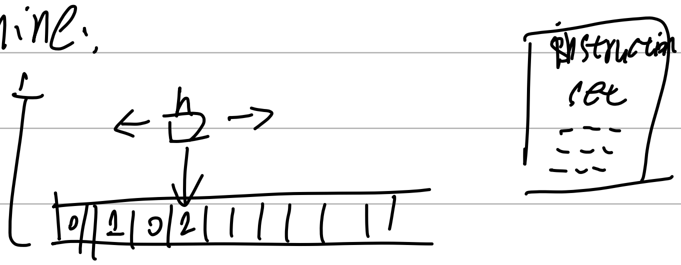
Computation
- Time complexity. ← $O(n^2)$
- Space complexity. ←

Classical Setting: (Comp. model)

- Turing Machine:

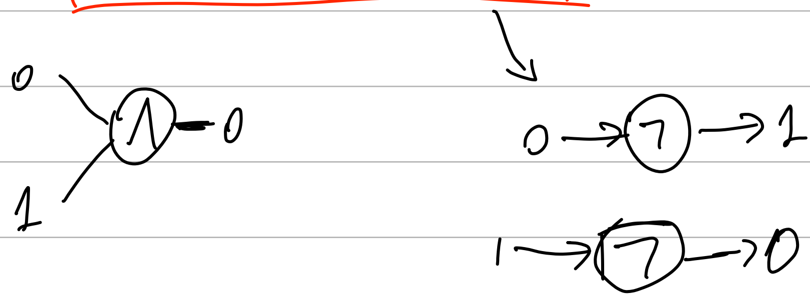


- Boolean Circuit:

Universal set of instructions

gates: AND, OR, NOT

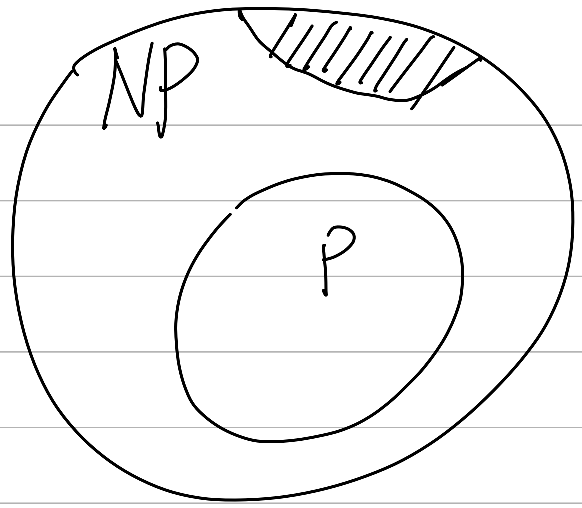
CPU instruction set



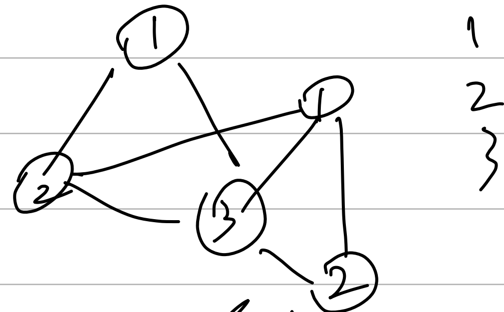
$f(x) = x^2 + 3x$ $\quad f(x) = e^x$

Boolean function:

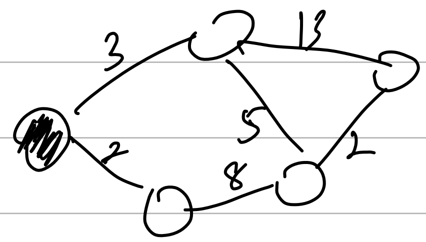
$$\begin{array}{ccc} f: \{0,1\}^n & \longrightarrow & \{0,1\}^m \\ \in & & \in \\ x & \longmapsto & f(x) \end{array}$$

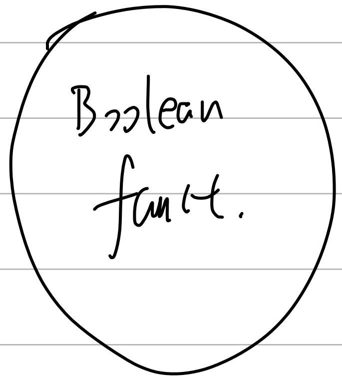


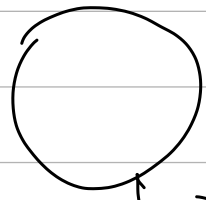
Graph 3 Coloring.



Traveling Salesman Problem







→ poly-sized Circuits using {AND, OR, NOT}

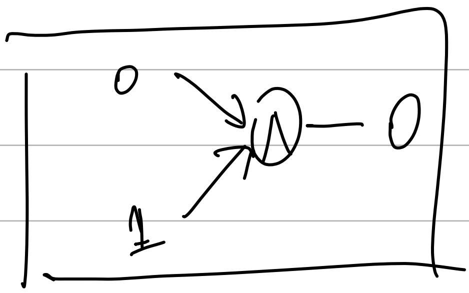
Quantum Circuits Model:

- Question 1: Do we still have a universal set of instructions?

- Question 2: How do we do approximation?

- Question 3: Is quantum computing a superset of classical computing?

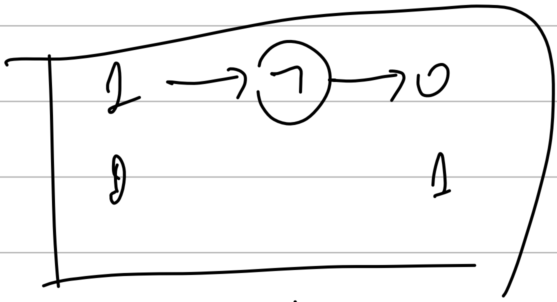
Question 3:



classical

$\Longrightarrow$ $\nexists$ unitary U s.t.

$$\underbrace{|a\rangle|b\rangle \xrightarrow{U} |a\wedge b\rangle}_{\text{quantum}}$$

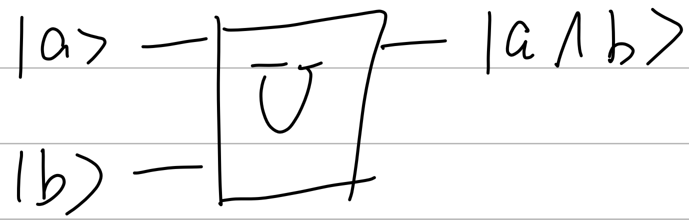


classical

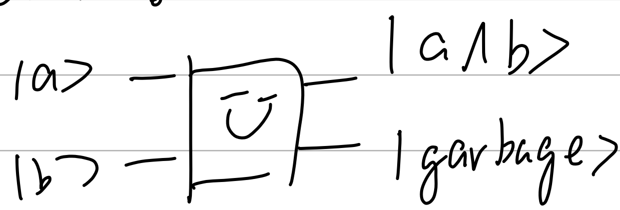
$$|0\rangle \to \boxed{X} \to |1\rangle$$
$$|1\rangle \qquad\qquad |0\rangle$$

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

$\nexists$ unitary U s.t.

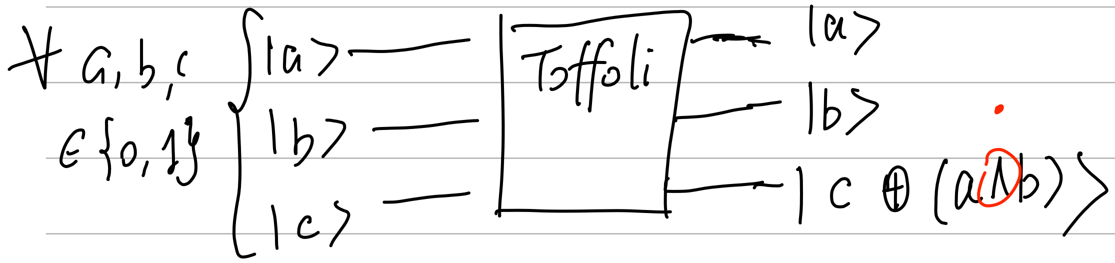


How about?



$[\ ]_{4\times1}$ $\qquad$ $[\ ]_{4\times2}$

Further Relaxed: there exists a unitary gate



$|0\rangle$ $\qquad$ $|0 \oplus (a \wedge b)\rangle = |a \wedge b\rangle$

$$|a\rangle = [\ \ ]_{2\times1} \qquad |b\rangle = [\ \ ]_{2\times1} \qquad |c\rangle = [\ \ ]_{2\times1}$$

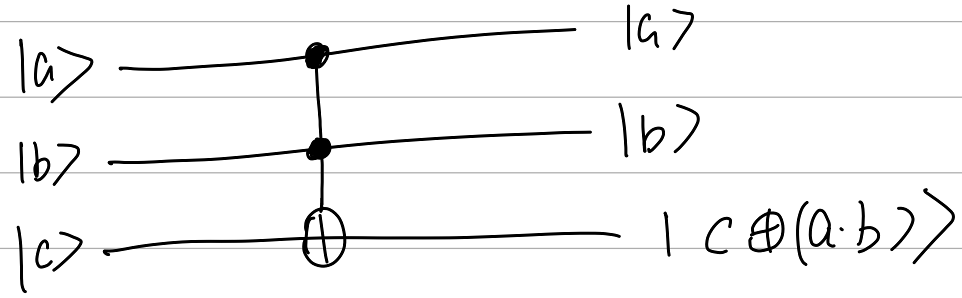
$$|a\rangle|b\rangle|c\rangle \qquad [\ \ ]_{2\times2} \otimes [\ \ ]_{2\times2} \otimes [\ \ ]_{2\times1}$$

$$2\times1 \otimes 2\times2 \otimes 2\times2$$

7x7 Identity

$$\text{Toffoli} = \left[\begin{array}{cc} \boxed{\begin{matrix}1 & & & 0\\ & 1 & & \\ & & 1 & 1\end{matrix}} & \begin{matrix}0&0\\0&0\\0&0\\0&0\end{matrix} \\ \begin{matrix}0 & 0 & 0\ 0\\ 0 & 0 & \cdots\end{matrix} & \begin{matrix}0&1\\1&0\end{matrix}\end{array}\right]_{8\times8} \Big[\ \ \Big] = \Big[\ \ \Big]_{8\times1}$$

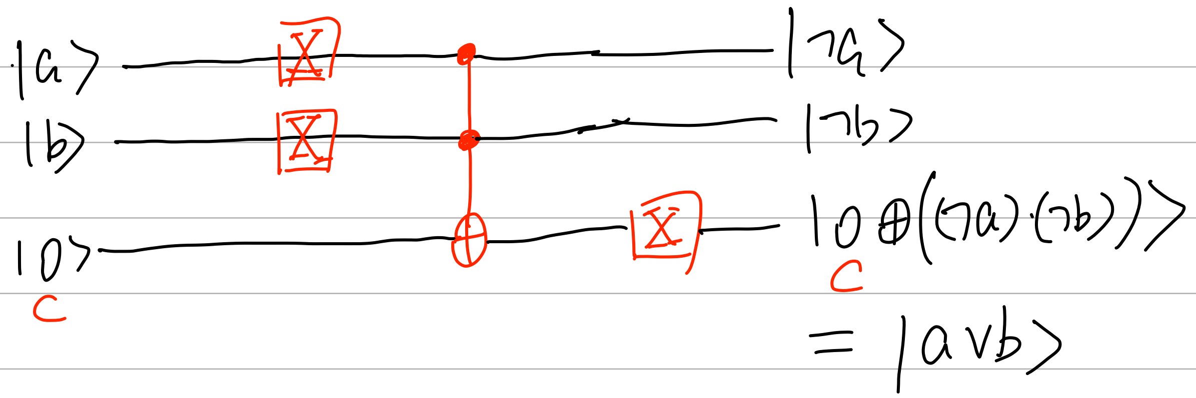
Toffoli Circuit in diagram form.



{NAND}

→ {AND, OR, NOT} has redundancy:

$$a \vee b = \underbrace{\neg(\neg a \wedge \neg b)}$$



Remark:

① Our quantum emulation of classical circuits is efficient. (It's linear $O(n)$ in the original classical circuit size)

② The purpose here is to replicate the classical basic gates. It requires careful analysis to determine the behavior of those circuits over truly quantum input.

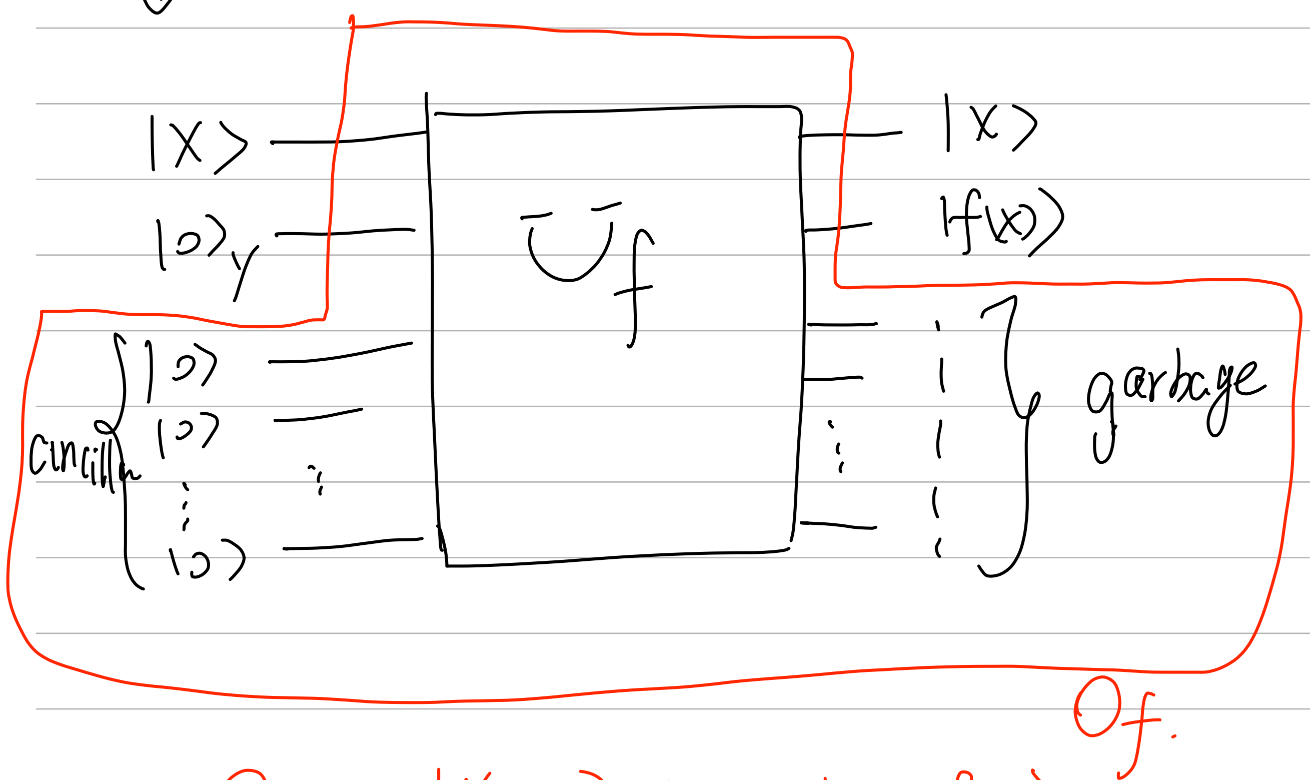
Reversible Computing:

In general: given a classical function f.
we can build a quantum circuit U_f that "agrees with f on every classical input", with the help of ancilla qubits:

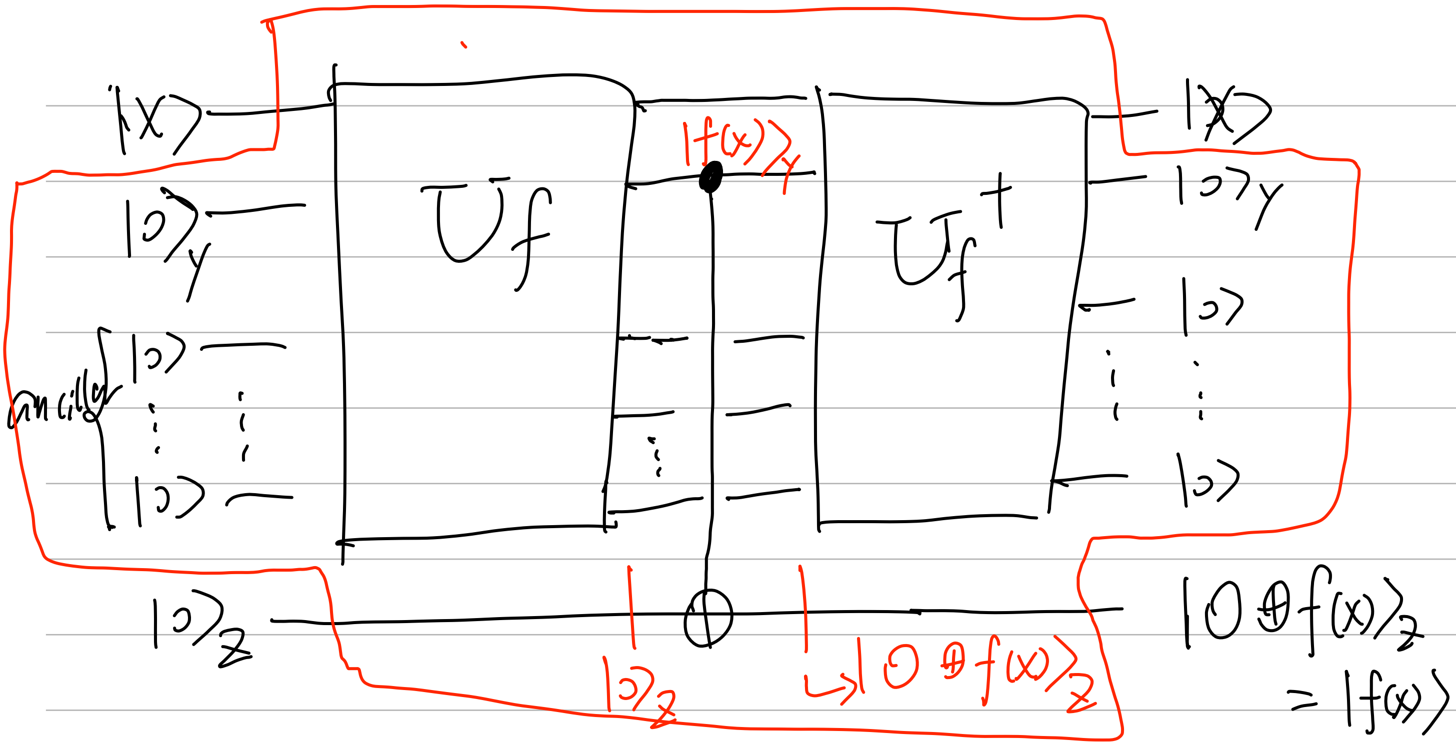
$$f: x \longmapsto f(x)$$

$$U_f: |x\rangle|0\rangle_y \underbrace{|0 \dots 0\rangle}_{\text{ancilla}} \longmapsto |x\rangle|f(x)\rangle_y \underbrace{|\text{garbage}\rangle}_{\text{ancilla.}}$$

$\downarrow$



$$O_f: |x, 0\rangle \longmapsto |x, f(x)\rangle$$



$$CNOT: |a\rangle_y |c\rangle_z \longmapsto |a\rangle_y |c \oplus a\rangle_z$$

$\forall\ x, z \in \{0,1\}^*$

$$O_f : |x\rangle|z\rangle \longmapsto |x\rangle|z \oplus f(x)\rangle$$

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

$$\Big\downarrow O_f$$

$$O_f \cdot |x\rangle|-\rangle = O_f \cdot |x\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right)_z$$

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

$$= \frac{1}{\sqrt{2}} O_f |x, 0\rangle - \frac{1}{\sqrt{2}} O_f |x, 1\rangle$$

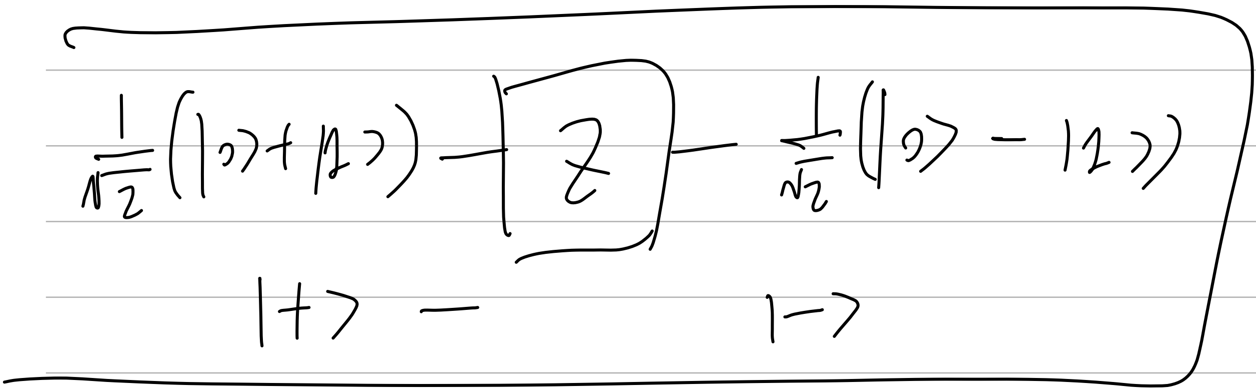
$$= \frac{1}{\sqrt{2}} |x, f(x)\rangle - \frac{1}{\sqrt{2}} |x, 1 \oplus f(x)\rangle$$

(If f has a binary output) $= |x\rangle \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |1 \oplus f(x)\rangle\right)$

$$= \begin{cases} |x\rangle|-\rangle & f(x)=0 \\ -|x\rangle|-\rangle & f(x)=1 \end{cases}$$

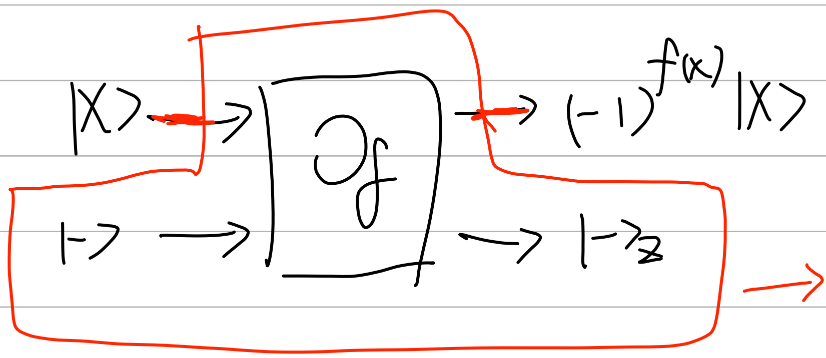
$$= (-1)^{f(x)}|x\rangle|-\rangle$$

"Phase kickback" trick



Summarize: when $f: \{0,1\}^n \to \{0,1\}$

$$O_f: |x\rangle\underbrace{|-\rangle}_{2} = (-1)^{f(x)}|x\rangle\underbrace{|-\rangle}_{2}$$



→ Phase Oracle

PhO_f

★ $PhO_f: |x\rangle \mapsto (-1)^{f(x)}|x\rangle$

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

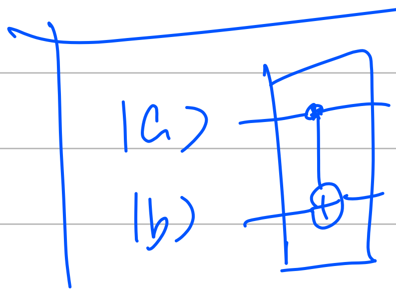
– Does there exist a finite set of quantum operations that allows us to approximate any unitary operator to our desired accuracy?

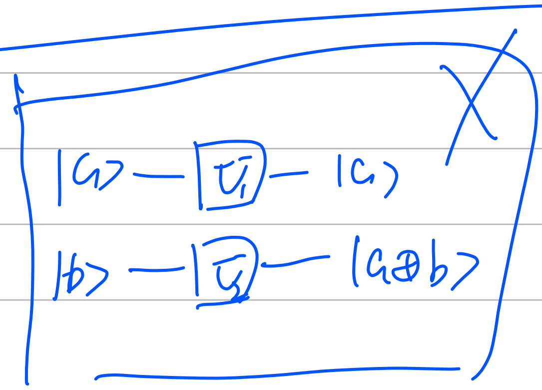
Theorem ("1+2" theorem):

$$\left.\begin{array}{l} \text{All 1-qubit gates} \\ \quad + \\ \text{one 2-qubit "entangling" gate} \end{array}\right\} \text{"basic" gates}$$

⇒ compute any unitary operation.

It requires $O(n^2 4^n)$ basic gates to compute a $2^n \times 2^n$ unitary.





Historical remark:

① "H2" Theorem was stated without a proof in:

[Kaye, Laflamme, Mosca:
An intro to Quantum Computing
Oxford Univ. press, 2006
as [Theorem 4.3.3.]]

The earlest proof is in

[Bremmer et al.:
Practical scheme for quantum computation
with any two qubit entangling qubit.
Physics Review Letter, (PRL2002)]

What to do with the infinite set of "All 1-qubit gate"?

— Solution: Solovay-Kitaev Theorem.

Solovay - Kitaev Thm:

Let Γ be a set of 1-qubit unitaries such that:

① Γ generates a dense subgroup of $SU(2)$.

② Γ is closed under inverse.

Then, any 1-qubit unitary in $SU(2)$ can be ε-approximated by a product of at most $O(\log^c \frac{1}{\varepsilon})$ gates from Γ, where $c \approx 2$.

$$\varepsilon = \frac{1}{2^n} \qquad \left(\log^c \frac{1}{\varepsilon}\right)$$

$$= \log^c 2^n$$

$$= n^c \cdot \log 2$$

$$= n^c$$

① $\mathcal{U}(2)$: 2×2 unitary matrices, (over $\mathbb{C}$)

$SU(2)$: 2×2 unitary matrices <u>with determinant 1</u>

claim: $A \in \mathcal{U}(2) \Rightarrow |\det(A)| = 1$

↳ Property of $\det(\cdot)$:

$$\det(B\cdot C) = \det(B)\cdot \det(C)$$

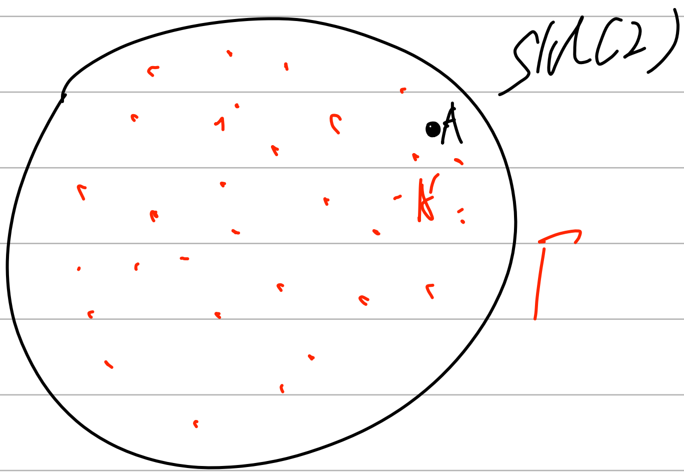
$$\det(A^{\dagger}) = \overline{\det(A)}$$

$A \in \mathcal{U}(2)$:

$$|\det(A)| = 1 \not\Rightarrow \det(A) = 1 \Leftrightarrow A \in SU(2)$$

$$|\det(A)| = 1 \Rightarrow \underline{\det(A) = e^{i\theta}} \quad \theta \in [0, 2\pi)$$

$$B \in SU(2) \Rightarrow \underline{\det(B) = 1}$$



$\forall A \in SU(2)$

$\exists A' \in \Gamma$

s.t. $\underbrace{\|A - A'\|}_{} \le \varepsilon$

$$\forall\, |\psi\rangle \in \mathbb{C}^2$$

$$\| A|\psi\rangle - A'|\psi\rangle \|_{tr} \leq \varepsilon$$

Examples of Universal gate sets:

$$T := \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \quad \frac{\pi}{8}\text{-gate}$$

$$S := T^2 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$P_\theta := \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \quad \begin{cases} P_{\frac{\pi}{2}} = S \\ P_{\frac{\pi}{4}} = T \end{cases}$$

$\{\overbrace{H, T}^{P}, CNOT\}$ is universal.

$\{H, S, \text{Toffoli}\}$ is also universal.