

# ACM Winter School 2022

## Quantum gates & circuits.

### qubit gates & circuits.

#### Outline:-

- Scope of the field
- gate model / circuit model of quantum computation.
- Single / Two - qubit / three qubits.

- Universal gate set / universal quantum computation.
- Clifford hierarchy
- Two fundamental theorems of quantum computation.

Examples:-

- State teleportation
- gate teleportation
- Hadamard gate identities

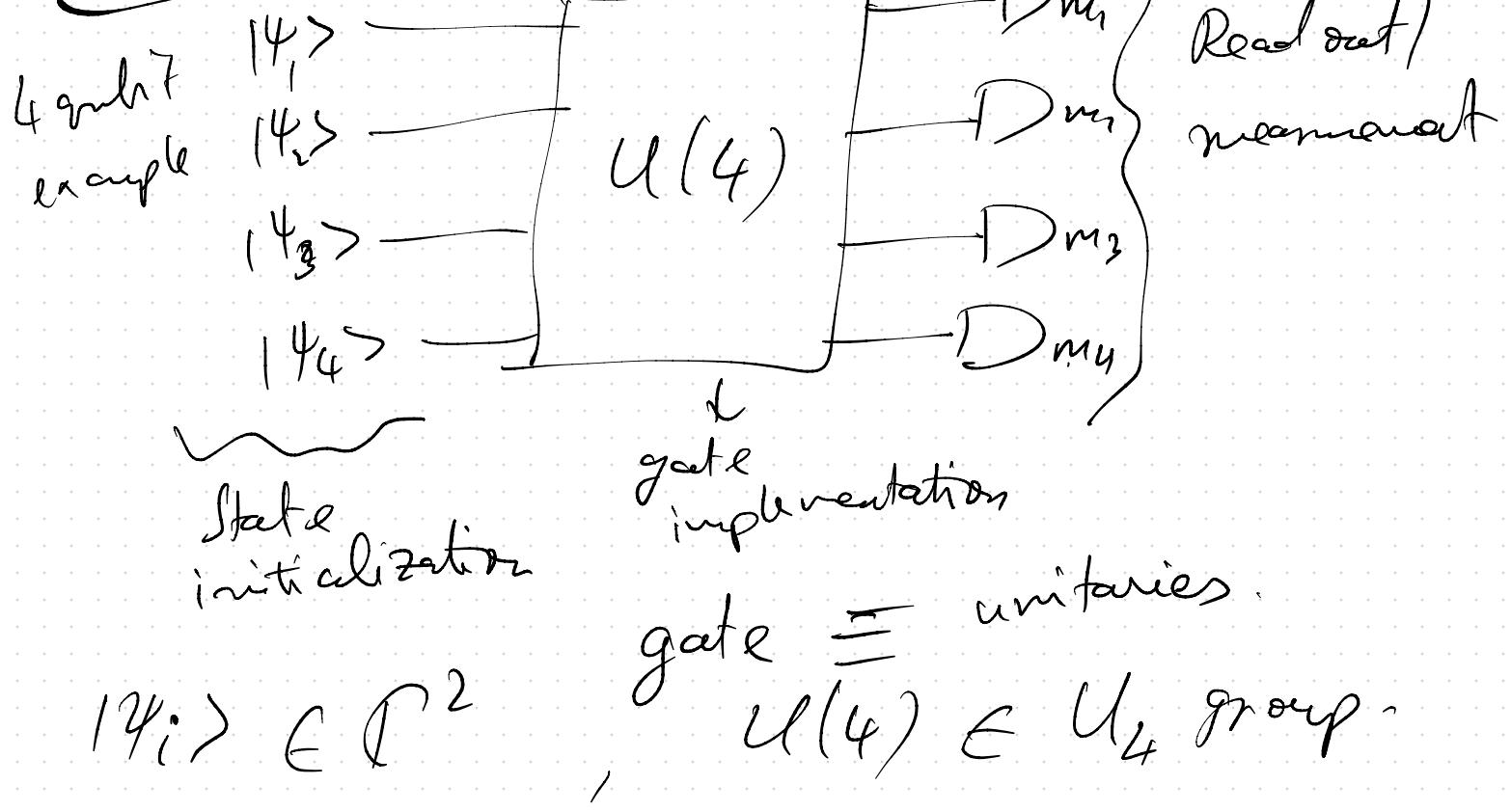
- 1D or 2D clusters.
- Repetition code

Imperfect gates

## Scope:-

- Quantum Algorithms / QML.
- Quantum error correction circuits
- Quantum simulation
- Quantum cryptographic protocols.
- Preparation of ground states of many-body states
- Quantum advantage:
  - Random circuit sampling
  - Boson sampling

# Gate Model



# Single qubit gates :-

$|0_z\rangle, |1_z\rangle$ : Pauli Z.

Bloch sphere :-

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$A^\dagger B A$

pure states

$$P(\alpha) |\psi_{0,\varphi}\rangle = \cos\theta/2 |0\rangle + e^{i(\varphi+\alpha)} \sin\theta/2 |1\rangle.$$

Pauli matrices :-

$$\left[ \begin{array}{l} \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}; \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}; \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \\ |0\rangle_z = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad |1\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \\ |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad |-i\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \end{array} \right]$$

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = 1.$$

$$[\sigma_j, \sigma_k] = 2i\epsilon_{jkl}\sigma_l. \quad \text{--- } \textcircled{1}$$

$$[\sigma_j, \sigma_k]_+ = \{\sigma_j, \sigma_k\} = 2\delta_{jk} \mathbb{1}. \quad \text{--- } \textcircled{2}$$

Identity:

$$-\boxed{\sigma_j \sigma_k = \delta_{jk} \mathbb{1} + i \epsilon_{jkl} \sigma_l.} \quad \text{--- } \textcircled{3}$$

$$-(\bar{a} \cdot \bar{\sigma})(\bar{b} \cdot \bar{\sigma}) = (\bar{a} \cdot \bar{b}) \mathbb{1} + i(\bar{a} \times \bar{b}) \cdot \bar{\sigma} \text{ where}$$

$$\overline{a} \in \mathbb{R}^3, \quad \bar{a} \cdot \bar{\sigma} = a_x \sigma_x + a_y \sigma_y + a_z \sigma_z.$$

$$e^A = \sum_{j=0}^{\infty} \frac{A^j}{j!}$$

In particular  $A^2 = \mathbb{1}$ :

$$e^{i\theta(\vec{n} \cdot \vec{o})} = \cos \mathbb{1} + i \sin (\vec{n} \cdot \vec{o}). \quad \text{X}$$

$$\rho = \frac{1}{2} [\mathbb{1} + \vec{n} \cdot \vec{o}] \quad \text{if } |\vec{n}| \leq 1.$$

pure state  $|\vec{n}|=1$

$$\text{Tr}(\rho_i) = 1$$

$$- B = \sum_{i=0}^3 \vec{a} \cdot \vec{o} ; \quad \mathbb{1}_0 = \mathbb{1} ; \quad \vec{a}_* \in \text{Reals.}$$

## Other single qubit gates:-

• Hadamard gate  $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} [\sigma_2 + \sigma_x]$

$$H^2 = \mathbb{I}.$$

$$\boxed{H^\dagger \sigma_x H = \sigma_2 \quad H^\dagger \sigma_z H = \sigma_x.}$$

$$H^\dagger \sigma_y H = -\sigma_y.$$

$$H = H^\dagger.$$

$$X \xrightarrow{H} Z$$

$$H|0\rangle = |+\rangle.$$

$$H|1\rangle = |- \rangle.$$

$$HH^\dagger = H^\dagger H = \mathbb{I}$$

Conjugation:  $H = H^\dagger$ .

S gate :  $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \xrightarrow{\text{diagonal gate}}$

$$\underline{S^2 = I} \quad : \quad \underline{SS^\dagger = S^\dagger S = 1}.$$

T-gate :-  $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \quad \begin{array}{l} \text{Diagonal gate} \\ T T^\dagger = 1 \end{array}$

$$\underline{T^2 = S} ; \quad \underline{S^2 = I} \Rightarrow \underline{T^4 = Z}.$$

$$T \xrightarrow{S} S \xrightarrow{S} Z. \quad \begin{array}{l} \text{[diagonal} \\ \text{(I, phase)} \end{array}$$

## Rotation gates : $\rightarrow$ universality.

$$\bullet R_x(\theta) = \underbrace{e^{-i\theta \sigma_x/2}}_{= \cos \theta/2 \mathbb{1} - i \sin \theta/2 \sigma_x}$$

$$R_x(\theta)^+ \sigma_x R_x(\theta) = \sigma_x.$$

$$R_x(\theta) = \begin{pmatrix} \sigma_y \\ \sigma_z \end{pmatrix}.$$

rotation about  $x$  in the  
anti clockwise direction.

$$\bullet R_y(\theta) = e^{-i\theta \sigma_y/2}$$

$$\bullet R_z(\theta) = e^{-i\theta \sigma_z/2} : \cos \theta/2 \mathbb{1} - i \sin \theta/2 \sigma_z.$$

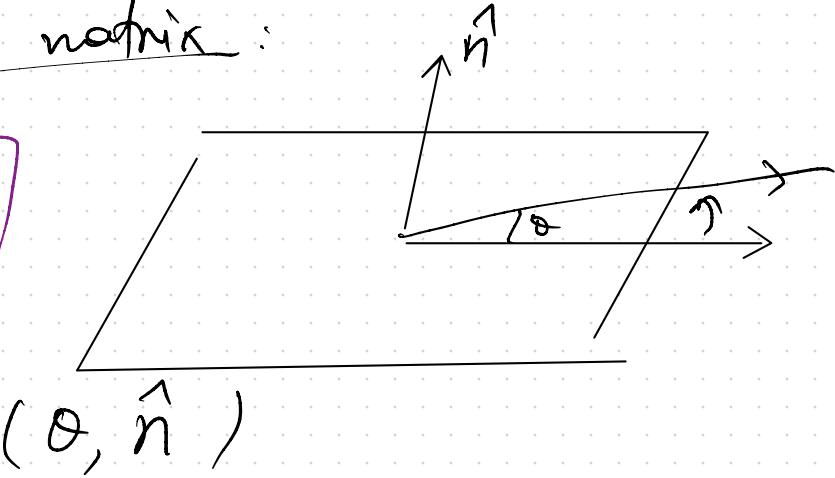
$\rightarrow$  diagonal operator

$$R_y(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

$$R_z(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} \rightarrow \text{diagonal in the Pauli } z\text{-basis.}$$

general rotation matrix:

$R_{\hat{n}}(\theta) :$   
 $= e^{-i\theta \hat{n} \cdot \vec{\sigma}/2}$



$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \{ \sigma_x + \sigma_z \}$$

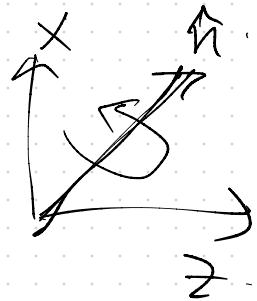
$$= \frac{1}{\sqrt{2}} \left\{ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\} + \frac{1}{\sqrt{2}} \left\{ \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right\}$$

Consider the following operator :

$$e^{i\pi/2} \boxed{R_{\hat{n}}(\pi)} ; \quad \hat{n} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

$$R_{\hat{n}}(\theta) = \cos \theta/2 \mathbb{1} - i \sin \theta/2 \hat{n} \cdot \vec{\sigma}$$

$$= e^{i\pi/2} \left\{ -i \frac{1}{\sqrt{2}} [\sigma_x + \sigma_z] \right\} = \boxed{H}$$



$U_{2 \times 2}$  i.e. any single qubit gate

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

decompose  
any

Angular momentum  
Chapter, Sakurai.

Adjoint representation:

$$R_n^+(\theta) \cancel{R}(\vec{\alpha} \cdot \vec{\sigma}) R_n(\theta) = ? (\vec{b} \cdot \vec{\sigma})$$

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \underbrace{\left[ \quad R(\vec{\alpha}, \theta) \quad \right]}_{3 \times 3} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

$$\cdot R_{\hat{n}}(\theta) \circ R_{\hat{m}}(\theta') = R_{\hat{k}}(\phi). \quad [Ex].$$

• Infinitesimal Rotation:

$$e^{-i\delta\theta \hat{n}/2} \underset{\text{in } S_0}{\approx} \begin{matrix} \text{linear} \\ \text{to } \delta\theta \end{matrix} \underset{\text{in } S_0}{\approx} \mathbb{I} - i\sin\delta\theta \hat{n} \cdot \hat{\sigma}$$

$$\approx \mathbb{I} - i(\delta\theta) \hat{n} \cdot \hat{\sigma}.$$

$\xrightarrow{\hspace{2cm}}$  Single qubit gates: - Pauli matrices  
 decomposition of any - Hadamard  $[\sigma_x \leftrightarrow \sigma_z]$ .  
 gate -  $S, T, P(\alpha)$  diagonal  $\equiv \sigma_z$ .  
 $\xleftarrow{\hspace{2cm}}$  Rotation gates.

$$P(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}.$$

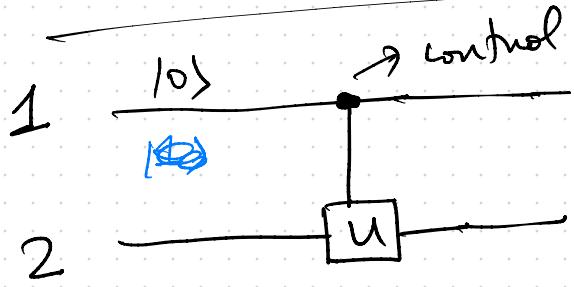
$$\underline{Z = P(\pi)} ; \quad \underline{S = P(\pi/2)} ; \quad \underline{T = R(\pi/4)}.$$

$$\begin{aligned} P(\theta) [a|0\rangle + b|1\rangle] & \quad (|0\rangle, |1\rangle \rightarrow |+\rangle, |-\rangle) \\ &= a|0\rangle + b e^{i\theta}|1\rangle. \end{aligned}$$

Two quantum gates

↳ generating entanglement

Controlled - U gates :-



$$Cu = 10 \times 0.1 \times 11 + 14 \times 1.1 \times 2.1$$

$$\overbrace{H|14\rangle \otimes |14\rangle}^{\text{Initial State}}$$

$CX = CNOT$

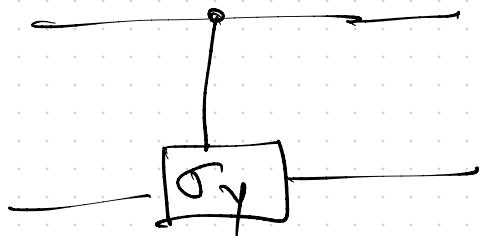
$|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_x$



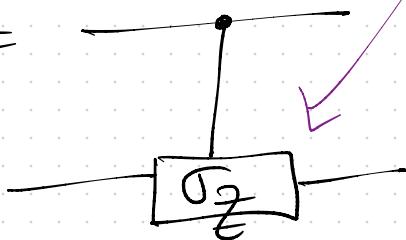
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4 \times 4}$$

$CY, CZ:$

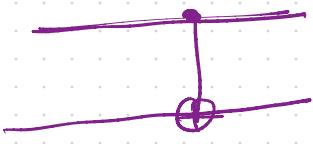
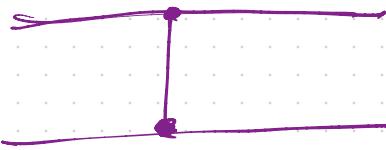
$CY:$

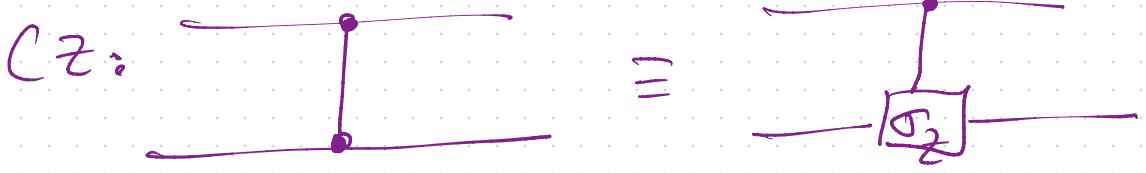


$CZ =$

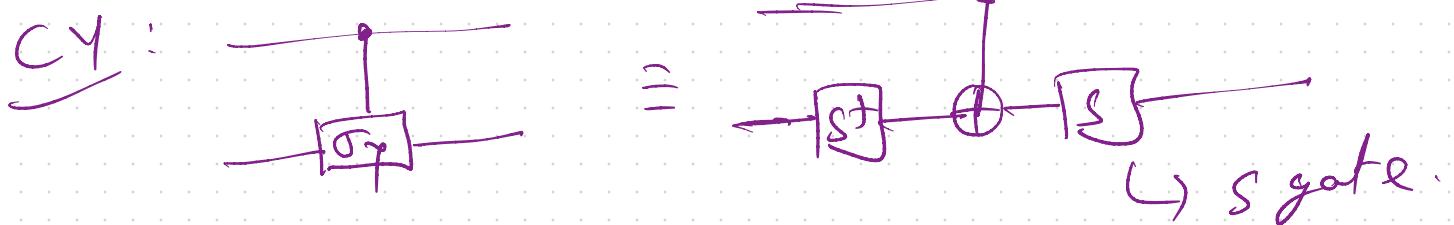
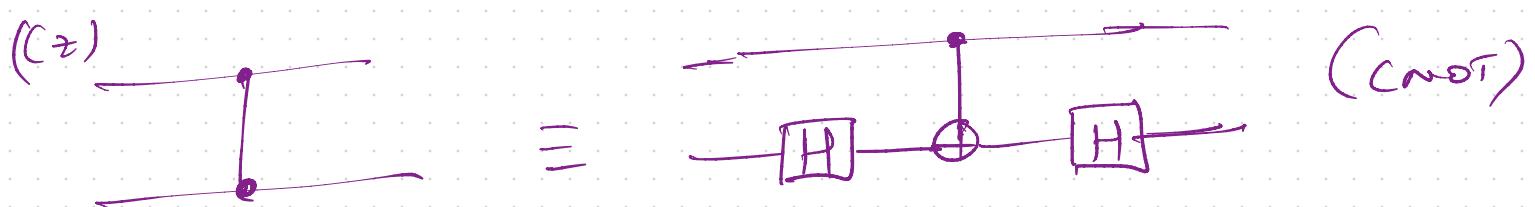


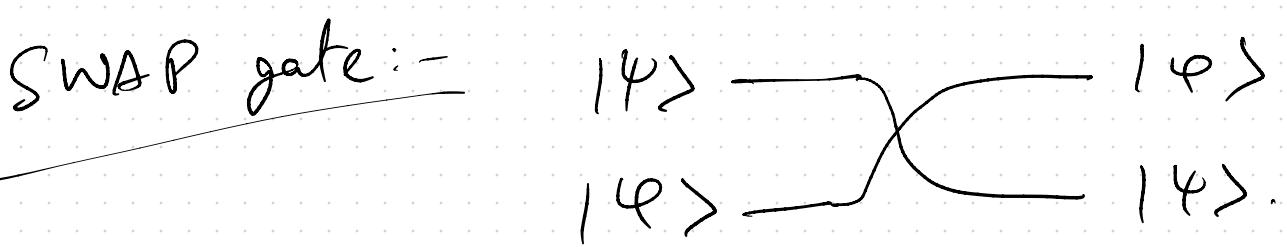
$\equiv$



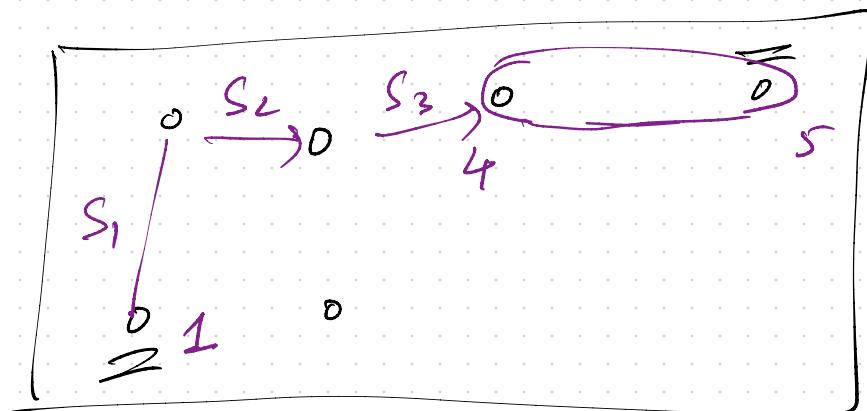


$$H \sigma_x H = \sigma_z ; \quad H \sigma_z H = \sigma_x .$$





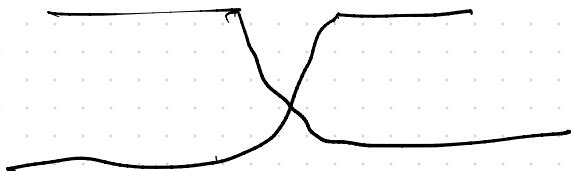
①



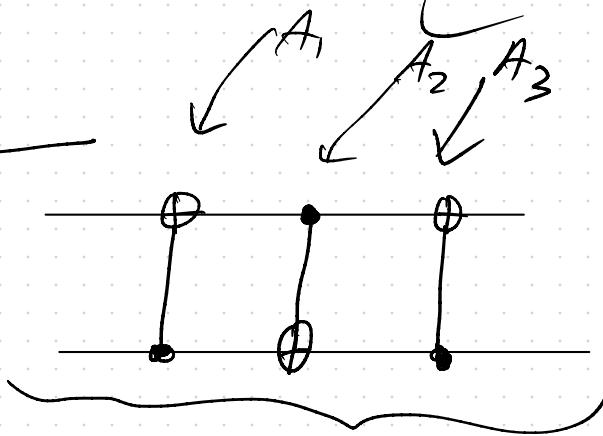
② Photonic computation: mux.

$$\text{SWAP} := \left[ \begin{array}{l} 10X_01 \otimes 10X_01 + 11X_11 \otimes 11X_11, \\ + 10X_11 \otimes 11X_01 + 11X_01 \otimes 10X_11. \end{array} \right]$$

CNOT's

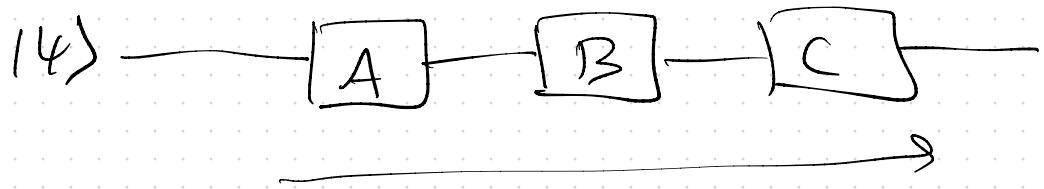


=



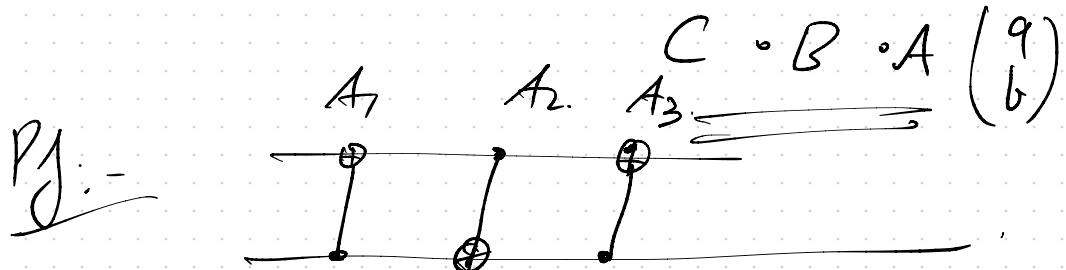
$$A_3 \circ A_2 \circ A_1 \quad / \quad 4 \times 4$$

$$\left[ \begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right]$$



$$4 = \binom{9}{6}$$

$$= a|0\rangle + b|1\rangle$$

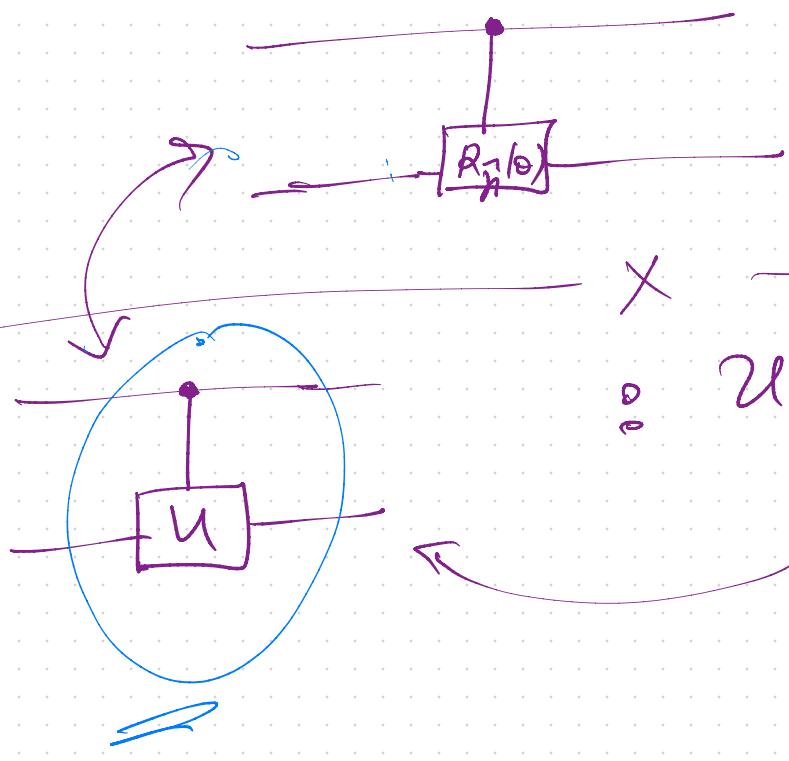


$$\left[ |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_x \right] \circ \left[ \mathbb{I} \otimes |0\rangle\langle 0| + \sigma_x \otimes |1\rangle\langle 1| \right].$$

$$\begin{aligned}
 &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes |1\rangle\langle 1| + |0\rangle\langle 1| \otimes |1\rangle\langle 0| \\
 &\quad + |1\rangle\langle 0| \otimes |0\rangle\langle 1|.
 \end{aligned}$$

CR OT:- controlled rotation gate.

superconducting.



$$\therefore U = e^{i\alpha} R_z(\beta) R_y(\theta) R_z(\delta)$$

$\Rightarrow$

[ABC form]

ABC representation for single qubit unitaries:-

$$U = e^{i\alpha} \underset{R_Z}{=} R_Z(\beta) \underset{=} R_Y(\gamma) \underset{=} R_Z(\delta)$$

Define A, B, C operators :

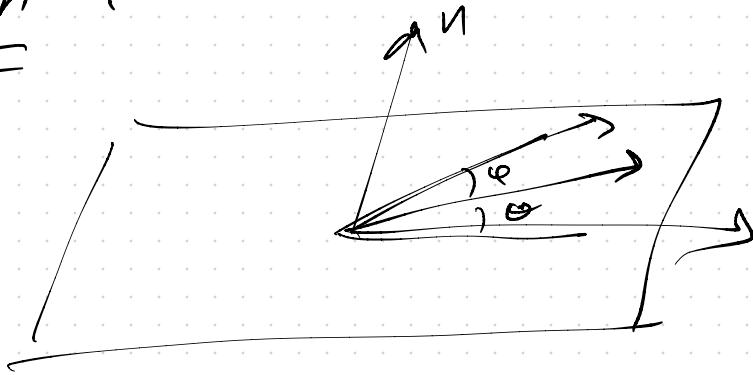
$$A = \overline{R_Z(\beta)} \left[ \begin{array}{c} R_Y(+\delta/2) \\ R_Y(-\delta/2) \end{array} \right]$$
$$B = \left[ \begin{array}{c} R_Y(-\delta/2) \\ R_Z(-\frac{\delta+\beta}{2}) \end{array} \right].$$
$$C = R_Z(\frac{\delta-\beta}{2}).$$

$$A \circ B \circ C = 1.$$

$$\begin{aligned}
 A \circ B \circ C &= R_2(\beta) R_2\left(-\frac{\alpha+\beta}{2}\right) R_2\left(\frac{\delta-\beta}{2}\right) \\
 &\quad = \quad = \\
 &= R_2(\beta) R_2(-\beta) = 11.
 \end{aligned}$$

$$\begin{aligned}
 & e^{i\alpha} A \sigma_x B \sigma_x C \\
 &= R_z(\beta) \cdot R_y(\delta/2) \left( \sigma_x R_y(-\delta/2) \cdot R_z\left(-\frac{\delta+\beta}{2}\right) \sigma_x R_z\left(\frac{\delta-\beta}{2}\right) \right) \\
 &\quad \xrightarrow{\text{Diagram}} R_y(\delta/2) \quad R_z\left(\frac{\delta+\beta}{2}\right) \cdot R_z\left(\frac{\delta-\beta}{2}\right) \\
 &= e^{i\alpha} R_z(\beta) R_y(\delta) R_z(\delta) = U_{2 \times 2}.
 \end{aligned}$$

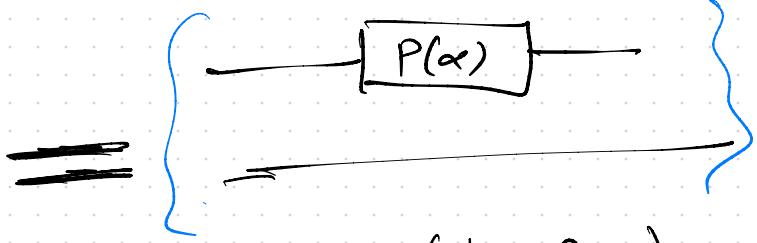
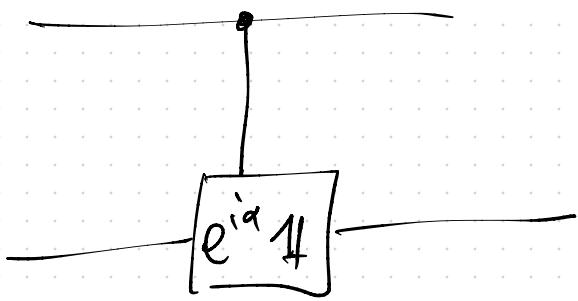
$$R_h(\theta) \circ R_h(\varphi) = R_h(\theta + \varphi).$$



$$U = e^{i\alpha} A \sigma_x B \sigma_x C.$$

$$\sigma_x \sigma_y \sigma_x = -\sigma_y$$

$$\sigma_x \sigma_z \sigma_x = -\sigma_z$$



$$P(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

$|0\rangle\langle 0| \otimes \mathbb{I}$

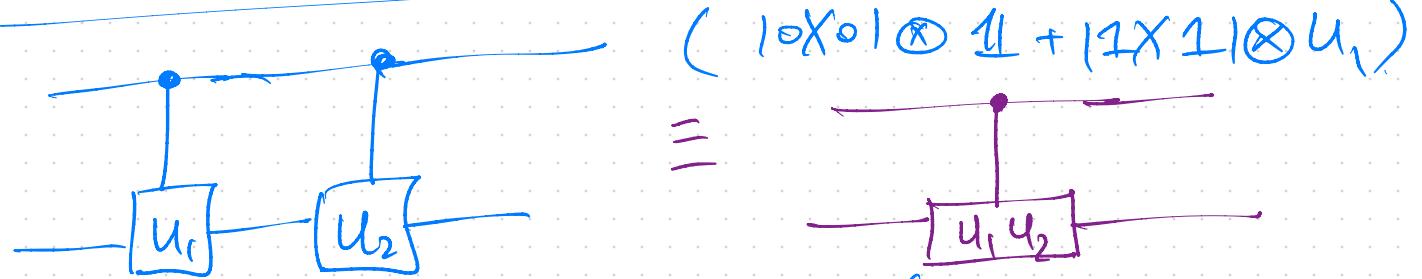
+  $|1\rangle\langle 1| \otimes e^{i\alpha} \mathbb{I}|.$

$|0\rangle |0\rangle$   
 $|0\rangle |1\rangle$   
 $e^{i\alpha} |1\rangle |0\rangle$   
 $e^{i\alpha} |1\rangle |0\rangle$ .



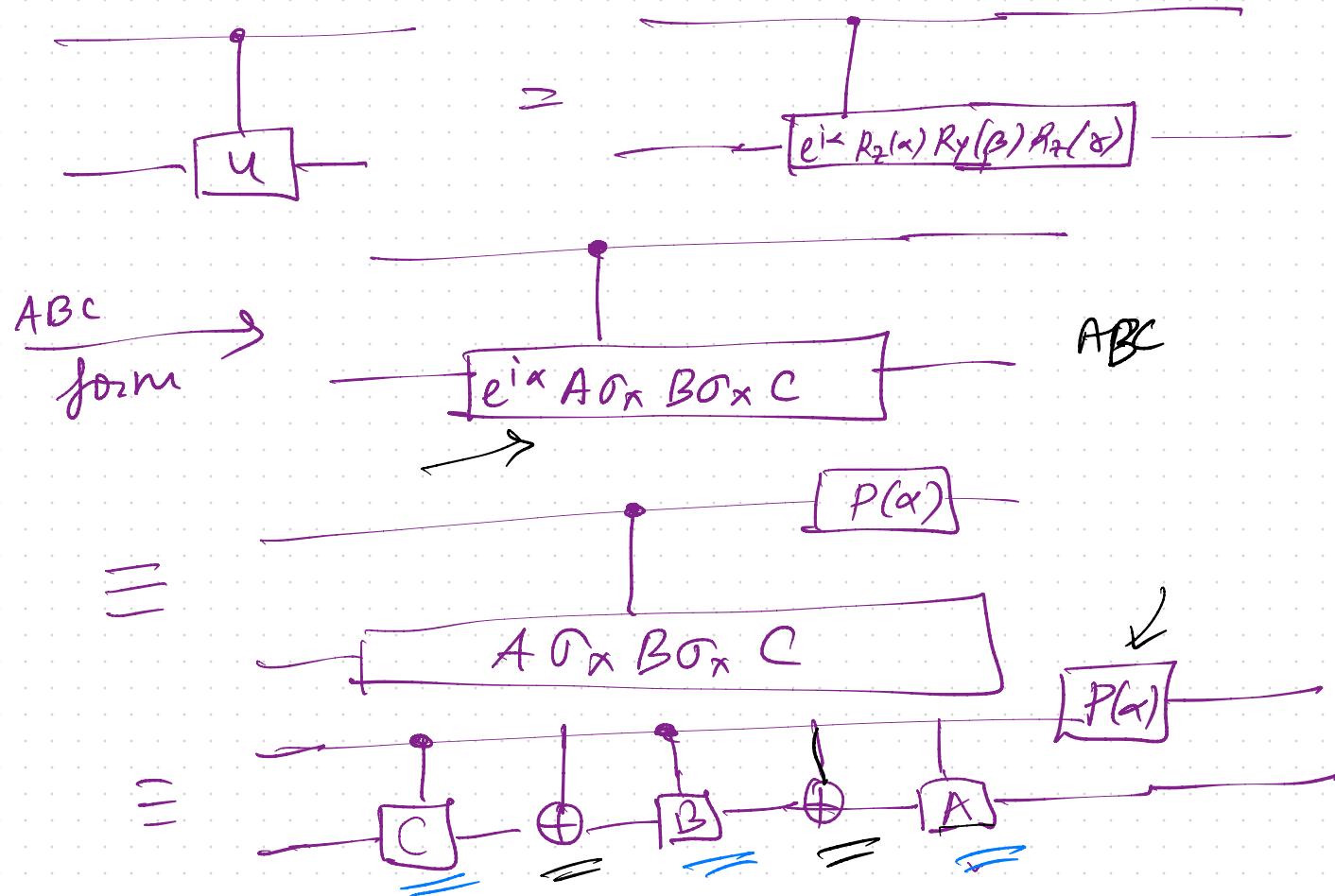
$$\begin{aligned} |0\rangle |0\rangle &\rightarrow |0\rangle |0\rangle \\ |0\rangle |1\rangle &\rightarrow |0\rangle |1\rangle \\ |1\rangle |0\rangle &\xrightarrow{e^{i\alpha}} |1\rangle |0\rangle \\ |1\rangle |1\rangle &\xrightarrow{e^{i\alpha}} |1\rangle |1\rangle. \end{aligned}$$

Composing controlled unitaries :-



$$\begin{aligned} & (|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U_2) \circ (|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes U_1) \\ &= |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes (U_2 U_1). \end{aligned}$$

↳ is a controlled unitary.

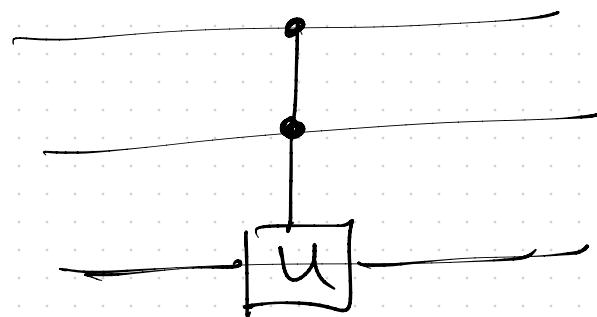


Three qubit gates :-

C-C-U.

CNOTS,

T



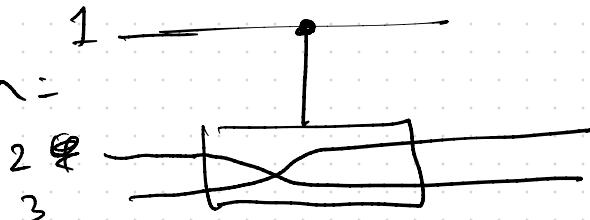
Toffoli:  $U = \sigma_x$

=

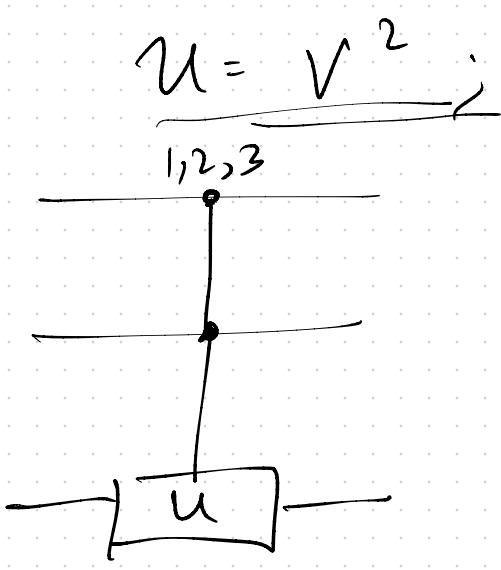
CC-Z

CC-Y

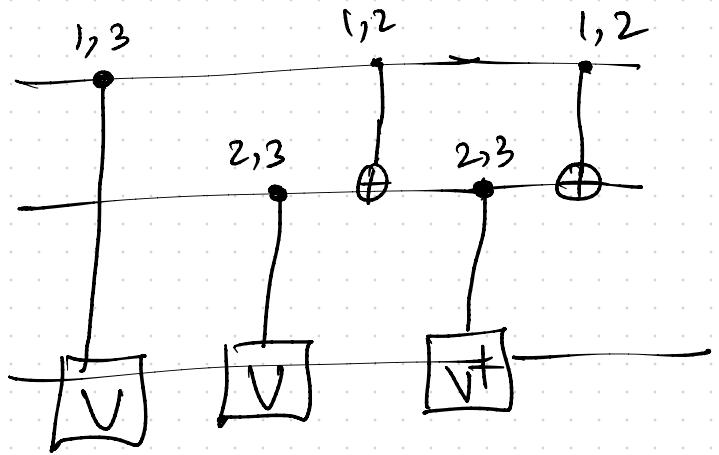
Fredkin =



CNOT's } 2 qubit  
C-U's } gates



$\equiv$



$\rightarrow 3$  controlled  $\mathcal{U}$ .  
 $\rightarrow 2$  CNOT's.

$$\sqrt{X} = HSX : CCX = C-HSX.$$

One ~~gates~~ can generalize this controlled gates  
to n-qubits:

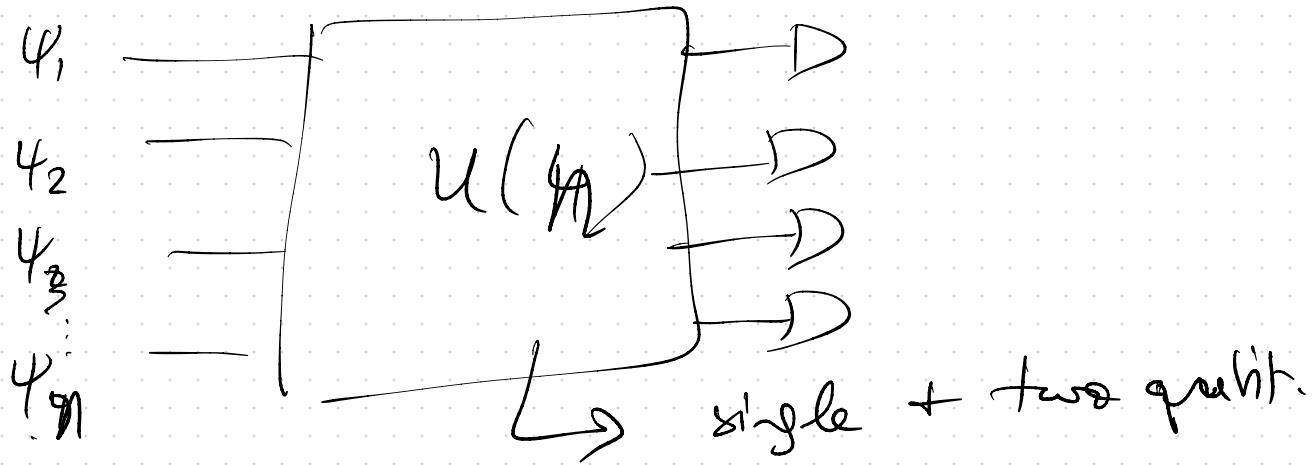
$$(C-C-C\cdots)^{\otimes n} - u \equiv \begin{matrix} \text{2 qubit C-U's} \\ \text{CNOT's.} \end{matrix}$$

\_\_\_\_\_ X \_\_\_\_\_

## Universal gate sets:-

$$\textcircled{1} \quad U(n) = e^{i\alpha} R_z(\cdot) R_y(\cdot) \cdot R_z(\cdot) + \text{CNOT}$$

continuous parameters.  $\hat{T}$



②

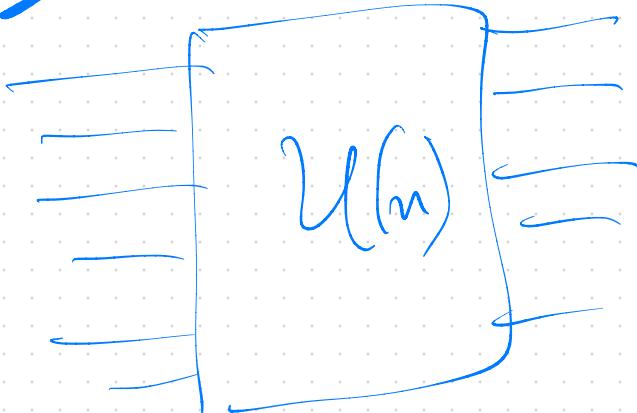
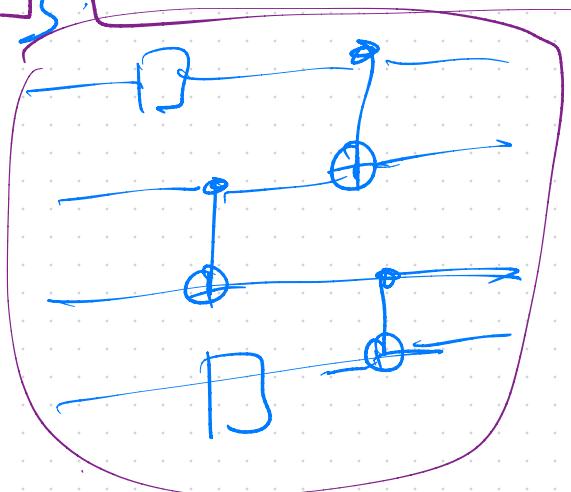
## Discrete sets:-

I:  $\{H, S, \boxed{T}, \underline{\text{CNOT}}\}$

II:  $\{H, S, \underline{\text{CNOT}}, \boxed{\text{Toffoli}}\}$

 $U(n)$ 

- Approximation
- Accuracy.

 $\boxed{\text{Toffoli}}$ 

## Clifford Hierarchy :

Pauli group :-  $(P_n)$

An  $n$ - qubit group is the group generated by  $\hat{g} = \langle \pm \mathbb{1}, \pm i \mathbb{1}, \sigma_x, \sigma_y, \sigma_z \rangle$

$g \in P_n : g_1 \otimes g_2 \otimes g_3 \dots$

$g_i \in \hat{g}$ .

## Clifford group :-

- group of automorphisms of the Pauli group:

$$\mathbb{P}^{(2)} = \left\{ U \mid UPU^T \in \mathbb{P}_n, \forall P \in \mathbb{P}_n \right\}$$

$$\cong \mathbb{P}^n \subset \mathbb{C}^{(2)}$$

- Clifford group elements are insufficient for universal.
  - so we need elements beyond Clifford.  
T, Toffoli, infinitesimal notation
- One set universal for clifford alone  $\equiv$   
are  $\langle H, S, \text{CNOT} \rangle$ .
- Clifford circuits
  - Stabilizer formalism in QECC.
  - cluster state generation
  - State & gate teleportation.

- Clifford circuits are classically simulable efficiently.
- $U = (\text{Clifford}) + \text{one non clifford element} \Rightarrow \text{CP}$ 
  - ↳ classically simulable
- Entanglement generated by Clifford alone is sufficient.
  - dictate

$P, \quad UPU^T \in P_n; \quad UPu^T \in C^{(2)}$

$C^{(2)}$

$C^{(3)}$

X

Z

# Fundamental theorems of quantum computation

Thm1:- Gottesman-Knill theorem (Clifford circuits).

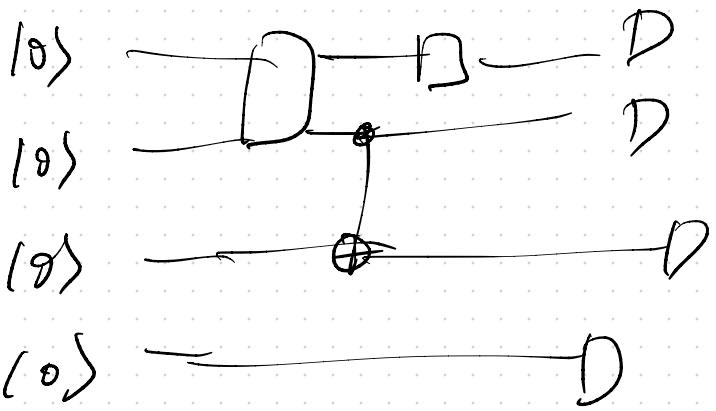
Any Q computer performing :-

(a) clifford group gates  $\langle H, S, \text{CNOT} \rangle$ .

(b) measurements of Pauli group operators

(c) clifford gates conditional on the classical outcome of measurements.

Can be perfectly simulated in polynomial time on a probabilistic classical computer.

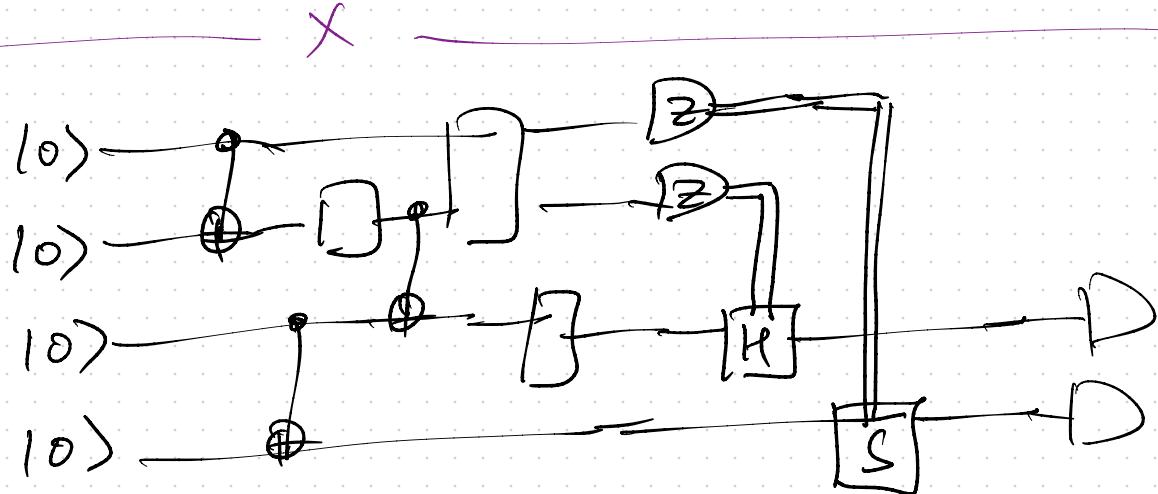


Efficiently  
Evaluable

clifford :  $\langle H, S, \text{CNOT} \rangle$ .

$\{T, \text{Toffoli}, \dots\} =$

II theorem: Solvay - Kitaev theorem (general universal circuits)



conditional feed-forward operation.

- e.g.: Teleportation.

## II Solvay - Kitaev theorem:

Def.:- INSTRUCTION set  $G$  for a qubit is a finite set of quantum gates that satisfies,

- 1: All gates in  $G$  are in  $SU(2)$
  - 2:  $g \in G$ ,  $g^{-1}$  also  $\in G$ .
  3.  $G$  is universal in  $SU(2)$ .
-

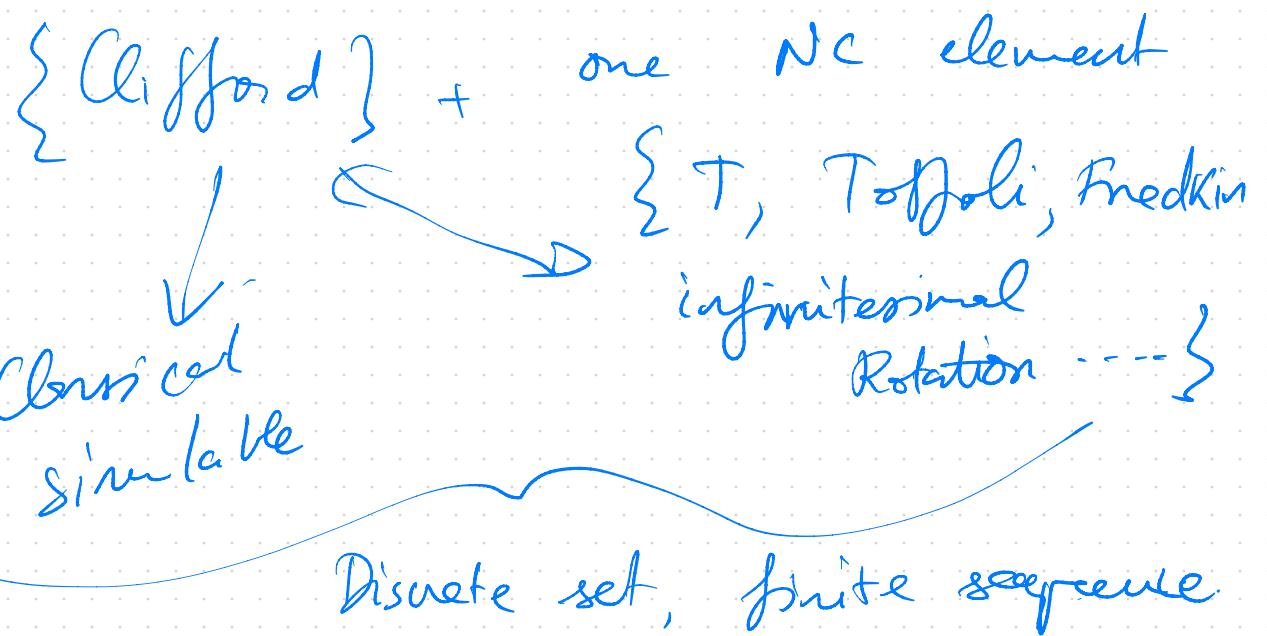
Let  $G$  be an instruction set for  $\text{SU}(2)$   
let  $\varepsilon > 0$  (accuracy);  $\exists 'c'$ : for any  $u \in G$ ,

$\exists$  a finite sequence  $S$  from  $G$  of  
length  $O(\log^c(1/\varepsilon))$  and such that

$$d(u, S) < \varepsilon.$$

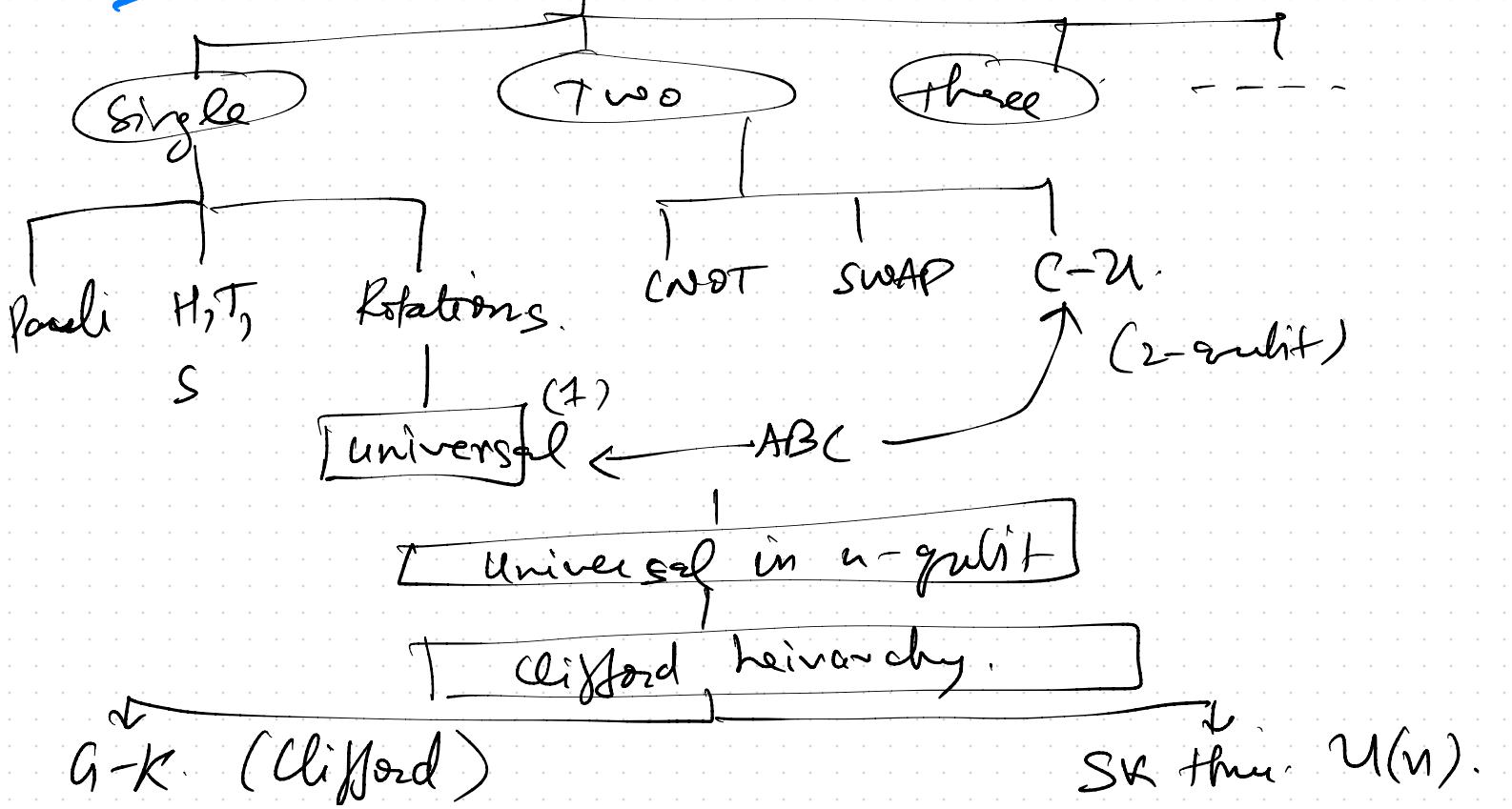
finite seqn:  $S$ ; finite set  $G$ ;

$$S = g_1, g_2, \dots, g_m \quad g_i \in G.$$



# Recap:

gate model



## Examples:-

1. State preparation:

$$\text{Bell state: } |\Psi_{AB}^+\rangle = \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}}$$

$|00\rangle \xrightarrow{H} |00\rangle \xrightarrow{\text{CNOT}} |00\rangle + \frac{|11\rangle}{\sqrt{2}}$

$$= \text{CNOT} \left[ \frac{|00\rangle + |11\rangle}{\sqrt{2}} \otimes |00\rangle \right]$$

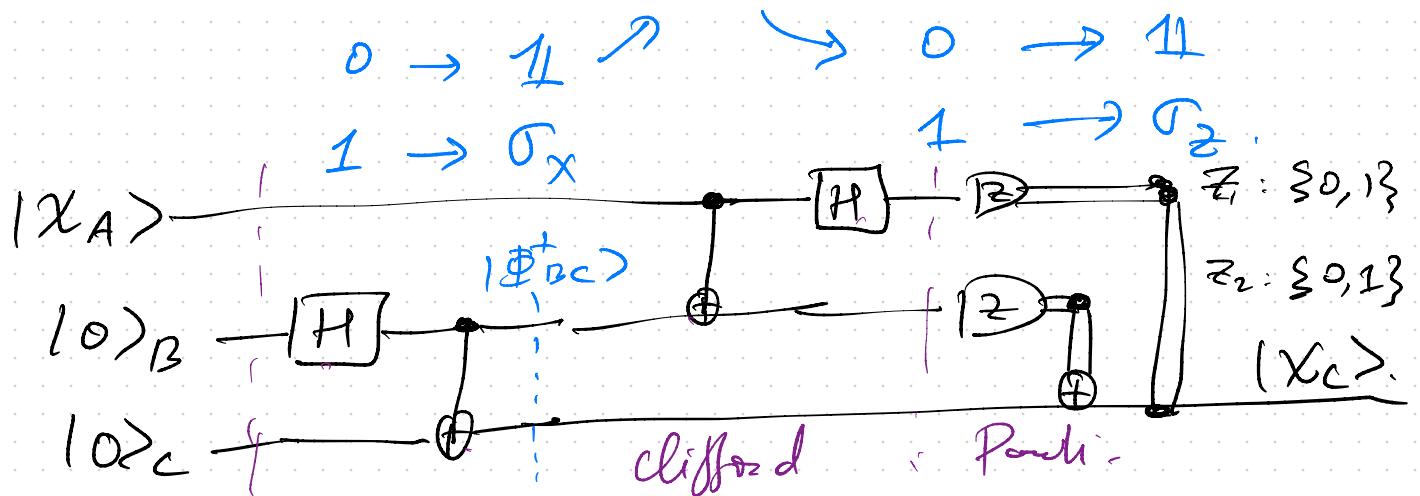
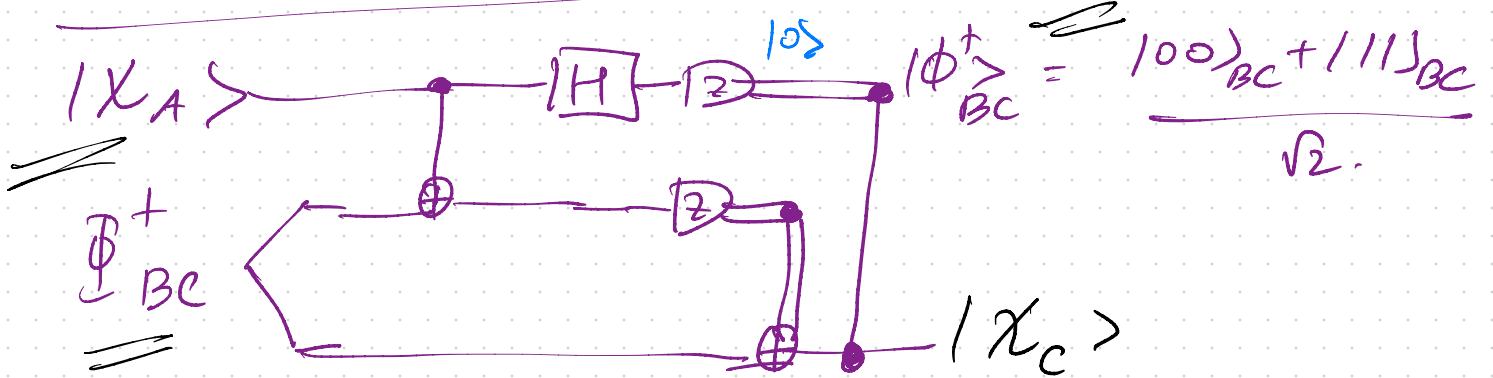
$$= \frac{1}{\sqrt{2}} \text{CNOT} [ |00\rangle + |11\rangle ] = \frac{1}{\sqrt{2}} [ |00\rangle + |11\rangle ]$$

$$= |\phi^+\rangle_{AB}$$

$$\begin{aligned} H|0\rangle &= |+\rangle \\ &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \end{aligned}$$

State Teleportation:-

$$|\chi_A\rangle = a|0\rangle_A + b|1\rangle_A$$



## Gate teleportation :-

- Implement, eg: non-clifford gate:  $(N)$ .
  - $N(|+\rangle)$ . → can be prepared.  
 ~~$\equiv$~~  resource state.  
+ clifford circuits.
- ⇒  $N(|\Psi\rangle)$   
 ~~$\equiv$~~

T-gate teleportation:-

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$T|+\rangle = \frac{1}{\sqrt{2}} [ |0\rangle + e^{i\pi/4} |1\rangle ]$$

$|0\rangle + b|1\rangle$

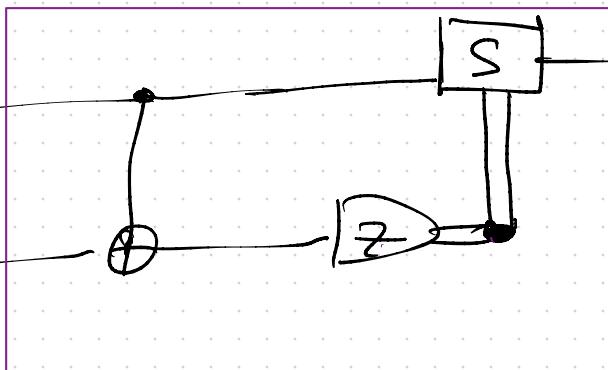
$\uparrow$

$|+\rangle$

$T|+\rangle$

$\equiv T$

resource state



$T|4\rangle$

$=$

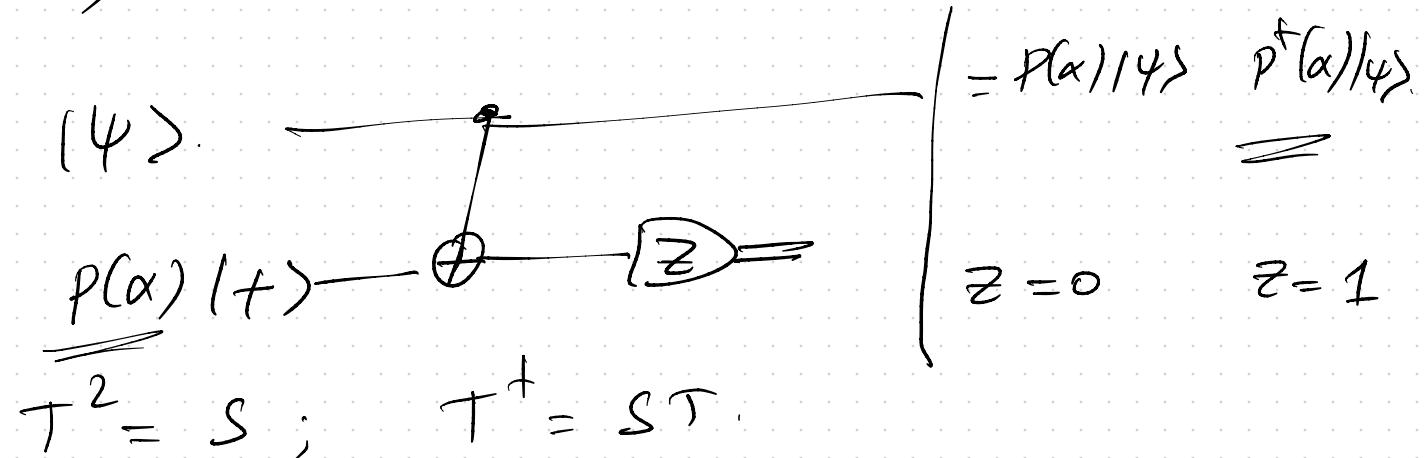
$\downarrow$

T on an  
unknown  
state.

$\downarrow$   
clifford gates  
+ Pauli matri.

This gate teleportation idea can be generalized:  $P(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$

$P(\alpha)|+\rangle$



$$\overline{\overline{P(\alpha)|+>}} \quad T^2 = S ; \quad T^* = ST.$$

