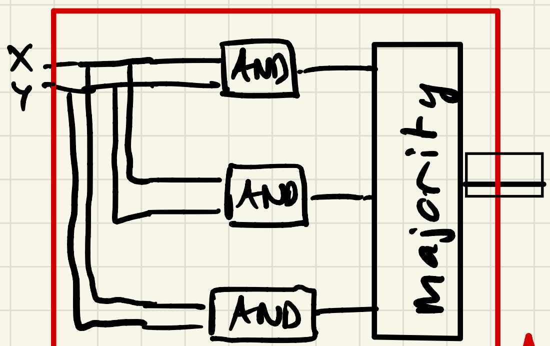
Quantum computation : lecture 11

Error correcting codes (classical, first)

- circuit with AND, OR, NOT gates
  each component has probability p of failing
  (assume independence & $p =$ same $\forall$ component)
- first idea: (repetition)



AND'

$$\text{AND} \qquad \text{AND}'$$
$$p \longrightarrow c p^2 = p'$$

We want $p' < p$, i.e. $cp^2 < p$, i.e. $p < \frac{1}{c}$

So if it is possible to build an AND gate with $\boxed{p < \frac{1}{c}}$, then it is possible to build an AND' with $p' < p$, and to repeat this an arbitrary number of times with $p, p', p'' \dots p^{(k)} \dots \to 0$

= <u>Threshold theorem</u>

<u>NB</u>: $p'' = c p'^2 = c(cp^2)^2 = \frac{1}{c}(cp)^4$; $p^{(k)} = \frac{1}{c}(cp)^{2^k}$

<u>Caveat</u>: majority gate to be built...

Let us now think about transmission of information (instead of circuits):

$$x = \begin{cases} 0 \\ 1 \end{cases} \longrightarrow \boxed{\text{channel}} \longrightarrow \text{observation } y \in \begin{Bmatrix} 0 \\ 1 \end{Bmatrix}$$

with $\mathbb{P}(x = y) = 1 - p$

($0 < p < \frac{1}{2}$ small)

<u>Repetition code</u> (length 3):

$$x = \begin{cases} 0 \to 000 \\ 1 \to 111 \end{cases} \longrightarrow \boxed{\text{channel}} \longrightarrow \text{observation } y_1 y_2 y_3$$

(independent for each bit)

How to retrieve x from $y_1 y_2 y_3$?

(In general, look for the most probable x given $y_1 y_2 y_3$)

<u>Here</u>: apply the majority rule:

<u>Ex</u>: $y_1 y_2 y_3 = 110 \longrightarrow$ output 1

$y_1 y_2 y_3 = 010 \longrightarrow$ output 0

What is the probability that we make a mistake?

$$\mathbb{P}(\text{output} = 1 \mid x = 0 \text{ is sent}) = \underbrace{p^3}_{\text{3 bit flips}} + \underbrace{3p^2(1-p)}_{\text{2 bit flips}} < p \quad \text{if } p < \tfrac{1}{2}$$

$$= \mathbb{P}(\text{output} = 0 \mid x = 1 \text{ is sent})$$

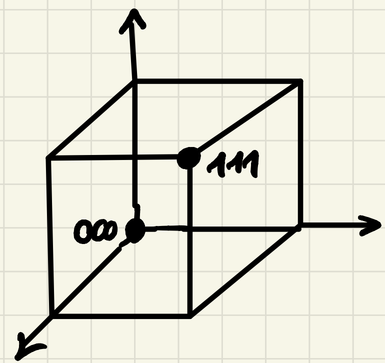
Here are some parameters:

n = length of codewords = 3

r = rate = $\frac{1}{3}$ (3 bits sent for 1 bit of information)

d = distance = 3

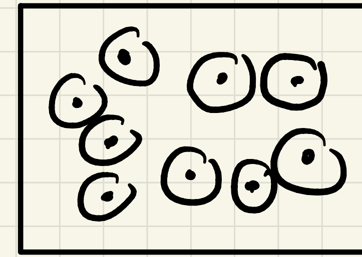
(= # diff. bits in the codewords)



We want both $\underline{\text{large } r}$ and $\underline{\text{large } d}$

lots of info/sec good error correction

$\mathbb{F}_2^n$



Binary codes of length n

- Code $\mathcal{C}$ = subset of $\mathbb{F}_2^n$

  $|\mathcal{C}| = 2^k$ in order to transmit k information bits ($k<n$)

- codewords should be separated by distance $\geq 2pn$ (pn = average number of errors on one codeword)

- decoding: look for nearest neighbour of the received sequence of bits

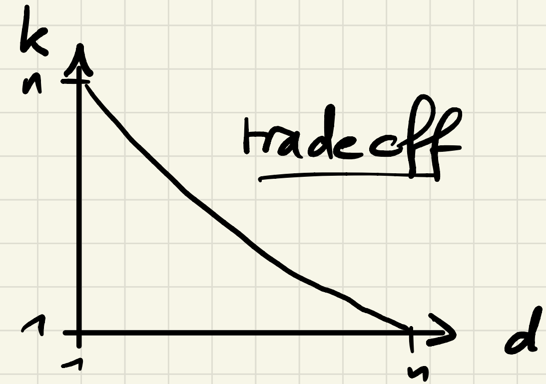
So $\mathcal{C} = \{ c_1, \dots, c_{2^k} \}$

$$d = \min \{ \text{distance}(c_i, c_j) : c_i, c_j \in \mathcal{C}, \; c_i \neq c_j \}$$

$\Rightarrow \mathcal{C}$ can correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors

The name of the game is now to place the 2^k codewords in $\mathbb{F}_2^n$ so that the minimum distance d is the largest possible.

- The 3 important parameters of the code are (n, k, d):



- Lots of codewords in $\mathcal{C}$; we need some structure

$\Rightarrow$ focus on linear codes, satisfying

$$c_i, c_j \in \mathcal{C} \Rightarrow \underset{(\text{XOR})}{c_i \oplus c_j} \in \mathcal{C} \quad (= \text{subspace})$$

Generator point of view:

$$\mathcal{C} = \{ c \in \mathbb{F}_2^n : c = u \cdot G \; ; \; u \in \mathbb{F}_2^k \}$$

$G = k \times n$ generator matrix

code $\mathcal{C}$ = raw space of G

Ex: repetition code $\mathcal{C} = \{000, 111\}$ (= linear code)

$n=3$, $k=1$, $G = (1 \; 1 \; 1)$

(take then $u = (0)$ or $u = (1) \in \mathbb{F}_2$)

Parity check view:

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

$H = (n-k) \times n$ parity check matrix ($\to \mathcal{C}$ of dim k)

Ex: $\mathcal{C} = \{000, 111\}$ $\quad n=3,\ k=1,\ n-k=2$

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

indeed: $H \cdot c^T = 0$

for both $c = (000)$

and $c = (111)$

Hamming code:

$k=4$, $n-k=3$, $n=2^{n-k}-1=7$

$$H=\begin{pmatrix} 0&0&0&1&1&1&1\\ 0&1&1&0&0&1&1\\ 1&0&1&0&1&0&1 \end{pmatrix}$$ (column j = binary expansion of j)

This code has minimum distance $d=3$. Indeed:

- for linear codes, min distance = min weight (= # 1's) of a non-zero codeword, as $d(c_i, c_j) = d(0, \overbrace{c_i \oplus c_j}^{\in \mathcal{C}})$ $\forall i,j$ (and $c_i \neq c_j$ iff $c_i \oplus c_j \neq 0$)

- $HC^T = 0$ implies at least weight$(c) \geq 1$,
  as H does not have a column of 0's
- But it is also the case that weight$(c) \geq 2$
  as H does not have identical colums.
- If weight$(c) = 3$, then it is indeed
  possible that $HC^T = 0$ (take eg $C = (1110000)$)

$\Rightarrow d = 3$.

Error correction with this code: (syndrom decoding)

Assume y is received $(= c + e)$:
$\uparrow$ error

$$H \cdot y^T = H \cdot (c^T + e^T) = \underbrace{H \cdot c^T}_{=0} + H \cdot e^T = H \cdot e^T$$

If $e = (0010000)$, then $H \cdot e^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \longrightarrow 3$:

in this case, we know the error occured in position 3.

Quantum error correction

Potential problems:

$0, 1 \longrightarrow$ state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

(1) repetition code ? ⚠ no cloning theorem

(2) type of errors ? continuous vector space !

(3) measurement destroys a state, potentially !

states cannot be observed (nor corrected)

???