Lecturer: Tongyang Li, scribed by Shuo Zhou, Yexin Zhang
Date: September 13, 2023

Lecture 2

Basic Definition in Quantum Computing

- Cricuits
- Reversible computing
- Quantum states
- Quantum dynamics
- Composite systems

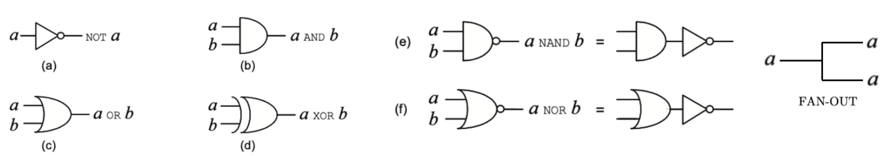
Last time we've mentioned that:

$$\text{classcial bit} : 0, 1 \quad \longrightarrow \quad \text{quantum bit (qubit)} : a\,|0\rangle + b\,|1\rangle\,, \quad |a|^2 + |b|^2 = 1$$

What can we apply upon qubits?

1 Classicial gate

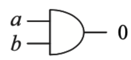
We call a set of gates universal if it can compute any $f : \{0,1\}^n \ \rightarrow \ \{0,1\}^m$



- {AND, OR, NOT} is universal.
- {AND, NOT} is universal, since OR can be made by AND and NOT.
- {NAND} is universal.

2 Reversible Computing

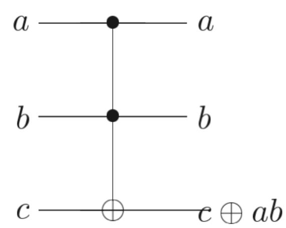
AND gate is NOT reversible: cannot recover (x, y) pairs with the output:



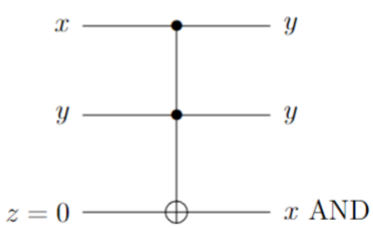
(0,0) or (1,0) or (0,1)?

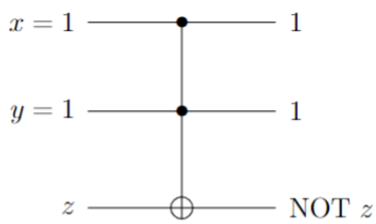
Nevertheless, in principle, any computation can be made reversible:

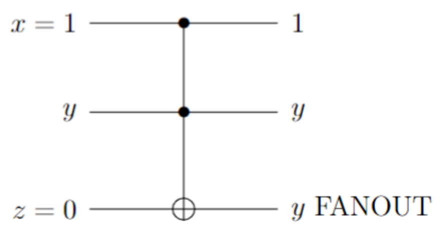
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Toffoli is universal:

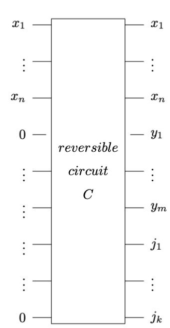


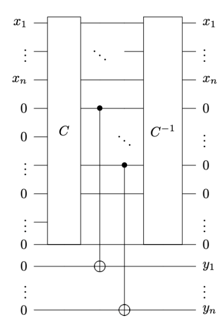




Ancilla: Extra bits not involved in the input or output.

By composing reversible gates, we can do any computation reversibly, Moreover, we can uncompute the junk:





Whenever we compute $x \longmapsto f(x)$ efficiently, we can efficiently reversibly compute:

$$(x, y, 0) \longmapsto (x, y \oplus f(x), 0)$$

3 Postulates in quantum computing

3.1 Quantum states

$$\text{Qubit} : \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \qquad \underbrace{a_0, a_1}_{\text{"amplitudes"}} \in \mathbb{C} \qquad |a_0|^2 + |a_1|^2 = 1$$

$$\text{Basic vectors} : \begin{matrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \\ \\ \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle \end{matrix}$$

$\{|0\rangle, |1\rangle\}$ is a computational basis for a qubit:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle \qquad \text{"ket"}$$

We denote the dual vector (conjugate transpose) by:

$$\langle\psi| = a_0^* \langle 0| + a_1^* \langle 1| \qquad \text{"bra"}$$

"ket"-column vector, "bra"-row vector
Bra-ket represents an inner product:

$$|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle \qquad |\phi\rangle = b_0 |0\rangle + b_1 |1\rangle$$

$$\langle\psi| \cdot |\phi\rangle = \langle\psi|\phi\rangle = \begin{pmatrix} a_0^* & a_1^* \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = a_0^* b_0 + a_1^* b_1$$

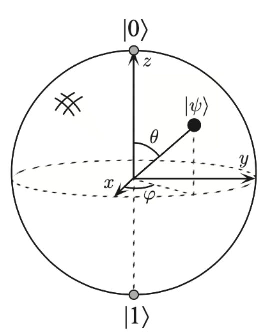
$$\langle\psi|\psi\rangle = 1$$

Ket-bra represents an outer product:

$$|0\rangle \langle 1| + |1\rangle \langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

How to express all quantum states? Bloch Sphere:



$$|\psi\rangle = e^{i\eta}\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$
$$\cos\frac{\theta}{2} = |a_0| \quad \sin\frac{\theta}{2} = |a_1|$$

Since the global phase is irrelevant, set $\eta = 0$ WLOG(without loss of generality):

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle \qquad \theta \in [0,\pi], \phi \in [0, 2\pi)$$

3.2 Quantum dynamics/evolutions

Time evolution in quantum mechanics is linear:

$$\text{if } |\psi\rangle \longmapsto |\psi'\rangle, |\phi\rangle \longmapsto |\phi'\rangle, \text{then}:$$
$$\alpha|\psi\rangle + \beta|\phi\rangle \longmapsto \alpha|\psi'\rangle + \beta|\phi'\rangle$$

Recall that all quantum states are l_2-norm unit vectors. To keep quantum states being states $\Longrightarrow$ quantum dynamics must be unitary:

$$|\psi\rangle \longmapsto U|\psi\rangle$$
$$1 = \langle\psi|\psi\rangle = \langle\psi|U^\dagger U|\psi\rangle \quad \text{true for } \forall\,|\psi\rangle$$
$$\Rightarrow U^\dagger U = I$$

The time evolution of a quantum system is described by a unitary operator:

$$\text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{matrix} \text{NOT}\,|0\rangle = |1\rangle \\ \text{NOT}\,|1\rangle = |0\rangle \end{matrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\therefore \text{NOT}^\dagger\text{NOT} = I$$

For example:

Some Common single-qubit gates:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ \text{Identity} \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \ \text{Pauli X, Y, Z}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \ \text{Hadamard} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \ \text{Phase} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix} = e^{i\frac{\pi}{8}}\begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix} \ \frac{\pi}{8}$$

In physics, U comes from Schrödinger equation:

$$i\frac{\mathrm{d}}{\mathrm{d}t}|\psi(t)\rangle = H|\psi(t)\rangle$$
$$H : \text{the “Hamiltonian”} \quad H = H^\dagger$$

When H is time independent,

$$|\psi(t)\rangle = \underline{e^{-iHt}}\,|\psi(0)\rangle$$

This can be defined by Taylor Series:

$$e^{-iHt} = I + (-iHt) + \frac{(-iHt)^2}{2!} + \cdots$$

3.3 Composite systems

The state space of a composite system is the tensor product of the individual space.

$$\text{Vector} : \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \otimes \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} = \begin{pmatrix} a_0 a_0 \\ a_0 a_1 \\ a_1 a_0 \\ a_1 a_1 \end{pmatrix}$$

$$\text{Matrices} : \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \otimes \begin{pmatrix} b_{00} & b_{01} \\ b_{10} & b_{11} \end{pmatrix} = \begin{pmatrix} a_{00}b_{00} & a_{00}b_{01} & a_{01}b_{00} & a_{01}b_{01} \\ a_{00}b_{10} & a_{00}b_{11} & a_{01}b_{10} & a_{01}b_{11} \\ a_{10}b_{00} & a_{10}b_{01} & a_{11}b_{00} & a_{11}b_{01} \\ a_{10}b_{10} & a_{10}b_{11} & a_{11}b_{10} & a_{11}b_{11} \end{pmatrix}$$

If the first and second subsystem is denoted as $|\psi\rangle$, $|\phi\rangle$ respectively, then the overall state is:

$$|\psi\rangle \otimes |\phi\rangle = |\psi\rangle |\phi\rangle = |\psi, \phi\rangle \qquad \text{tensor product}$$
$$(U_1 \otimes U_2)(|\psi\rangle \otimes |\phi\rangle) = U_1 |\psi\rangle \otimes U_2 |\phi\rangle$$
$$|\psi_1\rangle \langle\psi_2| \otimes |\phi_1\rangle \langle\phi_2| = (|\psi_1\rangle \otimes |\phi_1\rangle)(\langle\psi_2| \otimes \langle\phi_2|)$$

For example:

$$n \text{ qubits } \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 \cong \mathbb{C}^{2^n}$$
$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle$$

For example:

$$2 \text{ qubits states } |00\rangle, \ |01\rangle$$
$$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Independent operators on subsystems are described by a tensor product:

$$(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = A|\psi\rangle \otimes B|\phi\rangle$$

For example:

$$\text{Act with } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ on the second qubit of } \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) :$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$(I \otimes X)\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$$

For example:

$$(I \otimes X)\left(\sqrt{\frac{2}{3}}\,|00\rangle + \sqrt{\frac{1}{3}}\,|01\rangle\right) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \sqrt{\frac{2}{3}} \\ \sqrt{\frac{1}{3}} \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{1}{3}} \\ \sqrt{\frac{2}{3}} \\ 0 \\ 0 \end{pmatrix} = \sqrt{\frac{1}{3}}\,|00\rangle + \sqrt{\frac{2}{3}}\,|01\rangle$$

$$(I \otimes X)\left(|0\rangle \otimes (\sqrt{\frac{2}{3}}\,|0\rangle + \sqrt{\frac{1}{3}}\,|1\rangle)\right) = |0\rangle \otimes \left(\sqrt{\frac{2}{3}}\,|1\rangle + \sqrt{\frac{1}{3}}\,|0\rangle\right) = \sqrt{\frac{1}{3}}\,|00\rangle + \sqrt{\frac{2}{3}}\,|01\rangle$$

2-subsystem states with form $|\psi\rangle\,|\phi\rangle$ are called product states; otherwise they're called entangled states:

For example:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ is entangled.}$$

Proof. Assume that $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = (\alpha_0\,|0\rangle + \alpha_1\,|1\rangle)(\beta_0\,|0\rangle + \beta_1\,|1\rangle)$. Then $\alpha_0\beta_0 = \frac{1}{\sqrt{2}}, \alpha_0\beta_1 = 0, \alpha_1\beta_0 = 0, \alpha_1\beta_1 = \frac{1}{\sqrt{2}}.\alpha_0\beta_0\alpha_1\beta_1 = \frac{1}{2} \neq 0 = \alpha_0\beta_1\alpha_1\beta_0$, a contradiction. □