5

Quantum Gates, Quantum Circuit and Quantum Computation

5.1 Introduction

We have introduced qubits to store information, and used them for secure communications. It is time to consider operations acting on them. These operations are called gates, or more precisely **quantum gates**, in analogy with those in classical logic circuits. We will first introduced some simple quantum gates, and show that more complicated **quantum circuits** are composed of these simple gates. A collection of quantum circuits for executing a complicated algorithm, a **quantum algorithm**, is a part of a quantum computation. We have the following general description of quantum computing model as mentioned in Chapter 3.

DEFINITION 5.1.1. *(***Quantum Computation***) A quantum computation is a collection of the following three elements:*

(1) A register or a set of registers,

(2) A unitary matrix U, which is tailored to execute a given quantum algorithm, and

(3) Measurements to extract information we need.

More formally, we say a quantum computation is the set $\{\mathcal{H}, U, \{M_m\}\}$, where $\mathcal{H} = \mathbb{C}^{2^n}$ is the Hilbert space of an n-qubit register, $U \in \mathrm{U}(2^n)$ represents the quantum algorithm and $\{M_m\}$ is the set of measurement operators.

The hardware (1) along with equipment to control the qubits to perform (2) and (3) is called a quantum computer.

Suppose the register is set to a fiducial initial state, $|\psi_{\text{in}}\rangle = |00\ldots0\rangle$, for example. A unitary matrix U_{alg} is designed to represent an algorithm which we want to execute. Operation of U_{alg} on $|\psi_{\text{in}}\rangle$ yields the output state $|\psi_{\text{out}}\rangle = U_{\text{alg}}|\psi_{\text{in}}\rangle$. Information is extracted from $|\psi_{\text{out}}\rangle$ by appropriate measurements.

Actual quantum computation processes are very different from those of a classical counterpart. In a classical computer, we input the data from a keyboard or other input devices and the signal is sent to the I/O port of the

computer, which is then stored in the memory, then fed into the microprocessor, and the result is stored in the memory before it is printed or it is displayed on the screen. Thus information travels around the circuit. In contrast, information in quantum computation is stored in a register, first of all, and then external fields, such as oscillating magnetic fields, electric fields or laser beams are applied to produce gate operations on the register. These external fields are designed so that they produce desired gate operation, i.e., unitary matrix acting on a particular set of qubits. Therefore the information sits in the register and they are updated each time the gate operation acts on the register.

One of the other distinctions between classical computation and quantum computation is that the former is based upon digital processing and the latter upon hybrid (digital + analogue) processing. A qubit may take an arbitrary superposition of $|0\rangle$ and $|1\rangle$, and hence their coefficients are continuous complex numbers. A gate is also an element of a relevant unitary group, which contains continuous parameters. An operation such as "rotate a specified spin around the x-axis by an angle π" is implemented by applying a particular pulse of specified amplitude, angle and duration. These parameters are continuous numbers and always contain errors. These aspects might cause challenging difficulties in a physical realization of a quantum computer. We will use the IBM Q quantum computers to illustrate some of these issues.

Parts of this chapter depend on [1, 2] and [3].

5.2 Quantum Gates

We have so far studied the change of a state upon measurements. When measurements are not made, the time evolution of a state is described by the Schrödinger equation. The system preserves the norm of the state vector during time evolution. Thus the time development is unitary. Let U be such a time-evolution operator; $UU^\dagger = U^\dagger U = I$. We will be free from the Schrödinger equation in the following and assume there exist unitary matrices which we need. Physical implementation of these unitary matrices is another important area of quantum information processing. We will use the IBM Q quantum computers to illustrate the practical issues. One of the important conclusions derived from the unitarity of gates is that the computational process is reversible assuming that we are working on a closed system.

5.2.1 Simple Quantum Gates

Examples of quantum gates which transform a one-qubit state are given below. We call them one-qubit gates in the following. Linearity guarantees that the

action of a gate is completely specified as soon as its action on the basis $\{|0\rangle,\ |1\rangle\}$ is given. Let us consider the gate I whose action on the basis vectors are defined by $I:\ |0\rangle \mapsto |0\rangle,\ |1\rangle \mapsto |1\rangle$. The matrix expression of this gate is easily found as

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5.1}$$

Similarly we introduce $X:\ |0\rangle \mapsto |1\rangle,\ |1\rangle \mapsto |0\rangle$, $Y:\ |0\rangle \mapsto -|1\rangle,\ |1\rangle \mapsto |0\rangle$, and $Z:\ |0\rangle \mapsto |0\rangle,\ |1\rangle \mapsto -|1\rangle$, whose matrix representations are

$$X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x, \tag{5.2}$$

$$Y = |0\rangle\langle 1| - |1\rangle\langle 0| = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_y, \tag{5.3}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z. \tag{5.4}$$

The transformation I is the trivial (identity) transformation, while X is the negation (NOT), Z the phase shift and $Y = XZ$ the combination of them. It is easily verified that these gates are unitary.

The **CNOT** (**controlled-NOT**) gate is a two-qubit gate, which plays quite an important role in quantum computation. The gate flips the second qubit (the **target qubit**) when the first qubit (the **control qubit**) is $|1\rangle$, while leaving the second bit unchanged when the first qubit state is $|0\rangle$. Let $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ be a basis for the two-qubit system. In the following, we use the standard basis vectors with components

$$|00\rangle = (1,0,0,0)^t,\ |01\rangle = (0,1,0,0)^t,\ |10\rangle = (0,0,1,0)^t,\ |11\rangle = (0,0,0,1)^t.$$

The action of the CNOT gate, whose matrix expression will be written as U_{CNOT}, is

$$U_{\mathrm{CNOT}}:\ |00\rangle \mapsto |00\rangle,\ |01\rangle \mapsto |01\rangle,\ |10\rangle \mapsto |11\rangle,\ |11\rangle \mapsto |10\rangle.$$

It has two equivalent expressions

$$\begin{aligned} U_{\mathrm{CNOT}} &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\ &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X, \end{aligned} \tag{5.5}$$

having a matrix form

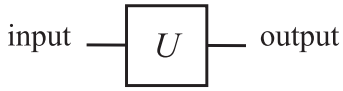
$$U_{\mathrm{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{5.6}$$

The second expression of the RHS in Eq. (5.5) shows that the action of U_{CNOT} on the target qubit is I when the control qubit is in the state $|0\rangle$, while it is σ_x

when the control qubit is in $|1\rangle$. Verify that $U_{\rm CNOT}$ is unitary and, moreover, idempotent, i.e., $U^2_{\rm CNOT} = I$.

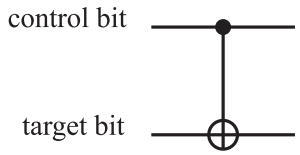
Let $\{|i\rangle\}$ be the basis vectors, where $i \in \{0, 1\}$. The action of CNOT on the input state $|i\rangle|j\rangle$ is written as $|i\rangle|i \oplus j\rangle$, where $i \oplus j$ is an addition mod 2, that is, $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1$ and $1 \oplus 1 = 0$.

It is convenient to introduce graphical representations of quantum gates. A one-qubit gate whose unitary matrix representation is U is depicted as



The left horizontal line is the input qubit state, while the right horizontal line is the output qubit state. Therefore the time flows from the left to the right.

A CNOT gate is expressed as

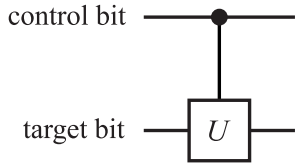


where $\bullet$ denotes the control qubit, while $\bigoplus$ denotes the conditional negation. There may be many control qubits (see CCNOT gate below).

More generally, we consider a controlled-U gate,

$$V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U, \tag{5.7}$$

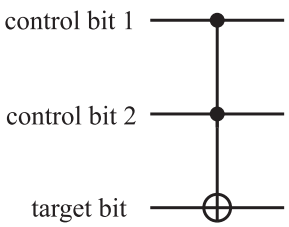
in which the target bit is acted on by a unitary transformation U only when the control qubit is $|1\rangle$. This gate is denoted graphically as



The **CCNOT** (**Controlled-Controlled-NOT**) gate has three inputs, and the third qubit flips when and only when the first two qubits are both in the state $|1\rangle$. The explicit form of the CCNOT gate is

$$U_{\rm CCNOT} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X. \tag{5.8}$$

This gate is graphically expressed as



The CCNOT gate is also known as the **Toffoli gate**.

5.2.2 Walsh-Hadamard Transformation

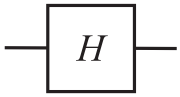
The **Hadamard gate** or the **Hadamard transformation** H is an important unitary transformation defined by

$$\begin{aligned} U_{\mathrm{H}} : |0\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{5.9}$$

It is used to generate a superposition state from $|0\rangle$ or $|1\rangle$. The matrix representation of H is

$$U_{\mathrm{H}} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{5.10}$$

A Hadamard gate is depicted as



There are numerous important applications of the Hadamard transformation. All possible 2^n states are generated, when U_{H} is applied on each qubit of the state $|00\ldots0\rangle$:

$$\begin{aligned} &(H \otimes H \otimes \ldots \otimes H)|00\ldots0\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \ldots \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \end{aligned} \tag{5.11}$$

Therefore, we produce a superposition of all the states $|x\rangle$ with $0 \leq x \leq 2^n - 1$ simultaneously. This action of H on an n-qubit system is called the **Walsh transformation**, or **Walsh-Hadamard transformation**, and denoted as W_n. Note that

$$W_1 = U_{\mathrm{H}}, \quad W_{n+1} = U_{\mathrm{H}} \otimes W_n. \tag{5.12}$$

5.2.3 SWAP Gate and Fredkin Gate

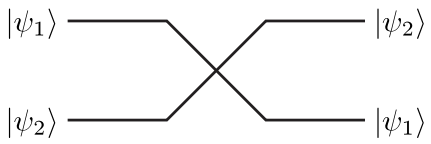
The **SWAP gate** acts on a tensor product state as

$$U_{\mathrm{SWAP}}|\psi_1, \psi_2\rangle = |\psi_2, \psi_1\rangle. \tag{5.13}$$

The explict form of $U_{\rm SWAP}$ is given by

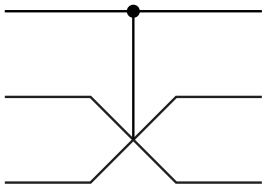
$$\begin{aligned} U_{\rm SWAP} &= |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \\ &= \begin{pmatrix} 1\,0\,0\,0 \\ 0\,0\,1\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,1 \end{pmatrix}. \end{aligned} \tag{5.14}$$

Needless to say, it works as a linear operator on a superposition of states. The SWAP gate is expressed as



Note that the SWAP gate is a special gate which maps an arbitrary tensor product state to a tensor product state. In contrast, most two-qubit gates map a tensor product state to an entangled state.

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 $|1\rangle$. Its explicit form is

$$U_{\rm Fredkin} = |0\rangle\langle 0| \otimes I_4 + |1\rangle\langle 1| \otimes U_{\rm SWAP}. \tag{5.15}$$

5.2.4 Universal Quantum Gates

It can be shown that any classical logic gate can be constructed by using a small set of gates, AND, NOT and XOR, for example. Such a set of gates is called the *universal* set of classical gates. Since the CCNOT gate can simulate these classical gates, quantum circuits simulate any classical circuits. It should be noted that the set of quantum gates is much larger than those classical gates which can be simulated by quantum gates; see Section 5.5. Thus we want to find a universal set of *quantum* gates from which any quantum circuits, i.e., any unitary matrix, can be constructed.

We will prove the following.

THEOREM 5.2.1. *(Barenco et al.) [14] The set of single qubit gates and the CNOT gate are universal. Namely, any unitary gate acting on an n-qubit register can be implemented with single qubit gates and CNOT gates.*

We need several lemmas to prove the theorem.

LEMMA 5.2.2. *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*

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

Proof. After some calculation, we obtain

$$R_z(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} e^{i(\alpha+\gamma)/2}\cos(\beta/2) & e^{i(\alpha-\gamma)/2}\sin(\beta/2) \\ -e^{i(-\alpha+\gamma)/2}\sin(\beta/2) & e^{-i(\alpha+\gamma)/2}\cos(\beta/2) \end{pmatrix}. \quad (5.16)$$

Any $U \in \mathrm{SU}(2)$ may be written in the form

$$U = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} = \begin{pmatrix} \cos\theta e^{i\lambda} & \sin\theta e^{i\mu} \\ -\sin\theta e^{-i\mu} & \cos\theta e^{-i\lambda} \end{pmatrix}, \quad (5.17)$$

where we used the fact that $\det U = |a|^2 + |b|^2 = 1$. Now we obtain $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$ by making identifications

$$\theta = \frac{\beta}{2}, \lambda = \frac{\alpha+\gamma}{2}, \mu = \frac{\alpha-\gamma}{2}. \quad (5.18)$$

∎

LEMMA 5.2.3. *Let $U \in \mathrm{SU}(2)$. Then there exist $A, B, C \in \mathrm{SU}(2)$ such that $U = AXBXC$ and $ABC = I$, where $X = \sigma_x$.*

Proof. Lemma 5.2.2 states that $U = R_z(\alpha)R_y(\beta)R_z(\gamma)$ for some $\alpha, \beta, \gamma \in \mathbb{R}$. Let

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

Then

$$\begin{aligned} AXBXC &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)XR_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)XR_z\left(-\frac{\alpha-\gamma}{2}\right) \\ &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)\left[XR_y\left(-\frac{\beta}{2}\right)X\right]\left[XR_z\left(-\frac{\alpha+\gamma}{2}\right)X\right]R_z\left(-\frac{\alpha-\gamma}{2}\right) \\ &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(\frac{\beta}{2}\right)R_z\left(\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right) \\ &= R_z(\alpha)R_y(\beta)R_z(\gamma) = U, \end{aligned}$$

where use has been made of the identities $X^2 = I$ *and* $X\sigma_{y,z}X = -\sigma_{y,z}$.

It is also verified that

$$\begin{aligned} ABC &= R_z(\alpha)R_y\left(\frac{\beta}{2}\right)R_y\left(-\frac{\beta}{2}\right)R_z\left(-\frac{\alpha+\gamma}{2}\right)R_z\left(-\frac{\alpha-\gamma}{2}\right) \\ &= R_z(\alpha)R_y(0)R_z(-\alpha) = I. \end{aligned}$$

This proves the Lemma. ∎

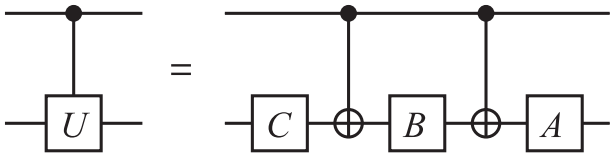


FIGURE 5.1
Controlled-U gate is made of at most three single-qubit gates and two CNOT gates for any $U \in \mathrm{SU}(2)$.

LEMMA 5.2.4. *Let* $U \in \mathrm{SU}(2)$ *be factorized as* $U = AXBXC$ *as in the previous Lemma. Then the controlled-U gate can be implemented with at most three single-qubit gates and two CNOT gates (see Fig. 5.1).*

Proof. The proof is almost obvious. When the control bit is 0*, the target bit* $|\psi\rangle$ *is operated by* C, B *and* A *in this order so that*

$$|\psi\rangle \mapsto ABC|\psi\rangle = |\psi\rangle,$$

while when the control qubit is 1*, we have*

$$|\psi\rangle \mapsto AXBXC|\psi\rangle = U|\psi\rangle.$$ ∎

So far, we have worked with $U \in \mathrm{SU}(2)$. To implement a general U-gate with $U \in \mathrm{U}(2)$, we have to deal with the phase. Let us first recall that any $U \in \mathrm{U}(2)$ is decomposed as $U = e^{i\alpha}V,\ V \in \mathrm{SU}(2), \alpha \in \mathbb{R}$.

LEMMA 5.2.5. *Let*

$$\Phi(\phi) = e^{i\phi}I = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

and

$$D = R_z(-\phi)\Phi\left(\frac{\phi}{2}\right) = \begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix}\begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}.$$

Then the controlled-$\Phi(\phi)$ gate is expressed as a tensor product of single qubit gates as

$$U_{\mathrm{C}\Phi(\phi)} = D \otimes I. \tag{5.19}$$

.

Proof. The LHS is

$$\begin{aligned} U_{\mathrm{C}\Phi(\phi)} &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \Phi(\phi) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes e^{i\phi} I \\ &= |0\rangle\langle 0| \otimes I + e^{i\phi}|1\rangle\langle 1| \otimes I, \end{aligned}$$

while the RHS is

$$\begin{aligned} D \otimes I &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \otimes I \\ &= \left[|0\rangle\langle 0| + e^{i\phi}|1\rangle\langle 1|\right] \otimes I = U_{\mathrm{C}\Phi(\phi)}, \end{aligned}$$

which proves the lemma. ∎

Figure 5.2 shows the statement of the above lemma.

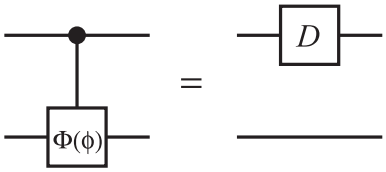


FIGURE 5.2
Equality $U_{\mathrm{C}\Phi(\phi)} = D \otimes I$.

Now we are ready to prove the main proposition.

PROPOSITION 5.2.6. *Let $U \in \mathrm{U}(2)$. Then the controlled-U gate U_{CU} can be constructed by at most four single-qubit gates and two CNOT gates.*

Proof. Let $U = \Phi(\phi)AXBXC$. According to the discussion above, the controlled-U gate is written as a product of the controlled-$\Phi(\phi)$ gate and the controlled-$AXBXC$ gate. Moreover, Lemma 5.2.5 states that the controlled-$\Phi(\phi)$ gate may be replaced by a single-qubit phase gate acting on the first qubit. The rest of the gate, the controlled-$AXBXC$ gate is implemented with three SU(2) gates and two CNOT gates as proved in Lemma 5.2.3. Therefore we have the following decomposition:

$$U_{CU} = (D \otimes A)U_{\mathrm{CNOT}}(I \otimes B)U_{\mathrm{CNOT}}(I \otimes C), \tag{5.20}$$

where

$$D = R_z(-\phi)\Phi(\phi/2)$$

and use has been made of the identity $(D \otimes I)(I \otimes A) = D \otimes A$. ∎

Figure 5.3 shows the statement of the proposition.

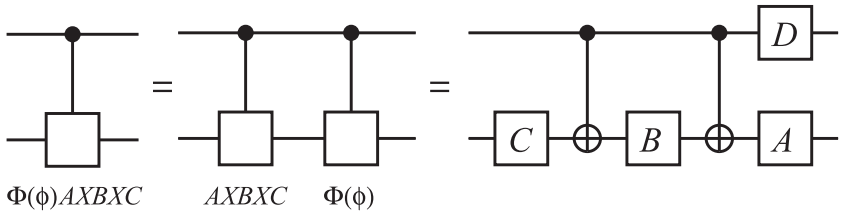


FIGURE 5.3
Controlled-U gate is implemented with at most four single-qubit gates and two CNOT gates.

STEP 3: CCNOT gate and its variants are implemented with CNOT gates and their variants.

Now our final task is to prove that controlled-U gates with $n-1$ control bits are also constructed using single-qubit gates and CNOT gates. Let us start with the simplest case, in which $n = 3$.

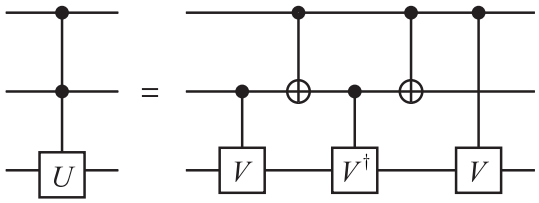


FIGURE 5.4
Controlled-controlled-U gate is equivalent to the gate made of controlled-V gates with $U = V^2$ and CNOT gates.

LEMMA 5.2.7. *The two quantum circuits in Fig. 5.4 are equivalent, where* $U = V^2$.

Proof. If both the first and the second qubits are 0 in the RHS, all the gates

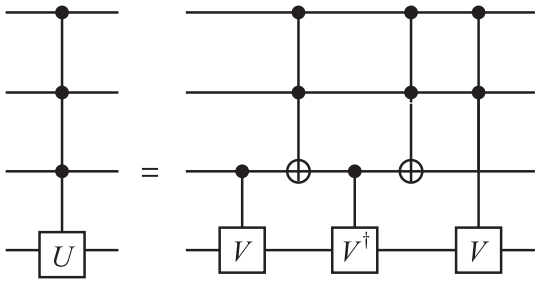


FIGURE 5.5
Decomposition of the C^3U gate.

are ineffective and the third qubit is unchanged; the gate in this subspace acts as $|00\rangle\langle 00| \otimes I$. *In case the first qubit is 0 and the second is 1, the third qubit is mapped as* $|\psi\rangle \mapsto V^\dagger V|\psi\rangle = |\psi\rangle$; *the gate is then* $|01\rangle\langle 01| \otimes I$. *When the first qubit is 1 and the second is 0, the third qubit is mapped as* $|\psi\rangle \mapsto VV^\dagger|\psi\rangle = |\psi\rangle$; *hence the gate in this subspace is* $|10\rangle\langle 10| \otimes I$. *Finally let both the first and the second qubits be 1. Then the action of the gate on the third qubit is* $|\psi\rangle \mapsto VV|\psi\rangle = U|\psi\rangle$; *namely the gate in this subspace is* $|11\rangle\langle 11| \otimes U$. *Thus it has been proved that the RHS of Fig. 5.4 is*

$$(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes U, \tag{5.21}$$

namely the controlled-controlled-U gate. ∎

This decomposition is explained intuitively as follows. The first V operates on the third qubit $|\psi\rangle$ if and only if the second qubit is 1. $V^\dagger$ is in action if and only if $x_1 \oplus x_2 = 1$, where x_k is the input bit of the kth qubit. The second V operation is applied if and only if the first qubit is 1. Thus the action of this gate on the third qubit is $V^2 = U$ only when $x_1 \wedge x_2 = 1$ and I otherwise. This intuitive picture is of help when we implement the U gate with more control qubits.

A simple generalization of the above construction is applied to a controlled-U gate with three control bits as Exercise 5.15 shows.

Now it should be clear how these examples are generalized to gates with more control qubits.

PROPOSITION 5.2.8. *The quantum circuit in Fig. 5.6 with* $U = V^2$ *is a decomposition of the controlled-U gate with* $n-1$ *control qubits.*

The proof of the above proposition is very similar to that of Lemma 5.2.7 and Exercise 5.15 and is left as an exercise to the readers.

Proof of Theorem 5.2.1. Let $U \in U(N)$ with $N = 2^n$. We prove by induction on n that there are elementary gates. The result trivially holds if $n = 1$.

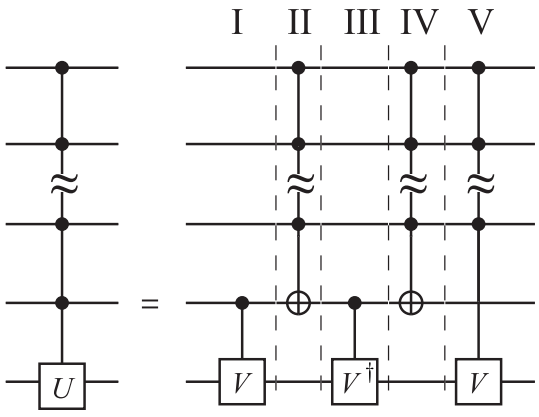


FIGURE 5.6
Decomposition of the $C^{(n-1)}U$ gate. The number on the top denotes the layer refered to in the text.

Suppose the result holds for matrices in $SU(N)$ with $N = 2^n$. Let $U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}$, where $U_{11}, U_{12}, U_{21}, U_{22} \in M_N$. There are $R_1, S_1 \in U(N)$ such that $R_1 U_{11} S_1 = \text{diag}(c_1, \ldots, c_N) = D_{11}$ with $0 \le c_1 \le \cdots \le c_N \le 1$. Let $\tilde{U} = (I_2 \otimes R_1) U (I_2 \otimes S_1) = \begin{pmatrix} \tilde{U}_{11} & \tilde{U}_{12} \\ \tilde{U}_{21} & \tilde{U}_{22} \end{pmatrix}$. Note that the first N rows of $\tilde{U}$ form an orthonormal set. So, $\tilde{U}_{12}$ also has orthogonal rows, and there is $S_2 \in U(N)$ such that $\tilde{U}_{12} S_2 = \text{diag}(s_1, \ldots, s_N) = D_{12}$ with $s_1, \ldots, s_N \ge 0$. Similarly, the first N columns form an orthonormal set. So, $\tilde{U}_{21}$ also has orthogonal columns, and there is $R_2 \in U(N)$ such that $R_2 \tilde{U}_{21} = \text{diag}(\tilde{s}_1, \ldots, \tilde{s}_N) = D_{21}$ with $\tilde{s}_1, \ldots, \tilde{s}_N \le 0$. Since the first N rows and the first N columns of $\tilde{U}$ has unit lengths, we see that $s_j = -\tilde{s}_j = \sqrt{1 - c_j^2}$ for $j = 1, \ldots, N$. Hence,

$$\hat{U} = (I_N \oplus R_2)(I_2 \otimes R_1) U (I_2 \otimes S_1)(I_n \oplus S_2) = \begin{pmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{pmatrix}$$

with $D_{22} = (d_{ij})$. Note that the jth row and the $(N+j)$th row of $\hat{U}$ form an orthnormal set. For $j = 1, \ldots, N$, $c_j s_j - s_j d_{jj} = 0$. If $s_j \ne 0$, then $d_{jj} = c_j$. Since the rows and columns of $\hat{U}$ have unit lengths, we see that $d_{jj} = c_j$ is the only nonzero entry in the jth row and jth column of $\hat{U}$. Consequently, if $s_1 \ge \cdots \ge s_k \ne 0 = s_{k+1} = \cdots = s_N$, then $\hat{D}_{22} = \text{diag}(c_1, \ldots, c_k) \oplus W$ with $W \in U(N-k)$. We may adjust R_2 and assume that $W = I_{N-k}$. As a result, $\hat{U}$ can be written as a product of k-controlled-U gates. By induction assumption, $I_N \oplus R_2, I_2 \otimes R_1, I_2 \otimes S_1, I_N \oplus S_2$ can be written as the product of elementary gates. So, $U = (I_2 \otimes R_1)^\dagger (I_N \oplus R_2)^\dagger \hat{U} (I_N \oplus S_2)^\dagger (I_2 \otimes S_1)^\dagger$ is a product of elementary gates. ∎

Note that in the last step of the proof, we can let $U_1 = \begin{pmatrix} c_1 & -s_1 \\ s_1 & c_1 \end{pmatrix} \otimes I_N$ so that the submatrix of $U_1\hat{U}$ in rows and columns $1, N+1$ is identity matrix I_2. Then we can apply a 1-controlled-U unitary matrix $U_2 \in U(2N)$ with so that the submatrix of $U_2U_1\hat{U}$ in rows and columns $1, 2, N+1, N+2$ is the identity matrix I_4. Continue this process, we can write $\hat{U}$ as the product of k-controlled-U matrix for $k = 0, \ldots, n$.

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-controlled-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

$$\gamma_{n,n-1} = 2\gamma_{n-1,n-2} + 1, \quad \gamma_{n,0} = 2\gamma_{n-1,0} + 1,$$
$$\gamma_{n,j} = 2(\gamma_{n-1,j} + \gamma_{n-1,j-1}) + 1, \quad j = 1, \ldots, n-2.$$

Other types of gates are also implemented with single-qubit gates and the CNOT gates. See Barenco *et al.* [14] for further details. A few remarks are in order. The above controlled-U gate with $(n-1)$ control bits requires $\Theta(n^2)$ elementary gates.*† Let us write the number of the elementary gates required

*We call single-qubit gates and the CNOT gates elementary gates from now on.

†We will be less strict in the definition of "the order of." In the theory of computational complexity, people use three types of "order of magnitude." One writes "$f(n)$ is $O(g(n))$" if there exist $n_0 \in \mathbb{N}$ and $c \in \mathbb{R}$ such that $f(n) \leq cg(n)$ for $n \geq n_0$. In other words, O sets the asymptotic upper bound of $f(n)$. A function $f(n)$ is said to be $\Omega(g(n))$ if there exist $n_0 \in \mathbb{N}$ and $c \in \mathbb{R}$ such that $f(n) \geq cg(n)$ for $n \geq n_0$. In other words, Ω sets the asymptotic lower bound of $f(n)$. Finally $f(n)$ is said to be $\Theta(f(n))$ if $f(n)$ behaves asymptotically as $g(n)$, namely if $f(n)$ is both $O(g(n))$ and $\Omega(g(n))$.

to construct the gate in Fig. 5.6 by $C(n)$. Construction of layers I and III requires elementary gates whose number is independent of n. It can be shown that the number of the elementary gates required to construct the controlled NOT gate with $(n-2)$ control qubits is $\Theta(n)$ [14]. Therefore layers II and IV require $\Theta(n)$ elementary gates. Finally the layer V, a controlled-V gate with $(n-2)$ control qubits, requires $C(n-1)$ basic gates by definition. Thus we obtain a recursion relation

$$C(n) - C(n-1) = \Theta(n). \tag{5.22}$$

The solution to this recursion relation is

$$C(n) = \Theta(n^2). \tag{5.23}$$

Therefore, implementation of a controlled-U gate with $U \in \mathrm{U}(2)$ and $(n-1)$ control qubits requires $\Theta(n^2)$ elementary gates.

5.3 Some applications of Quantum gates

Now we are ready to introduce three simple applications of qubits and quantum gates: **dense coding**, **quantum teleportation**, and **quantum state tomography**.

The Bell state has been delivered beforehand, and one of the qubits carries two classical bits of information in the dense coding system. In the quantum teleportation, on the other hand, two classical bits are used to transmit a single qubit. At first glance, the quantum teleportation may seem to be in contradiction with the no-cloning theorem. However, this is not the case since the original state is destroyed.

Entanglement is the keyword in the first two applications. The setting is common for both cases. Suppose Alice wants to send Bob information. Each of them has been sent each of the qubits of the Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{5.24}$$

in advance. Suppose Alice has the first qubit and Bob has the second.

5.3.1 Dense Coding

Alice: Alice wants to send Bob a binary number $x \in \{00, 01, 10, 11\}$. She picks up one of $\{I, X, Y, Z\}$ according to x she has chosen and applies the transformation on her qubit (the first qubit of the Bell state). Applying the

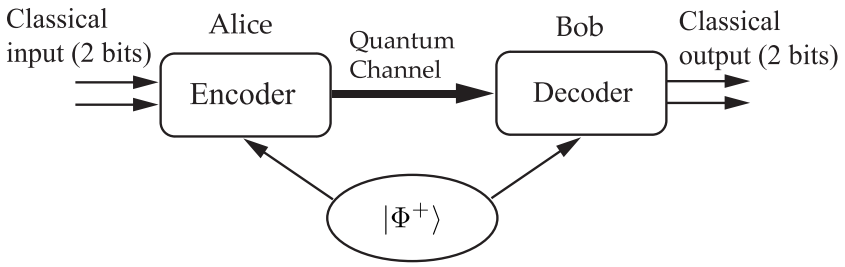


FIGURE 5.7
Communication from Alice to Bob using dense coding. Each qubit of the Bell state $|\Phi^+\rangle$ has been distributed to each of them beforehand. Then two bits of classical information can be transmitted by sending a single qubit through the quantum channel.

transformation to only her qubit means she applies an identity transformation to the second qubit which Bob keeps with him. This results in

$$\begin{array}{lll} x \quad \text{transformation } U & & \text{state after transformation} \\ 0 = 00 & I \otimes I & |\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ 1 = 01 & X \otimes I & |\psi_1\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \\ 2 = 10 & Y \otimes I & |\psi_2\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \\ 3 = 11 & Z \otimes I & |\psi_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \end{array} \tag{5.25}$$

Alice sends Bob her qubit after the transformation given above is applied. Note that the set of four states in the rightmost column is nothing but the four Bell basis vectors.

Bob: Bob applies CNOT to the entangled pair in which the first qubit, the received qubit, is the control qubit, while the second one, which Bob keeps, is the target bit. This results in a tensor-product state:

$$\begin{array}{llll} \text{Received state} & \text{Output of CNOT} & \text{1st qubit} & \text{2nd qubit} \\ |\psi_0\rangle & \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & |0\rangle \\ |\psi_1\rangle & \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) & \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) & |1\rangle \\ |\psi_2\rangle & \frac{1}{\sqrt{2}}(|11\rangle - |01\rangle) & \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) & |1\rangle \\ |\psi_3\rangle & \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & |0\rangle \end{array} \tag{5.26}$$

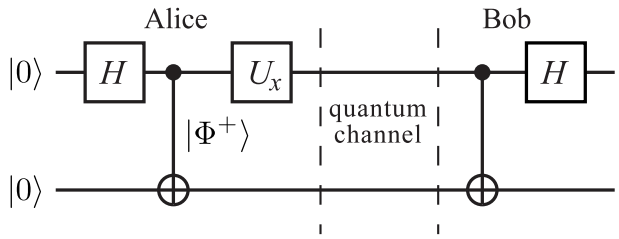


FIGURE 5.8
Quantum circuit implementation of the dense coding system. The leftmost Hadamard gate and the next CNOT gate generate the Bell state. Then a unitary gate U, depending on the bits Alice wants to send, is applied to the first qubit. Bob applies the rightmost CNOT gate and the Hadamard gate to decode Alice's message.

Note that Bob can measure the first and second qubits independently since the output is a tensor-product state. The number x is either 00 or 11 if the measurement outcome of the second qubit is $|0\rangle$, while it is either 01 or 10 if the meansurement outcome is $|1\rangle$.

Finally, a Hadamard transformation H is applied on the first qubit. Bob obtains

$$\begin{array}{lll} \text{Received state} & \text{1st qubit} & U_{\rm H}|\text{1st qubit}\rangle \\ |\psi_0\rangle & \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) & |0\rangle \\ |\psi_1\rangle & \frac{1}{\sqrt{2}}(|1\rangle+|0\rangle) & |0\rangle \\ |\psi_2\rangle & \frac{1}{\sqrt{2}}(|1\rangle-|0\rangle) & -|1\rangle \\ |\psi_3\rangle & \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) & |1\rangle \end{array} \tag{5.27}$$

The number x is either 00 or 01 if the measurement of the first qubit results in $|0\rangle$, while it is either 10 or 11 if it is $|1\rangle$. Therefore, Bob can tell what x is in every case.

Quantum circuit implementation for the dense coding is given in Fig. 5.8

5.3.2 Quantum Teleportation

The purpose of **quantum teleportation** is to transmit an unknown quantum *state* of a qubit using two classical bits such that the recipient reproduces exactly the same state as the original qubit state. Note that the qubit itself is not transported but the information required to reproduce the quantum state is transmitted. The original state is destroyed such that quantum teleportation should not be in contradiction with the no-cloning theorem. Quantum

teleportation has already been realized under laboratory conditions using photons [6, 7, 8, 9], coherent light field [10], NMR [11], and trapped ions [12, 13]. The teleportation scheme introduced in this section is due to [11]. Figure

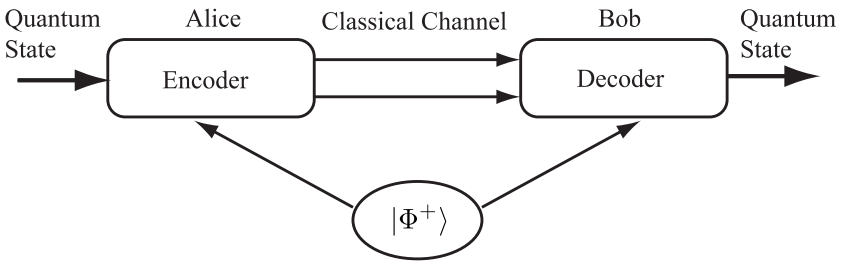


FIGURE 5.9
In quantum teleportation, Alice sends Bob two classical bits so that Bob reproduces a qubit state Alice used to have.

5.9 shows the schematic diagram of quantum teleportation, which will be described in detail below.

Alice: Alice has a qubit, whose state she does not know. She wishes to send Bob the quantum state of this qubit through a classical communication channel. Let

$$|\phi\rangle = a|0\rangle + b|1\rangle \tag{5.28}$$

be the state of the qubit. Both of them have been given one of the qubits of the entangled pair

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

as in the case of the dense coding.

Alice applies the decoding step in the dense coding to the qubit $|\phi\rangle = a|0\rangle + b|1\rangle$ to be sent and her qubit of the entangled pair. They start with the state

$$\begin{aligned} |\phi\rangle \otimes |\Phi^+\rangle &= \frac{1}{\sqrt{2}}\left[a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)\right] \\ &= \frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right), \end{aligned} \tag{5.29}$$

where Alice has the first two qubits while Bob has the third. Alice applies

$U_{\text{CNOT}} \otimes I$ followed by $U_{\text{H}} \otimes I \otimes I$ to this state, which results in

$$\begin{aligned}
&(U_{\text{H}} \otimes I \otimes I)(U_{\text{CNOT}} \otimes I)(|\phi\rangle \otimes |\Phi^+\rangle) \\
&= (U_{\text{H}} \otimes I \otimes I)(U_{\text{CNOT}} \otimes I)\frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle\right) \\
&= \frac{1}{2}\left[a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\right] \\
&= \frac{1}{2}[|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) \\
&\qquad +|10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)]. \qquad (5.30)
\end{aligned}$$

If Alice measures the two qubits in her hand, she will obtain one of the states $|00\rangle, |01\rangle, |10\rangle$ or $|11\rangle$ with equal probability 1/4. Bob's qubit (a qubit from the Bell state initially) collapses to $a|0\rangle + b|1\rangle, a|1\rangle + b|0\rangle, a|0\rangle - b|1\rangle$ or $a|1\rangle - b|0\rangle$, respectively, depending on the result of Alice's measurement. Alice then sends Bob her result of the measurement using two classical bits.

Notice that Alice has totally destroyed the initial qubit $|\phi\rangle$ upon her measurement. This makes quantum teleportation consistent with the no-cloning theorem.

Bob: After receiving two classical bits, Bob knows the state of the qubit in his hand;

Received bits	Bob's state	Decoding
00	$a\|0\rangle + b\|1\rangle$	I
01	$a\|1\rangle + b\|0\rangle$	X
10	$a\|0\rangle - b\|1\rangle$	Z
11	$a\|1\rangle - b\|0\rangle$	Y

(5.31)

Bob reconstructs the intial state $|\phi\rangle$ by applying the decoding process shown above. Suppose Alice sends Bob the classical bits 10, for example. Then Bob applies Z to his state to reconstruct $|\phi\rangle$ as follows:

$$Z: \ (a|0\rangle - b|1\rangle) \mapsto (a|0\rangle + b|1\rangle) = |\phi\rangle.$$

Figure 5.10 shows the actual quantum circuit for quantum teleportation.

5.3.3 Quantum State Tomography

Quantum tomography or quantum state tomography is the process by which a quantum state is reconstructed using measurements on an ensemble of identical quantum states. Note that every measurement will collapse the given quantum state ρ into the eigenprojections of the measurement operator. So, we need an ensemble of identical quantum states to extract information of the quantum state ρ. Suppose we have an ensemble of identical qubit states

$$\rho = \frac{1}{2}\begin{pmatrix} 1+a & b-ic \\ b+ic & 1-a \end{pmatrix} \qquad \text{with } a, b, c \in \mathbb{R}, a^2 + b^2 + c^2 \leq 1.$$

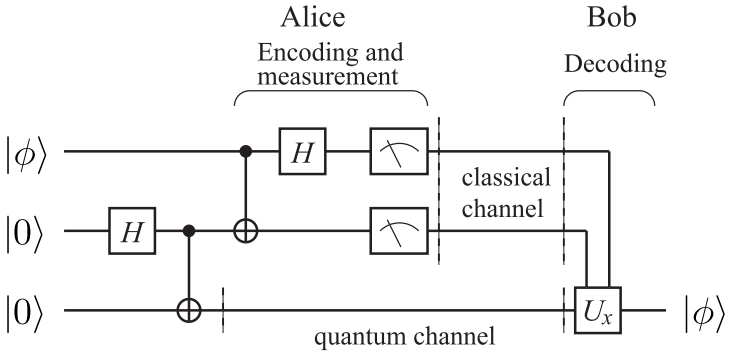


FIGURE 5.10
Quantum circuit implementation of quantum teleportation. Alice operates gates in the left side. The first Hadamard gate and the next CNOT gates generate the Bell state $|\Phi^+\rangle$ from $|00\rangle$. The bottom qubit is sent to Bob through a quantum channel while the first and the second qubits are measured after applying the second set of the CNOT gate and the Hadamard gate on them. The measurement outcome x is sent to Bob through a classical channel. Bob operates a unitary operation U_x, which depends on the received message x, on his qubit.

If we use a fixed measurement operator, say, corresponding to σ_z, hen the measurements will give us information about a, but no information about b, c. In order to get information on b and c, we will apply a rotation to ρ by $U_1, U_2 \in U(2)$ with

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \qquad \text{and} \qquad U_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -i \\ 1 & i \end{pmatrix}. \tag{5.32}$$

Then

$$U_1 \rho U_1^\dagger = \frac{1}{2} \begin{pmatrix} 1+b & c-ia \\ c+ia & 1-b \end{pmatrix} \qquad \text{and} \qquad U_2 \rho U_2^\dagger = \frac{1}{2} \begin{pmatrix} 1+c & a-ib \\ a+ib & 1-c \end{pmatrix}.$$

In the above process, one may assume that we apply the same measurement operator associated with A to the quantum states $\rho, U_1 \rho U_1^\dagger, U_2 \rho U_2^\dagger$. Alternatively, one may assume that we are applying measurement operators associated with $A, U_1^\dagger A U_1, U_2^\dagger A U_2$ to the ensemble of identical states ρ.[‡]

One can extend this idea to do the quantum state tomography to $\rho \in \mathbf{D}_d$.

THEOREM 5.3.1. *Let $\rho \in \mathbf{D}_d$. There exist $U_0, \ldots, U_d \in U(d)$ with $U_0 = I_d$ such that ρ can be determined by the diagonal entries of $U_0 \rho U_0^\dagger, \ldots, U_d \rho U_d^\dagger$.*

[‡]This is nothing but Shrödinger picture and Heisenberg picture of a quantum system.

Note that every $\rho = (\rho_{ij}) \in \mathbf{D}_d$ has trace 1, and is determined by $d^2 - 1$ real entries; ρ_{rr} for $r = 1, \ldots, d-1$, and the real parts and imaginary parts of ρ_{rs} for $1 \le r < j \le d$. For every $U_j \rho U_j^\dagger$, its diagonal entries can provide $d-1$ pieces of (real data) information of ρ. So, the diagonal entries of k such matrices can provide $k(d-1)$ piece of information of ρ. So, using $d+1$ such matrices is minimum.

Because of measurement errors, one may not be able to find a quantum state which fits all the measurement. In such a case, one may either get more measurements, or find the quantum state which best fits the measurements.

In applications, one often considers qubit state $\rho \in \mathbf{D}_d$ with $d = 2^n$. Of course, the above theorem applies to this case as well. For easy implementation, one may want to use special types of unitary $U \in U(d)$ and do the measurements of $UAU^\dagger$. Recall that a unitary $V \in U(2^n)$ is a local unitary if $V = R_1 \otimes \cdots \otimes R_n$ with $R_1, \ldots, R_n \in U(2)$. Physically, it means that the quantum gate V is acting on n-qubits individually. We have the following.

THEOREM 5.3.2. *Let $\rho \in \mathbf{D}_d$ with $d = 2^n$. Let $\mathcal{S}$ be the set of local unitary matrices of the form $V_1 \otimes \cdots \otimes V_d \in U(2^d)$ with $V_j \in \{I_2, U_1, U_2\}$, where U_1, U_2 are defined as in* (5.32)*. Then ρ can be determined by the diagonal entries of $V\rho V^\dagger$ for $V \in \mathcal{S}$.*

Proof. The proof can be done by induction on n. For $n = 1$, the result follows from Theorem 5.3.1. Assume that the result is true for n-qubit states. We will show that there cannot be two $(n+1)$-qubit states ρ_1, ρ_2 such that $V\rho_1 V^\dagger$ and $V\rho_2 V^\dagger$ have the same diagonal entries for all $V \in \mathcal{S}$. We will show that for any A with $\operatorname{Tr} A = 0$ and $VAV^\dagger$ has zero diagonal entries for all $V \in \mathcal{S}$, then A is zero. Let $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$ Now, consider $V \in \mathcal{S}$ of the form $I_2 \otimes V_0$ with $V_0 = V_1 \otimes \cdots \otimes V_n$. Since $VAV^\dagger = \begin{pmatrix} V_0 A_{11} V_0\dagger & V_0 A_{12} V_0^\dagger \\ V_0 A_{21} V_0^\dagger & V_0 A_{22} V_0^\dagger \end{pmatrix}$ always has diagonal zero diagonal entries, we see that $V_0 A_{11} V_0^\dagger$ and $V_0 A_{22} V_0^\dagger$ have zero diagonal entries for any $V_0 = V_1 \otimes \cdots \otimes V_n$. By induction assumption, $A_{11} = A_{22} = 0$. Next, let $A_{12} = B + iC$ with $B = (A_{12} + A_{21}^\dagger)/2$ and consider $V \in \mathcal{S}$ of the form $U_1 \otimes V_0$ with $V_0 = V_1 \otimes \cdots \otimes V_n$. We see that $VAV^\dagger = \begin{pmatrix} V_0 B V_0\dagger & V_0 C V_0^\dagger \\ V_0 C V_0^\dagger & -V_0 B V_0^\dagger \end{pmatrix}$ always has zero diagonal entries, and hence $B = 0$. Finally, consider $V \in \mathcal{S}$ of the form $U_2 \otimes V_0$ with $V_0 = V_1 \otimes \cdots \otimes V_n$, we see that $VAV^\dagger \begin{pmatrix} V_0 C V_0\dagger & 0 \\ 0 & -V_0 C V_0^\dagger \end{pmatrix}$ always have zero diagonal entries will imply $C = 0$. ∎

5.3.4 Implementations using IBM Q computers

IBM Q provides a wonderful platform for testing quantum algorithms.

For general introduction, see
https://qiskit.org/textbook/preface.html

For teleportation, see
https://qiskit.org/textbook/ch-algorithms/teleportation.html

For Superdense coding, see
https://qiskit.org/textbook/ch-algorithms/superdense-coding.html

For Quantum tomography, see
https://qiskit.org/documentation/tutorials/noise/8_tomography.html

5.4 Quantum Parallelism and Entanglement

Given an input x, a typical quantum computer computes $f(x)$ in such a way as

$$U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle, \tag{5.33}$$

where U_f is a unitary matrix that implements the function f.

Suppose U_f acts on the input which is a superposition of many states. Since U_f is a linear operator, it acts simultaneously on all the vectors that constitute the superposition. Thus the output is also a superposition of all the results;

$$U_f : \sum_x |x\rangle|0\rangle \mapsto \sum_x |x\rangle|f(x)\rangle. \tag{5.34}$$

Namely, when the input is a superposition of n states, U_f computes n values $f(x_k)$ $(1 \leq k \leq n)$ simultaneously. This feature, called the *quantum parallelism*, gives a quantum computer an enormous power. A quantum computer is advantageous compared to a classical counterpart in that it makes use of this quantum parallelism and also entanglement.

A unitary transformation acts on a superposition of all possible states in most quantum algorithms. This superposition is prepared by the action of the Walsh-Hadamard transformation on an n-qubit register in the state $|00\ldots0\rangle = |0\rangle \otimes |0\rangle \otimes \ldots \otimes |0\rangle$ resulting in

$$\frac{1}{\sqrt{2^n}} \left(|00\ldots0\rangle + |00\ldots1\rangle + \ldots |11\ldots1\rangle\right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \tag{5.35}$$

This state is a superposition of vectors encoding all the integers between 0 and $2^n - 1$. Then the linearity of U_f leads to

$$U_f \left(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle \right) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f|x\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle. \tag{5.36}$$

Note that the superposition is made of $2^n = e^{n \ln 2}$ states, which makes quantum computation exponentially faster than the classical counterpart in a certain kind of computation.

What about the limitation of a quantum computer? Let us consider the CCNOT gate, for example. This gate flips the third qubit if and only if the first and the second qubits are both in the state $|1\rangle$, while it leaves the third qubit unchanged otherwise. Let us fix the third input qubit to $|0\rangle$. It was shown in §5.5.3 that the third output is $|x \wedge y\rangle$, where $|x\rangle$ and $|y\rangle$ are the first and the second input qubit states, respectively. Suppose the input state is a superposition of all possible states while the third qubit is fixed to $|0\rangle$. This can be achieved by the Walsh-Hadamard transformation as

$$\begin{aligned} U_{\rm H}|0\rangle \otimes U_{\rm H}|0\rangle \otimes |0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ &= \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle). \end{aligned} \tag{5.37}$$

By operating CCNOT on this state, we obtain

$$U_{\rm CCNOT}(U_{\rm H}|0\rangle \otimes U_{\rm H}|0\rangle \otimes |0\rangle) = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle). \tag{5.38}$$

This output may be thought of as the truth table of AND: $|x, y, x \wedge y\rangle$. It is extremely important to note that the output is an entangled state and the measurement projects the state to *one line* of the truth table, i.e., a single term in the RHS of Eq. (5.38). The order of the measurements of the three qubits does not matter at all. The measurement of the third qubit projects the state to the superposition of the states with the given value of the third qubit. Repeating the measurements on the rest of the qubits leads to the collapse of the output state to one of $|x, y, x \wedge y\rangle$.

There is no advantage of quantum computation over classical at this stage. This is because only *one* result may be obtained by a single set of measurements. What is worse, we cannot choose a specific vector $|x, y, x \wedge y\rangle$ at our will! Thus any quantum algorithm should be programmed so that the particular vector we want to observe should have larger probability to be measured compared to other vectors. This step has no classical analogy and is very special in quantum computation. The programming strategies to deal with this feature are [2]

1. to amplify the amplitude, and hence the probability, of the vector that we want to observe. This strategy is employed in the Grover's database search algorithm.

2. to find a common property of all the $f(x)$. This idea was employed in the quantum Fourier transform to find the order[§] of f in the Shor's factoring algorithm.

[§]Let $m, N \in \mathbb{N}$ $(m < N)$ be numbers coprime to each other. Then there exists $P \in \mathbb{N}$ such

Now we consider the power of entanglement. Suppose we have an n-qubit register, whose Hilbert space is 2^n-dimensional. Since each qubit has two basis vectors $|0\rangle$ and $|1\rangle$, there are $2n$ basis vectors (n $|0\rangle$'s and n $|1\rangle$'s) involved to span this 2^n-dimensional Hilbert space. Imagine that we have a single quantum system, instead, which has the same Hilbert space. One might think that the system may do the same quantum computation as the n-qubit register does. One possible problem is that one cannot measure the "kth digit". Even worse, consider how many different basis vectors are required for this system. This single system must have an enormous number, 2^n, of basis vectors! Let us consider 20 spin-1/2 particles in a magnetic field. We can employ the spin-up and spin-down energy eigenstates of each particle as the qubit basis vectors. Then there are merely 40 energy eigenvectors involved. Suppose we use energy eigenstates of a certain molecule to replace this register. Then we have to use $2^{20} \sim 10^6$ eigenstates. Separation and control of so many eigenstates are certainly beyond current technology. These simple consideration shows that multipartite implementation of a quantum algorithm requires an exponentially smaller number of basis vectors than monopartite implementation since the former makes use of entanglement as a computational resource.

Note that a quantum computer can simulate arbitrary classical logic circuits. Then how about copying data? It should be kept in mind that the no-cloning theorem states that we cannot copy an *arbitrary* state $|\psi\rangle = a|0\rangle + b|1\rangle$. The loophole is that the theorem does not apply if the states to be cloned are limited to $|0\rangle$ and $|1\rangle$. For these cases, the copying operator U should work as

$$U : |00\rangle \mapsto |00\rangle, \quad : |10\rangle \mapsto |11\rangle.$$

We can assign arbitrary action of U on a state whose second input is $|1\rangle$ since this case does not happen. What we have to keep in our mind is only that U be unitary. An example of such U is

$$U = (|00\rangle\langle 00| + |11\rangle\langle 10|) + (|01\rangle\langle 01| + |10\rangle\langle 11|), \tag{5.39}$$

where the first set of operators renders U the cloning operator and the second set is added just to make U unitary. We immediately notice that U is nothing but the CNOT gate introduced in §5.2.

Therefore, if the data under consideration are limited within $|0\rangle$ and $|1\rangle$, we can copy the qubit states even with a quantum computer. This fact is used to construct quantum error correcting codes.

---

that $m^P \equiv 1 \pmod{N}$. The smallest such number P is called the **period** or the **order**. It is easily seen that $m^{x+P} \equiv m^x \pmod{N}$, $\forall x \in \mathbb{N}$.

5.5 Correspondence with Classical Logic Gates

Before we proceed further, it is instructive to show that all the elementary logic gates, NOT, AND, XOR, OR and NAND, in classical logic circuits can be implemented with quantum gates. In this sense, quantum information processing contains the classical one.

5.5.1 NOT Gate

Let us consider the **NOT gate** first. It is defined by the following logic function,

$$\mathrm{NOT}(x) = \neg x = \begin{cases} 0 & x = 1 \\ 1 & x = 0 \end{cases} \tag{5.40}$$

where $\neg x$ stands for the **negation** of x. Under the correspondence $0 \leftrightarrow |0\rangle,\ 1 \leftrightarrow |1\rangle$, we have already seen in Eq. (5.2) that the gate X negates the basis vectors as

$$X|x\rangle = |\neg x\rangle = |\mathrm{NOT}(x)\rangle,\ (x = 0, 1). \tag{5.41}$$

Now let us measure the output state. We employ the following measurement operator:

$$M_1 = |1\rangle\langle 1|. \tag{5.42}$$

M_1 has eigenvalues 0 and 1 with the eigenvectors $|0\rangle$ and $|1\rangle$, respectively. When the input is $|0\rangle$, the output is $|1\rangle$ and the measurement gives the value 1 with the probability 1. If, on the other hand, the input is $|1\rangle$, the output is $|0\rangle$ and the measurement yields 1 with probability 0, or in other words, it yields 0 with probability 1. It should be kept in mind that the operator X acts on an arbitrary linear combination $|\psi\rangle = a|0\rangle + b|1\rangle$, which is classically impossible. The output state is then $X|\psi\rangle = a|1\rangle + b|0\rangle$.

We show in the following that the CCNOT gate implements all classical logic gates. The first and the second input qubits are set to $|1\rangle$ to obtain the NOT gate as

$$U_{\mathrm{CCNOT}}|1, 1, x\rangle = |1, 1, \neg x\rangle. \tag{5.43}$$

5.5.2 XOR Gate

Since a quantum gate has to be reversible, we cannot construct a unitary gate corresponding to the classcial **XOR gate** whose function is $x, y \mapsto x \oplus y$ ($x, y \in \{0, 1\}$), where $x \oplus y$ is an addition mod 2. Clearly this operation has no inverse. This operation may be made reversible if we keep the first bit x during the gate operation, namely, if we define

$$f(x, y) = (x, x \oplus y), \quad x, y \in \{0, 1\}. \tag{5.44}$$

We call this function f, also the XOR gate. The quantum gate that does this operation is nothing but the CNOT gate defined by Eq. (5.5),

$$U_{\rm XOR} = U_{\rm CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X. \tag{5.45}$$

Note that the XOR gate may be also obtained from the CCNOT gate. Suppose the first qubit of the CCNOT gate is fixed to $|1\rangle$. Then it is easy to verify that

$$U_{\rm CCNOT}|1, x, y\rangle = |1, x, x \oplus y\rangle. \tag{5.46}$$

Thus the CCNOT gate can be used to construct the XOR gate.

5.5.3 AND Gate

The logical **AND gate** is defined by

$$\mathrm{AND}(x, y) \equiv x \wedge y \equiv \begin{cases} 1 & x = y = 1 \\ 0 & \text{otherwise} \end{cases} \quad x, y \in \{0, 1\}. \tag{5.47}$$

Clearly this operation is not reversible and we have to introduce the same sort of prescription which we employed in the XOR gate.

Let us define the logic function

$$f(x, y, 0) \equiv (x, y, x \wedge y), \tag{5.48}$$

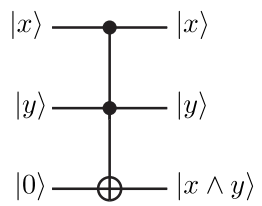
which we also call AND. Note that we have to keep both x and y for f to be reversible since $x = x \wedge y = 0$ implies *both* $x = y = 0$ and $x = 0, y = 1$. The unitary matrix that computes f is

$$\begin{aligned} U_{\rm AND} = &(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I \\ &+|11\rangle\langle 11| \otimes X. \end{aligned} \tag{5.49}$$

It is readily verified that

$$U_{\rm AND}|x, y, 0\rangle = |x, y, x \wedge y\rangle, \quad x, y \in \{0, 1\}. \tag{5.50}$$

Observe that the third qubit in the RHS is 1 if and only if $x = y = 1$ and 0 otherwise. Thus the CCNOT gate may be employed to implement the AND gate. It follows from Eq. (5.50) that the AND gate is denoted graphically as



5.5.4 OR Gate

The **OR gate** represents the logical function

$$\mathrm{OR}(x,y) = x \vee y = \begin{cases} 0 & x = y = 0 \\ 1 & \text{otherwise} \end{cases} \qquad x, y \in \{0,1\}. \tag{5.51}$$

This function OR is not reversible either and special care must be taken.

Let us define

$$f(x,y,0) \equiv (\neg x, \neg y, x \vee y), \quad x, y \in \{0,1\}, \tag{5.52}$$

which we also call OR. Although the first and the second bits are negated, it is not essential in the construction of the OR gate. These negations appear due to our construction of the OR gate based on the de Morgan theorem

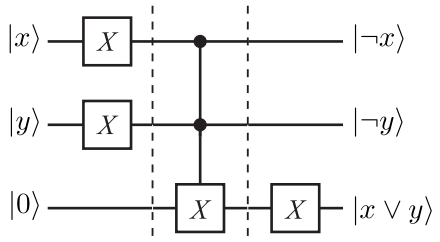
$$x \vee y = \neg(\neg x \wedge \neg y). \tag{5.53}$$

They may be removed by adding extra NOT gates if necessary.

Let $|x,y,0\rangle$ be the input state. The unitary matrix that represents f is

$$U_{\mathrm{OR}} = |00\rangle\langle 11| \otimes X + |01\rangle\langle 10| \otimes X + |10\rangle\langle 01| \otimes X + |11\rangle\langle 00| \otimes I. \tag{5.54}$$

Now it is obvious why negations in the first and the second qubits appear in the OR gate. Since we have already constructed the NOT gate and AND gate, we take advantage of this in the construction of the OR gate. The equality (5.53) leads us to the following diagram:



Accordingly, the first and the second qubits are negated. The unitary matrix obtained from this diagram is

$$\begin{aligned} U_{\mathrm{OR}} = {} & (I \otimes I \otimes X) \\ & \cdot(|00\rangle\langle 00| \otimes I + |01\rangle\langle 01| \otimes I + |10\rangle\langle 10| \otimes I + |11\rangle\langle 11| \otimes X) \\ & \cdot(X \otimes X \otimes I). \end{aligned} \tag{5.55}$$

The matrix products are readily evaluated to yield

$$\begin{aligned} U_{\mathrm{OR}} &= (|00\rangle\langle 00| \otimes X + |01\rangle\langle 01| \otimes X + |10\rangle\langle 10| \otimes X + |11\rangle\langle 11| \otimes I) \\ &\quad \cdot(X \otimes X \otimes I) \\ &= |00\rangle\langle 11| \otimes X + |01\rangle\langle 10| \otimes X + |10\rangle\langle 01| \otimes X + |11\rangle\langle 00| \otimes I, \end{aligned}$$

which verifies Eq. (5.54).

Observe that the OR gate is implemented with the X and the CCNOT gates and, moreover, the X gate is obtained from the CCNOT gate by putting the first and the second bits to $|1\rangle$.

If we want to have a gate $V_{\rm OR}|x,y,0\rangle = |x,y,x\vee y\rangle$, we may multiply $X\otimes X\otimes I$ to $U_{\rm OR}$ from the left so that $V_{\rm OR} = (X\otimes X\otimes I)U_{\rm OR}$.

In summary, we have shown that all the classical logic gates, NOT, AND, OR, XOR and NAND gates, may be obtained from the CCNOT gate. Thus all the classical computation may be carried out with a quantum computor. Note, however, that these gates belong to a tiny subset of the set of unitary matrices.

5.6 Notes and Open problems

In the construction of quantum operations for open system, we need to construct U such that the partial trace of $U(E_{11}\otimes\rho)U^\dagger$ provide us useful information. In particular, we need the first 2^m columns of U and the result of the columns are flexible. So, we consider $[U_1|U_2]$, where $U_1\in M_{2^n,2^m}$ and U_2 is arbitrary, and find elementary matrices $V_1,\ldots,V_k$ such that $V_1\cdots V_k = [U_1|\hat{U}_2]$ for whatever $\hat{U}_2$ would be. So, it is desirable to find elementary matrices

$$V_k^\dagger\cdots V_1^\dagger U_1 = \begin{pmatrix} I_{2^m} \\ 0 \end{pmatrix}.$$

Note that if $m=0$, we are initialing the pure state $|0\cdots 0\rangle$ to a state equal to U_1; see [15, 16].

Quantum state tomography is an actively research area. Here are some open problems.

1. For an n-qubit state ρ, prove or disprove that $k=3^n$ is the minimum number of local unitary gates such that the measurements of the diagonal entries of $U_j^\dagger\rho U_j$ for $j=1,\ldots,k$, will determine ρ.

2. Determine a general quantum state tomography schemes using other quantum computers such as NMR or linear optics based.

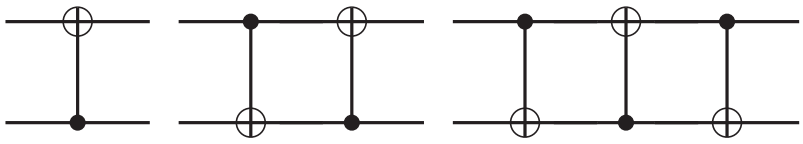
3. Quantum process tomography is the procedure to determine/estimate a given quantum operation system assuming that one can use many quantum states ρ to test $\Phi(\rho)$. Design effective quantum process tomography schemes using different quantum computing platforms.

Exercises for Chapter 5

EXERCISE 5.1. *Show that the $U_{\rm CNOT}$ cannot be written as a tensor product of two one-qubit gates.*

EXERCISE 5.2. *Let $(a|0\rangle + b|1\rangle) \otimes |0\rangle$ be an input state to a CNOT gate. What is the output state?*

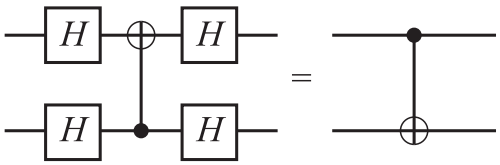
EXERCISE 5.3. *(1) Find the matrix representation of the "upside down" CNOT gate (a) in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.*



(2) Find the matrix representation of the circuit (b).
(3) Find the matrix representation of the circuit (c). Find the action of the circuit on a tensor product state $|\psi_1\rangle \otimes |\psi_2\rangle$.

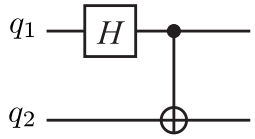
EXERCISE 5.4. *Show that W_n is unitary.*

EXERCISE 5.5. *Show that the two circuits below are equivalent:*



This exercise shows that the control qubit and the target qubit in a CNOT gate are interchangeable by introducing four Hadamard gates.

EXERCISE 5.6. *Let us consider the following quantum circuit*



(5.56)

where q_1 denotes the first qubit, while q_2 denotes the second. What are the outputs for the inputs $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$?

EXERCISE 5.7. *Show that the above $U_{\rm SWAP}$ is written as*

$$U_{\rm SWAP} = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X)(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|) \\ (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X). \tag{5.57}$$

This shows that the SWAP gate is implemented with three CNOT gates as given in Exercise 5.3 (3).

EXERCISE 5.8. *Verify that the above matrix $U_{\rm OR}$ indeed satisfies*

$$U_{\rm OR}|x, y, 0\rangle = |\neg x, \neg y, x \vee y\rangle, \quad x, y \in \{0, 1\}. \tag{5.58}$$

EXERCISE 5.9. *Show that the NAND gate can be obtained from the CC-NOT gate. Here NAND is defined by the function*

$$\mathrm{NAND}(x, y) = \neg(x \wedge y) = \begin{cases} 0 & x = y = 1 \\ 1 & \text{otherwise} \end{cases} \quad x, y \in \{0, 1\}. \tag{5.59}$$

EXERCISE 5.10. *Let $|\psi\rangle = a|00\rangle + b|11\rangle$ be a two-qubit state. Apply a Hadamard gate to the first qubit and then measure the first qubit. Find the second qubit state after the measurement corresponding to the outcome of the first qubit measurement.*

EXERCISE 5.11. *Let U be a general 4×4 unitary matrix. Find two-level unitary matrices U_1, U_2 and U_3 such that*

$$U_3 U_2 U_1 U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & * \\ 0 & * & * & * \\ 0 & * & * & * \end{pmatrix}.$$

EXERCISE 5.12. *Let*

$$U = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{5.60}$$

Decompose U into a product of two-level unitary matrices.

EXERCISE 5.13. *Let us consider the controlled-V_1 gate $U_{\rm CV_1}$ and the controlled-V_2 gate $U_{\rm CV_2}$. Show that the controlled-V_1 gate followed by the controlled-V_2 gate is the controlled-V_2V_1 gate $U_{\rm C(V_2V_1)}$ as shown in Fig. 5.11.*

EXERCISE 5.14. *Prove Lemma 5.2.7 by writing down the action of each gate in the RHS of Fig. 5.4 explicitly using bras, kets and $I, U, V, V^\dagger$. (For example, $U_{\rm CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$ for a two-qubit system.)*

EXERCISE 5.15. *Show that the circuit in Fig. 5.5 is a controlled-U gate with three control qubits, where $U = V^2$.*

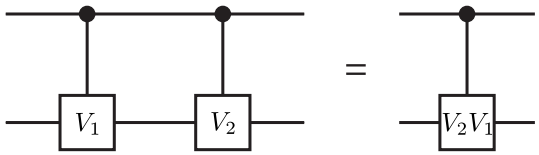


FIGURE 5.11
Equality $U_{CV_2}U_{CV_1} = U_{C(V_2V_1)}$.

References

[1] M. A. Neilsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[2] E. Riefell and W. Polak, ACM Computing Surveys (CSUR) **32**, 300 (2000).

[3] Y. Uesaka, *Mathematical Principle of Quantum Computation*, Corona Publishing, Tokyo, in Japanese (2000).

[4] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[5] D. Dieks, Phys. Lett. A **92**, 271 (1982).

[6] D. Bouwmeester *et al.*, Nature **390**, 575 (1997).

[7] D. Boschi *et al.*, Phys. Rev. Lett. **80**, 1121 (1998).

[8] I. Marcikic *et al.*, Nature **421**, 509 (2003).

[9] R. Ursin *et al.*, Nature **430**, 849 (2004).

[10] A. Furusawa *et al.*, Science **282**, 706 (1998).

[11] M. A. Nielsen *et al.*, Nature **396**, 52 (1998).

[12] M. Riebe *et al.*, Nature **429**, 734 (2004).

[13] M. D. Barret *et al.*, Nature **429**, 737 (2004).

[14] A. Barenco *et al.*, Phys. Rev. A **52**, 3457 (1995).

[15] Vivek V. Shende, Stephen S. Bullock, Igor L. Markov, Synthesis of Quantum Logic Circuits, https://arxiv.org/pdf/quant-ph/0406176.pdf.

[16] IBM qiskit-tutorial - Summary of Quantum Operations https://github.com/Qiskit/qiskit-tutorials/blob/master/tutorials/circuits/3_summary_of_quantum_operations.ipynb