Basics for Quantum Gates

Yi-Ming Ding

Updated: May 05, 2023

References

[1] Nielsen&Chuang. *Quantum computation and quantum information*.

[2] Benenti *et al. Pinciples of quantum computation and quantum information*..

Contents

1 Concept of quantum computer

1.1 Motivation

In **Schrödinger picture**, the evolution of a closed closed quantum system is described by

$$|\psi'(t)\rangle = U(t)\,|\psi(0)\rangle \tag{1}$$

where $U(t) \equiv U$ is some unitary operator, i.e. $U^\dagger U = I$.

Notice that exactly simulating a quantum system on classical computers would generally need exponentially large resources due to the exponentially increasing of the Hilbert space.

A basic idea to solve this problem is, if we have a controllable quantum system $\mathbf{Q}_0$, which means we can evolve its state $|\psi\rangle$ into any $|\psi'\rangle$ we want, we are able to investigate another quantum system $\mathbf{Q}$ we are interested in by mimicing/simulating the behavior of $\mathbf{Q}$ on $\mathbf{Q}_0$. Now the problems become

1. How to physically build this controllable quantum system (hardware level)?
2. With what kinds of U can we evolve $|\psi\rangle$ to some $|\psi'\rangle$ we want (algorithm or software level)?

The controllable system Q_0 in actually what we call a **quantum computer**. The answers to the first question is to find a technical route to build such a quantum computer. For the second question, we have to mathematically design a good U (algorithm) to achieve our goal. Such kind of algorithms are called **quantum algorithms** as they are run on a quantum computer.

1.2 From classical computation to quantum computation

Since the theory of classical computation is mature, it is natural to analogously develop the theory of quantum computation based on it. In classical computing, the elemental computational unit is a bit, which is a binary number

$$c \in \{0, 1\} \tag{2}$$

which physically is realized by some logic circuits on a semiconductor chip.

Since quantum mechanics permits superposition, therefore we can define the quantum bit, or **qubit**, which takes the form $\alpha\,|0\rangle + \beta\,|1\rangle$. A classical bit therefore can be viewed as the special case of a qubit when $\alpha = 0, \beta = 1$ or $\alpha = 1m\beta = 0$. Physically, a qubit can be realized by some quantum two-level system, like the spin of an electron.

2 Single qubit

2.1 Bloch sphere and single-qubit rotation gates

Based on the definition above, a general qubit $|q\rangle$ can be written as

$$|q\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle \tag{3}$$

where

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \quad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix} \tag{4}$$

then

$$|q\rangle = \begin{bmatrix}\cos\frac{\theta}{2}\\ \sin\frac{\theta}{2}e^{i\phi}\end{bmatrix} \tag{5}$$

The vector space $\{|q\rangle\}$ is isomorphic to a sphere, called **Bloch sphere** (see Fig. 1), which can be represented by a unit vector

$$\vec{r} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta) \tag{6}$$

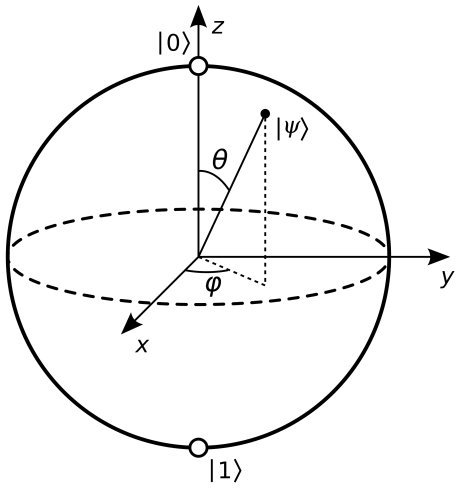

Figure 1: Bloch sphere (image from Wikipedia).

Therefore, the effect of a unitary operator U on a qubit is thus

$$U : (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta) \longrightarrow (\sin\theta'\cos\phi', \sin\theta'\sin\phi', \cos\theta') \tag{7}$$

with $U \in \mathrm{SU}(2)$. A common choice of generators of are $\{J^j = \sigma^j/2\}$, where σ^j are **Pauli operators**. In quantum computation and quantum information, we prefer the notations that

$$X \equiv \sigma^x, \quad Y \equiv \sigma^y, \quad Z \equiv \sigma^z \tag{8}$$

Under the representation of Z, we define the **rotation gates (unitaries)** as

$$R_x(\theta) = e^{-\frac{i}{2}\theta X} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{9}$$

$$R_y(\theta) = e^{-\frac{i}{2}\theta Y} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{10}$$

$$R_z(\theta) = e^{-\frac{i}{2}\theta Z} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} \tag{11}$$

which are elemental single-qubit operations, and any single qubit operator U can be reduced to a combination of them. As a global factor does not affect a state, typically we do not distinguish two gates up to a global phase. For example, we sometimes write

$$R_z(\theta) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \tag{12}$$

2.2 Frequently-used single-qubit gates

For convenience, there are some predefined single-qubit operations.

Pauli gates:

$$X := iR_x(\pi) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{13}$$

$$Y := iR_y(\pi) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{14}$$

$$Z := iR_z(\pi) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{15}$$

- where X is also called the **NOT gate**.

Hadamard gate

$$H := iR_x(\pi)R_y(\frac{\pi}{2}) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{16}$$

- It is easy to check that $H = (X + Z)/\sqrt{2}$. The effect of H is to map a classical bit to a qubit, and vice versa. In other words, it generates superposition.

Phase gate or S gate

$$S := R_z(\frac{\pi}{2}) = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{17}$$

T gate

$$T := R_z(\frac{\pi}{4}) = e^{i\frac{\pi}{8}} \begin{bmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix} \tag{18}$$

- This gate relates to an important concept called **non-stabilizerness** or **magic** (see another note of me).

3 Multi-qubits

3.1 Universal quantum computation

Suppose $|\psi\rangle$ and $|\psi'\rangle$ are two arbitary states of a n-qubit quantum system (computer). If If there exists a set of quantum gates, s.t. one can use them approximate $|\psi'\rangle$ to any precision starting from $|\psi\rangle$, then we call this set a **universal set of quantum gates**. If a quantum computer has a universal set of quantum gates, it is called a **universal quantum computer**. Otherwise, it is typically refered to as a **special quantum computer** such as a quantum annealor.

Apparently, for a single qubit system, the collection of all the single-qubit gates, i.e. the $\mathrm{SU}(2)$ group, forms a universal set of quantum gates. However, only with single-qubit unitaries, it is not sufficient to perform universal quantum computation when there are two qubits since we cannot generate entanglement.

To generate entanglement, we introduce the **CNOT gate**, which is a double-qubit unitary. We specify one qubit to be the **controlled qubit**, and the other one to be the **target qubit**. Then the effect of CNOT gate is

- If the controlled qubit is in $|1\rangle$ do we perform a X gate on the target qubit
- Otherwise, we do nothing.

The matrix representation of CNOT gate is

$$\mathrm{CNOT}_{j\to k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \mathrm{CNOT}_{k\to j} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \tag{19}$$

for $j < k$ and with big-endian convention.

(Theorem) *The three single-qubit rotation gates and CNOT gate compose a universal set of quantum gates for any n-qubit systems.*

This universal set of quantum gates is not unique. For example, $\{H, S, \text{CNOT}, T\}$ also forms a universal set of quantum gates.

3.2 Frequently-used multi-qubit gates

SWAP gate

$$\text{SWAP} : |a, b\rangle \longrightarrow |b, a\rangle \tag{20}$$

- For two qubits, the matrix representation is

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{21}$$

Multi-controlled-U gate or C$^m - U_{n\times n}$ gate

- This is a generalization of the CNOT gate, for which we have m controlled qubits and n target qubits. Here, the rule does not have to be that all controlled qubits to be $|1\rangle$. It can be more general to specify their states. If and only if the m qubits are in the required states, perform $U_{n\times n}$ to the n target qubits.
- Therefore, CNOT gate is also called CX gate.
- CCNOT or C^{2}NOT gate has another name called **Toffoli gate**.
- CSWAP gate is also called the **Fradkin gate**.