Quantum gates and quantum circuits

In this chapter, we introduce the basic quantum operations can use to manipulate quantum states. In principle, one all quantum operations on vector states are unitary operations $|\psi\rangle \mapsto U|\psi$, and all quantum operations on density matrices are unitary similarity $\rho \mapsto UAU^\dagger$ for some unitary U. In practice, we need to decompose a general unitary operation into a product of simple unitary operations so that they are ready for implementation.

4.1 Basic set up of Quantum computing

(1) Prepare a set of registers (qubits).

(2) Apply some unitary transforms to carry out quantum algorithms.

(3) Measure the outcome to derive conclusion.

Mathematically, qubit is a unit vector $|x\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ with $|a|^2 + |b|^2 = 1$.

Physically, it may realized by vertically and horizontally polarized photons, or spin 1/2 in NMR system.

One often starts with a pure state $|\psi\rangle = |0 \dots 0\rangle$.

Then apply a series of **simple** quantum gates (unitary transformations) $U_1, U_2, \dots$, to the initial states.

Then a (careful) measurement of the resulting state will provide us the needed information.

4.2 Quantum gates

We can apply the following quantum gates associated with the Pauli matrices to qubits.

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

Note that $XY = Z$.

Walsh-Hadamard gate:

$U_H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Consider the effects on $|\psi\rangle = a|0\rangle + b1\rangle$.

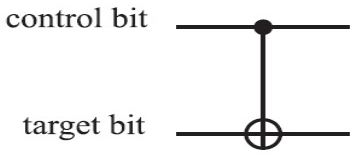
Quantum gates involving states represented by multiple qubits.

CNOT (controlled-NOT) gate:

$U_{\text{CNOT}} : |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|$

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

The circuit diagram:

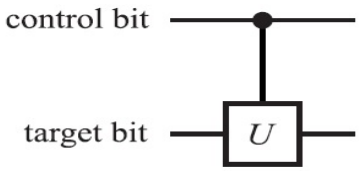


C-unitary (controlled-unitary) gate:

$C\text{-}U$: $= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}.$$

The circuit diagram:

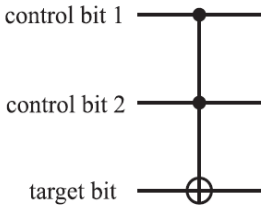


CCNOT (controlled-controlled-NOT) gate

(a.k.a. **Toffoli gate**):

$$U_{CCNOT}$$
$$= (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X.$$

The circuit diagram:



SWAP gate: $\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

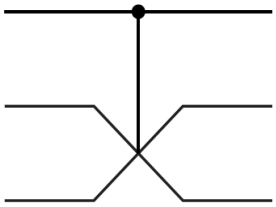
The circuit diagram:

EXERCISE 4.7 Show that the above U_{SWAP} is written as

$$U_{\mathrm{SWAP}} = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)$$
$$(|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X). \qquad (4.16)$$

This shows that the SWAP gate is implemented with three CNOT gates as given in Exercise 4.3 (3).

The controlled-SWAP gate



is also called the **Fredkin gate**. It flips the second (middle) and the third (bottom) qubits when and only when the first (top) qubit is in the state $|1\rangle$.

Walsh-Hadamard transformation $H \otimes H \otimes H \cdots$ to a quantum gate on n qubits.

4.3 Comparison with Classical logical gates

It is interesting to compare their actions on qubits to the classical Boolean gates.

NOT gate: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, i.e., $X|x\rangle = |\neg x\rangle$.

CCNOT gate can produced everything.

- $CCNOT|1,1,x\rangle = |1,1,\neg x\rangle$

- XOR Gate: $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$. $CCNOT|1,x,y\rangle = |1,x,x \oplus y\rangle$.

- AND Gate: $0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0$, $1 \wedge 1 = 1$. $CCNOT|x,y,0\rangle = |x,y,x \wedge y\rangle$.

- OR Gate: $0 \vee 0 = 0, 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1$. Use DeMorgan's Law, $x \vee y = \neg(\neg x \wedge \neg y)$.

  See Exercise 4.8.

- NAND gate: $NAND(x,y) = \neg(x \wedge y) = \neg x \vee \neg y$.

  See Exercise 4.9.

4.6 Universal quantum gates

Theorem The set of single qubit gates and the CNOT gates (with one control bit and one target bit) form a universal set.

Proof. Sketch and research opportunity.

Lemma Let $U \in \mathrm{SU}(2)$. Then there exist $\alpha, \beta, \gamma \in \mathbb{R}$ such that $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$, where

$$\begin{aligned} R_z(\alpha) &= \exp(i\alpha\sigma_z/2) = \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix} \\ R_y(\beta) &= \exp(i\beta\sigma_y/2) = \begin{pmatrix} \cos(\beta/2) & \sin(\beta/2) \\ -\sin(\beta/2) & \cos(\beta/2) \end{pmatrix} \end{aligned}$$

Note:

$$R_z(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} e^{i(\alpha+\gamma)/2}\cos(\beta/2) & e^{i(\alpha-\gamma)/2}\sin(\beta/2) \\ -e^{i(-\alpha+\gamma)/2}\sin(\beta/2) & e^{-i(\alpha+\gamma)/2}\cos(\beta/2) \end{pmatrix}.$$

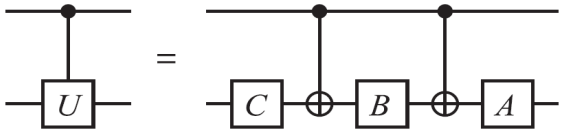
□

Lemma Let $U \in \mathrm{SU}(2)$. Then there exist $A, B, C \in \mathrm{SU}(2)$ such that $U = AXBXC$ and $ABC = I$, where $X = \sigma_x$ and

$$A = R_z(\alpha)R_y\left(\frac{\beta}{2}\right), B = R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right), C = R_z\left(-\frac{\alpha-\gamma}{2}\right).$$

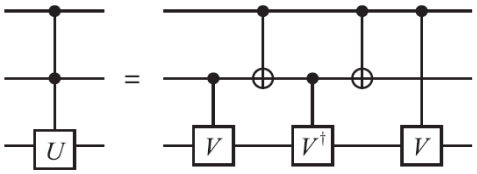
provided $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$ for some $\alpha, \beta, \gamma \in \mathbb{R}$. □

CU gate:



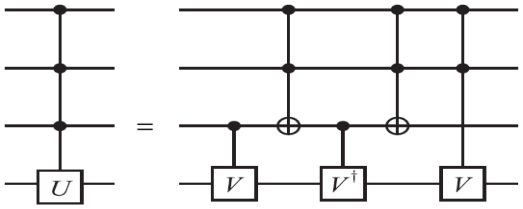
$CU = (I \otimes A)(CX)(I \otimes B)(CX)(I \otimes C)$

C^2U gate:



Here $U = V^2$ by Lemma 4.6.

C^3U:



For $k > 3$, C^kU is done by induction.

Proof of Theorem Let $U \in SU(N)$ with $N = 2^n$. We prove by induction on n that there are elementary gates. The result trivially holds if $n = 1$.

Suppose the result holds for matrices in $SU(N)$ with $N = 2^n$. We use CS decomposition to reduce $U \in SU(2N)$ ...

Denote by $\gamma_{n,k}$ be the number of k-controlled-U gates used in the decomposition of a unitary in $SU(2^n)$, where $k = 0, \ldots, n-1$. We can determine $\gamma_{n,k}$ recursively.

For $n = 1$, we need 1 0-controlled U gate. So, $\gamma_{1,0} = 1$.

For $n = 2$, for R_1, S_1, we need 2 0-controlled-U gates; for R_2, S_2, we need 2 1-controlled-U gates. Then we get

$$\hat{U} = \begin{pmatrix} c_1 & 0 & s_1 & 0 \\ 0 & c_2 & 0 & s_2 \\ -s_1 & 0 & c_1 & 0 \\ 0 & \tilde{s}_2 & 0 & \delta_2 \end{pmatrix} = \left(\begin{pmatrix} c_1 & s_1 \\ -s_1 & c_1 \end{pmatrix} \otimes I_2 \right) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & w_{11} & 0 & w_{12} \\ 0 & 0 & 1 & 0 \\ 0 & w_{21} & 0 & w_{22} \end{pmatrix},$$

which is a product of a 0-control-U gate and a 1-controlled-U gate. Thus, we need 3 0-controlled-U gates, and 3 1-controlled-U gates. Thus, $\gamma_{2,1} = \gamma_{2,0} = 3$.

For $n = 3$, for R_1, S_1, we need 2 times the gates in the previous steps, i.e., adding $2\gamma_{2,1}$ and $2\gamma_{2,0}$ for $\gamma_{3,1}$ and $\gamma_{3,0}$. For R_2, S_2, we need 2 times the gates in the previous steps with 1 additional control for each gates, i.e., adding $2\gamma_{2,1}$ and $2\gamma_{2,0}$ to $\gamma_{3,2}$ and$\gamma_{3,1}$. Finally, $\hat{U}$ is a product of a 2-controlled-U, a 1-controlled-U and a 0-contolled-U. Thus,

$$\gamma_{3,2} = 2\gamma_{2,1} + 1, \gamma_{3,1} = 2(\gamma_{2,1} + \gamma_{2,0}) + 1, \gamma_{3,0} = 2\gamma_{2,0} + 1.$$

In general, we have

$$\gamma_{n,n-1} = 2\gamma_{n-1,n-2} + 1, \quad \gamma_{n,0} = 2\gamma_{n-1,0} + 1,$$

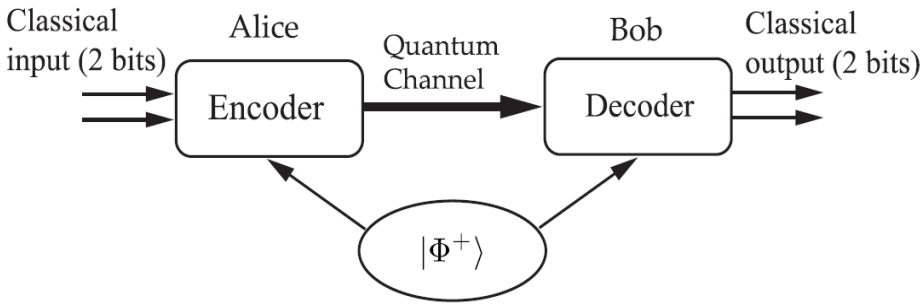
$$\gamma_{n,j} = 2(\gamma_{n-1,j} + \gamma_{n-1,j-1}) + 1, \quad j = 1, \ldots, n-2.$$

Open problems

- Decompose $U \in M_{2^n}$ using single qubit gates and the minimum number of CNOT gates.
- Prepare the initial states $|\psi\rangle \in \mathbb{C}^N$ by using a "simple" $U \in U(N)$ such that $U|\psi\rangle = |0 \cdots 0\rangle$ so that $U^\dagger|0 \cdots 0\rangle = |\psi\rangle$.

4.5 Dense Coding and Teleportation

Dense Coding Using an entangled pair (Bell state), one can send two binary bits of classical information using one quantum bit.



- Alice and Bob share the entangled pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.
- Alice applies I, X, Z, Y to her quantum state depending whether she wants to send $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ to Bob.

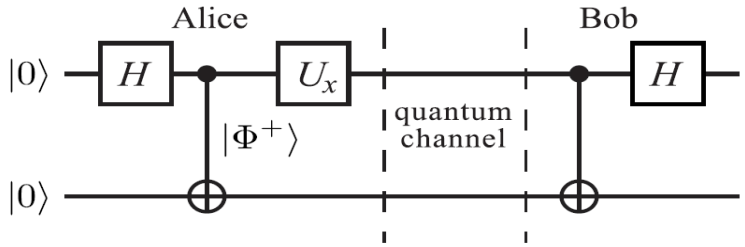
  The 2-qubit state becomes:

  $(|00\rangle + |11\rangle)/\sqrt{2}$, $(|10\rangle + |01\rangle)/\sqrt{2}$,

  $(|00\rangle - |11\rangle)/\sqrt{2}$, $(|10\rangle - |01\rangle)/\sqrt{2}$, respectively.
- Then Alice sends her quantum state to Bob.
- Bob applies $CNOT$ gate to the two quantum states using the first quantum state (of Alice) as control. The 2-qubit state becomes:

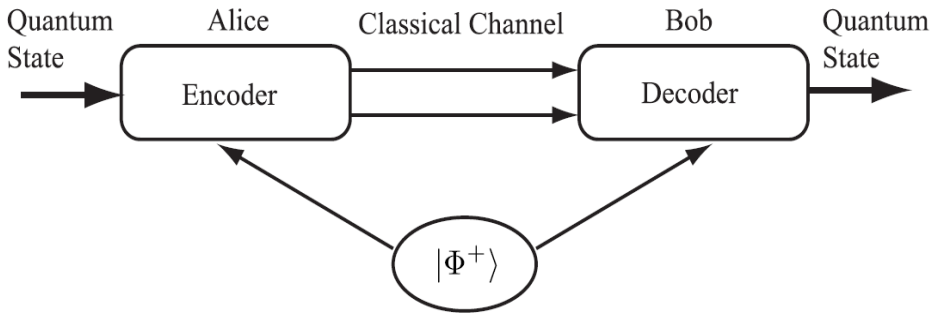
  $(|00\rangle + |10\rangle)/\sqrt{2}$, $(|11\rangle + |01\rangle)/\sqrt{2}$,

  $(|00\rangle - |10\rangle)/\sqrt{2}$, $(|11\rangle - |01\rangle)/\sqrt{2}$, respectively.
- Then Bob applies Hadamard gate to the first state.
- He then measures to see $|00\rangle, |01\rangle, |10\rangle, -|11\rangle$.



Teleportation Using an entangled pair (Bell state), one can use two classical bit information to transmit a qubit.

- Suppose Alice has a qubit $|\phi\rangle = a|0\rangle + b|1\rangle$ and she want to send to Bob.
- Alice and Bob share the entangled pair $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.



- Consider $|\phi\rangle|\Phi^+\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)$.
- Alice applies $UCNOT \otimes I$ followed by $U_H \otimes I \otimes I$ to this state, which results in

$$
\begin{aligned}
&(U_{\mathrm{H}} \otimes I \otimes I)(U_{\mathrm{CNOT}} \otimes I)\frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right) \\
&= \frac{1}{2}\left[a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\right] \\
&= \frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)].
\end{aligned}
$$

- Alice measures her two qubits, and send the two (classical) bits to Bob.
- Bob applies I, X, Z, Y according to the two bits as $00, 01, 10, 11$. Then his qubit will become $|\phi\rangle$ ($-|\phi\rangle$ in the last case).