Qubit and Quantum Gates

School on Quantum Computing @Yagami
Day 1, Lesson 1
9:00-10:00, March 22, 2005

Eisuke Abe
Department of Applied Physics and Physico-Informatics,
and CREST-JST, Keio University

From classical to quantum

Information is physical
- Rolf Landauer

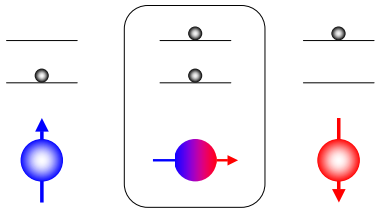
- QUANTUM information or quantum INFORMATION?
- It depends on your background (physics or information science)
- Ultimately, you need both
- At the beginning, it would be better to keep one perspective (physics here)

References

- Quantum Computation and Quantum Information (and references therein), M. A. Nielsen and I. L. Chuang, Cambridge University Press (2000)
  - Day 1, Lesson 1- Day 2, Lesson 2
- Physical Review A 65, 012320 (2001), N. D. Mermin
  - Day 1, Lesson 2
- L. M. K. Vandersypen, Ph. D Thesis (available at arXiv: quant-ph/0205193)
  - Day 2, Lesson 2

Quantum bit

For physicists, "*quantum bit* (*qubit*)" is a synonym for "*quantum mechanical two-level system*"



$|g\rangle \equiv |0\rangle$ Superposition $|e\rangle \equiv |1\rangle$

Quantum bit

Vector notation for *computational basis* states

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

POSTULATE State space (Hilbert space)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$\alpha, \beta \in \mathbf{C}$: Probability amplitude

$|\alpha|^2 + |\beta|^2 = 1$: Probabilities sum to 1

Unitary evolution

POSTULATE

The evolution of a qubit system is described by a *unitary transformation* such as

$$|\psi(t_2)\rangle = U_{12}|\psi(t_1)\rangle$$

Hermitian conjugate: $A^\dagger = (A^T)^*$
Hermitian (self-adjoint): $A = A^\dagger$
Unitary: $UU^\dagger = I$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$$

Unitary evolution

Connection between the *Schrödinger equation*

$$i\hbar\frac{d|\psi\rangle}{dt}=H|\psi\rangle \;\Rightarrow\; |\psi(t_2)\rangle=\exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]|\psi(t_1)\rangle\equiv U_{12}|\psi(t_1)\rangle$$

H: Hamiltonian of the qubit system (Hermitian)

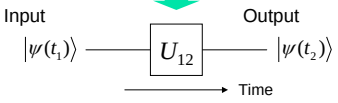
Exponential operator = unitary

Any unitary operator U can be realized in the form $U=\exp(iH)$ where H is some Hermitian operator

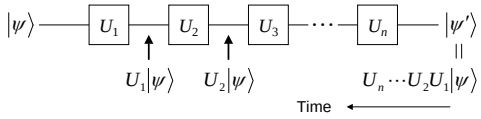
For now, actual physical systems that realize necessary Hamiltonians are NOT our interest

Quantum gate

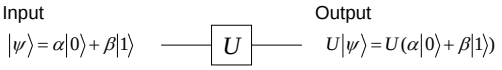
$$|\psi(t_2)\rangle=U_{12}|\psi(t_1)\rangle$$



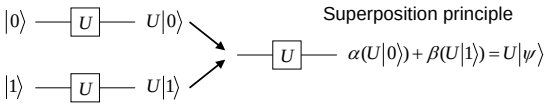
Successive implementation



Quantum gate



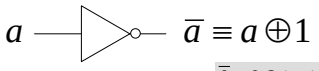
We have *infinite* inputs, but it suffices to consider only the computational basis states



NOT gate

Classical NOT

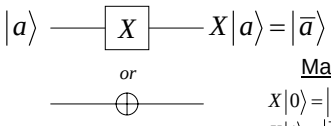
Input	output
0	1
1	0



The only non-trivial one-bit gate in the classical case

$\bar{0}=0\oplus 1=1$
$\bar{1}=1\oplus 1=0$

Quantum NOT



Matrix representation

$$X|0\rangle=|\bar{0}\rangle=|1\rangle \quad X|1\rangle=|\bar{1}\rangle=|0\rangle \Leftrightarrow X=\begin{bmatrix}0&1\\1&0\end{bmatrix}$$

Matrix representation

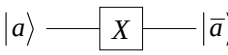
$$\begin{cases}X|0\rangle=|\bar{0}\rangle=|1\rangle\\X|1\rangle=|\bar{1}\rangle=|0\rangle\end{cases}\Leftrightarrow\begin{cases}X\begin{bmatrix}1\\0\end{bmatrix}=\begin{bmatrix}0\\1\end{bmatrix}\\X\begin{bmatrix}0\\1\end{bmatrix}=\begin{bmatrix}1\\0\end{bmatrix}\end{cases}\Leftrightarrow X=\begin{bmatrix}0&1\\1&0\end{bmatrix}$$

The first column represents the final state of $|0\rangle$

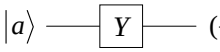
$$X=\begin{bmatrix}0&1\\1&0\end{bmatrix}$$

The second column represents the final state of $|1\rangle$

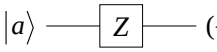
Pauli-X, Y, Z gates



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



$$Y|0\rangle=i|1\rangle,\quad Y|1\rangle=-i|0\rangle \Leftrightarrow Y=\begin{bmatrix}0&-i\\i&0\end{bmatrix}$$



$$Z|0\rangle=|1\rangle,\quad Z|1\rangle=|0\rangle \Leftrightarrow Z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}$$

Hermitian

$$X^2=Y^2=Z^2=I$$

Commutation relations

$$[X,Y]=XY-YX=2iZ \qquad \{X,Y\}=0$$
$$[Y,Z]=2iX \qquad \{Y,Z\}=0$$
$$[Z,X]=2iY \qquad \{Z,X\}=ZX+XZ=0$$

Hadamard gate

$$|a\rangle \;\text{—}\boxed{H}\text{—}\; \frac{1}{\sqrt{2}}\sum_{b=0,1}(-1)^{a\cdot b}|b\rangle = \frac{|0\rangle+(-1)^a|1\rangle}{\sqrt{2}}$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\sum_{b=0,1}|b\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$
$$H|1\rangle = \frac{1}{\sqrt{2}}\sum_{b=0,1}(-1)^b|b\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$$\Leftrightarrow \quad H\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, \; H\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

$$\Leftrightarrow \quad H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Hermitian

$$H^2 = I$$

Circuit identities

$$HXH = Z \quad HYH = -Y \quad HZH = X$$

Measurement gate

POSTULATE

Quantum bit → Classical bit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \;\text{—}\boxed{\;\;}\text{—}\; a$$

0 with probability $|\alpha|^2$, or
1 with probability $|\beta|^2$

Mathematical description
- ✓ General measurement
- ✓ Projective measurement
- ✓ POVM

Multiple-qubit

How do we describe multiple-qubit states?

Speculation…
- ✓ Computational basis states for two-qubit states may be written as $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$
- ✓ We require them to be orthogonal, so they may be written as

$$|00\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \; |10\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \; |01\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \; |11\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

POSTULATE

A multiple-qubit state is the *tensor product* of the component qubit systems

Tensor product

Matrix representation

$$\mathbf{a}\otimes\mathbf{b} = \begin{bmatrix}a_1\\a_2\end{bmatrix}\otimes\begin{bmatrix}b_1\\b_2\end{bmatrix} = \begin{bmatrix}a_1\times\begin{bmatrix}b_1\\b_2\end{bmatrix}\\ a_2\times\begin{bmatrix}b_1\\b_2\end{bmatrix}\end{bmatrix} = \begin{bmatrix}a_1b_1\\a_1b_2\\a_2b_1\\a_2b_2\end{bmatrix}$$

Computational basis set for 2-qubit states

$$|00\rangle = |0\rangle|0\rangle = |0\rangle\otimes|0\rangle = \begin{bmatrix}1\times\begin{bmatrix}1\\0\end{bmatrix}\\ 0\times\begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}1\\0\\0\\0\end{bmatrix} \qquad |10\rangle = |1\rangle|0\rangle = |1\rangle\otimes|0\rangle = \begin{bmatrix}0\times\begin{bmatrix}1\\0\end{bmatrix}\\ 1\times\begin{bmatrix}1\\0\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

$$|01\rangle = |0\rangle|1\rangle = |0\rangle\otimes|1\rangle = \begin{bmatrix}1\times\begin{bmatrix}0\\1\end{bmatrix}\\ 0\times\begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \qquad |11\rangle = |1\rangle|1\rangle = |1\rangle\otimes|1\rangle = \begin{bmatrix}0\times\begin{bmatrix}0\\1\end{bmatrix}\\ 1\times\begin{bmatrix}0\\1\end{bmatrix}\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

Multiple-qubit gates

$$|a_1\rangle \;\text{—}\boxed{\;\;}\text{—}\; U|a_1\rangle|a_2\rangle|a_3\rangle\cdots|a_n\rangle$$
$$|a_2\rangle \;\text{—}\boxed{U}\text{—}$$
$$|a_3\rangle \;\text{—}\boxed{\;\;}\text{—}$$
$$\vdots \qquad\qquad \vdots$$
$$|a_n\rangle \;\text{—}\boxed{\;\;}\text{—}$$

$|a_1a_2\ldots a_n\rangle$: 2^n-dimensional vector

U : 2^n by 2^n unitary matrix

Independent gates

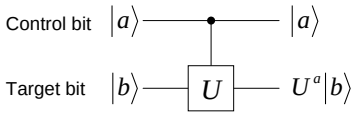
$$|a\rangle \;\text{—}\boxed{H}\text{—}\boxed{Y}\text{—}\; YH|a\rangle \qquad = \qquad \text{—}\boxed{H}\text{—}\boxed{Y}\text{—}$$
$$|b\rangle \;\text{—}\boxed{X}\text{—}\boxed{H}\text{—}\; HX|b\rangle \qquad = \qquad \text{—}\boxed{X}\text{—}\boxed{H}\text{—}$$
$$|c\rangle \;\text{—}\boxed{Z}\text{—}\; Z|c\rangle \qquad\qquad\quad \text{—}\boxed{Z}\text{—}$$

$$|a\rangle|b\rangle|c\rangle \rightarrow \underbrace{(YH\otimes HX\otimes Z)}_{U}|a\rangle|b\rangle|c\rangle = (YH|a\rangle)\otimes(HX|b\rangle)\otimes Z|c\rangle$$

U (8 by 8 unitary matrix)

$$A\otimes B = \begin{bmatrix}a_1 & a_3\\ a_2 & a_4\end{bmatrix}\otimes\begin{bmatrix}b_1 & b_3\\ b_2 & b_4\end{bmatrix} = \begin{bmatrix}a_1\times B & a_3\times B\\ a_2\times B & a_4\times B\end{bmatrix} = \begin{bmatrix}a_1b_1 & a_1b_3 & a_3b_1 & a_3b_3\\ a_1b_2 & a_1b_4 & a_3b_2 & a_3b_4\\ a_2b_1 & a_2b_3 & a_4b_1 & a_4b_3\\ a_2b_2 & a_2b_4 & a_4b_2 & a_4b_4\end{bmatrix}$$

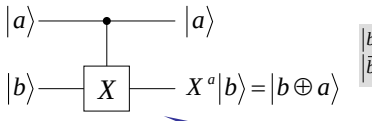
Controlled-U gates



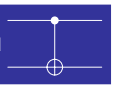
$|b\rangle$ if $a=0$
$U|b\rangle$ if $a=1$

- ✓ U can be an arbitrary single-qubit gate
- ✓ $U^a|b\rangle$ is just a formal expression
- ✓ U works only when $a = 1$

CNOT gate



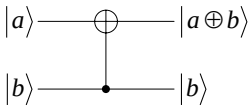
$|b\rangle = |b\oplus 0\rangle$ if $a=0$
$|\bar{b}\rangle = |b\oplus 1\rangle$ if $a=1$

Frequently used 

$C_{12}|00\rangle = |0\rangle|0\oplus 0\rangle = |00\rangle$
$C_{12}|01\rangle = |0\rangle|1\oplus 0\rangle = |01\rangle$
$C_{12}|10\rangle = |1\rangle|0\oplus 1\rangle = |11\rangle$
$C_{12}|11\rangle = |1\rangle|1\oplus 1\rangle = |10\rangle$

$$\Leftrightarrow C_{12}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}, C_{12}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}, C_{12}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}, C_{12}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix} \Leftrightarrow C_{12}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

CNOT gate



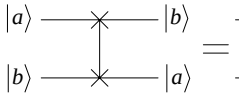
$$C_{21}=\begin{bmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0\end{bmatrix}$$

$C_{21}|00\rangle = |0\oplus 0\rangle|0\rangle = |00\rangle$
$C_{21}|01\rangle = |0\oplus 1\rangle|1\rangle = |11\rangle$
$C_{21}|10\rangle = |1\oplus 0\rangle|0\rangle = |10\rangle$
$C_{21}|11\rangle = |1\oplus 1\rangle|1\rangle = |01\rangle$

$$\Leftrightarrow C_{21}\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\0\\0\\0\end{bmatrix}, C_{21}\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}0\\0\\0\\1\end{bmatrix}, C_{21}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}=\begin{bmatrix}0\\1\\0\\0\end{bmatrix}, C_{21}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

Never mistake… $C_{21} \neq \begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix}$

SWAP gate

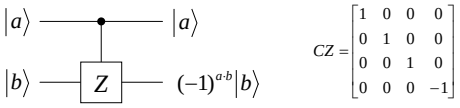


$$SWAP=\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$$

$|a\rangle|b\rangle \xrightarrow{C_{12}} |a\rangle|b\oplus a\rangle$ $\quad a\oplus a=0$ (1)
$\xrightarrow{C_{21}} |a\oplus(b\oplus a)\rangle|b\oplus a\rangle = |b\rangle|b\oplus a\rangle$ (2) (3)
$\xrightarrow{C_{12}} |b\rangle|(b\oplus a)\oplus b\rangle = |b\rangle|a\rangle$ (4)

To implement SWAP, we need to…
1. Encode information on $|a\rangle$ into 2nd qubit
2. Erase information on $|a\rangle$ from 1st qubit
3. Encode information on $|b\rangle$ into 1st qubit
4. Erase information on $|b\rangle$ from 2nd qubit

Controlled-Z gate

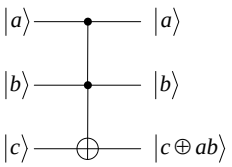


$$CZ=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$$

$$|a\rangle|b\rangle \xrightarrow{CZ} (-1)^{a\cdot b}|a\rangle|b\rangle$$

Controlled-Z is *nonlocal*

Toffoli



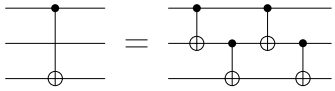
$$Toffoli=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$$

$ab=1 \Leftrightarrow a=1 \wedge b=1$

Toffoli is often referred to as
"controlled-controlled-NOT (C^2-NOT)"

Quiz

Prove the following circuit identity



Also prove the followings

$$H^2 = I$$

$$HZH = X$$

Use the following expressions for quantum gates

$$C_{12}|a\rangle|b\rangle = |a\rangle|b \oplus a\rangle$$

$$H|a\rangle = \frac{1}{\sqrt{2}} \sum_b (-1)^{a \cdot b} |b\rangle, \quad Z|a\rangle = (-1)^a |a\rangle$$