

① Classical Computation: manipulation of bits via logic gates (AND, OR, NOT, XOR).

For input $x \in \{0,1\}^n$, calculate $f(x)$ for some f .

(How to realize f with a circuit? How many gates/depth is necessary and/or sufficient?)

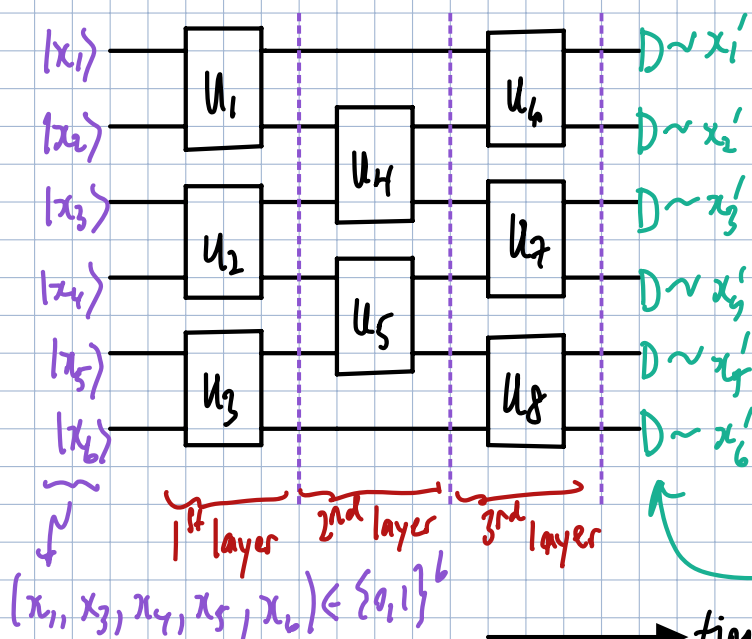
⊛ We rarely think about computation in these terms anymore!

⊛ We program in some high-level language (C++, python, julia) and then the code gets compiled into the machine-level language.

⊛ Quantum computing is still thought about at the gate level.

(Although "quantum programming languages" are being developed - qiskit is a simple example.)

② Quantum Computation: logic gates are unitaries! ($U : U^\dagger U = U U^\dagger = \mathbb{1}$).



⊛ To calculate the output state, multiply the matrices in the correct order.

$$U_8 U_7 U_6 U_5 U_4 U_3 U_2 U_1 |x\rangle$$

Measurement/read-out.

⊛ Observe: H Hermitian $\Rightarrow \left(e^{-iHt} \right)^\dagger = e^{iH^\dagger t} = e^{iHt}$ is unitary!

Tasks : • Classical problems (e.g., factoring, search)

→ How to (best) encode the classical input into the q. computer?

→ Is there an advantage/speedup over known classical algorithms?

(14) • For $x \in \{0,1\}^n$, prepare $U|x\rangle$ for some unitary U .

→ How to realize U as a circuit? (optimally?).

→ Special case: prepare $U|0\rangle^{\otimes n}$ (e.g., ground state of a Hamiltonian)

Recall: $H = \sum_{k=1}^K \lambda_k (I \otimes \dots \otimes X_k \otimes \dots \otimes I)$

"ground state" is an eigenstate corresponding to $\lambda_{\min}(H) \rightarrow$ the smallest eigenvalue of H .

→ Prepare samples from some probability distribution.
(usually the probability distribution (or amplitudes) contains the answer to classical problems).

We want a
"universal gate
set"

③ Quantum gates

* Pauli gates:

$$\text{---} \boxed{X} \text{---} \rightarrow X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (X|0\rangle = |1\rangle, X|1\rangle = |0\rangle)$$

$$\text{---} \boxed{Y} \text{---} \rightarrow Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (Y|0\rangle = i|1\rangle, Y|1\rangle = -i|0\rangle)$$

$$-\boxed{Z}- \rightarrow Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle)$$

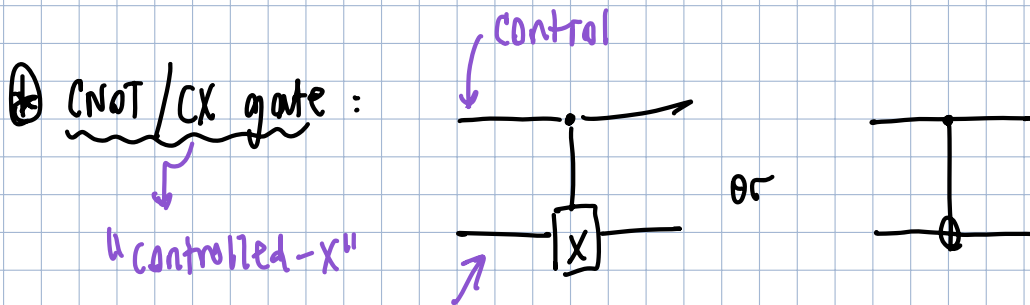
* Hadamard gate: $-\boxed{H}- \rightarrow H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

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

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

* Phase gate: $-\boxed{S}- \rightarrow S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

* T-gate: $-\boxed{T}- \rightarrow T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$



$$CNOT = \begin{matrix} & \begin{matrix} 00 & 01 & 10 & 11 \end{matrix} \\ \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{matrix}$$

target

$$= |0\rangle \otimes |0\rangle \otimes I + |1\rangle \otimes |1\rangle \otimes X$$

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |0\rangle|0\rangle \\ |0\rangle|1\rangle &\mapsto |0\rangle|1\rangle \\ |1\rangle|0\rangle &\mapsto |1\rangle \otimes X|0\rangle = |1\rangle|1\rangle \\ |1\rangle|1\rangle &\mapsto |1\rangle \otimes X|1\rangle = |1\rangle|0\rangle \end{aligned}$$

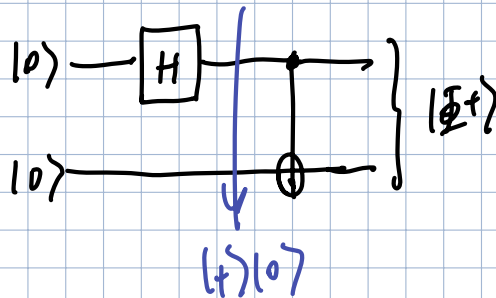
B/c of linearity, this determines the action on any state!

$$|\gamma\rangle = a|0,0\rangle + b|0,1\rangle + c|1,0\rangle + d|1,1\rangle \mapsto a|0,0\rangle + b|0,1\rangle + \underline{c|1,1\rangle} + \underline{d|1,0\rangle}$$

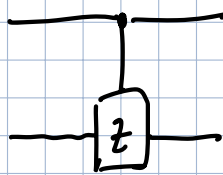
CNOT is an entangling gate

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

$$\text{CNOT}|+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle) = \underline{\underline{|\Phi^+\rangle}}$$



* Controlled-Z / CZ gate :



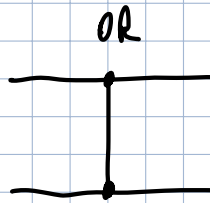
$$|0\rangle|0\rangle \mapsto |0\rangle|0\rangle$$

$$|0\rangle|1\rangle \mapsto |0\rangle|1\rangle$$

$$|1\rangle|0\rangle \mapsto |1\rangle Z|0\rangle = |1\rangle|0\rangle$$

$$|1\rangle|1\rangle \mapsto |1\rangle Z|1\rangle = -|1\rangle|1\rangle$$

$$CZ = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & 0 \\ 0 & & & -1 \end{pmatrix}$$



This is also an entangling gate!

Graph States

$G = (V, E)$ is a graph

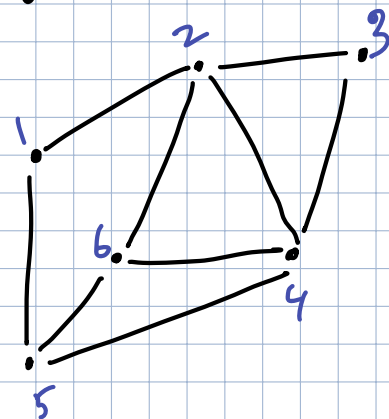
vertices/nodes

edges

Recipe: 1. Every node is a qubit

2. Prepare all qubits in $|+\rangle$

3. If there is an edge b/w



two nodes, apply CZ b/w the corresponding qubits.

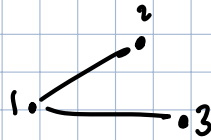
$$|+\rangle^{\otimes n} = \left(\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right)^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle$$

$$CZ |x_1, x_2\rangle = (-1)^{x_1 x_2} |x_1, x_2\rangle$$

$$\Rightarrow |+\rangle^{\otimes n} \mapsto \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{\frac{1}{2} x^T A x} |x\rangle$$

adjacency matrix of graph.

Example:



$$A = \begin{matrix} & \begin{matrix} 1 & 2 & 3 \end{matrix} \\ \begin{matrix} 1 \\ 2 \\ 3 \end{matrix} & \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{matrix}$$

$$|+\rangle|+\rangle|+\rangle = \frac{1}{\sqrt{2^3}} \left(|0\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle \right)$$

$$\mapsto \frac{1}{\sqrt{2^3}} \left(|0\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle - |1\rangle|0\rangle|1\rangle - |1\rangle|1\rangle|0\rangle + (-1)^2 |1\rangle|1\rangle|1\rangle \right)$$

$$= \frac{1}{\sqrt{2^3}} \left(|0\rangle|0\rangle(|0\rangle + |1\rangle) + |0\rangle|1\rangle(|0\rangle + |1\rangle) + |1\rangle|0\rangle(|0\rangle - |1\rangle) - |1\rangle|1\rangle(|0\rangle - |1\rangle) \right)$$

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

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

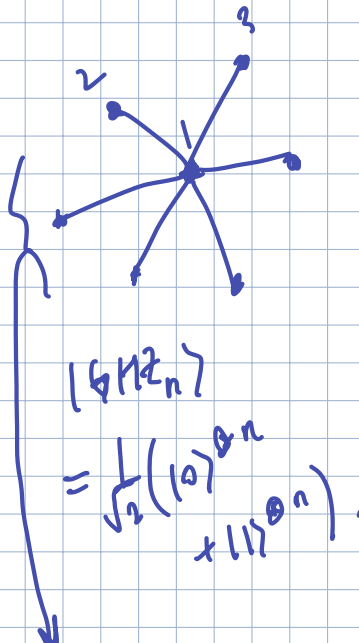
$$= \frac{1}{\sqrt{2}} \left(|0\rangle|+\rangle|+\rangle + |1\rangle|-\rangle|-\rangle \right)$$

$$= (I \otimes H \otimes H) \frac{1}{\sqrt{2}} \left(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle \right)$$

$$|GHZ_{x,z}\rangle = (X^x \otimes Z^z) |GHZ\rangle$$

is an ONB for $(\mathbb{C}^2)^{\otimes 3}$

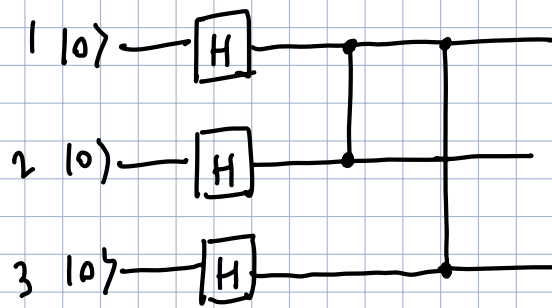
$$|\Phi^f\rangle_{n,n_B} = \frac{1}{\sqrt{2^n}} \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}, \vec{x}\rangle \approx |\Phi^f\rangle_{A,B} \otimes |\Phi^f\rangle_{A,B} \otimes \dots \otimes |\Phi^f\rangle_{A_n B_n}$$



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

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

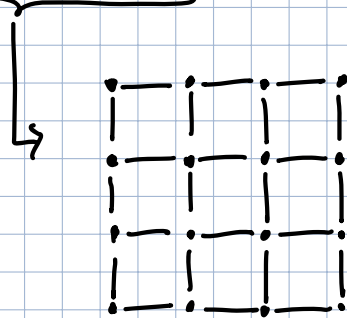
At a circuit:



Star graphs $\longleftrightarrow$ GHZ states.

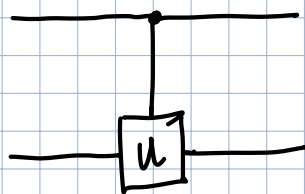
$$\begin{aligned}
 \begin{array}{c} \bullet \\ 1 \end{array} - \begin{array}{c} \bullet \\ 2 \end{array} &\longleftrightarrow |+\rangle|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \\
 &\mapsto \frac{1}{\sqrt{2}} (|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) \\
 &= \frac{1}{\sqrt{2}} (|0\rangle|+\rangle + |1\rangle|-\rangle) \\
 &= (I \otimes H) \underbrace{\frac{1}{\sqrt{2}} (|0\rangle|0\rangle + |1\rangle|1\rangle)}_{|\Phi^+\rangle}
 \end{aligned}$$

Square lattice $\longleftrightarrow$ Cluster states.



⊛ Controlled Unitary

$$CU = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix} = \rightarrow |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.$$

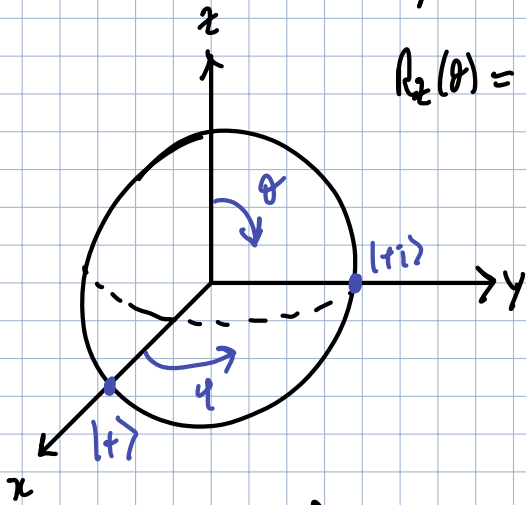


$$\begin{aligned}
 |0\rangle|0\rangle &\mapsto |0\rangle|0\rangle \\
 |0\rangle|1\rangle &\mapsto |0\rangle|1\rangle \\
 |1\rangle|0\rangle &\mapsto |1\rangle U|0\rangle \\
 |1\rangle|1\rangle &\mapsto |1\rangle U|1\rangle
 \end{aligned}$$

(*) Rotation Gates: $R_x(\theta) = e^{-i\frac{\theta}{2}X} \rightarrow$ rotation around X-axis by angle θ .

$R_y(\theta) = e^{-i\frac{\theta}{2}Y} \rightarrow$ rotation around Y-axis by angle θ .

$R_z(\theta) = e^{-i\frac{\theta}{2}Z} \rightarrow$ rotation around Z-axis by angle θ .



$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

$$|+i\rangle: \theta = \pi/2, \varphi = \pi/2$$

$$|+\rangle: \theta = \pi/2, \varphi = 0$$

$$R_z\left(-\frac{\pi}{2}\right)|+i\rangle = \left(\frac{1}{\sqrt{2}}\mathbb{1} + i\frac{1}{\sqrt{2}}Z\right)|+i\rangle$$

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

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

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

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

$$= e^{i\pi/4}|+\rangle \sim |+\rangle \text{ (up to global phase).}$$

$$e^M = \sum_{k=0}^{\infty} \frac{1}{k!} M^k$$

$$\Rightarrow e^{-i\frac{\theta}{2}X} = \sum_{k=0}^{\infty} \frac{1}{k!} \left(-i\frac{\theta}{2}X\right)^k$$

$$\left(\begin{array}{l} X^2 = \mathbb{1} \\ \Rightarrow X^k = \mathbb{1}, k \text{ even} \\ X^k = X, k \text{ odd} \end{array} \right)$$

$$= \sum_{k=0}^{\infty} \frac{1}{(2k)!} \underbrace{\left(-i\frac{\theta}{2}X\right)^{2k}}_{0, 2, 4, k, \dots} + \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} \underbrace{\left(-i\frac{\theta}{2}X\right)^{2k+1}}_{1, 3, 5, 7, \dots}$$

$$= \sum_{k=0}^{\infty} \frac{1}{(2k)!} \left(\frac{\theta}{2}\right)^{2k} \underbrace{(-i)^{2k}}_{\substack{\downarrow \\ (-i)^2 = -i \cdot -i = -1}} \mathbb{1} + \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} \left(\frac{\theta}{2}\right)^{2k+1} (-i)^{2k+1} X$$

$$(-i)^1 = -i \quad (k=0)$$

$$(-i)^3 = \underbrace{-i \cdot -i \cdot -i}_{-1} = i \quad (k=1)$$

$$(-i)^5 = -i \quad (k=2)$$

$\vdots$

$$(-i)^{2k+1} = -i(-1)^k$$

$$(-i)^2 = -i \cdot -i = -1 \quad (k=1)$$

$$(-i)^4 = ((-i)^2)^2 = 1 \quad (k=2)$$

$$(-i)^6 = -1 \quad (k=3)$$

$\vdots$

$$(-i)^{2k} = (-1)^k$$

$$\begin{aligned}
 &= \sum_{k=0}^{\infty} \frac{1}{(2k)!} \left(\frac{\theta}{2}\right)^{2k} (-1)^k \mathbb{1} - i \sum_{k=0}^{\infty} \frac{1}{(2k+1)!} \left(\frac{\theta}{2}\right)^{2k+1} (-1)^k X \\
 &\quad \underbrace{\hspace{10em}}_{\cos(\frac{\theta}{2})} \quad \underbrace{\hspace{10em}}_{\sin(\frac{\theta}{2})} \\
 &\downarrow \\
 &= \cos\left(\frac{\theta}{2}\right) \mathbb{1} - i \sin\left(\frac{\theta}{2}\right) X
 \end{aligned}$$

⊛ Similar argument to show $R_Y(\theta) = e^{-i\frac{\theta}{2}Y} = \cos\left(\frac{\theta}{2}\right)\mathbb{1} - i\sin\left(\frac{\theta}{2}\right)Y$

$$R_Z(\theta) = e^{-i\frac{\theta}{2}Z} = \cos\left(\frac{\theta}{2}\right)\mathbb{1} - i\sin\left(\frac{\theta}{2}\right)Z$$

⊛ Note: $R_Z(\theta) = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$ $\left(\cos\left(\frac{\theta}{2}\right) \pm i\sin\left(\frac{\theta}{2}\right)\right) = e^{\pm i\frac{\theta}{2}}$

$$R_Z\left(\frac{\pi}{2}\right) = \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 \\ 0 & \underbrace{e^{i\pi/2}}_i \end{pmatrix} = e^{-i\frac{\pi}{4}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \sim \text{gate! (up to global phase).}$$

④ Clifford gates $\longrightarrow$ Important class of gates!

Quantum Error Correction Via Codes Over GF(4)

A. Robert Calderbank, *Fellow, IEEE*, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane, *Fellow, IEEE*

Surviving as a Quantum Computer in a Classical World

Daniel Gottesman (Chapter 6).

May 7, 2024

<http://www.cs.umd.edu/class/spring2024/cmsc858G/QECCbook-2024-ch1-15.pdf>

Clifford group

Maris Ozols

July 31, 2008

- Recall Pauli operators on n qubits: $\mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n} \rightarrow 4^n$

$\rightarrow$ Let $\mathcal{P}_n^* = \mathcal{P}_n \setminus \{I^{\otimes n}\}$

- Define the n -qubit Clifford group as

$$\mathcal{C}_n := \{ U : P \in \pm \mathcal{P}_n^* \Rightarrow U P U^\dagger \in \pm \mathcal{P}_n^* \} / U(1)$$

$\rightarrow$ mod out global phase

$\rightarrow$ Transforms Paulis to Paulis!
(up to sign)

⊛ There are other ways to define it! (See Gottesman book).

- Examples: Consider the Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$H X H = Z, \quad H Y H = -Y, \quad H Z H = X$$

$$\Rightarrow \underline{\underline{H \in \mathcal{C}_1!}}$$

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \rightarrow S X S^\dagger = Y, \quad S Y S^\dagger = -X, \quad S Z S^\dagger = Z$$

$$\Rightarrow \underline{\underline{S \in \mathcal{C}_1!}}$$

$$CNOT = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & 1 \\ & & 1 & 0 \end{pmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$\begin{aligned} X \otimes I &\mapsto X \otimes X \\ Z \otimes I &\mapsto Z \otimes I \\ I \otimes X &\mapsto I \otimes X \\ I \otimes Z &\mapsto Z \otimes Z \end{aligned}$$

$$\begin{aligned}
 Z \otimes X &= (Z \otimes I)(I \otimes X) \mapsto \text{CNOT}(Z \otimes I)(I \otimes X)\text{CNOT} \\
 &= \underbrace{\text{CNOT}(Z \otimes I)\text{CNOT}}_{Z \otimes I} \underbrace{\text{CNOT}(I \otimes X)\text{CNOT}}_{I \otimes X} \xrightarrow{=I} \\
 &= Z \otimes X
 \end{aligned}$$

$\Rightarrow \underline{\underline{\text{CNOT} \in \mathcal{C}_2}}$!

- Size of $\mathcal{C}_n$:

n	1	2	3	4	5
$ \mathcal{C}_n $	24	11520	92897280	12128668876800	25410822678459187200

$$|\mathcal{C}_n| = \prod_{j=1}^n 2(4^j - 1)4^j = 2^{n^2+2n} \prod_{j=1}^n (4^j - 1).$$

- Theorem: $\mathcal{C}_n = \langle H_i, S_i, \text{CNOT}_{i,j} : i, j \in \{1, 2, \dots, n\} \rangle / \langle I \rangle$

⊛ H, S, CNOT are generators of the Clifford group!

⊛ (Take all possible products of H, S, CNOT , and ignore global phase.)

Proof: See Sec. 6.3 of Gottesman book (requires some additional math).

- Theorem (Gottesman-Knill): Circuits consisting of only Clifford gates can be simulated classically in poly time.

⊛ In particular, Clifford gates are not universal!

PHYSICAL REVIEW A 70, 052328 (2004)

arXiv:quant-ph/0406196

Improved simulation of stabilizer circuits

Scott Aaronson*

Computer Science Department, University of California, Berkeley, California 94720, USA

Daniel Gottesman[†]

Perimeter Institute, Waterloo, Canada N2L 2Y5

(Received 25 June 2004; published 30 November 2004)

- Theorem: Clifford gates + one single-qubit non-Clifford gate is universal!