $= \frac{1}{3}$

2 codewords

$d(000, 111) = 3$

$d_{min} = 3$



take the closest code word

LINEAR CODES

- all (n,k)-codes $\mathbb{K} \subset \mathbb{V}_n = \{0,1\}^n$ (sub-space of dimension k)

$\Rightarrow$ sub-space has to have k basis vectors $\{\vec{v}_0, \vec{v}_1, \dots, \vec{v}_{k-1}\}$

2^k code words
2^n possible words

code word $\vec{v} = (v_0, v_1, \dots, v_{n-1})$

plaintext $\vec{u} = (u_0, u_1, u_2, u_3, \dots, u_{k-1})$

$$\vec{v} = u_0 \vec{v}_0 \oplus u_1 \vec{v}_1 \oplus \dots \oplus u_{k-1} \vec{v}_{k-1}$$

$$\vec{v} = \vec{u} \cdot G \qquad G = \begin{pmatrix} \vec{v}_0 \\ \vec{v}_1 \\ \dots \\ v_{k-1} \end{pmatrix}$$

generator matrix

$G_{k \times n}$

All codes can be described by a homogeneous system of equations for $v_0, v_1, \dots, v_{n-1}$

Verification of a code-word:

parity check matrix H

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

or

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

$\vec{u} \cdot G \cdot H^T = 0$

syndrome

Example:

parity (3,2)

000
011
101
110

$\vec{u} = \{00, 01, 10, 11\}$

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

$$(000) = (00)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$
$$(011) = (01)\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$
$$\vdots$$

$v_0 \oplus v_1 \oplus v_2 = 0$

repetition code (3,1)

000
111

$\vec{u} = \{0, 1\}$

$G = (1\ 1\ 1)$

$111 = 1 \cdot (111)$
$000 = 0 \cdot (111)$

$v_0 \oplus v_1 = 0$
$v_1 \oplus v_2 = 0$
$v_0 \oplus v_2 = 0$

LINEAR CODES

- all (n,k)-codes $\mathbb{K} \subset \mathbb{V}_n = \{0,1\}^n$ (sub-space of dimension k)

$\Rightarrow$ sub-space has to have k basis vectors $\{\vec{v}_0, \vec{v}_1, \dots, \vec{v}_{k-1}\}$

2^k code words
2^n possible words

$u_0 u_1$	$v_2 v_3$

code word $\vec{v} = (v_0, v_1, \dots, v_{n-1})$

plaintext $\vec{u} = (u_0, u_1, u_2, u_3, \dots, u_{k-1})$

$$\vec{v} = u_0 \vec{v}_0 \oplus u_1 \vec{v}_1 \oplus \dots \oplus u_{k-1} \vec{v}_{k-1}$$

$$\vec{v} = \vec{u} \cdot G \qquad G = \begin{pmatrix} \vec{v}_0 \\ \vec{v}_1 \\ \dots \\ \vec{v}_{k-1} \end{pmatrix}$$

generator matrix

$G_{k \times n}$

All codes can be described by a homogeneous system of equations for $v_0, v_1, \dots, v_{n-1}$

Verification of a code-word:

parity check matrix H

$$G \cdot H^T = \vec{0} \quad \text{or} \quad \vec{v} \cdot H^T = \vec{0}$$

$\vec{u} \cdot G \cdot H^T = 0$

syndrome

Example: $(4,2)$-code $\quad G = [I_{k \times k} \; P_{k \times n-k}]$ $\quad H = [P^T_{n-k \times k} \; I_{n-k \times n-k}]$

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

$$G_{sys} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad I \quad P$$

systematic code (separate information and parity blocks)

$$P = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \rightarrow P^T = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

$$H_{sys} = \left[\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right]$$

$$\vec{v}' = (1110) \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$\vec{u} = (01)$

$$\vec{v} = (01) \begin{pmatrix} 1011 \\ 0110 \end{pmatrix} = (0110)$$

$$\vec{v} \cdot H^T = (0110) \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$\hookrightarrow \vec{v}$ is a code word!