QIP1 Quantum Information Processing:Concept

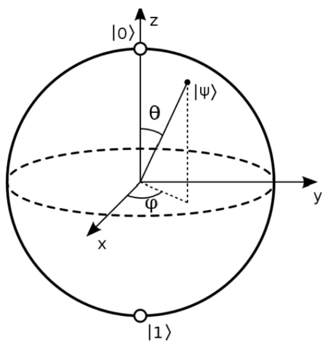
professor : Jonathan Home
author : walkerchi

Quantum State

- **unitary** : $S^\dagger S = SS^\dagger = I$
- **Hermitian** : $S^\dagger = S$
- **projector** : $SS = S$
- $\otimes$: tensor product

Bloch Sphere

$$\begin{aligned} |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \qquad\qquad \|\alpha\|^2 + \|\beta\|^2 = 1 \\ &= \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle \\ &= \cos(\theta/2)|0\rangle + (\cos\phi + i\,\sin\phi)\sin(\theta/2)|1\rangle \end{aligned}$$



- z axis : $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \quad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$
- x axis : $|+\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} \quad |-\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$
- y axis : $|+\rangle_y = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix} \quad |-\rangle_y = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}$

  pauli matrices : $\hat{\sigma}_x = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} \quad \hat{\sigma}_y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix} \quad \hat{\sigma}_z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$

No-cloning theorem

$$\nexists \hat{U}\ \forall \psi, \phi \quad U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle \quad U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$$

Entanglement

$$|\Psi\rangle_{AB} \neq |\alpha\rangle_A \otimes |\beta\rangle_B$$

- **Bell states** : maximally entangled states for two qubits

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

- **identify entanglement** : more than 1 non-zero eigen values $\exists \lambda_1, \lambda_2 \neq 0$
- **product state** : $|\Psi\rangle_{AB} = |\alpha\rangle_A \otimes |\beta\rangle_B$ no entanglement
- **Schmidt decomposition** :
  $|\Psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \to |\Psi\rangle = \sum_{i=1}^{m} \lambda_i |u_i\rangle \otimes |v_i\rangle \quad |u_i\rangle \in \mathcal{H}_1, |v_i\rangle \in \mathcal{H}_2$
  - *Schmidt rank* : m
    - independent from the choice of basis of $\mathcal{H}_A$ and $\mathcal{H}_B$
  - *Schmidt coefficient* : α_i

> Example
>
> $\Psi = \frac{|00\rangle+|11\rangle+2|++\rangle}{\sqrt{10}} = \frac{3|00\rangle+2|01\rangle+2|10\rangle+3|11\rangle}{\sqrt{10}}$
>
> schmidt rank : 4
>
> schmidt coefficient : $\frac{1}{\sqrt{10}}[3, 2, 2, 3]$

Bell Inequality

	location A	location B	
CHSH inequatlity	$Q = \pm 1 \quad R = \pm 1$	$S = \pm 1 \quad T = \pm 1$	$\langle QS\rangle + \langle RT\rangle + \langle RS\rangle - \langle QT\rangle \leq 2$
Quantum Violation	$\hat{Q} = \hat{\sigma}_z \otimes I$ $\hat{R} = \hat{\sigma}_x \otimes I$	$\hat{S} = \frac{-1}{\sqrt{2}} \hat{I} \otimes (\hat{\sigma}_z + \hat{\sigma}_x)$ $\hat{T} = \frac{1}{\sqrt{2}} \hat{I} \otimes (\hat{\sigma}_z - \hat{\sigma}_x)$	$\langle QS\rangle + \langle RT\rangle + \langle RS\rangle - \langle QT\rangle = 2\sqrt{2} > 2$

Quantum Gate

Rotation

- $R_x(\theta) = e^{-i\theta X/2} = \cos(\theta/2)I - i\ sin(\theta/2)X = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$
- $R_y(\theta) \quad = e^{-i\theta Y/2} = \cos(\theta/2)I - i\ sin(\theta/2)Y = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$

- $R_z(\theta) \quad = e^{-i\theta Z/2} = \cos(\theta/2)I - i\ sin(\theta/2)Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$

Pauli Gates

$\sigma_{\{x,y,z\}}$ rotate around $\{x, y, z\}$ axis by π in Bloch sphere

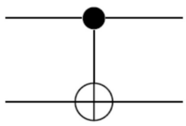
Hadamard Gate

H rotation about axis $\frac{1}{\sqrt{2}}(\hat{x} + \hat{z})$ by π

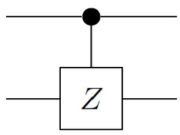
- $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$
- $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$
- $H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$
- $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$

Two qubits Gate

- $\mathrm{CNOT} = |0\rangle_c \langle 0|_c \otimes \hat{I}_t + |1\rangle_c \langle 1|_c \otimes \hat{X}_t$



- $\mathrm{CPAHSE} = |0\rangle_c \langle 0|_c \otimes \hat{I}_t + |1\rangle_c \langle 1|_c \otimes \hat{Z}_t$



Matrix Table

Operator	Matrix	Operator	Matrix	Operator	Matrix
Pauli-x (σ_x)	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	Pauli-Y (σ_y)	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	Pauli-Z (σ_z)	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	Identity (I)	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$		
Phase (S,P)	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$	$\frac{\pi}{8}$ (T, not Clifford gate)	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$		
Controlled Not ($CNOT$, CX)	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	Controlled Z ($CZ, CSIGN, CPHASE$)	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$	SWAP	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Universal quantum gates

- Rotation gates $R_x(\theta)$, $R_y(\theta)$, $R_z(\theta)$, phase gate $P(\phi)$, CNOT
- $\{\mathrm{CNOT}, H, T\}$
- $\{\mathrm{CNOT}\} \cup \mathcal{U}(2)$

- $\{\text{Toffoli}(\text{CCNOT}), H\}$

Clifford group : $\mathcal{C}_n = \left\{U \in \mathcal{U}(2^n) : \forall P \in \mathcal{P}_n : UPU^\dagger \in \mathcal{P}_n\right\}$ where $\mathcal{U}$ means unitary

---

Algorithms

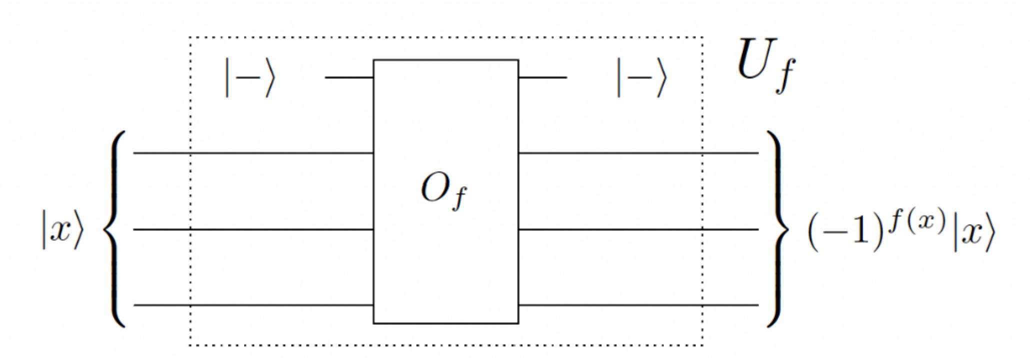
Complexity

complexity class	problem	polynomial in time/space	classical / quantum
P	decision problem	time	classical
BPP	probabilistic algorithm failure at most $\frac{1}{3}$	time	classical
NP	proof the answer is yes	time	classical
PSPACE	decision problem	space	classical
BQP	decision problem failure at most $\frac{1}{3}$	time	quantum

- $\text{BPP} \subset \text{BQP}$: quantum simulation of classical circuits
- $\text{P} \subset \text{BPP}$
- $\text{P} \subset \text{NP} \subset \text{PSAPCE}$

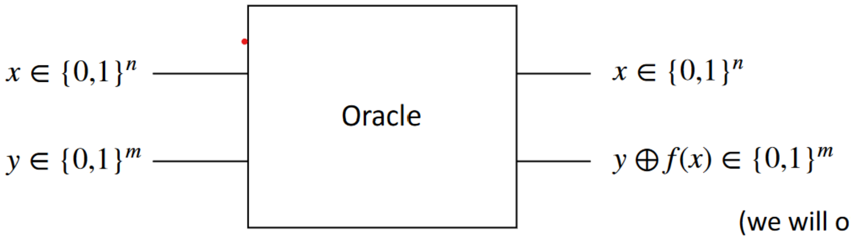
Oracle

- Phase oracle : $U_f\left|x\right\rangle = (-1)^{f(x)}\left|x\right\rangle$

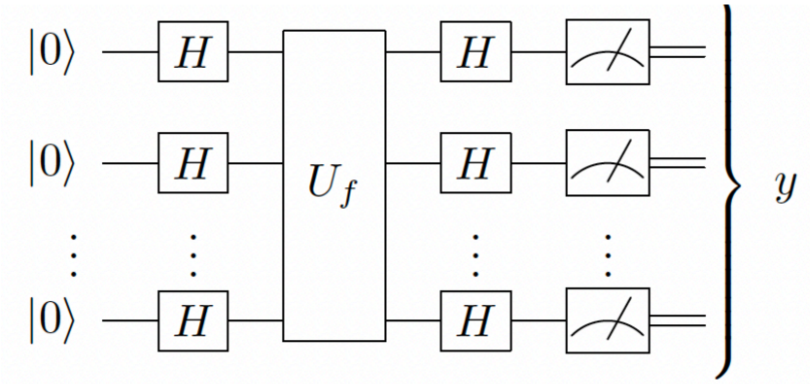


$$
\begin{aligned}
O_f\left|y\right\rangle\left|x\right\rangle &= \left|y \oplus f(x)\right\rangle\left|x\right\rangle \\
O_f\left|-\right\rangle\left|x\right\rangle &= O_f\frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)\left|x\right\rangle \\
&= \frac{1}{\sqrt{2}}(\left|f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle)\left|x\right\rangle \\
&= (-1)^{f(x)}\left|-\right\rangle\left|x\right\rangle
\end{aligned}
$$

- Bit oracle : $O_f\left|y\right\rangle\left|x\right\rangle = \left|y \oplus f(x)\right\rangle\left|x\right\rangle$



Deutsch-Josza



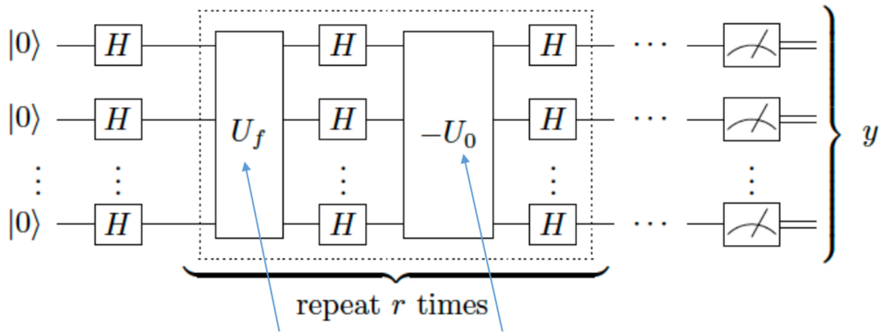
Distinguish $f(x)$ whether is **constant** function or **balanced** function. $\mathcal{O}(N) \to \mathcal{O}(1)$

- **constant**: evaluates to the same value regardless of input
- **balanced**: the number of inputs which output 1 equals the number of inputs which output 0

$$
\begin{aligned}
\langle 0|^{\otimes n} H^{\otimes n} U_f H^{\otimes n} |0\rangle^{\otimes n} &= \langle 0|^{\otimes n} H^{\otimes n} U_f \underbrace{\left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \right)}_{H^{\otimes n}|0\rangle^{\otimes n}} \\
&= \langle 0|^{\otimes n} H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right) \\
&= \langle 0|^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \right) \\
&= \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} (-1)^{f(x)} (-1)^{x \cdot y} \langle 0^{\otimes n} | y \rangle \\
&= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \\
&= \begin{cases} 0 & f(x) \text{ is balanced} \\ \pm 1 & f(x) \text{ is constant} \end{cases}
\end{aligned}
$$

> Notation :
>
> 1. n : length of bit string
> 2. N : total number of quantum state $N = 2^n$
> 3. H : Hadamard gate

Grover



find the unique x_0 that $f(x_0) = 1$ $\quad f:\{1,\cdots,N\} \to \{0,1\}$, $O(N) \to O(\sqrt{N})$

- **oracle operator** : $U_f = I - 2\left|x_0\right\rangle\left\langle x_0\right| \quad U_0 = I - 2\left|0\right\rangle^{\otimes n}\left\langle 0\right|^{\otimes n}$
- **grover diffusion** : $U_s = H^{\otimes n}(-U_0)H^{\otimes n} = 2\left|+^n\right\rangle\left\langle +^n\right| - I$

Reflection

- Reflection about $\left|\psi_\perp\right\rangle$: $R_{\psi_\perp}\left|\phi\right\rangle = (I - 2\left|\psi\right\rangle\left\langle\psi\right|)\,(\alpha\left|\psi\right\rangle + \beta\left|\psi_\perp\right\rangle) = -\alpha\left|\psi\right\rangle + \beta\left|\psi_\perp\right\rangle$
  - $U_f = R_{x_0^\perp}$ reflect about $\left|x_0^\perp\right\rangle$
- Reflection about $\left|\psi\right\rangle$: $R_\psi\left|\phi\right\rangle = (2\left|\psi\right\rangle\left\langle\psi\right| - I)\,(\alpha\left|\psi\right\rangle + \beta\left|\psi_\perp\right\rangle) = \alpha\left|\psi\right\rangle - \beta\left|\psi_\perp\right\rangle$
  - $U_s = R_+$: reflection about $\left|+^n\right\rangle$

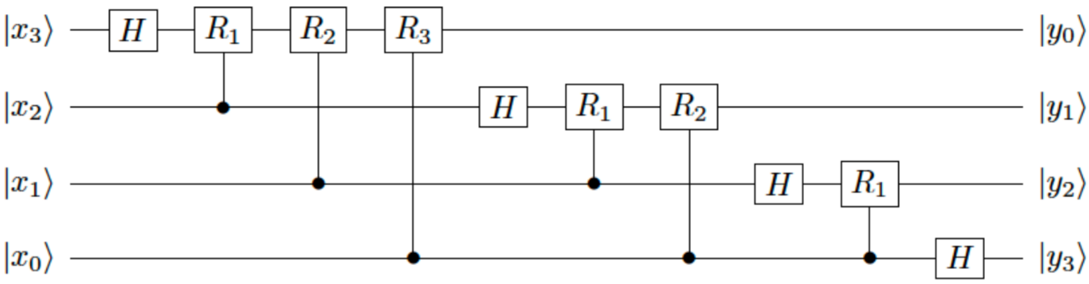
$$\begin{aligned}\left\langle x_0\right|U_sU_f\left|\phi\right\rangle &= \cos\left(\arccos(\langle x_0|\phi\rangle) - 2\mathrm{arcsin}(\langle x_0|+\rangle)\right)\\ \left\langle x_0\right|(U_sU_f)^r\left|+^n\right\rangle &= \cos(\arccos(\langle x_0|+\rangle) - 2r\arcsin(\langle x_0|+\rangle))\end{aligned}$$

$$\Rightarrow r = \frac{\arccos(\frac{1}{\sqrt{N}})}{2\arcsin(\frac{1}{\sqrt{N}})} \approx \frac{\pi\sqrt{N}}{4}$$

> Algorithm
>
> 1. $\left|\Psi\right\rangle \leftarrow H^{\otimes n}\left|0\right\rangle^{\otimes n}$: after this step $\left|\Psi\right\rangle = \left|+^n\right\rangle$
> 2. for r times, $r = \frac{\mathrm{artcos}(\frac{1}{\sqrt{N}})}{2\mathrm{arcsin}(\frac{1}{\sqrt{N}})}$
>   1. $\left|\Psi\right\rangle \leftarrow U_sU_f\left|\Psi\right\rangle$
> 3. measure $\left|\Psi\right\rangle$, the greatest probability will be x_0

> Notation
>
> - n : length of bit string
> - N : total number of quantum state $N = 2^n$
> - $\left|+^n\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=\{0,1\}^n}\left|x\right\rangle = \frac{1}{\sqrt{N}}\sum_{x=\{0,1\}^n}\left|x\right\rangle$

[QFT] Quantum Fourier transform



$$Q_N\left|x\right\rangle = \tfrac{1}{\sqrt{N}}\sum_{y=0}^{N-1} e^{2\pi ixy/N}\left|y\right\rangle : \mathcal{O}(N\log N) \rightarrow \mathcal{O}(n^2)$$

$$\begin{aligned}
Q_N\left|x\right\rangle &= \frac{1}{\sqrt{N}}\sum_{y\in\{0,1\}^n} e^{2\pi ixy/N}\left|y\right\rangle \\
&= \frac{1}{\sqrt{N}}\sum_{y\in\{0,1\}^n} \underbrace{e^{2\pi ix\sum_k^n 2^k y_k/N}\left|y_{n-1}\right\rangle\cdots\left|y_0\right\rangle}_{\text{single bits of } e^{2\pi ixy/N}} \\
&= \frac{1}{\sqrt{N}}\otimes_{j=1}^{n}\left(\sum_{y_{n-j}\in\{0,1\}} e^{2\pi ixy_{n-j}/2^j}\left|y_{n-j}\right\rangle\right) \\
&= \frac{1}{\sqrt{N}}(\left|0_{n-1}\right\rangle + e^{.x_0 2\pi i}\left|1_{n-1}\right\rangle)\otimes(\left|0_{n-2}\right\rangle + e^{.x_1x_0 2\pi i}\left|1_{n-2}\right\rangle)\cdots(\left|0_0\right\rangle + e^{.x_{n-1}\cdots x_0 2\pi i}\left|1_0\right\rangle) \\
&= \frac{1}{\sqrt{N}}(H\left|x_0\right\rangle)\otimes(R_1H\left|x_1\right\rangle)\ldots(R_{n-1}\ldots R_1H\left|x_{n-1}\right\rangle)
\end{aligned}$$

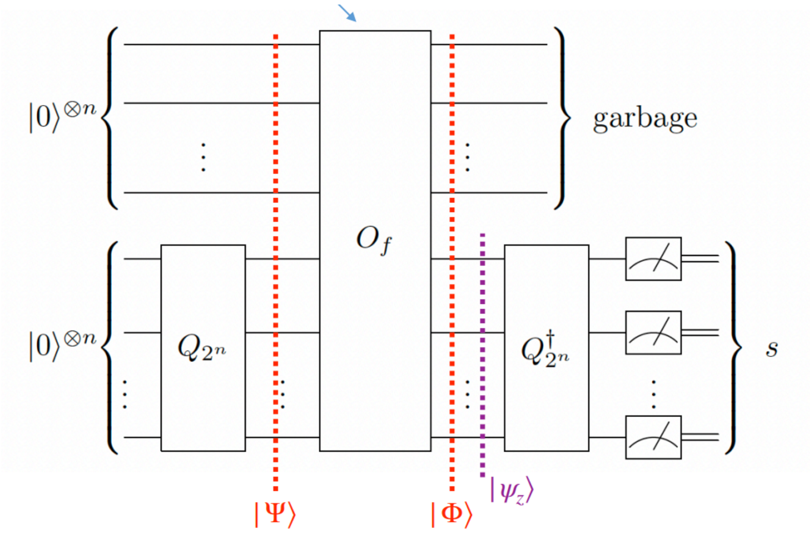
Number of gates in QFT of n bit string

- CR_j (Controled-R_j) : $\frac{n(n-1)}{2}$
- SWAP : $\frac{n}{2}$ used to reverse the qubit, $\left|y_0y_1y_2y_3\right\rangle \rightarrow \left|y_3y_2y_1y_0\right\rangle$
- $H : n$

> Notation
>
> - n : length of bit string
> - N : total number of quantum state $N = 2^n$
> - R_d : rotation matrix : $R_d = \begin{bmatrix} 1 & 0 \\ 0 & e^{\pi i/2^d} \end{bmatrix}$
> - H : Hadamard gate : $H = \dfrac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $H\left|x_k\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + e^{.x_k 2\pi i}\left|1\right\rangle)$
> - $e^{.x_1x_0} : e^{\frac{1}{2}x_1 + \frac{1}{4}x_0}$

> Example
>
> $$Q_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = H \quad Q_3 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & e^{2\pi i/3} & e^{-2\pi i/3} \\ 1 & e^{-2\pi i/3} & e^{2\pi i/3} \end{bmatrix} \quad Q_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

Shor factoring



given a non-prime integer N represented as a bit string, find a non-trivial factor $a^x \text{mod } N$, $a^r \text{mod} N = 1 \rightarrow (a^{r/2}+1)(a^{r/2}-1)\text{mod} N = 0$

$$
\begin{aligned}
|\Phi\rangle &= O_f(\text{id}^{\otimes n} \otimes H^{\otimes n})|0\rangle^{\otimes n}|0\rangle^{\otimes n} \\
&= O_f \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |0\rangle^{\otimes n} |x\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |f(x)\rangle |x\rangle
\end{aligned}
$$

$$
|\Psi_z\rangle = \sqrt{\frac{r}{N}} \sum_{t=0}^{N/r-1} |x_0 + rt\rangle \quad \propto \sum_{x: f(x)=z} |x\rangle
$$

$$
\begin{aligned}
\left|\tilde{\Psi}_z\right\rangle &= Q^\dagger_N |\Psi_z\rangle \\
&= \sqrt{\frac{r}{N^2}} \sum_{t=0}^{N/r-1} \sum_{y=0}^{N-1} e^{-2\pi i(x_0+rt)y/N} |y\rangle \\
&= \sqrt{\frac{r}{N^2}} \sum_{y=0, ry \text{mod}=0}^{N-1} e^{-2\pi i x_0 y/N} \frac{N}{r} |y\rangle \\
&= \frac{1}{\sqrt{r}} \sum_{y=0, ry \text{mod}=0}^{N-1} e^{-2\pi i x_0 y/N} |y\rangle
\end{aligned}
$$

> Algorithm
>
> 1. find the order r that $a^x \bmod N = a^{x+r} \bmod N$ using **period finding** in $\mathcal{O}(\text{poly}(n))$
>   1. $|\Psi\rangle = I^{\otimes n} \otimes H^{\otimes n} |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n} = |0\rangle^{\otimes n} \otimes \left(\frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}} |x\rangle \right)$
>   2. $|\Phi\rangle = O_f |\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}} |f(x)\rangle |x\rangle$
>   3. measure $f(x) = z$ then $|\Psi_z\rangle = \sqrt{\frac{r}{N}} \sum_{t=0}^{N/r-1} |x_0 + rt\rangle \quad \propto \sum_{x:f(x)=z} |x\rangle$
>   4. $|\tilde{\Phi}\rangle = Q^\dagger_N |\Psi\rangle_z = \sqrt{\frac{r}{N^2}} \sum_{t=0}^{N/r-1} \sum_{y=0}^{N-1} e^{-2\pi i(x_0+rt)y/N} |y\rangle = \frac{1}{\sqrt{r}} \sum_{y=0, ry\text{mod}N=0}^{N-1} e^{-2\pi i x_0 y/N} |y\rangle$

>   5. measure $|\tilde{\Phi}\rangle$ multiple times $s_1, \cdots, s_i$, the results are multiples of r, use **euclid algorithm** to compute the $r = N/\gcd(s_1, \cdots, s_i)$
> 2. if $r \bmod 2 = 0$ and $a^{r/2} \pm 1 \bmod N \neq 0$
>   1. candidate factor $\tilde{p} = \gcd(a^{r/2} - 1, N)$ using **euclid algorithm**
> 3. else go to 1

```
@classical
def euclid_gcd(a, b):
    # O(logn)
    return b if a==0 else euclid_gcd(b%a, a)
@quantum
def period_finding(a, n, N):
    # a^r mod N = 1, O(N)
    Of = lambda x: a**x % N
    s0, s1 = None, None
    while True:
        x0, x1 = zeros(n), zeros(n)
        x0, x1 = I(x0), H(x1)
        x0, x1 = Of(x0, x1)
        if not measure(x0).all_equals(): # O(2^n/n) = O(N/n) fail
            continue
        x1 = IQFT(x1)
        if s0 is None:  # fail O(1)
            s0 = measure(x1)
            continue
        s1 = measure(x1)
        N_r= euclid_gcd(s0, s1) # N/r if k coprime k'
        s0, s1 = None, None
        r = N / N_r
        break

    return r

def shor_factoring(N):
    # find a factor of N
    n = ceil(log2(N))

    while True:
        a = random(N)
        K = euclid_gcd(a, N):
        if K != 1:
            return K

        r = period_finding(a, n, N)
        if is_odd(r): continue
        g = eulid_gcd(N, a**(r//2 + 1))
        if g != 1:
            return g
```

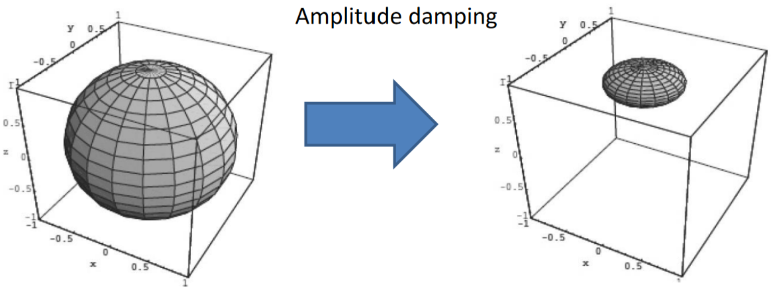
Error Correction

Quantum operations

- **Density operator** : $\hat{\rho} = \sum_{i,j} \rho_{i,j} \left| i \right\rangle \left\langle j \right|$
  - diagonal gives the probability of the state
- **Partial trace** : $\mathrm{Tr}_B(\left| a_1 \right\rangle \left\langle a_2 \right| \otimes \left| b_1 \right\rangle \left\langle b_2 \right|) = \left| a_1 \right\rangle \left\langle a_2 \right| \mathrm{Tr}(\left| b_1 \right\rangle \left\langle b_2 \right|)$
- **Purification** : $\rho^A = \mathrm{Tr}_R(\left| AR \right\rangle \left\langle AR \right|)$
- **Evolution** : $\rho_t = U \rho_0 U^\dagger$
- **Trace Preserving CP map** : $\rho(t) = \tau_A(\rho_A(0))$
  - trace preserving : $\mathrm{Tr}(\rho) = 1$
  - positive : $\lambda_\rho \geq 0$
  - complete positivity
- **Kraus Operator** : $\rho' = \sum_i \hat{E}_i \rho_0 \hat{E}_i^\dagger \quad \hat{E}_i = \left\langle e_i \right| \hat{U} \left| e_0 \right\rangle$

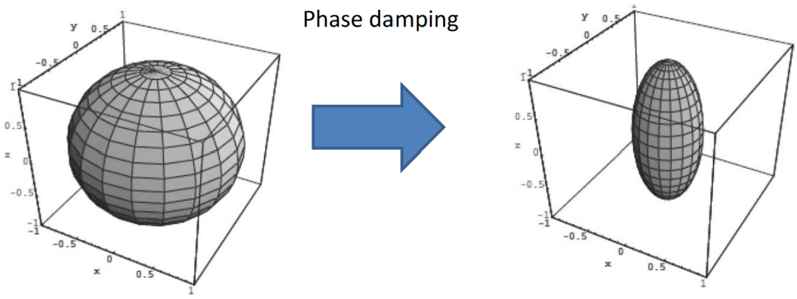
Damping channel

- **Amplitude Dampling** : $\hat{E}_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \quad \hat{E}_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix}$



  - excited state $\left| 1 \right\rangle$ damping to $\left| 0 \right\rangle$ due to loss of energy

- **Phase Damping** : $\hat{E}_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{r} \end{bmatrix} \quad \hat{E}_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-r} \end{bmatrix}$



  - lossing phase information, energy conserved

Error Channels

- **Bit Flip** : $\hat{E}_1 = \sqrt{p} X \quad E_0 = \sqrt{1-p} I$
- **Phase Flip** : $\hat{E}_1 = \sqrt{p} Z \quad E_0 = \sqrt{1-p} I$
- **Phase+Bit Flip** : $\hat{E}_1 = \sqrt{p} Y \quad \hat{E}_0 = \sqrt{1-p} I$

- **Depolarizing(Bit/Phase/Bit+Phase Flip)** :
  $\hat{E}_1 = \frac{p}{4}X \quad \hat{E}_2 = \frac{p}{4}Y \quad \hat{E}_3 = \frac{p}{4}Z \quad \hat{E}_0 = \left(1 - \frac{3p}{4}\right)I$
- if code can correct Pauli X and Pauli Z errors then it can correct all the Pauli operator errors

Tomography

- **Process tomography** : determine the effect of a quantum operation $\mathcal{E}(\hat{\rho}) = \sum_{i,j} \rho_{i,j}\mathcal{E}(|i\rangle\langle j|)$
  - the map $\mathcal{E}$ is linear
  - 4 inputs ($|1\rangle\langle 1|, |0\rangle\langle 0|, |+_x\rangle\langle +_x|, |+_y\rangle\langle +_y|$) for 1 qubit, measure output ρ for each input
- **State tomography** : determine the state of a quantum system $\rho = \frac{I+\vec{r}\cdot\vec{\sigma}}{2}$
  - 3 measurement for 1 qubit
  - $d^2 - 1$ ($4^n - 1$?) measure for n-qubit state

Classical Error Correction

classical coding theory :

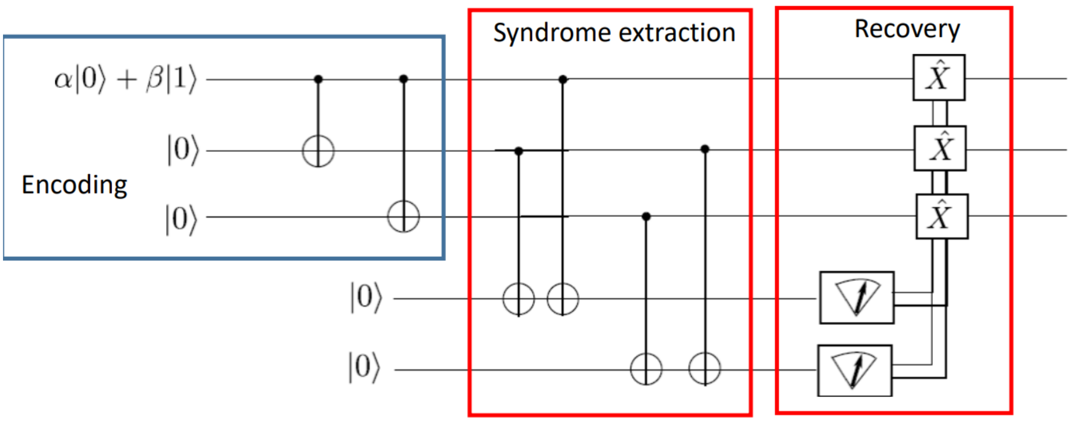
- number of physical bits : n
- number of logical bits : k
- minimal bit flip to change the code : d
- number of errors can be corrected : $t = \frac{d-1}{2}$

Quantum Error Correction

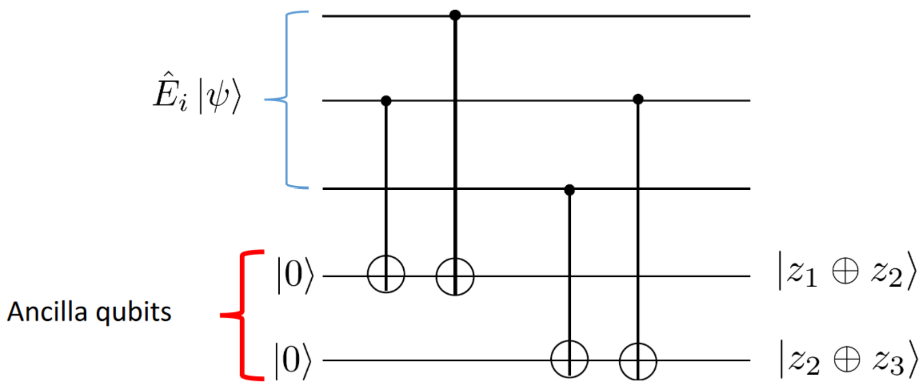
Fidelity : distance between quantum states

- two pure states : $F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2$
- two mixed state : $F(\rho, \sigma) = \sqrt{\sigma}\rho\sqrt{\sigma}$
- one pure state one mixed state : $F(\rho, |\psi\rangle) = \langle\psi|\rho|\psi\rangle$

3-qubit bit-flip code : $(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \otimes |0\rangle \to \alpha|000\rangle + \beta|111\rangle$



syndrome extraction



- no error

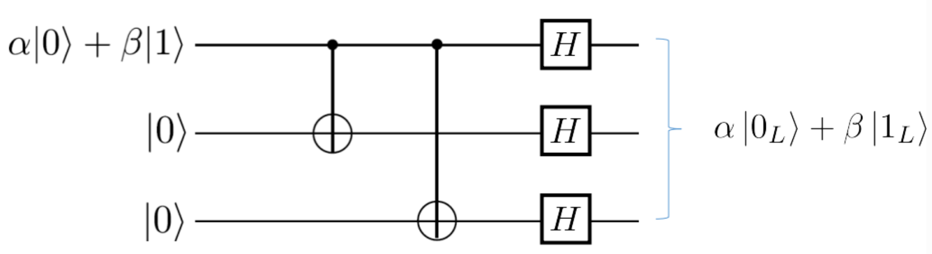
$$(\alpha\,|000\rangle + \beta\,|111\rangle)\,|00\rangle \rightarrow (\alpha\,|000\rangle + \beta\,|111\rangle)\,|00\rangle$$

- one error

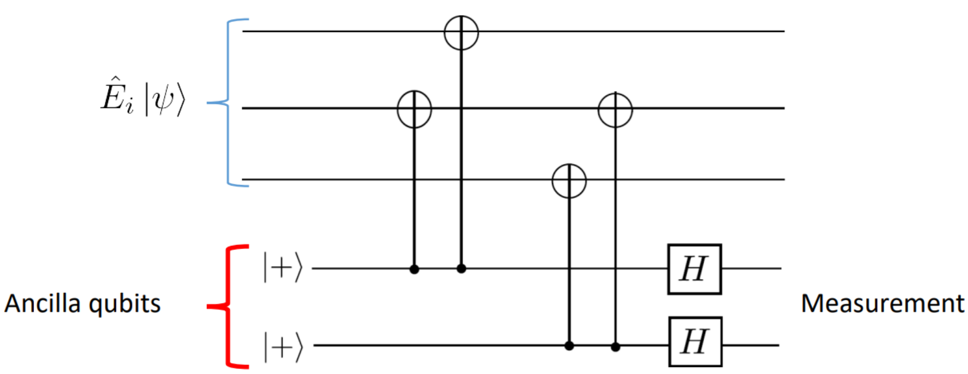
$$(\alpha\,|001\rangle + \beta\,|110\rangle)\,|00\rangle \rightarrow (\alpha\,|001\rangle\beta\,|110\rangle)\,|01\rangle$$
$$(\alpha\,|010\rangle + \beta\,|101\rangle)\,|00\rangle \rightarrow (\alpha\,|010\rangle\beta\,|101\rangle)\,|11\rangle$$
$$(\alpha\,|100\rangle + \beta\,|011\rangle)\,|00\rangle \rightarrow (\alpha\,|100\rangle\beta\,|011\rangle)\,|10\rangle$$

error	**state**	**probability**	**syndrome**	**correction**
III	$\alpha\,|000\rangle + \beta\,|111\rangle$	$(1-p)^3$	$0, 0$	III
XII	$\alpha\,|100\rangle + \beta\,|011\rangle$	$p(1-p)^2$	$1, 0$	XII
IXI	$\alpha\,|010\rangle + \beta\,|101\rangle$	$p(1-p)^2$	$1, 1$	IXI
IIX	$\alpha\,|001\rangle + \beta\,|110\rangle$	$p(1-p)^2$	$0, 1$	IIX

3-qubit phase-flip code : $(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |0\rangle \otimes |0\rangle \rightarrow \alpha\,|+++\rangle + \beta\,|---\rangle$



syndrome extraction



$$|+\rangle|+\rangle \overset{\mathrm{CNOT}}{\rightarrow} |+\rangle|+\rangle$$
$$|+\rangle|-\rangle \overset{\mathrm{CNOT}}{\rightarrow} |-\rangle|-\rangle$$

- no error

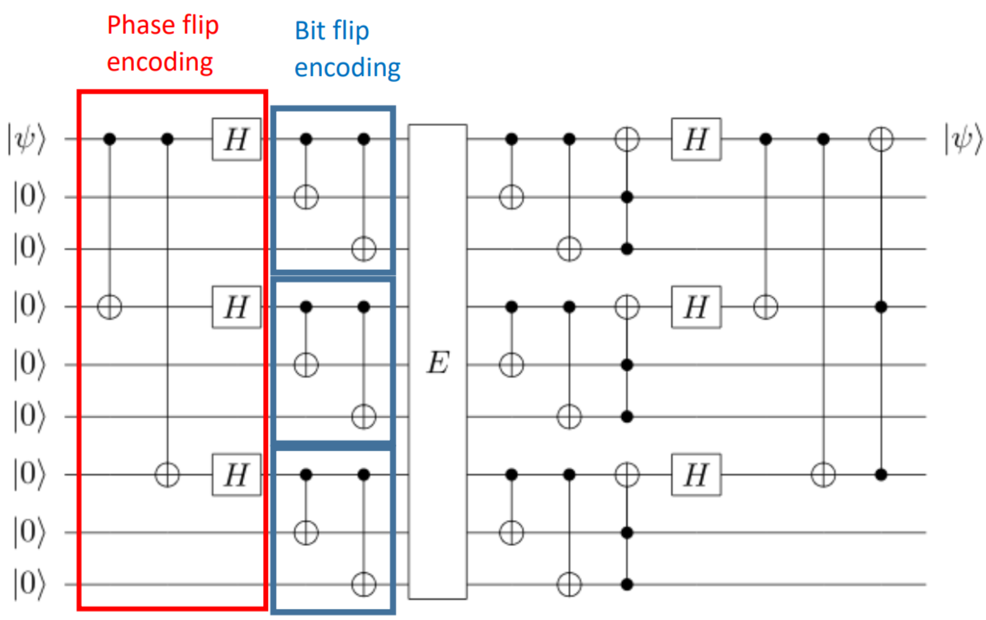
$$|+++\rangle|++\rangle \rightarrow |+++\rangle|++\rangle$$
$$|---\rangle|++\rangle \rightarrow |---\rangle|++\rangle$$

- one error

$$|++-\rangle|++\rangle \rightarrow |++-\rangle|+-\rangle$$
$$|+-+\rangle|++\rangle \rightarrow |+-+\rangle|--\rangle$$
$$|-++\rangle|++\rangle \rightarrow |-++\rangle|-+\rangle$$

error	state	probability	syndrome	correction
III	$\alpha\|+++\rangle + \beta\|---\rangle$	$(1-p)^3$	$0,0$	III
ZII	$\alpha\|-++\rangle + \beta\|+--\rangle$	$p(1-p)^2$	$1,0$	ZII
IZI	$\alpha\|+-+\rangle + \beta\|-+-\rangle$	$p(1-p)^2$	$1,1$	IZI
IIZ	$\alpha\|++-\rangle + \beta\|--+\rangle$	$p(1-p)^2$	$0,1$	IIZ

Shor 9-qubit concatenated code :
$\alpha|0\rangle_L + \beta|1\rangle_L = \alpha(|111\rangle + |000\rangle)^{\otimes 3} + \beta(|111\rangle - |000\rangle)^{\otimes 3}$



syndrome

- Bit errors : $Z_1Z_2, Z_2Z_3,\ Z_4Z_5, Z_5Z_6,\ Z_7Z_8, Z_8Z_9$
- Phase errors : $X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9$

- shor code can correct any single-qubit error that can be expressed as a linear combination of Pauli matrices

Knill-Laflamme condition

different errors lead to orthogonal states, $E_{\{a,b\}}$ are error operators

$$\langle\Phi_i|E_a^\dagger E_b\,|\Phi_j\rangle = C_{ab}\delta_{ij}$$

error operators are linearly independent

$$\text{if} \quad E_a^\dagger E_b = I \quad \text{then} \quad C_{ab} = \sigma_{ab}$$

> Notation
>
> - $\delta_{ij} : \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & \text{otherwise} \end{cases}$
> - C_{ab} : constant independent of i, j

Stabilizer

applying any of the stabilizer operators to a codeword returns the same codeword

$$S\,|\phi\rangle = |\phi\rangle$$

> Example: Bell state $|\Phi^+\rangle$ stabilized by two operators
>
> - $ZZ\,|\Phi^+\rangle = |\Phi^+\rangle$
> - $XX\,|\Phi^+\rangle = |\Phi^+\rangle$

> Notation
>
> - $\mathcal{P}$: pauli group : $\mathcal{P} = \{\pm I, \pm iI, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\}$
>   - $\mathcal{P}_n = \mathcal{P}^{\otimes n}$
>   - $\mathcal{P}_n\mathcal{P}'_n = \bigotimes(\mathcal{P}_{n,i} \cdot \mathcal{P}'_{n,i})$
>   - $A \cdot A = I \quad A \in \{X, Y, Z\}$
>   - $A \cdot B = \epsilon_{ABC} iC \quad A, B, C \in \{X, Y, Z\}$
>
>   > Example
>   >
>   > $XZZXI \cdot IXZZX = X(iY)I(-iY)X$
>
>   - $[\mathcal{P}_n, \mathcal{P}'_n] = 0 \Leftrightarrow \forall i\ [\mathcal{P}_{n,i}, \mathcal{P}'_{n,i}] = 0$
>
>   commute if all element commute
>   - $[\mathcal{P}_n, \mathcal{P}'_n] = 0 \Leftrightarrow \sum_i \mathbb{1}_{\{\mathcal{P}_{n,i}, \mathcal{P}'_{n,i}\}=0} \bmod 2 = 0$
>
>   commute if even number of elements anti commute
>   - $\{\mathcal{P}_n, \mathcal{P}'_n\} = 0 \Leftrightarrow \sum_i \mathbb{1}_{\{\mathcal{P}_{n,i}, \mathcal{P}'_{n,i}\}=0} \bmod 2 = 1$
>
>   anti commute if odd number of elements anti commute
> - $\sigma_x, \sigma_y, \sigma_z$: pauli matrices, $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
>   - $[\sigma_i, \sigma_j] = 2i\epsilon_{ijk}\sigma_k$, e.g.$[\sigma_i, \sigma_i] = 0 \quad [\sigma_i, I] = 0$
>   - $\{\sigma_i, \sigma_j\} = 2\delta_{ij}$, e.g.$\{\sigma_i, \sigma_j\} = 0 \quad i \neq j$
>   - $\sigma_i^2 = 1$
> - $[\cdot, \cdot]$: commute $[A, B] = AB - BA$

- A, B commute $\Leftrightarrow [A, B] = 0$
- $\{\cdot,\cdot\}$: anti commute $\{A, B\} = AB + BA$
  - A, B anti-commute $\Leftrightarrow \{A, B\} = 0$
- ϵ_{ijk} : Levi-Civita symbol
  - even permutation : $\epsilon_{\{123,231,312\}} = 1$
  - odd permutation : $\epsilon_{\{213,132,321\}} = -1$
  - two of i, j, k equal : $\epsilon_{ijk} = 0$
- k : number of element in stabilizer generator
- n : number of element in the pauli group

Stabilizer group :

- all elements commute with each other
- does not contain $I^{\otimes n}$

Stabilizer generator : minimal set of operators generate all members by multiplication
$\langle S_1, \cdots, S_k \rangle \to \{S_1^{a_1} \cdots S_k^{a_k}\} \quad a_i \in \{0, 1, 2\}$

Example

$$\underbrace{\langle ZZI, IZZ \rangle}_{\text{stabilizer generator}} \to \underbrace{\{III, ZZI, ZIZ, IZZ\}}_{\text{stabilizer group}} \quad \begin{matrix} k=2 \\ n=3 \end{matrix}$$

Example :

- 3-qubit bit-flip code : $\begin{array}{c|ccc} S_1 & Z & Z & I \\ S_2 & I & Z & Z \\ \hline Z_L & Z & Z & Z \\ X_L & X & X & X \end{array}$
- 3-qubit phase-flip code : $\begin{array}{c|ccc} S_1 & X & X & I \\ S_2 & I & X & X \\ \hline Z_L & X & X & X \\ X_L & Z & Z & Z \end{array}$
- shor code : $\begin{array}{c|ccccccccc} S_1 & Z & Z & I & I & I & I & I & I & I \\ S_2 & I & Z & Z & I & I & I & I & I & I \\ S_3 & I & I & I & Z & Z & I & I & I & I \\ S_4 & I & I & I & I & Z & Z & I & I & I \\ S_5 & I & I & I & I & I & I & Z & Z & I \\ S_6 & I & I & I & I & I & I & I & Z & Z \\ S_7 & X & X & X & X & X & X & I & I & I \\ S_8 & I & I & I & X & X & X & X & X & X \\ \hline Z_L & X & X & X & I & I & I & I & I & I \\ X_L & Z & I & I & Z & I & I & Z & I & I \end{array}$

> - stean code : $\begin{array}{c|ccccccc} S_1 & I & I & I & Z & Z & Z & Z \\ S_2 & I & Z & Z & I & I & Z & Z \\ S_3 & Z & I & Z & I & Z & I & Z \\ S_4 & I & I & I & X & X & X & X \\ S_5 & I & X & X & I & I & X & X \\ S_6 & X & I & X & I & X & I & X \\ \hline Z_L & Z & Z & Z & Z & Z & Z & Z \\ X_L & X & X & X & X & X & X & X \end{array}$
> - 5-qubit code : $\begin{array}{c|ccccc} S_1 & X & Z & Z & X & I \\ S_2 & I & X & Z & Z & X \\ S_3 & X & I & X & Z & Z \\ S_4 & Z & X & I & X & Z \\ \hline Z_L & Z & Z & Z & Z & Z \\ X_L & X & X & X & X & X \end{array}$

Stabilizer subspace dimension : 2^{n-k}

- code subspace e.g. $|0\rangle_L$
- orthogonal projector in subspace : $P_S|0\rangle_L = |0\rangle_L \quad P_S|1\rangle_L = |1\rangle_L \quad P_S\,|\psi\rangle = 0$

Stabilizer group element : 2^k

Error-Syndrome : $\begin{array}{l} [E, S_i] = 0 \Leftrightarrow \text{error not detected } (1) \\ \{E, S_i\} = 0 \Leftrightarrow \text{error detected } (-1) \end{array}$

> Example : bit flip error (X error) at position 1
>
> $$S = \{XZZXI, IXZZX, XIXZZ, ZXIXZ, ZZXIX\} \quad E = XIIII$$
>
> result : $\{1, 1, 1, -1, -1\}$

stabilizer + EC : for $[E_b^\dagger E_a, S_k] = 0 \quad \langle j|E_b^\dagger E_a S_k\,|i\rangle = \lambda$

projector into subspace : $P_j = \frac{I^{\otimes n} + S_j}{2}$, the eigen value of projected state will only contains $\{0, 1\}$

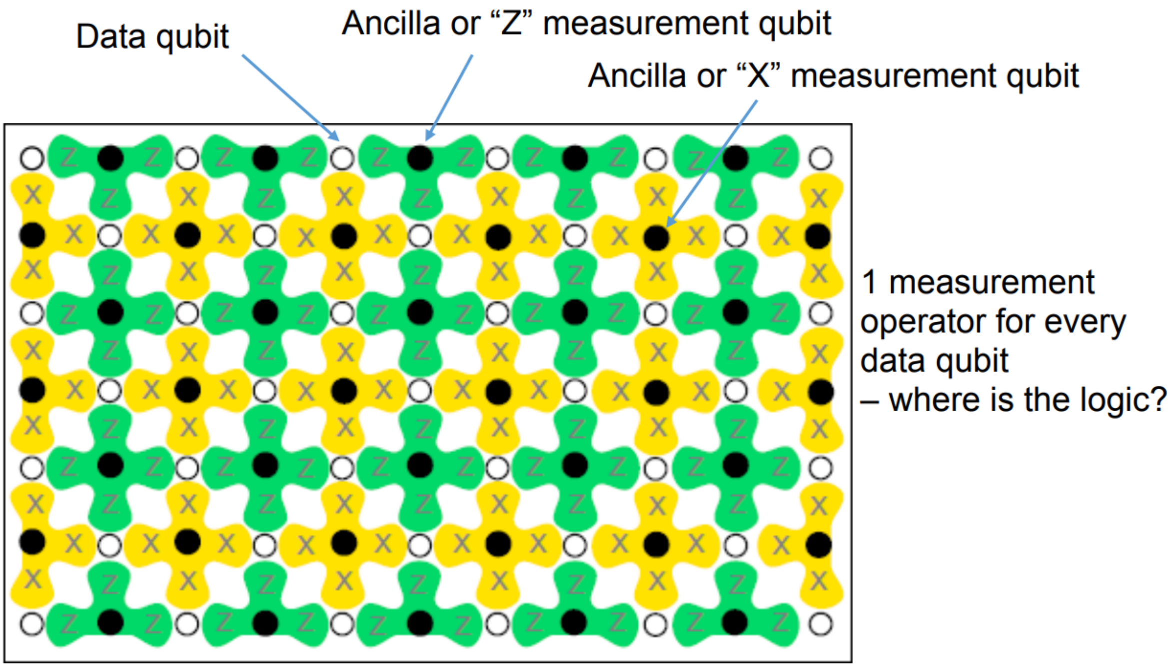
complexity : $O(n)$ stabilizer operators with $O(n)$ Paulis - $O(n^2)$ updates per gate

Gottesman-Knill theorem : A quantum circuit performing

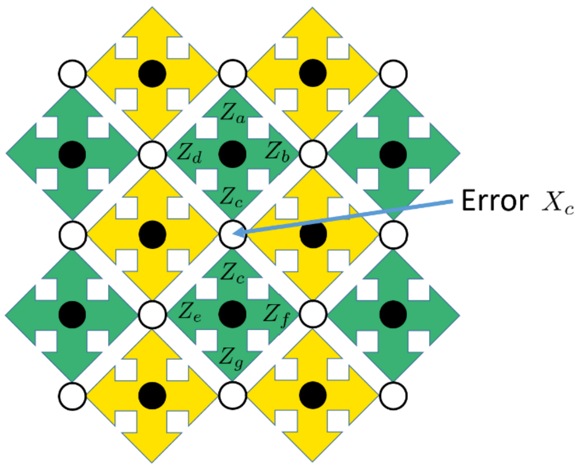
1. Clifford gates (exception : T-gate, Toffoli gate)
2. measurement of the Pauli group operators
3. conditional Clifford group operations

can be simulated efficiently on a classical computer

surface code



syndrome



Hamiltonian Simulation

k-local Hamiltonian : $H=\sum_{i=1}^m H_i \quad H_i$ acting on no more than k qubits

> Example : $X-Y$ model
>
> $$H=\sum_{i=1}^n (J_x X_i X_{i+1} + J_y Y_i Y_{i+1} + J_z Z_i Z_{i+1} + hZ_i)$$
>
> 2-local hamiltonian

Solovay-Kitaev theorem : unitary operator $U\in\mathcal{U}(2^n)$ which acts non-trivially on k qubits, a universal set of gates $\mathcal{S}$ and $\varepsilon>0$, $\exists\tilde{U}\in\mathcal{U}(2^n)$ composed of $\mathcal{O}(\log^c(1/\varepsilon))$ gates from $\mathcal{S}$ such that $\|\tilde{U}-U\|<\varepsilon$ with $c<4$

- if all H_i commute, $e^{-i\sum H_i t}=\prod_{i=1}^m e^{-iH_i t}$

Suzuki-Trotter decomposition : $e^{iHt}=(e^{iH_1 t/K}e^{iH_2 t/K}\cdots e^{iH_m t/K})^K+\mathcal{O}(m^2h^2\frac{t^2}{K})$

- total error :$\epsilon_T=m\epsilon_L K+\mathcal{O}\left(\frac{m^2h^2t^2}{K}\right)$

- **Lie-Trotter** decomposition : $e^{(A+B)x} = e^A e^B - \frac{1}{2}x^2[A,B] + \mathcal{O}(x^3)$, if $[A,B]=0$ then $\|e^{x(A+B)} - e^A e^B\| \leq \epsilon$
- number of local terms in a k-local n-qubit Hamiltonian : n^k

> Notation
>
> - m : number of terms for Hamiltonian decomposition $H = \sum_{i=1}^m H_i$
> - h : maximal norm of Hamiltonian term : $\|H_i\| \leq h$
> - K : Trotter step, $\Delta t = \frac{t}{K}$
> - ϵ_T, ϵ_L : total error, local error for Trotter step