Shor's Algorithm:

Given number, N

a : random $(2, N-1)$ and $\gcd(a, N) = 1$

r = findOrder (a, N)

if r is even:

$$x = a^{r/2} - 1 \pmod N$$

$$d = \gcd(x, N)$$

if $d > 1$:

return d

r is the smallest integer $a^r \equiv 1 \pmod N$ - (1)

$$(a^r - 1) \bmod N = 0$$

if $r \rightarrow$ even

$$(a^{r/2} - 1)(a^{r/2} + 1) \bmod N = 0$$

So $(a^{r/2} - 1) \bmod N$ or $(a^{r/2} + 1) \bmod N$ can be zero. Need Not be.

$(a^{r/2} - 1) \bmod N$ is never 0. if it was $r/2$ is the smallest integer (1)

So try $\gcd(x, N)$

$$P(r = \text{even} \quad \text{AND} \quad (a^{r/2} - 1) \bmod N \neq 0) \geq 1/2$$

FIND ORDER:

$$\omega = e^{2\pi i / r}$$

TAKE

$$|\psi_k\rangle = \frac{1}{\sqrt{r}} \left(|1\rangle + \omega^{-k} |a\rangle + \omega^{-2k} |a^2\rangle + \dots + \omega^{-(r-1)k} |a^{r-1}\rangle \right)$$

We pass $|1\rangle$ and this can be seen as a uniform distribution over all $|\psi_i\rangle$

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\psi_k\rangle$$

PROOF:

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |\psi_k\rangle = \frac{1}{r} \sum_{k=0}^{r-1} \sum_{l=0}^{r-1} \omega^{-lk} |a^l\rangle$$

$$= \frac{1}{r} \sum_{l=0}^{r-1} \left(\sum_{k=0}^{r-1} \omega^{-lk} \right) |a^l\rangle$$

$$= |1\rangle + \frac{1}{n} \sum_{l=1}^{n-1} \underbrace{\left(\sum_{k=0}^{n-1} \omega^{-lk} \right)}_{\frac{1-(\omega^{-l})^n}{1-\omega^{-l}}} |a^l\rangle$$

$$\frac{1-(\omega^n)^{-l}}{1-\omega^{-l}}$$

$$\omega^n = (e^{2\pi i/n})^n = e^{2\pi i} = (e^{2\pi})^i$$

$$= (\cos 2\pi + i \sin 2\pi)^i$$

$$= 1$$

$$\frac{1-1}{1-\omega^{-l}} = 0$$

$$\frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |\psi_k\rangle = |1\rangle \; //$$

Assume

$$M_a|x\rangle = |ax \pmod N\rangle$$

Now Let us Prove that $|\psi_k\rangle$ are eigenvectors of M_a.

$$\boxed{M_a|\psi_k\rangle = \omega^k|\psi_k\rangle}$$

Let us Prove for $|\psi_1\rangle$

$$M_a|\psi_1\rangle = \omega|\psi_1\rangle$$

$$M_a|\psi_1\rangle = M_a \frac{1}{\sqrt{n}}\left(|1\rangle + \omega^{-1}|a\rangle + \omega^{-2}|a^2\rangle + \cdots + \omega^{-(n-1)}|a^{n-1}\rangle\right)$$

$$= \frac{1}{\sqrt{n}}\left(|a\rangle + \omega^{-1}|a^2\rangle + \omega^{-2}|a^3\rangle + \cdots + \omega^{-(n-1)}|a^n\rangle\right)$$

$$= \frac{\omega}{\sqrt{n}}\left(\omega^{-1}|a\rangle + \omega^{-2}|a^2\rangle + \omega^{-3}|a^3\rangle + \cdots + \omega^{-n}|a^n\rangle\right)$$

$$a^n \equiv 1 \pmod N$$

$$\omega^n = 1$$

$$= \omega |\psi_1\rangle$$

SO FIND ORDER CALLS PHASE ESTIMATION

WITH M_a, $|1\rangle$ → uniform distribution of all eigenvectors of M_a.

EACH ITERATION, A RANDOM $|\psi_k\rangle$ WOULD BE CHOSEN AND ITS PHASE RETURNED.

$$M_a |\psi_k\rangle = \omega^k |\psi_k\rangle$$
$$= e^{2\pi i k/n} |\psi_k\rangle$$

RETURNS k/n

⟶ USE CONTINUED FRACTION ALGORITHM TO FIND n.

PHASE ESTIMATION:

INPUT : M_a, $|\psi_k\rangle$ ⟶ Passed as $|1\rangle$

OUTPUT : $\theta = k/n$

Let's define an operation (modular exponentiation)

$$\lambda_m(M_a)\,|k\rangle|\psi\rangle = |k\rangle(M_a^k|\psi\rangle)$$

Assume n TARGET QUBITS

m EXPONENT QUBITS $\rightarrow$ VALUE $= k$

$k \in \{0, \ldots, 2^m - 1\}$

(1) SET TARGET TO $|1\rangle \rightarrow$ Superposition of $|\psi_k\rangle$

(2) APPLY HADAMARD TO EXPONENT

$$\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle$$

(3) APPLY MODULAR EXPONENTIATION:

$$\lambda_m(M_a)\,|k\rangle|\psi\rangle = |k\rangle(M_a^k|\psi\rangle)$$

$$\underbrace{\text{target} \times a^{\text{exponent}} \bmod N}_{|\psi\rangle}$$

$$M_a|\psi\rangle = a|\psi\rangle \bmod N$$

$$M_a^k|\psi\rangle = a^k|\psi\rangle \bmod N$$

$$\text{exponent} = \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle$$

$$\text{target} = |1\rangle \rightarrow \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |\psi_i\rangle$$

$$\lambda_m(M_a) \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle |\psi\rangle$$

$$= \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} |k\rangle \underbrace{(M_a^k |\psi\rangle)}_{\text{eigenvector}}$$

$$= \omega^k |\psi\rangle$$

$$= e^{2\pi i k\theta} |\psi\rangle$$

$$= \left(\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} e^{2\pi i k\theta} |k\rangle \right) \underbrace{|\psi\rangle}_{\text{target}}$$

Discard!

Exponent has θ.

④ Apply QFT^{+} to Exponent:

$$QFT_{2^m}^{+}|k\rangle = \frac{1}{2^{m/2}} \sum_{j=0}^{2^m-1} \omega^{-kj}|j\rangle$$

$$\omega = e^{2\pi i/2^m}$$

If θ is of the form $j/2^m$

$$QFT_{2^m}^{+}|\text{exponent}\rangle = QFT_{2^m}^{+}\left(\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} e^{2\pi i k j/2^m}|k\rangle\right)$$

$$= QFT_{2^m}^{+}\left(1/2^{m/2} \sum_{k=0}^{2^m-1} \omega^{kj}|k\rangle\right)$$

$$= \frac{1}{2^m} \sum_{k=0}^{2^m-1} \omega^{kj} \sum_{i=0}^{2^m-1} \omega^{-ki}|i\rangle$$

$$= \frac{1}{2^m} \sum_{i=0}^{2^m-1} \left(\sum_{k=0}^{2^m-1} \omega^{k(j-i)}\right)|i\rangle$$

↓

if $j \neq i$

$$\left(\omega^{(j-i)}\right)^k = \frac{1-\omega^{(j-i)2^m}}{1-\omega^{j-i}}$$

$$(\omega^{2^m})^{j-i}$$

$$= (e^{2\pi i/2^m \cdot 2^m})^{j-i}$$

$$= 1$$

So if $j \neq i$

$$\omega^{k(j-i)} = 0$$

else

$$\omega^{k(j-i)} = 1$$

$j = i$ AND $\sum_{k=0}^{2^m-1} \omega^{k(j-i)} = 2^m$

$$= \frac{1}{2^m} \cdot 2^m \cdot |j\rangle$$

$$= |j\rangle //$$

ALWAYS GET j AND DO

$\theta = j/2^m$ to get θ.

Then $\theta =$ (some value) $/_{2^n}$ → FIND n //

WHAT IF θ IS NOT IN THE FORM $j/2^m$

$$\omega = e^{2\pi i/2^m}$$

$$\omega^{2^m} = e^{2\pi i}$$

GENERIC:

$$QFT^{\dagger}_{2^m} \left(\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} e^{2\pi i k\theta} |k\rangle \right)$$

$$= QFT^{\dagger}_{2^m} \left(\frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} \omega^{k 2^m \theta} |k\rangle \right)$$

$$= \frac{1}{2^{m/2}} \sum_{k=0}^{2^m-1} \omega^{k 2^m \theta} \left(\frac{1}{2^{m/2}} \sum_{j=0}^{2^m-1} \omega^{-kj} |j\rangle \right)$$

$$= \frac{1}{2^m} \sum_{j=0}^{2^m-1} \left(\sum_{k=0}^{2^m-1} \omega^{k(2^m\theta - j)} \right) |j\rangle$$

SO, WE MEASURE j WITH PROBABILITY

$$P_j = \frac{1}{2^{2m}} \left| \sum_{k=0}^{2^m-1} \omega^{(2^m\theta - j)k} \right|^2$$

$$= \frac{1}{2^{2m}} \left| \frac{1 - \left(\omega^{(2^m\theta - j)}\right)^{2^m}}{1 - \omega^{(2^m\theta - j)}} \right|^2$$

LET US SEE WHAT IS THE PROBALITY TO FIND A θ THAT HAS A FORM CLOSE TO $j/2^m$

$$\theta = j/2^m + \varepsilon \pmod 1$$

$$|\varepsilon| \leq 1/2^{m+1} \quad]$$

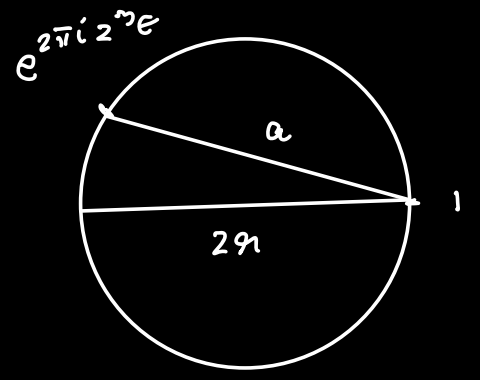
$$2^m\theta - j = 2^m\varepsilon$$

$$P'_j = \frac{1}{2^{2m}} \left| \frac{\left(\omega^{2^m\varepsilon}\right)^{2^m} - 1}{\omega^{2^m\varepsilon} - 1} \right|^2$$

$$= \frac{1}{2^{2m}} \frac{\left|\omega^{2^{2m}\varepsilon} - 1\right|^2}{\left|\omega^{2^m\varepsilon} - 1\right|^2}$$

$$= \frac{1}{2^{2m}} \frac{a^2}{b^2}$$

$$a = |\omega^{2^m G} - 1| = |e^{2\pi i 2^m \epsilon} - 1|$$



$$\frac{(\text{arc length})}{a} \leq \frac{\pi}{2}$$

$$\text{arc length} = \frac{\theta}{2\pi} \times (2\pi r) = \theta \times r = \theta$$
$$r = 1$$

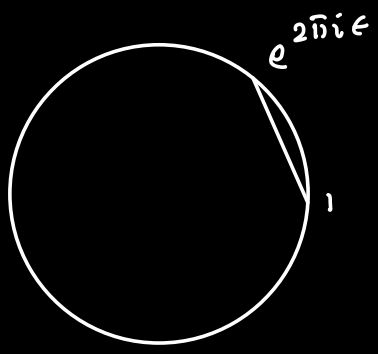
$e^{i\theta}$ $\qquad \theta = 2\pi 2^m \epsilon$

$$\frac{2\pi 2^m \epsilon}{a} \leq \frac{\pi}{2}$$

$$a \geq 4\epsilon 2^m$$

$$b = |\omega^{2m\epsilon} - 1|$$

$$= |e^{2\pi i \epsilon} - 1|$$



$\theta = 2\pi\epsilon$

chord $\leq$ arc length

$$b \leq 2\pi\epsilon$$

$$P_J = \frac{1}{2^{2m}} \frac{a^2}{b^2} \geq \frac{1}{2^{2m}} \frac{(4\epsilon 2^m)^2}{(2\pi\epsilon)^2}$$

$$\geq 4/\pi^2$$

$$\geq 0.4$$

FOR $\epsilon \geq \alpha/2^m$

$$P_J = 1/4\alpha^2$$

$$|\varepsilon| \leq 1/2^{m+1}$$

$$p_j \geq 4/\pi^2 \quad (10.4)$$

$$\frac{\alpha}{2^m} \leq |\varepsilon| < 1/2$$

$$p_j \leq \frac{1}{4\alpha^2}$$

QFT NUMBER OF GATES:

$$g(m) = \frac{1}{2} m(m+1) \qquad O(m^2)$$

$$g(m+1) = g(m) + m + 1$$

$$g(1) = 1$$

QAOA:

Max 2SAT:

n variables

m clauses

INPUT: t, $\bigwedge_{j=1}^{m} (l_{j_1} \vee l_{j_2})$

eg: $n = 7$, $m = 9$

$t = 8$ AND $(x_1 \vee x_1) \wedge (x_2 \vee \neg x_5) \wedge (\neg x_3 \vee \neg x_4) \wedge \dots$

$(x_4 \vee x_6)$.

OUTPUT: $z \in \{0,1\}^n$

DEFINE:

$$\text{Count}_j(z) = \begin{cases} 1 & \text{if } z \text{ satisfies } j^{TH} \text{ clause} \\ 0 & \text{otherwise} \end{cases}$$

$$\text{Count}(z) = \sum_{j=1}^{m} \text{Count}_j(z)$$

$$C_j|z\rangle = \text{Count}_j(z)\,|z\rangle$$

$$C|z\rangle = \sum_{j=1}^{2^n} c_j |z\rangle$$

So C helps to "mark the good ones".

$$B = \sum_{k=0}^{n-1} NOT_k = NOT \otimes I^{\otimes n-1} + I \otimes NOT \otimes I^{\otimes(n-2)} + \dots + I^{\otimes n-1} \otimes NOT$$

Apply NOT to each qubit.

SEPARATOR MATRIX

$$Sep(\gamma) = e^{-i\gamma C}$$

$$\gamma \in [0, 2\pi]$$

MIXER MATRIX

$$Mix(\beta) = e^{-i\beta B}$$

$$\beta \in [0, \pi]$$

for different choices of $(\gamma, \beta) \in [0, 2\pi] \times [0, \pi]$

{

measure $Mix(\beta)\, Sep(\gamma)\, H^{\otimes n} |0^n\rangle$

}

pick the measurement z that maximizes $Cost(z)$.

$$\mathrm{Sep}(\gamma) \sum_{z \in \{0,1\}^n} a_z |z\rangle = e^{-i\gamma C} \sum_{z \in \{0,1\}^n} a_z |z\rangle$$

$$= \sum_{z \in \{0,1\}^n} a_z \, e^{-i\gamma C} |z\rangle$$

$$= \sum_{z \in \{0,1\}^n} a_z \underbrace{(e^{-i\gamma})^{\mathrm{count}(z)}} |z\rangle$$

So $e^{-i\gamma}$ factor for each clause z satisfies.

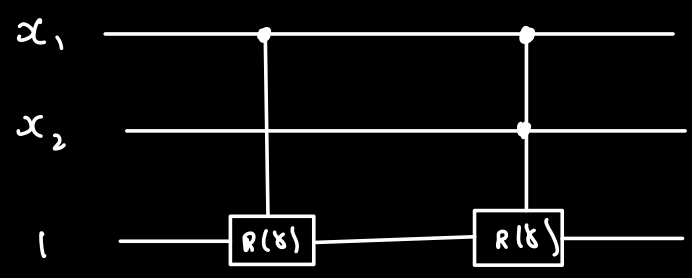
eg: $x_0 \wedge (x_0 \wedge x_1)$

$$\mathrm{Sep}(\gamma)\,(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle)$$

	↓	↓	↓	↓
count →	None	None	1	2

$$a_{00}|00\rangle + a_{01}|01\rangle + (e^{-i\gamma})\, a_{10}|10\rangle + (e^{-i\gamma})^2 a_{11}|11\rangle.$$

$$R(\gamma) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\gamma} \end{pmatrix}$$



$$Mix(\beta) = (\otimes n)\, R_x(2\beta) \qquad R_x(2\beta) = \begin{bmatrix} \cos\beta & -i\sin\beta \\ -i\sin\beta & \cos\beta \end{bmatrix}$$

$$\gamma = \pi/4$$

$$e^{-i\gamma} = \cos\gamma - i\sin\gamma = 1/\sqrt{2} - i/\sqrt{2}$$

$$\beta = \pi/4$$

$$R_x(\pi/2) = \begin{bmatrix} 1/\sqrt{2} & -i/\sqrt{2} \\ -i/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} = \frac{1}{\sqrt{2}}(I - i\,NOT)$$

$$NOT \rightarrow \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$x_0 \wedge (x_0 \wedge x_1)$

$\mathrm{Mix}(\beta)\ \mathrm{Sep}(\delta)\ \underbrace{H^{\otimes 2}\ |00\rangle}$

$\downarrow$

$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

$\frac{1}{2}|00\rangle + |01\rangle + (1/\sqrt{2} - i/\sqrt{2})|10\rangle + \underbrace{(1/\sqrt{2} - i/\sqrt{2})^2}_{(\frac{1}{2} - \frac{1}{2} - i)}|11\rangle)$

$\frac{1}{2}(|00\rangle + |01\rangle + (1/\sqrt{2} - i/\sqrt{2})|10\rangle - i|11\rangle)$

$\downarrow$

$(\frac{1}{\sqrt{2}}(I - i\,\mathrm{NOT}) \otimes \frac{1}{\sqrt{2}}(I - i\,\mathrm{NOT}))\ \frac{1}{2}(|00\rangle + |01\rangle + (1/\sqrt{2} - i/\sqrt{2})|10\rangle - i|11\rangle)$

$\frac{1}{4}[(|0\rangle - i|1\rangle) \otimes (|0\rangle - i|1\rangle) +$

$(|0\rangle - i|1\rangle) \otimes (|1\rangle - i|0\rangle) +$

$(1/\sqrt{2} - i/\sqrt{2})[(|1\rangle - i|0\rangle) \otimes (|0\rangle - i|1\rangle)] -$

$$i\left[\left(|1\rangle - i|0\rangle\right)\otimes\left(|1\rangle - i|0\rangle\right)\right]$$

$$\tfrac{1}{4}\Big[\left(|00\rangle - i|01\rangle - i|10\rangle - |11\rangle\right) +$$

$$\left(|01\rangle - i|00\rangle - i|11\rangle - |10\rangle\right) +$$

$$\left(1/\sqrt{2} - i/\sqrt{2}\right)\left(|10\rangle - i|11\rangle - i|00\rangle - |01\rangle\right) -$$

$$i\left(|11\rangle - i|10\rangle - i|01\rangle - |00\rangle\right)\Big]$$

$$\tfrac{1}{4}\Big[\left(1 - i - 1/\sqrt{2}\,i - 1/\sqrt{2} + i\right)|00\rangle +$$

$$\left(-i + 1 - 1/\sqrt{2} + i/\sqrt{2} - 1\right)|01\rangle +$$

$$\left(-i - 1 + 1/\sqrt{2} - i/\sqrt{2} - 1\right)|10\rangle +$$

$$\left(-1 - i - i/\sqrt{2} - 1/\sqrt{2} - i\right)|11\rangle\Big]$$

$$\frac{1}{4}\Big[\Big(1-\tfrac{1}{\sqrt{2}}-\tfrac{1}{\sqrt{2}}i\Big)|00\rangle+$$

$$\Big(-\tfrac{1}{\sqrt{2}}-i+\tfrac{i}{\sqrt{2}}\Big)|01\rangle+$$

$$\Big(-2-i+\tfrac{1}{\sqrt{2}}-\tfrac{i}{\sqrt{2}}\Big)|10\rangle+$$

$$\Big(-1-\tfrac{1}{\sqrt{2}}-2i-\tfrac{i}{\sqrt{2}}\Big)|11\rangle\Big]$$

$$P(00) = \frac{1}{16}\times\left|\left(1-\tfrac{1}{\sqrt{2}}\right)-\left(\tfrac{1}{\sqrt{2}}\right)i\right|^2$$

$$= \frac{1}{16}\times\left[\left(1-\tfrac{1}{\sqrt{2}}\right)^2+\tfrac{1}{2}\right]$$

$$= \frac{1+\frac{1}{2}-\sqrt{2}+\frac{1}{2}}{16}$$

$$= \frac{2-\sqrt{2}}{16} = 3.7\%$$

$P(01) = 3.7\%$

$P(10) = 28.6\%$

$P(11) = 67\%$

Classical Errors:

Redundancy:

$[n, k]$ code

convert k bits to n. $k < n$.

G $(n \times k)$

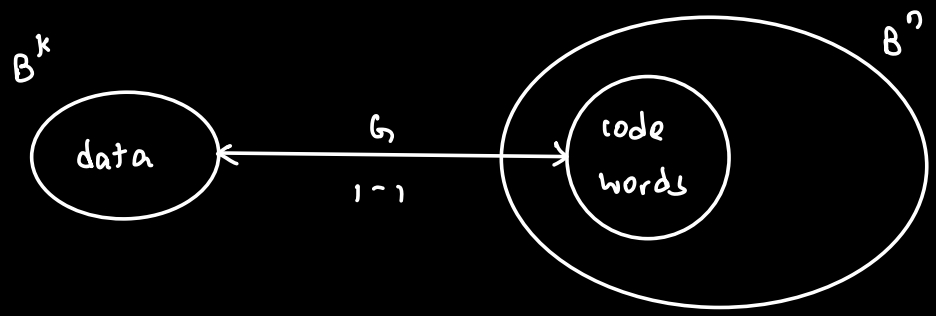
$$3 \left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \right. \qquad n = 3, \quad k = 1$$

$$G|0\rangle = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

All zeroes $\longrightarrow$ All zeroes

$$G|1\rangle = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$$

Detection:



$G(B^k)$ → Code Space

↓

Span of the columns of G.

Parity Check Matrix:

P → Rows span $B^n - G(B^k)$

$(n-k)$ Dimensional subspace.

↓

$(n-k) \times n$

$n = 3$

$k = 1$

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

$PG = 0$

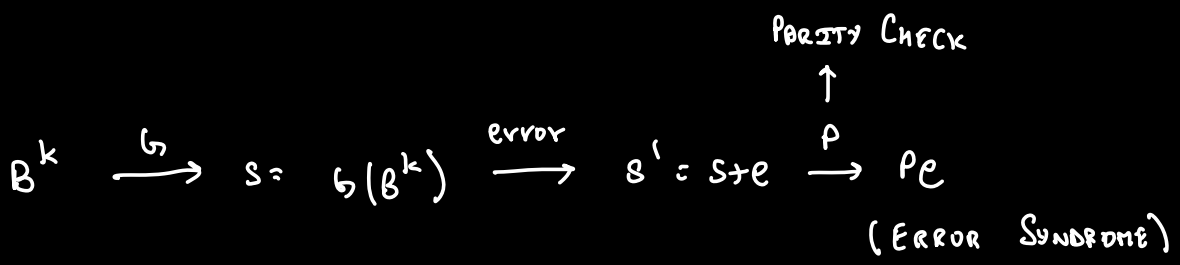
$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

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

B^k : B^1 $\{0,1\}$

$G(B^1) = \{000, 111\} \longrightarrow P_S = 0$

B^n : $\{000, 010, 011, 100, 101, 110, 111\} \rightarrow P_S \neq 0.$



$P_{S'} = P(s+e) = P_S + P_e = P_e$

$S = 000$

$S' \in \{100, 010, 001\}$

$$P_{S_1'} = P_{e_1} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$P_{S_2'} = P_{e_2} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

$$P_{S_3'} = P_{e_3} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Each row does a parity check!
(of P)

Use Q to detect the errors.

if Pe is unique

$$Q(Pe) = e$$

$$Q\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \qquad Q\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

$$Q\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

CORRECTION:

$$\text{received} + \text{fix} = s' + Q(Ps') = s' + Q(Pe)$$

$$= s' + e$$

$$= s \;//$$

PARITY CHECK ($P_3 = 0$ NO ERROR)

REDUNDANCY

$B^k \xrightarrow{G} S = G(B^k) \xrightarrow{\text{error}} S' = S + e \xrightarrow{P} Pe$

(ERROR SYNDROME)

[If every error has nonzero error syndrome → ERROR DETECTION]

$\downarrow Q$

e (UNIQUE)

$\downarrow + S'$

S

[If every error → unique syndrome → ERROR CORRECTION]

HAMMING DISTANCE:

$$d(s,t) = \underbrace{w(s-t)}_{\text{bit difference between } s,t.}$$

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

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

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

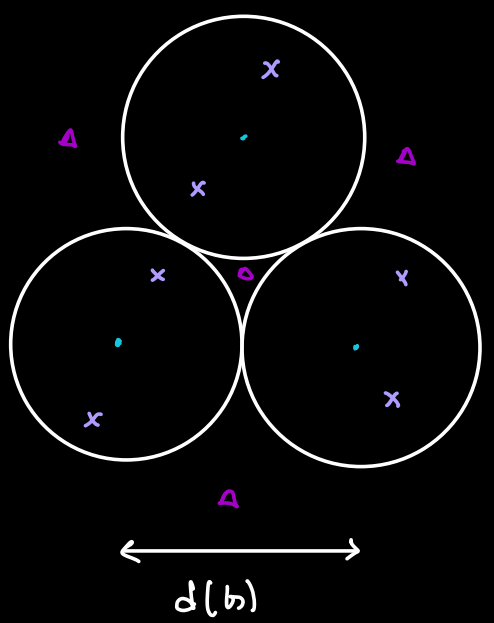
$G(B^k)$ closed under vector addition

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

$d(G) = 3.$

G creates $[n, k, d(G)]$ code

$[3, 1, 3]$



- Code Words
- x Can be corrected (closest code word)
- Δ Detected

if $d(b)$ bit flips, one code word becomes another → No DETECTION

Detected upto $d(b) - 1$.
Corrected upto $n = \frac{d(b) - 1}{2}$.

$w(e) \leq n$ corrected

$[3, 1, 3]$ $d(b) = 3$

$n = 1$

Single bit flip corrected.

2 bit flips detected.

P(error after G) < P(error if you send 1)

↓

2 or 3 errors (1 can be corrected)

$p \rightarrow$ error probability

$$^3C_2 \times p^2 \times (1-p) + p^3 < p$$

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

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

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

$$2p^2 - 2p - p + 1 > 0$$

$$2p(p-1) - (p-1) > 0$$

$$(2p-1)(p-1) > 0$$

$$2p - 1 < 0$$

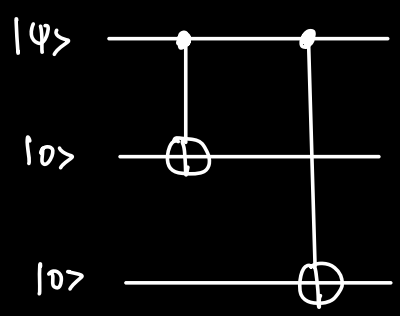
$$p < 1/2$$

Quantum Error Correction:

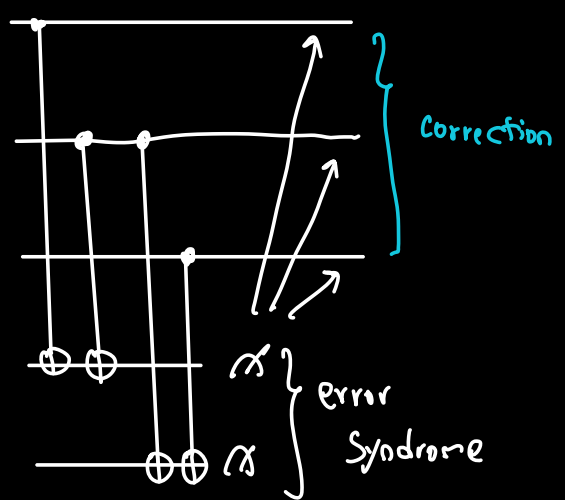
Redundancy → Parity Check → Error Syndrome → Correction

(Encode)

Encode



Parity Check



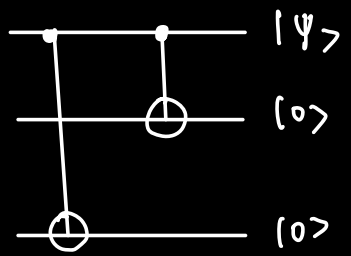
00 → nothing

10 → flip 1st

11 → flip 2nd

01 → flip 3rd

Decode (Reset additional qubits)



Shor Code:

$P(\text{2 error in Shor}) < P(\text{1 error})$

↓

9 qubits

$${}^{9}C_{2} \times p^2 \times (1-p)^7 < p$$

$$\approx \quad 36p^2 < p$$

$$p < 1/36.$$

1 more Shor Code

$$p' = 36p^2$$

$$36p'^2$$

$$36(36p^2)^2 \quad \rightarrow 81 \text{ qubits}$$

Threshold prob(error) $< 1/36$ here

SWAPPINGS:

$\Psi : [0 \to 0, 1 \to 1, 2 \to 2]$

$M : (0,1) \to 1$

$(0,2) \to 2$

$(1,2) \to 3$

1 — 0

|

2

$Sd(0,1) = 1$

$Sd(0,2) = 2$

$Sd(1,2) = 1$

$M(0,1) \times 2(1-1) + M(0,2) \times 2(2-1) + M(1,2) \times 2(1-1)$

$: 2 \times 2 = 4 //$

u $|0\rangle$ $\quad$ v $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$$

$\langle u|v\rangle$ $\quad$ $|u\rangle^{\dagger}|v\rangle$

$$\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = 1/\sqrt{2}$$