ERROR: $\boxed{\begin{array}{l} 0 \rightarrow 1 \\ 1 \rightarrow 0 \end{array}}$ noise

Solution: Add redundancy.

→ Spread out the information.

Replicate 2 times:

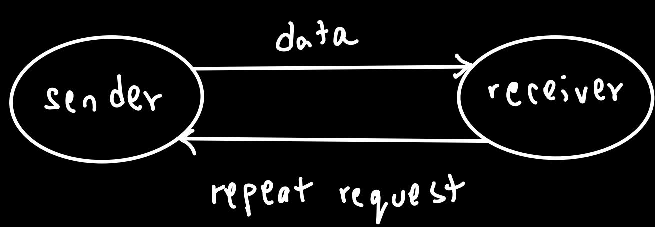
$0 \rightarrow 00$

$1 \rightarrow 11$

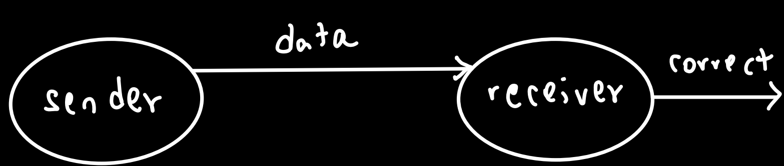
if a single error, then receive 01, 10.

ERROR DETECTED

ERROR DETECTION:



ERROR CORRECTION:



Replicate 3 times:

$0 \longrightarrow 000$

$1 \longrightarrow 111$

(single error)

if we receive

$\begin{Bmatrix} 000, & 100 \\ 010, & 001 \end{Bmatrix} \longrightarrow 0$

$\begin{Bmatrix} 111, & 011 \\ 101, & 110 \end{Bmatrix} \longrightarrow 1$

CORRUPTED CODEWORD	ERROR SYNDROME	CONCLUSION
000, 111	00 → Parity bit	no error
100, 011	10	bit 1 flipped
010, 101	11	bit 2 flipped
001, 110	01	bit 3 flipped

↓

ERROR CORRECTED

Error syndrome:

$$0 \oplus 0 = 0$$

$$1\overbrace{0\,0}\ \Rightarrow 10$$

$$\underbrace{1\,0}\,0$$

$$1 \oplus 0 = 1$$

2 errors:

$0 \xrightarrow{\text{encode}} 000 \xrightarrow{\text{error}} 011 \xrightarrow{\text{correct}} 111 \xrightarrow{\text{decode}} 1$

CANNOT CORRECT.

3 errors:

$000 \rightarrow 111$ CANNOT DETECT.

LINEAR ALGEBRA

$B = \{0,1\}$

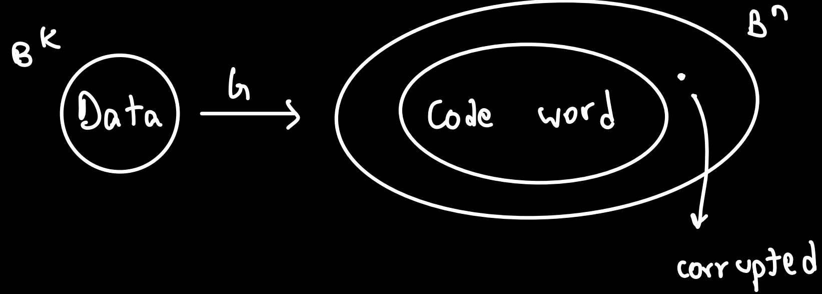
Encoding : $B^k \rightarrow B^n$

$[n,k]$-code

$n > k$

LINEAR 1-1 FUNCTION (MATRIX $G(n \times k)$)

Generator



Convert B^1 to B^3

$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$ $[3,1]$ CODE

$$G(0) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} [0] = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

$$G(1) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} (1) = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

ERROR CORRECTION USING LINEAR ALGEBRA:

Matrix P

↳ Parity

Rows of P span $B^n \setminus G(B^k)$

So B^n is B^3

B^k is B^1

$G(B^1) = \{000, 111\}$

So $B^n \setminus G(B^k)$ can be spanned by 2 independent vectors.

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

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

xor sum

$(n-k)$ zeroes.

So if s is in $G(B^k)$,

then $Ps = 0$

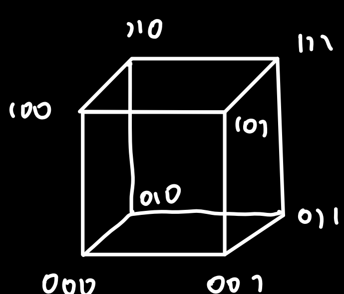
$\forall s \in B^n : \quad Ps = 0 \quad \text{iff} \quad s \in G(B^k).$

ERROR VECTOR:

e

$$s' = s + e$$

corrupted original



Single error is one move along edge.

$$Ps' = P(s+e)$$
$$= Ps + Pe$$
$$= 0 + Pe$$
$$= Pe \rightarrow \text{error syndrome}$$

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

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

Theory : Error Detection is possible iff every error has a nonzero syndrome.

Theory : Error Correction is possible iff every error has a unique syndrome.

Q : error Syndrome $\longrightarrow$ error

$$QPe = e$$

$$\begin{aligned}
\text{Received} + \text{fix} &= s' + QPs' \\
&= s' + QP(s+e) \\
&= s' + QPs + QPe \\
&= s' + QPe \\
&= s' + e \\
&= (s+e)+e = s
\end{aligned}$$

Q need not be a linear function.

HAMMING DISTANCE:

$w : B^n \to \mathbb{N}$

$ws = \#$ 1's in s

Hamming Distance :

$$d(s,t) = w(s-t)$$
$$= w(s+t)$$

$s, t \in B^n$

Distance between s and t.

$$d(G) = \min\{d(s,t) \mid s,t \in G(B^k) \wedge s \neq t\}$$

↳ This shows the power of G to detect and correct error.

$$= \min\{w(z) \mid z \in G(B^k) \wedge z \neq 0\}$$

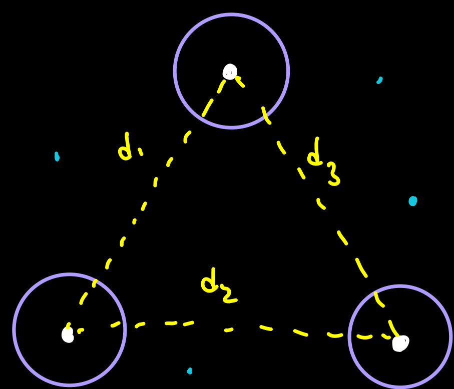
$$d\begin{pmatrix}1\\1\\1\end{pmatrix} = \min\{w(z) \mid z \in \{000, 111\} \wedge z \neq 0\} = \min\{w(111)\}$$
$$= 3$$

Also,

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

$$d\begin{pmatrix}1\\1\\1\end{pmatrix} = \min\left\{ d\left(\begin{matrix}0\\0\\0\end{matrix}\middle|\begin{matrix}1\\1\\1\end{matrix}\right) \right\} = 3 \,/\!/$$

$$d(s, s') = w(s+s') = w(s+(s+e)) = w(e)$$



If this is the case, we can reach codeword from single error.

- • : codewords
- ○ : single error
- · : >1 error

$$d(G) = \min(d_1, d_2, d_3)$$

$$\text{Radius}, r = \frac{d(G) - 1}{2}$$

if $d(G) = 3$ $\quad (3-1)/2 = 1$, it can correct upto 1 error only.

$p = P(\text{a bit flips})$

$[3, 1, 3]$ - code

$d(C)$

Detect 2 errors

Correct 1 error.

$P(\text{at least two bits flip}) = p^3 + 3p^2(1-p)$

out of 3

$= p^3 + 3p^2 - 3p^3$

$= 3p^2 - 2p^3$

$0 < p < 1$

Probability (cannot correct)

We made 1 bit to 3,

$3p^2 - 2p^3 < p$

When is it useless

$3p - 2p^2 < 1$

$2p^2 - 3p + 1 < 0$

$p = \frac{3 \pm \sqrt{9-8}}{4} = \frac{3 \pm 1}{4}$

$= 1, \frac{1}{2}$

$$(p-1)(p-1/2) < 0$$

$p < 1$ and $p < 1/2$

$$\boxed{p < 1/2}$$

or $p > 1$ and $p > 1/2$

↳ not possible.

So its good to send 3 bits when $p < 1/2$.

$[12, 4, 3]$ - code

$[7, 4, 3]$ - code

↳ more useful, less wasteful.

GOLAY:

$[24, 12, 8]$

encode 12 bits to 24 and send.

Detect 7 bit errors

and correct 3 errors.

PROBLEMS FOR QUANTUM:

→ No Cloning theorem
Cannot copy qubits

→ Error in quantum is not discrete
Here it is adding 1.
There any change in complex number.

→ We want to measure qubit to see if
there is error → But measurement
destroys qubit.