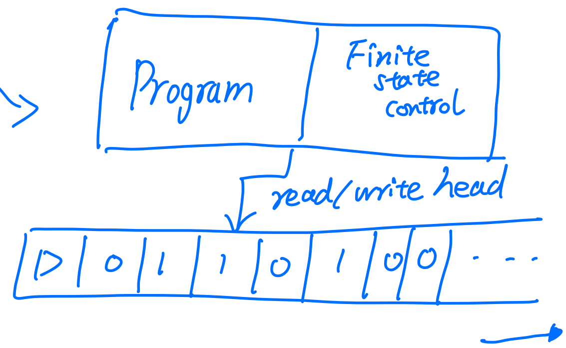
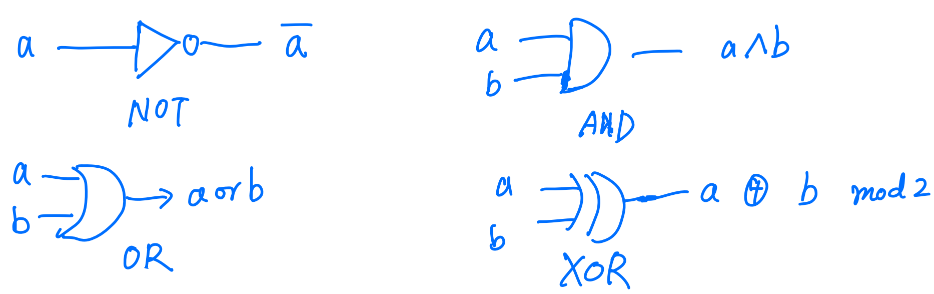
Computation model — Turing Machine / Circuits

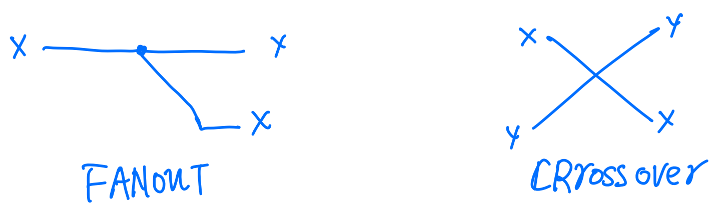


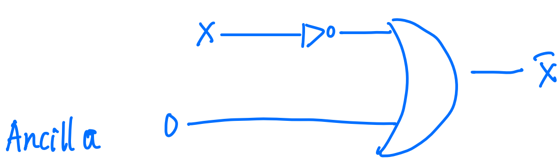
wires : carry information (binary bits)

gates : simple computational tasks

e.g.







Circuit $\Longleftrightarrow$ Turing model

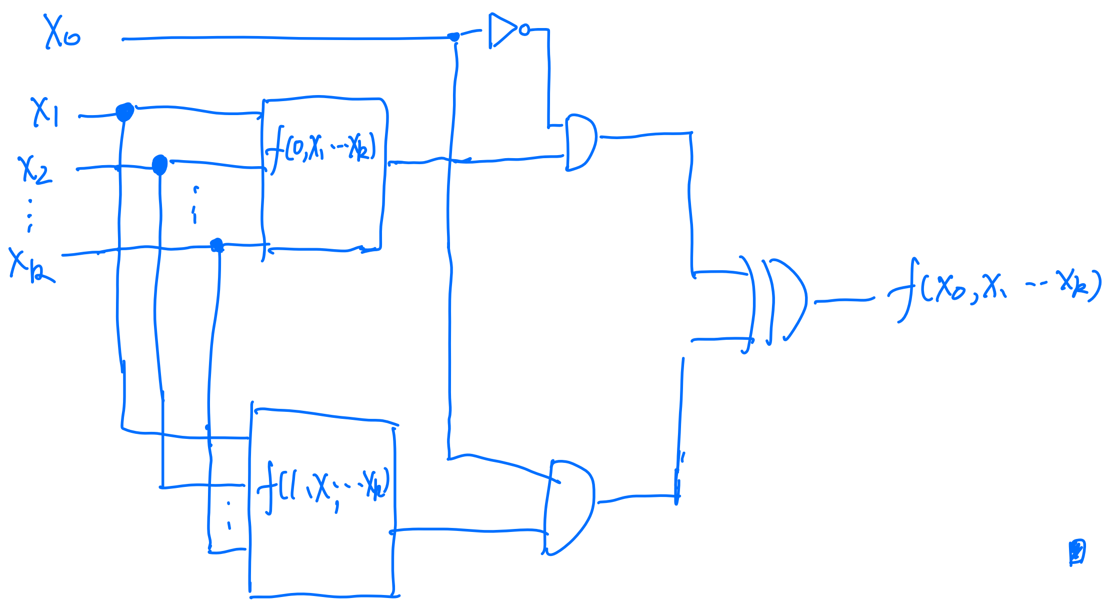
Any logic gate $f: \{0,1\}^n \longrightarrow \{0,1\}^m$ can be realized as circuit

Pf: Sufficient to consider $f: \{0,1\}^n \to \{0,1\}$ Boolean Function.

Induction on n. ① $n=1$: $f \equiv 1$ $f \equiv 0$, $f(x) = x$ $f(x) = \bar{x}$

② Assume $n=k$. For $n=k+1$,

$$f(x_0 \cdots x_k) = \begin{cases} f(0, x_1 \cdots x_k) & \text{if } x_0 = 0 \\ f(1, x_1 \cdots x_k) & \text{if } x_0 = 1 \end{cases}$$



Universal circuit construction:

① Wires ② ancilla ③ FANOUT ④ crossover ⑤ AND OR NOT

Quantum circuit

State space $H = (\mathbb{C}^2)^{\otimes n}$ n qubits

computational basis $\{ |x_1 \cdots x_n\rangle \mid x_i \in \{0,1\} \} \cong \{0,1\}^n$

$|0101\rangle \longleftrightarrow 0101$

Wire $|\varphi\rangle$ ———— $|\varphi\rangle$

Ancilla $|0\rangle$ ————

Unitary Operations: $|\varphi\rangle - \boxed{U} - U|\varphi\rangle$ (In computational model, we assume our gate are ideal, no noise, given by unitary)

① Single qubit gates

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

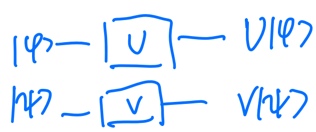
Theorem: $\forall$ unitary $U \in M_2$, $\exists\ \alpha, \beta, \gamma, \delta \in \mathbb{R}$, s.t.

$$U = e^{i\alpha} e^{i\beta X} e^{i\gamma Y} e^{i\delta Z}$$

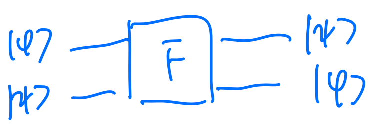
Pf: $$U = e^{i\alpha} \begin{bmatrix} e^{-i(\beta+\delta)} \cos\gamma & -e^{i(\delta-\beta)} \sin\gamma \\ e^{i(\beta-\delta)} \sin\gamma & e^{i(\beta+\delta)} \cos\gamma \end{bmatrix}$$

Multiple qubits gate

Product gate $U \otimes V$, $U \in M_2$, $V \in M_2$



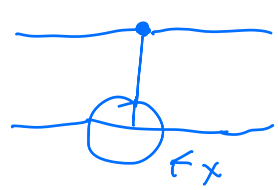
Swap gate



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

(non entangling)

Controlled - Not

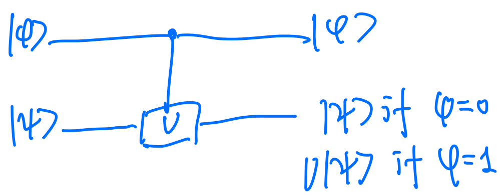


00	00
01	01
10	11
11	10

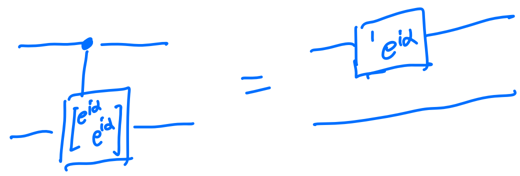
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad |+\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \longrightarrow \frac{1}{\sqrt{2}} |00\rangle + |11\rangle = |\Phi^+\rangle$$

entangling

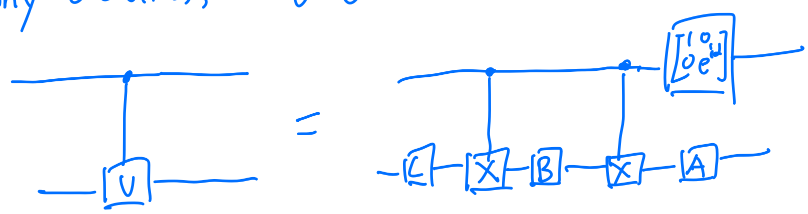
Controlled-U



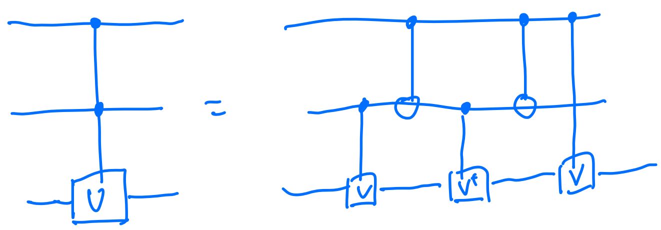
Controlled phase shift



Any $U \in U(M_2)$, $U = e^{i\alpha} AXBXC$ so



Conditional on More qubits



$V^2 = U$

No-cloning Theorem ① There is no quantum gate cloning a qubit $U|\varphi\rangle = |\varphi\rangle|\varphi\rangle$ for $\forall |\varphi\rangle \in \mathbb{C}^2$.

Pf: Suppose $U|0\rangle = |0\rangle \otimes |0\rangle$ $\quad U|1\rangle = |1\rangle \otimes |1\rangle$

$U|+\rangle = U(\frac{1}{\sqrt{2}}|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |+\rangle|+\rangle$

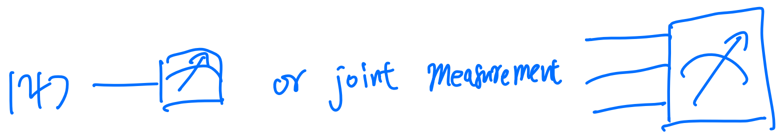
② There is no quantum channel $\Phi(\rho) = \rho \otimes \rho \ \forall \rho \in M_n$

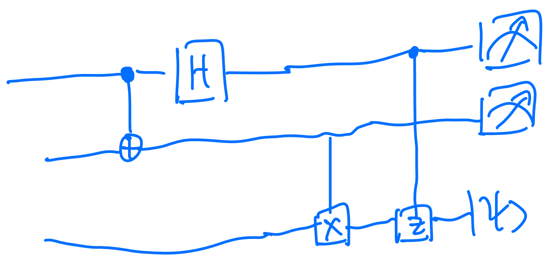
Pf: Suppose $\Phi(\rho) = \rho \otimes \rho$ $\quad \Phi(\sigma) = \sigma \otimes \sigma$ $\quad \Phi(\frac{1}{2}\rho + \frac{1}{2}\sigma) = \frac{1}{2}\rho \otimes \rho + \frac{1}{2}\sigma \otimes \sigma$

Quantum Theory is linear!

Principle 1: Classical control operation $\rightsquigarrow$ quantum control operation

Principle 2: Any unterminated wires at the end of circuit can be assumed to be measure.





Since there is no-cloning, a measurement will destroy the quantum states.

Universal gate set

A set of unitary gate $S \subseteq \bigcup_{n=1}^{\infty} U(\mathbb{C}^{2^n})$ is universal if

$$\overline{\langle S \rangle} = \bigcup_{n=1}^{\infty} U(\mathbb{C}^{2^n})$$

where $\langle S \rangle = \{ U_1 U_2 \cdots U_m \mid \forall m \in \mathbb{N},\ U_i \in S \}$

Namly, $\forall$ n qubit gate $U \in U(\mathbb{C}^{2^n})$, $\forall \varepsilon > 0$ $\exists$

$$\| U_1 \cdots U_m - U \| < \varepsilon, \quad U_i \in S$$

Here $\|X\| = \sup_{|h\rangle \in H} \frac{\| X|h\rangle \|}{\| |h\rangle \|}$.

Universal gate set

① All 2-level unitarys : $\begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & a & & b & \\ & & & 1 & & \\ & & c & & d & \\ & & & & & 1 \end{bmatrix}$

Fact : $\forall \; U \in U(\mathbb{C}^n)$

$$U = U_1 \cdots U_n \qquad U_i \text{ 2-level unitary}$$

Proof : Gaussian Elimination

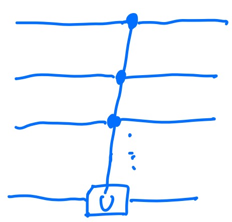
$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \xrightarrow{U_1} \begin{bmatrix} a & 0 & c \\ d & e & f \\ g & h & i \end{bmatrix} \xrightarrow{U_2} \begin{bmatrix} a & 0 & 0 \\ d & e & f \\ g & h & i \end{bmatrix}$$

|| b/c unitary

$$\begin{bmatrix} a & 0 & 0 \\ 0 & e & f \\ 0 & h & i \end{bmatrix}$$

② Single qubit gates + CNOT.

$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & a & b \\ & & & c & d \end{bmatrix}$ =

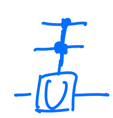


is achievable

In general, $\begin{bmatrix} 1 & & & & & \\ & 1 & & & & \\ & & a & \cdots & b & \\ & & \vdots & 1 & \vdots & \\ & & c & \cdots & d & \\ & & & & & 1 \end{bmatrix}$ Can be converted to $\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & a & b \\ & & & c & d \end{bmatrix}$

using a sequence of Control^2 – Not

For example $\begin{bmatrix} a & & & & & & & b \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & 1 & \\ c & & & & & & & d \end{bmatrix}$ 8x8



$|000\rangle \to |100\rangle \to |110\rangle \longrightarrow U|110\rangle$

$|111\rangle \to |111\rangle \to |111\rangle \longrightarrow U|111\rangle$

③ $\left\{ \underset{H}{\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}}, \underset{T}{\begin{bmatrix} e^{i\frac{\pi}{8}} & \\ & e^{-i\frac{\pi}{8}} \end{bmatrix}}, \underset{S}{\begin{bmatrix} 1 & \\ & i \end{bmatrix}}, \text{CNOT} \right\}$ discrete

Sufficient to show $\overline{\langle H, T, S \rangle} = U(M_2)$

$$T = e^{-i\frac{\pi}{8}Z}, \quad HTH = e^{-i\frac{\pi}{8}X}$$

$$e^{-i\frac{\pi}{8}Z} e^{-i\frac{\pi}{8}X} = R_{\vec{n}}(\theta) \quad \text{for } n = (\cos\tfrac{\pi}{8}, \sin\tfrac{\pi}{8}, \cos\tfrac{\pi}{8})$$

$$R_{\vec{n}}(\theta) = e^{-i\theta \vec{n}\cdot\vec{\sigma}/2} \qquad \cos(\theta/2) = \cos^2\tfrac{\pi}{8}$$

$\frac{\theta}{2\pi}$ irrational

$\vec{n}\cdot\vec{\sigma} = n_1 X + n_2 Y + n_3 Z$

Since θ is irrational. $\{\theta^n \bmod 2\pi \mid n \in \mathbb{Z}\}$ dense in $[0, 2\pi]$

So we can approximate $R_{\vec{n}}(\alpha)$ for $\forall \alpha \in [0, 2\pi]$.

$$H R_{\hat{n}}(\alpha) H = R_{\hat{m}}(\alpha) \qquad \vec{m} = \langle \cos\tfrac{\pi}{8}, -\sin\tfrac{\pi}{8}, \cos\tfrac{\pi}{8} \rangle$$

$\forall\, U \in U(M_2)$, $\quad U = R_{\hat{n}}(\beta) R_{\hat{m}}(\gamma) R_{\hat{n}}(\delta)$ for some β, γ, δ

How many gates needed to approximate a generic $U \in U(\mathbb{C}^{2^n})$

Exponentially many!

Suppose we have g many gates, each on f qubits, in total we have $\left[\begin{smallmatrix} n \\ f \end{smallmatrix}\right]^g$ gates

For a circuit of m gates, we have $\left[\begin{smallmatrix} n \\ f \end{smallmatrix}\right]^{gm} = O(n^{fgm})$ many different unitary

All pure states in $\mathbb{C}^{2^n}$ = unit complex sphere $S^{2^n} = \{(z_1 \cdots z_n) \mid |(z_1 \cdots z_n)| = 1\}$

A ε-neighborhood in S^{2^n} $\quad B_\varepsilon(\varphi) = \{|\psi\rangle \in S^{2^n} \mid d(\varphi, \psi) \le \varepsilon\}$

$\forall |\varphi\rangle \in S^{2^n}$, one need at lease one unitary U s.t. $d(\varphi, \psi) \le \varepsilon$

$$\frac{A(S^{2^n})}{A(B_\varepsilon(\varphi))} = \frac{\sqrt{\pi}\,\Gamma(2^n - \frac{1}{2})(2^{n+1} - 1)}{\Gamma(2^n)\varepsilon^{2n+1} - 1}$$

Since $\Gamma(2^n - \frac{1}{2}) \ge \Gamma(2^n)/2^n$, we need

$$\Omega\left(\frac{1}{\varepsilon^{2^{n+1}} - 1}\right)$$

unitary. If $O(n^{fgm}) \ge \Omega\left(\frac{1}{\varepsilon^{2n+1} - 1}\right) \Rightarrow m = \Omega\left(\frac{2^n \log(1/\varepsilon)}{\log n}\right)$

many gates

Summary of quantum circuit

① Classical Resource: classical registor and computer

② Quantum State space (register): $(\mathbb{C}^2)^{\otimes n}$ $\quad$ n qubits

③ State preparation: $x_1 \cdots x_n \longmapsto |x_1 \cdots x_n\rangle$

bit string $\qquad$ computational basis

encode classical data into quantum register

④ Quantum gate: arbitrary U on $(\mathbb{C}^2)^{\otimes n}$
via universal gate set

⑤ Measurement: Usually in computational basis
read-off computational result to classical message.