Quantum Computation

Thursday, May 7, 2020 9:52 AM

§ 4.1. Models for Quantum Computation

1. Classical circuit model

Computation : $\boxed{\text{input}} \longrightarrow \boxed{\text{Output}}$

$f: \{0,1\}^n \longrightarrow \{0,1\}^m$

$f \equiv (f_0, f_1, \cdots, f_{m-1})$ m binary functions

$\Rightarrow$ reduce to decision problem

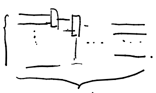
Classical Universality:

Any decision function can be decomposed as a sequence of elementary gates.

$\wedge\ \vee\ \neg$. COPY.

Circuit Model. $d \times w$. Complexity

width



Depth

2. Quantum Computation

$\boxed{\text{input}} \xrightarrow{\text{Compute}} \boxed{\text{Output}} \longrightarrow \boxed{\text{measurement}}$

$|\psi_{in}\rangle \xrightarrow{\mathcal{U}} |\psi_{out}\rangle \longrightarrow \mathcal{M}$

$\rho_{in} \xrightarrow{\hat{\$}} |\rho_{out}\rangle \longrightarrow$ POVM

with ancilla

in extended space

$|\psi'_{in}\rangle \xrightarrow{\mathcal{U}'} |\psi'_{out}\rangle \longrightarrow \mathcal{M}$.

All can be reduced to: $|0\rangle^{\otimes n} \xrightarrow{\mathcal{U}_{prep.}} |\psi_{out}\rangle$ measure in Z basis $\{Z_1, Z_2, \cdots, Z_n\}$

Zero state

Requirement:

1) State preparation of $|0\rangle^{\otimes n}$

2) ancilla in state $|0\rangle$ available

3) Measurement in Z basis

4) Achieve any unitary transformation $\mathcal{U}$.

3. Elementary Quantum Gates.

Single-bit $\mathcal{U}_{(2\times2)} = e^{i\alpha} \begin{pmatrix} \cos\theta & -\sin\theta e^{i\phi} \\ \sin\theta e^{i\phi} & \cos\theta \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{i\beta} \end{pmatrix}$

$\Rightarrow$ A discrete set of gates:

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Hadamard $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $\begin{cases} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$

Phase gate $S = \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$.

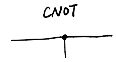
$\frac{\pi}{8}$ - gate $T = \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{8}} \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}$.

Two-bit gate $\mathcal{U}_{(4\times4)}$.

$|00\rangle \to |00\rangle$ first bit: control.

$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}$

CNOT



control

Two - bit gate $\mathcal{U}(4\times4)$.

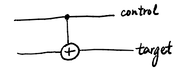
CNOT gate (C-X)

$$\begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{cases}$$

first bit : control.
second bit : target

$$C_{12} = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & & 1 \\ & & 1 & \end{pmatrix}$$

CNOT

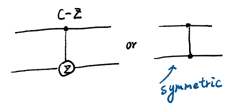


CPF (controlled phase flip) (C-Z)

$$\begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |10\rangle \\ |11\rangle \to -|11\rangle \end{cases}$$

$$C\text{-}Z = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

C-Z



In general. $C\mathcal{U}$ gate

$$C\mathcal{U} = |0\rangle_1\langle 0| \otimes I_2 + |1\rangle_1\langle 1| \otimes \mathcal{U}_2$$

SWAP

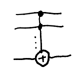
$$\begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |10\rangle \\ |10\rangle \to |01\rangle \\ |11\rangle \to |11\rangle \end{cases}$$

$$\text{SWAP} = \begin{pmatrix} 1 & & & \\ & 0 & 1 & \\ & 1 & 0 & \\ & & & 1 \end{pmatrix}$$

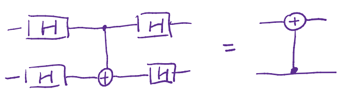
$$|\psi\rangle_{12} \to |\psi\rangle_{21}$$

N-bit Toffoli gates

C^{N-1} - NOT $\quad |1\rangle^{\otimes N-1}\langle 1| \otimes X_N + (I_{N-1} - |1\rangle^{\otimes N-1}\langle 1|) \otimes I_N$.



Properties :

1) 

2) 

3) $\text{SWAP}_{12} = C_{12}\, C_{21}\, C_{12} \quad \leftarrow$ (CNOT)

4. Universality Theorem

Lemma. If gates $\mathcal{U} = e^{iA}$, $\mathcal{U}' = e^{iB}$. (A, B are "generic operator") are realizable, then any gate of the form.

$$e^{i(\alpha A + \beta B) + \gamma [A,B]}$$

can be implemented by $\mathcal{U}, \mathcal{U}'$.

Explanation and Proof

1) $\mathcal{U}(2^k \times 2^k)$ gate with eigenvalues $e^{i\theta_1}, e^{i\theta_2}, \dots, e^{i\theta_{2^k}}$

Each θ_i/π is an irrational number $\Rightarrow$ Generic

$\mathcal{U}^n \to$ eigenvalues $e^{in\theta_i} \xrightarrow{\theta_i/\pi \text{ irrational}} n\theta_i$ is dense in $\mathbb{R}$.

Hence $\mathcal{U}^n$ can approximate any gate $e^{i\alpha A}$

with $\mathcal{U}$ and $\mathcal{U}'$, $\Rightarrow e^{i\alpha A}, e^{i\beta B}$ avcilable

2) Trotter decomposition :

$$\lim_{n\to\infty}\left(e^{i\alpha A/n} e^{i\beta B/n}\right)^n = \lim_{n\to\infty}\left[1 + \frac{i}{n}(\alpha A + \beta B)\right]^n = e^{i(\alpha A + \beta B)}$$

$$\lim_{n\to\infty}\left(e^{\frac{i\sqrt{\gamma}A}{\sqrt{n}}} e^{\frac{i\sqrt{\gamma}B}{\sqrt{n}}} e^{-i\frac{A\sqrt{\gamma}}{\sqrt{n}}} e^{-i\frac{B\sqrt{\gamma}}{\sqrt{n}}}\right)^n = \lim\left(1 - \frac{\gamma}{n}(AB - BA)\right)^n = e^{-[A,B]\gamma}$$

If $\mathcal{U}, \mathcal{U}'$ available $\Rightarrow e^{i(\alpha A + \beta B)}, e^{-[A,B]\gamma}, e^{i\delta[A,[A,B]]}, \dots$

Lie Algebra $\quad A, B \xrightarrow{\text{commutators}} [A,B]$, $[A,[A,B]]$. ...

Universality Theorem 1.

CNOT + any generic single-bit gate are universal
$\mathcal{U}_g$

$\mathcal{U}_g^n \to$ any single bit.

$\mathcal{U}_1 \otimes \mathcal{U}_2\, C_{12}\, \mathcal{U}_1' \otimes \mathcal{U}_2'$ is generic $\Rightarrow$ realize any two-bit gates.

Recursively $\Rightarrow$ any n-bit gates

Universality Theorem 2.

Gates {CNOT, H, S, T} are universal.

Construct a single-bit generic gate:

$THTH = e^{-i\frac{\pi}{8}Z} e^{-i\frac{\pi}{8}X}$. is a rotation along $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$. with angle $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$

$\Rightarrow \frac{\theta}{\pi}$ is irrational

$\Rightarrow$ THTH generic.

5. Gate Simulation Efficiency

Solovey-kitaev theorem: For simulation of any single-bit gate with a distance (error) ε from a discrete set. # of steps $n \sim \log^c(\frac{1}{\varepsilon})$ where $c \sim 2$.

In general, simulation for $U(2^n \times 2^n)$ is inefficient.

Quantum circuit: composed by elementary gates (only on constant # of bits).

Quantum complexity:

B.Q.P. $\stackrel{\text{def}}{=}$ {decision problem that can be solved with poly. size quantum circuit with bounded error prob.}

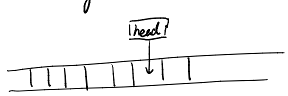
$P_{success} > \frac{1}{2} + \varepsilon$

B.P.P $\stackrel{\text{def}}{=}$ {decision probs that can be solved by classical poly-size circuit with bounded error prob.}

$P \subset B.P.P \subset B.Q.P$

6. Models.

1) Quantum Turing Machines



infinite cells. $\Leftrightarrow$ Quantum circuit model

$|h, x, q, T\rangle$ tranfer: Unitary $\mathcal{U}$.

halt position state tape.