Qubits: $|0\rangle, |1\rangle$ instead of $|+\rangle, |-\rangle$ for basis of $\mathbb{C}^2$

Errors: $|0\rangle \to |1\rangle$ bit flip error
$|1\rangle \to |0\rangle$

$|0\rangle \to |0\rangle$ phase error
$|1\rangle \to -|1\rangle$

$|0\rangle, |1\rangle \to U|0\rangle, U|1\rangle$ unitary continuous errors

# Classical Error Correction

## Repitition code

1970 Mariner Probe going to Mars - greyscale pictures

16 shades of grey $\to$ 1001 $\to$ 111 000 000 111

↓ 1 bit error

$\underbrace{111}_{1}$ $\underbrace{010}_{0}$ $\underbrace{000}_{0}$ $\underbrace{111}_{1}$ majority wins

4 bits $\to$ 12 bits, correct 1 error

## Hamming Code

4 bits $\to$ 7 bits correct any 1-bit errors

$\mathbb{F}_2$ - Field w/ 2 elements

addition mod 2

$0+0=0$ $\quad$ $0*0=0$
$0+1=1$ $\quad$ $0*1=1*0=0$
$1+0=1$ $\quad$ $1*1=0$
$1+1=0$

$\mathbb{F}_2^n$ - vector space over $\mathbb{F}_2$ w/ elements $(x_1, x_2, \dots, x_n)$ $x_i \in \mathbb{F}_2$

$\mathbb{F}_2^4$ - 4 elements $(0,0), (1,0), (0,1), (1,1)$

codes: A binary $\mathbb{F}_2$, linear code $C$ of length $n$ and rank $k$, $[n,k]$, is a linear subspace of $\mathbb{F}_2^n$ of dimension $k$ : $2^k$

$w_1, w_2 \in \mathcal{C}$ $\qquad$ $w_1 + w_2 \in \mathcal{C}$

$\mathbb{F}_2^2$ w/elements $\qquad$ $(0,0), (1,0), (0,1), (1,1)$

$\mathcal{C} = \{(0,0), (1,1)\}$ - linear subspace of $\mathbb{F}_2^2$ $\quad$ $2^1$ vectors

$\uparrow$ 1 basis vectors

$n=2$ components
$k=1$ basis vectors

$(1,1)$ is basis of $\mathcal{C}$ $\qquad$ this is a $[2,1]$ code

$(1,1) + (1,1) = (0,0)$

Hamming code

7 bits, 4 basis $\to$ $[7,4]$ $\qquad$ Binary linear code

Four basis bits: $(x_1, x_2, x_3, x_4)$ $\qquad$ some data to encode

Codeword : $(x_1, x_2, x_3, x_4, x_5, x_6, x_7)$

$$\begin{aligned} x_5 &= x_1 + x_2 + x_4 \mod 2 \\ x_6 &= x_1 + x_3 + x_4 \mod 2 \\ x_7 &= x_2 + x_3 + x_4 \mod 2 \end{aligned}$$

$w = (x_1, x_2, \dots, x_7)$
$d = (x_1, x_2, x_3, x_4)$

$w = dG$

$\uparrow$ row vector $(x_1, \dots, x_4)$

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

Literature sometimes uses $w = G^T d$

Claim: Hamming code can (detect 2 bit error &) correct 1 bit error in length 7 word

Develop formalism

$G$ - generating matrix

if $d = (x_1, x_2, \dots, x_k)$ is data word & $W = (x_1, x_2, \dots, x_n)$ if codeword for $d$

$\longrightarrow$ $W = dG$, $G = [\mathbb{1}_k, A]$

$\mathbb{1}_k$: k×k identity; $A$: k×(n-k) matrix, 7x4

$H$ - parity check matrix

$\mathcal{C}^\perp$ - dual code

Given an $[n,k]$ code $\mathcal{C}$, the dual code $\mathcal{C}^\perp$ is given by

$\longrightarrow$ $\mathcal{C}^\perp = \{ v \in \mathbb{F}_2^n \mid v \cdot w = 0 \text{ for all } w \in \mathcal{C} \}$

$v \cdot w = \sum_{i=1}^{n} v_i w_i \mod 2$

check 1) $\mathcal{C}^\perp$ is also a binary linear code
2) $\mathcal{C}^\perp$ is a $[n, n-k]$ code

$\mathcal{C} = [7,4]$ 16 words $2^4$
$\mathcal{C}^\perp = [7,3]$ 8 words $2^3$

$\mathcal{C}^\perp$ has generator matrix: $H$ (parity check matrix)

parity check

$(x_1, x_2, \dots, x_n)$ $x_i \in \mathbb{F}_2^n$ $x_{n+1} = \sum_{i=1}^{n} x_i \mod 2$

then $(x_1, x_2, \dots, x_n, x_{n+1})$ $x_i \in \mathbb{F}_2^{n+1}$ has even parity

parity of $(x_1, x_2, \dots x_{n+1})$ is: even if $\sum_{i=1}^{n+1} x_i = 0$
odd if $\sum_{i=1}^{n+1} x_i = 1$

if $v \in \mathcal{C}^\perp$, then $v \cdot w = 0$ for all $w \in \mathcal{C}$

All $w \in \mathcal{C}$ are $d \cdot G$ for some data word

All $v \in \mathcal{C}^\perp$ are $d'H$ for some word $d'$ by def$^{\underline{n}}$ of $H$

$v \cdot w = 0 = v \cdot w^{\perp} = d\,G H^{T} d'^{T}$ for all $d, d'$

$\rightarrow GH^{T} = 0 \rightarrow HG^{T} = 0$

$w = dG \rightarrow Hw^{T} = \underbrace{HG^{T}}_{0} d^{T} = 0$