Lecturer: Tongyang, scribed by Shuo Zhou, Yexin Zhang
Date: September 27, 2023

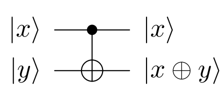
Lecture 4

Quantum Circuits; Introduction to Quantum Algorithms

- Controlled gates
- Universality
- Phase kickback
- Deutsch's problem
- Deutsch-Jozsa problem

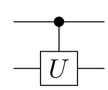
1 Controlled-U gates

CNOT



$$|00\rangle \longmapsto |00\rangle\,, \quad |01\rangle \longmapsto |01\rangle$$
$$|10\rangle \longmapsto |11\rangle\,, \quad |11\rangle \longmapsto |10\rangle$$
$$x, y \in \{0, 1\}$$

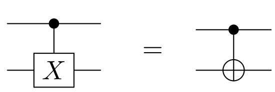
In general: Controlled -U

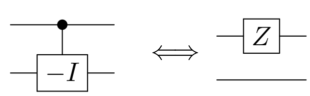


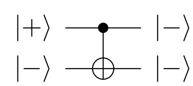
U : 2*2 unitary matrix

$$|0\rangle|\psi\rangle \longmapsto |0\rangle|\psi\rangle$$
$$|1\rangle|\psi\rangle \longmapsto |0\rangle U|\psi\rangle$$
$$|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U = \begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}$$

For example:







2 Quantum circuit for teleportation

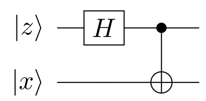
Procedure:

1. Alice measures qubit 1 & 2 in Bell basis.

2. If the outcome is $\begin{cases} |\beta_{00}\rangle \\ |\beta_{01}\rangle \\ |\beta_{10}\rangle \\ |\beta_{11}\rangle \end{cases}$, Alice sends $xz = \begin{cases} 00 \\ 10 \\ 01 \\ 11 \end{cases}$ to Bob.

3. Bob applies $Z^z X^x$ to qubit 3.

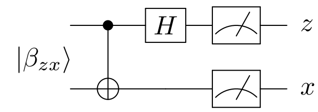
Prepare $|\beta_{zx}\rangle$



where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

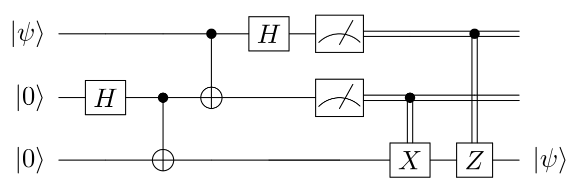
$H|0\rangle = |+\rangle, \ H|1\rangle = |-\rangle$

Measure



The reverse of the preparation process

Quantum circuit for teleportation:



3 Universality

We would like to use a finite gate set to quantify complexity and fault tolerance.

This needs approximation and a metric between states.

$$\| |\psi\rangle - |\phi\rangle \| := \sqrt{(\langle\psi| - \langle\phi|)(|\psi\rangle - |\phi\rangle)}$$

$$\| |\psi\rangle - |\psi\rangle \| = 0, \ \ \| |\psi\rangle - |-\psi\rangle \| = 2, \ \ \langle\psi|\phi\rangle = 0 \Rightarrow \| |\psi\rangle - |\phi\rangle \| = \sqrt{2}$$

Distance between unitaries:

$$E(U, V) = \max_{|\psi\rangle} \| U|\psi\rangle - V|\psi\rangle \|$$

For example:

$$\| X|-\rangle - I|-\rangle \| = \| -|-\rangle - |-\rangle \| = 2 \Rightarrow E(X, I) = 2$$

Note that E is subadditive:

$$E(U_1U_2, V_1V_2) \leq E(U_1, V_1) + E(U_2, V_2)$$

Definition: A set of quantum gates is universal if for any positive integer n, any n-qubit unitary U and any $\epsilon > 0$, we can find gates $V_1, V_2, \cdots, V_k$ from the set s.t. $E(U, V_1V_2\cdots V_k) \leq \epsilon$.

For example: {Toffoli} can only map product states to product states: not universal.

For example: {H,X,Y,Z} can only map product states to product states: not universal.

Facts about universality:

- If we can rotate by an angle that is not a rational multiple of π, then we can approximate a rotation about that axis by any angle arbitrarily closely.

- If we can rotate about two non-parallel axes by arbitrary angles, we can perform an arbitrary rotation.

- For multi-qubit gates, universal set must include an entangling gate (can map product state to entangled state).

- In fact, universal 1-qubit gate set + any entangling gate gives universality.

Common universal gate set: {CNOT,H,T}, where $T = R_Z(\frac{\pi}{4}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}$

$HTHT$, $THTH \rightarrow$ irrational angle.

1-qubit gate: Good approximation, Solovay-Kitaev Theorem.

With any fixed universal set of 1-qubit gates that is closed under inverses, any 1-qubit gate can be approximated to within ϵ using $O(\log^k(\frac{1}{\epsilon}))$ gates.

This can be generalized to multiple qubits.

Reference: Dawson and Nielsen, The Solovay-Kitaev Theorem. QIC 2006.

n-qubit gates: NOT every unitary on n qubits has a cricuit of poly(n) gates by a counting argument.

Classically:

- Number of permutations of the 2^n strings with n bits: $(2^n)!$

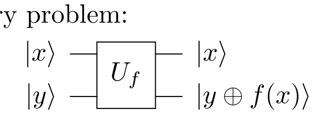
- Number of cricuits consisting of m gates is only exponentially large in m.

  For example: $\left(3C_7^3\right)^m$ for Toffoli gates.

In general, exponentially many gates are needed to do an arbitrary unitary.

4 Phase kickback

Simplest query problem:



U_f: “Orcale”

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	0	1
1	0	1	1	0
	constant		balanced	

Phase kickback:

Put $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ in the second register.

$|x\rangle|-\rangle = \frac{1}{\sqrt{2}}(|x\rangle|0\rangle - |x\rangle|1\rangle) \longmapsto \frac{1}{\sqrt{2}}|x\rangle(|f(x)\rangle - |\overline{f(x)}\rangle)$

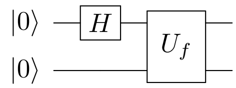
$\frac{1}{\sqrt{2}}|x\rangle(|f(x)\rangle - |\overline{f(x)}\rangle) = |x\rangle \begin{cases} |-\rangle & f(x) = 0 \\ -|-\rangle & f(x) = 1 \end{cases} = (-1)^{f(x)}|x\rangle|-\rangle$

Hence, $|x\rangle|-\rangle \longmapsto (-1)^{f(x)}|x\rangle|-\rangle$. This is formally known as phase kickback.

5 Deutsch's problem

Given black box for $f : \{0,1\} \longrightarrow \{0,1\}$. Problem: Is f constant or balanced? (Or the parity of $f(0) \oplus f(1)$)

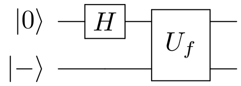
Quantumly, query in superposition:



$$|0\rangle\,|0\rangle \overset{H\otimes I}{\longmapsto} |+\rangle\,|0\rangle \overset{U_f}{\longmapsto} \tfrac{1}{\sqrt{2}}\left(|0, f(0)\rangle + |1, f(1)\rangle\right)$$

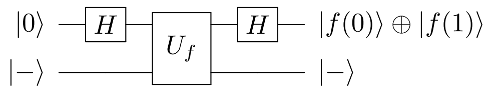
Not so helpful... cannot get the information of both $f(0)$ and $f(1)$ at the same time.

Instead, we use phase kickback:



$$|0\rangle\,|-\rangle \overset{H\otimes I}{\longmapsto} |+\rangle\,|-\rangle \overset{U_f}{\longmapsto} \tfrac{1}{\sqrt{2}}\left((-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle\right)|-\rangle$$

$$\tfrac{1}{\sqrt{2}}\left((-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle\right)|-\rangle = \tfrac{(-1)^{f(0)}}{\sqrt{2}}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}\,|1\rangle\right)|-\rangle \propto \begin{cases} |+\rangle\,|-\rangle & f(0)\oplus f(1) = 0 \\ |-\rangle\,|-\rangle & f(0)\oplus f(1) = 1 \end{cases}$$



Here we leave out the global phase:$(-1)^{f(0)}$

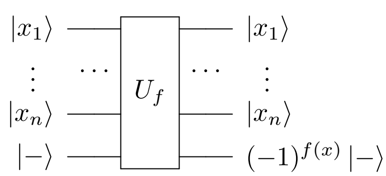
6 Deustch-Jozsa problem

- Given: $f : \{0,1\}^n \longmapsto 0, 1$(by a black box).
- Promise: f is either constant or balanced.
- Determine for sure which holds in the promise.

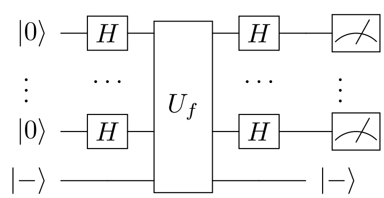
Classically: we need $2^{n-1} + 1$ queries.

Quantumly: $x \in \{0,1\}^n, \quad x = x_1 \cdots x_n,\ x_i \in \{0,1\}$.

$$|x\rangle\,|-\rangle \longmapsto \frac{1}{\sqrt{2}}\,|x\rangle\left(|f(x)\rangle - \overline{|f(x)\rangle}\right) = (-1)^{f(x)}\,|x\rangle\,|-\rangle$$



Algorithm:



$$|0\rangle^{\otimes n}\,|-\rangle \overset{H^{\otimes n}\otimes I}{\longmapsto} |+\rangle^{\otimes n}\,|-\rangle = \sum_{x\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|x\rangle\,|-\rangle \overset{U_f}{\longmapsto} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}\,|x\rangle\,|-\rangle \qquad (*)$$