Quantum Computing
4 – Qubits & Gates

Angelo Bassi

The Qubit

The bit is the fundamental concept of classical computation and classical information. Just as a classical bit has a state – either 0 or 1 – a qubit also has a state. Two possible states for a qubit are the states $|0\rangle$ and $|1\rangle$, which as you might guess correspond to the states 0 and 1 for a classical bit. The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ or $|1\rangle$. It is also possible to form **linear combinations of states**, often called superpositions:

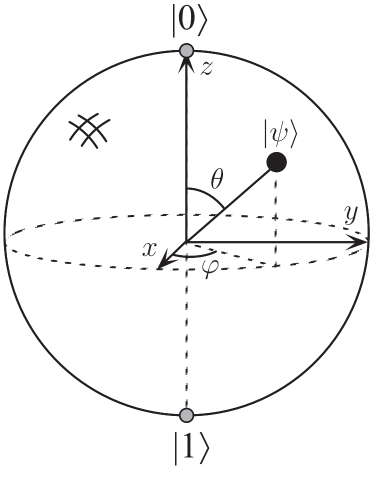
$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad\qquad |\alpha|^2 + |\beta|^2 = 1$$

The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states, and form an orthonormal basis for this vector space .

Because $|\alpha|^2 + |\beta|^2 = 1$, we may rewrite the above relation as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle.$$

Up to an global phase factor, which has no physical significance. The numbers θ and ϕ define a point on the unit three-dimensional sphere, often called the **Bloch sphere.**



Multiple Qubits

Suppose we have **two qubits**. If these were two classical bits, then there would be four possible states, 00, 01, 10, and 11. Correspondingly, a two qubit system has four computational basis states denoted $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. A pair of qubits can also exist in **superpositions of these four states**, so the quantum state of two qubits involves associating a complex coefficient – sometimes called an amplitude – with each computational basis state, such that the state vector describing the two qubits is

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

Similar to the case for a single qubit, the measurement result x (= 00, 01, 10 or 11) occurs with probability $|\alpha_x|^2$, with the state of the qubits after the measurement being $|x\rangle$. The condition that probabilities sum to one is therefore expressed by the normalization condition

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$$

More generally, we may consider a system of n qubits. The computational basis states of this system are of the form $|x_1 x_2 \ldots x_n\rangle$, and so a quantum state of such a system is specified by 2^n amplitudes.

Two ways of denoting the qubits

Binary basis: sequence of 0 and 1, i.e. $|x_{n-1}\, x_{n-2} \ldots x_0\rangle$
Decimal basis: $|x\rangle$, with $x = x_{n-1}\, 2^{n-1} + x_{n-2}\, 2^{n-2} + \ldots + x_0$

Examples
$|10\rangle = |\ 1 \times 2^1 + 0 \times 2^0\ \rangle\ = |2\ \rangle$
$|101\rangle = |\ 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0\rangle\ = |6\ \rangle$

The set

$$\{|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\}$$

is an orthonormal basis of a two-qubit system and is called the **Bell basis**. Each vector is called the Bell state or the Bell vector. Note that all the Bell states are entangled.

EXERCISE. The Bell basis is obtained from the binary basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ by a unitary transformation. Write down the unitary transformation explicitly.

Among **three-qubit entangled states**, the following two states are important for various reasons and hence deserve special names. The state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

is called the **Greenberger-Horne-Zeilinger state** and is often abbreviated as the **GHZ state**. Another important three-qubit state is the **W state**

$$|\mathrm{W}\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$$

Quantum Computation

A quantum computation is a collection of the following three elements:

- A register or a set of registers,
- A unitary matrix U, which is tailored to execute a given quantum algorithm
- Measurements to extract information we need.

More formally, we say **a quantum computation is the set $\{H,U,\{M_m\}\}$**, where $H = C^{2n}$ is the Hilbert space of an n-qubit register, $U \in U(2^n)$ represents the quantum algorithm and $\{M_m\}$ is the set of measurement operators. The hardware along with equipment to control the qubits is called a quantum computer.

Single Qubit Quantum Gates

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

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

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

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

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.

Exercise: Find the Hamiltonian that implements these gates, and show how they are implemented.

Three other quantum gates will play a large part in what follows, the Hadamard gate (denoted H), phase gate (denoted S), and $\pi/8$ gate (denoted T):

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}; \quad T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{bmatrix}. \tag{4.2}$$

A couple of useful algebraic facts to keep in mind are that $H = (X+Z)/\sqrt{2}$ and $S = T^2$. You might wonder why the T gate is called the $\pi/8$ gate when it is $\pi/4$ that appears in the definition. The reason is that the gate has historically often been referred to as the $\pi/8$ gate, simply because up to an unimportant global phase T is equal to a gate which has $\exp(\pm i\pi/8)$ appearing on its diagonals.

$$T = \exp(i\pi/8)\begin{bmatrix} \exp(-i\pi/8) & 0 \\ 0 & \exp(i\pi/8) \end{bmatrix}. \tag{4.3}$$

Nevertheless, the nomenclature is in some respects rather unfortunate, and we often refer to this gate as the T gate.

The Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the *rotation operators* about the $\hat{x}$, $\hat{y}$, and $\hat{z}$ axes, defined by the equations:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.4}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{4.5}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}. \tag{4.6}$$

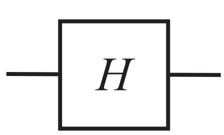
The **Hadamard gate** or the **Hadamard transformation** H is an important unitary transformation defined by

$$\begin{aligned} U_{\mathrm{H}} : |0\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{4.9}$$

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

$$U_{\mathrm{H}} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{4.10}$$

A Hadamard gate is depicted as



Hadamard-Walsh Gate

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 $|00\dots0\rangle$:

$$\begin{aligned}&(H \otimes H \otimes \dots \otimes H)|00\dots0\rangle\\&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \dots \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\\&= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle. \end{aligned} \tag{4.11}$$

Therefore, we produce a superposition of all the states $|x\rangle$ with $0 \le x \le 2^n - 1$ 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

$$W_1 = U_{\mathrm{H}}, \quad W_{n+1} = U_{\mathrm{H}} \otimes W_n. \tag{4.12}$$

Exercises

Exercise 4.7: Show that $XYX = -Y$ and use this to prove that $XR_y(\theta)X = R_y(-\theta)$.

Exercise 4.8: An arbitrary single qubit unitary operator can be written in the form

$$U = \exp(i\alpha)R_{\hat{n}}(\theta) \tag{4.9}$$

for some real numbers α and θ, and a real three-dimensional unit vector $\hat{n}$.

1. Prove this fact.
2. Find values for α, θ, and $\hat{n}$ giving the Hadamard gate H.
3. Find values for α, θ, and $\hat{n}$ giving the phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}. \tag{4.10}$$

Exercise 4.13: (Circuit identities) It is useful to be able to simplify circuits by inspection, using well-known identities. Prove the following three identities:

$$HXH = Z; \quad HYH = -Y; \quad HZH = X. \tag{4.18}$$

Exercise 4.14: Use the previous exercise to show that $HTH = R_x(\pi/4)$, up to a global phase.

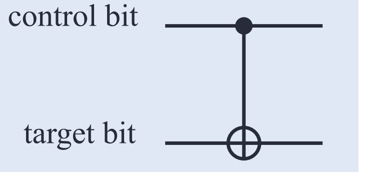
Two qubit gates: CNOT Gate

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 $|0\rangle$.

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

$$U_{\text{CNOT}} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X,$$

$$U_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$



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 $1 \oplus 1 = 0$.

The following identity holds

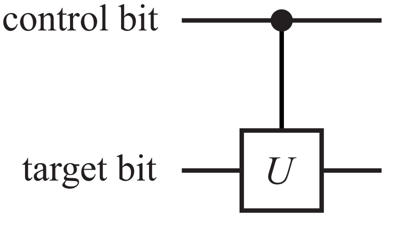
$$\begin{aligned} \text{CNOT} &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\ &= \frac{1}{2}(I + Z) \otimes I + \frac{1}{2}(I - Z) \otimes X \\ &= \frac{1}{2} I \otimes (I + X) + \frac{1}{2} Z \otimes (I - X) \end{aligned}$$

Control-U Gate

More generally, we consider a controlled-U gate,

$$V = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U, \tag{4.7}$$

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



Swap Gate

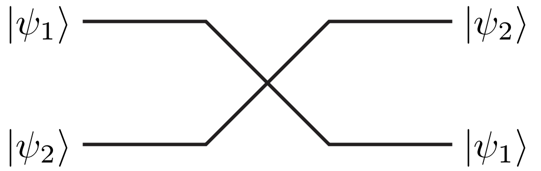
The SWAP gate acts on a tensor product state as

$$U_{\mathrm{SWAP}}|\psi_1, \psi_2\rangle = |\psi_2, \psi_1\rangle. \tag{4.14}$$

The explict form of U_{SWAP} is given by

$$\begin{aligned} U_{\mathrm{SWAP}} &= |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11| \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \end{aligned} \tag{4.15}$$

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



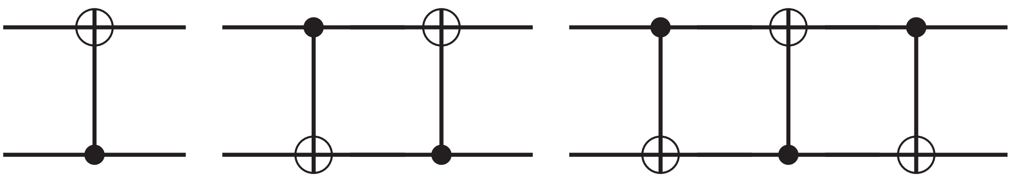
Note that the SWAP gate is a special gate which maps an arbitrary tensor product state to a tensor product state. In contrast, most two-qubit gates map a tensor product state to an entangled state.

Exercise

EXERCISE 4.1 Show that the U_{CNOT} cannot be written as a tensor product of two one-qubit gates.

EXERCISE 4.2 Let $(a|0\rangle + b|1\rangle) \otimes |0\rangle$ be an input state to a CNOT gate. What is the output state?

EXERCISE 4.3 (1) Find the matrix representation of the "upside down" CNOT gate (a) in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.



(a) (b) (c)

(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 $|\psi_1\rangle \otimes |\psi_2\rangle$.

Given the outcome of Exercise 4.3(c) and the mathematical expression of the CNOT gate, one can write

$$
\begin{aligned}
\mathrm{SWAP} &= \mathrm{CNOT}\,\overline{\mathrm{CNOT}}\,\mathrm{CNOT} \\
&= \frac{1}{2}(I \otimes I + Z \otimes Z) + \frac{1}{2} X \otimes X (I \otimes I - Z \otimes Z)
\end{aligned}
$$

This expression (using the relation Y = XZ) can be rewritten as:

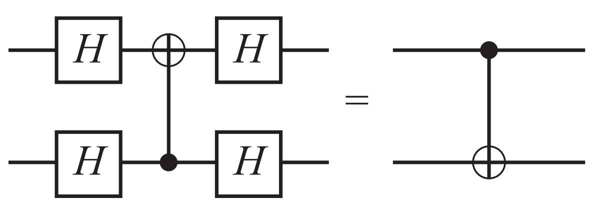
$$
\mathrm{SWAP} = \frac{1}{2}(I \otimes I + X \otimes X - Y \otimes Y + Z \otimes Z)
$$

Given the relation between the gates X, Y, Z and the Pauli matrices, we have also:

$$
\boxed{\mathrm{SWAP} = \frac{1}{2}(I \otimes I + \bar{\sigma} \otimes \bar{\sigma}) = \frac{1}{2}(I \otimes I + \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z)}
$$

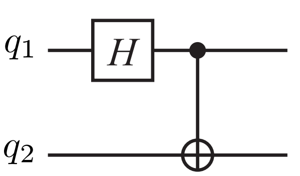
Exercise

EXERCISE 4.5 Show that the two circuits below are equivalent:



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

EXERCISE 4.6 Let us consider the following quantum circuit



(4.13)

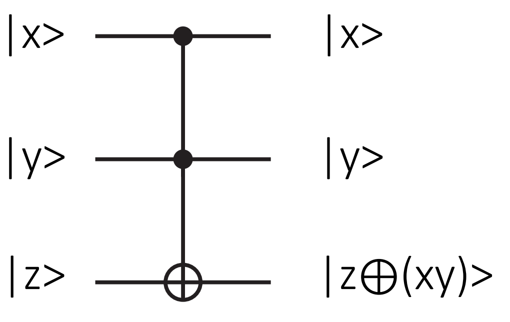
where q_1 denotes the first qubit, while q_2 denotes the second. What are the outputs for the inputs $|00\rangle, |01\rangle, |10\rangle$ and $|11\rangle$?

3 qubit gate: CCNOT (Toffoli) Gate

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

$$U_{\mathrm{CCNOT}} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X. \tag{4.8}$$

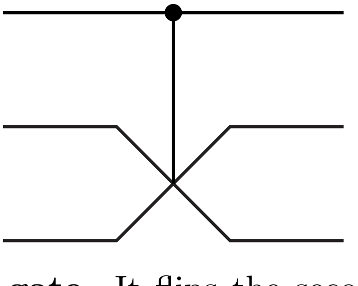
This gate is graphically expressed as



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

Fredkin Gate

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

$$U_{\mathrm{Fredkin}} = |0\rangle\langle 0| \otimes I_4 + |1\rangle\langle 1| \otimes U_{\mathrm{SWAP}}. \tag{4.17}$$

Exercise

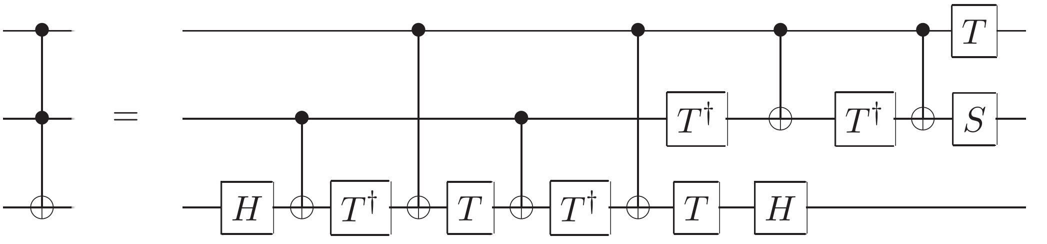


Figure 4.9. Implementation of the Toffoli gate using Hadamard, phase, controlled-NOT and $\pi/8$ gates.

Exercise 4.24: Verify that Figure 4.9 implements the Toffoli gate.

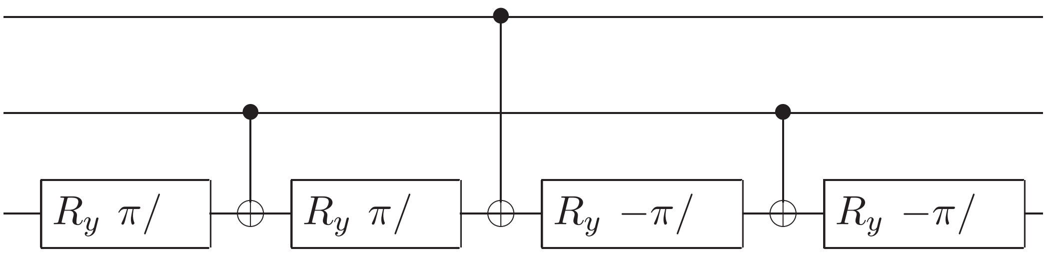
Exercise 4.25: (**Fredkin gate construction**) Recall that the Fredkin (controlled-swap) gate performs the transform

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} . \tag{4.30}$$

(1) Give a quantum circuit which uses three Toffoli gates to construct the Fredkin gate (*Hint*: think of the swap gate construction – you can control each gate, one at a time).
(2) Show that the first and last Toffoli gates can be replaced by CNOT gates.
(3) Now replace the middle Toffoli gate with the circuit in Figure 4.8 to obtain a Fredkin gate construction using only six two-qubit gates.
(4) Can you come up with an even simpler construction, with only five two-qubit gates?

Exercise

Exercise 4.26: Show that the circuit:



differs from a Toffoli gate only by relative phases. That is, the circuit takes $|c_1, c_2, t\rangle$ to $e^{i\theta(c_1,c_2,t)}|c_1, c_2, t \oplus c_1 \cdot c_2\rangle$, where $e^{i\theta(c_1,c_2,t)}$ is some relative phase factor. Such gates can sometimes be useful in experimental implementations, where it may be much easier to implement a gate that is the same as the Toffoli up to relative phases than it is to do the Toffoli directly.

Exercise 4.27: Using just CNOTs and Toffoli gates, construct a quantum circuit to perform the transformation

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} . \tag{4.31}$$

This kind of partial cyclic permutation operation will be useful later, in Chapter 7.

Recovering classical Gates

The (classical) Toffoli gate is universal, therefore it reproduces all reversible and irreversible classical gates. Its quantum version generalizes the classical gates into quantum gates.

In general:

1. Take a classical gate. If irreversible, consider its reversible variant.
2. Define the quantum counterpart so that on the computational basis it acts as the reversible classical gate.
3. Extend it by linearity to the whole space.

The gate thus obtained is the quantum generalization of the classical gate.

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.

Exercise

Exercise 4.36: Construct a quantum circuit to add two two-bit numbers x and y modulo 4. That is, the circuit should perform the transformation $|x, y\rangle \rightarrow |x, x + y \bmod 4\rangle$.

What the circuit should do is the following

			0		1		2		3	
			y_1	y_0	y_1	y_0	y_1	y_0	y_1	y_0
			0	0	0	1	1	0	1	1
	x_1	x_0								
0	0	0	0	0	0	1	1	0	1	1
1	0	1	0	1	1	0	1	1	0	0
2	1	0	1	0	1	1	0	0	0	1
3	1	1	1	1	0	0	0	1	1	0

We see that:

$x_0 \rightarrow x_0$

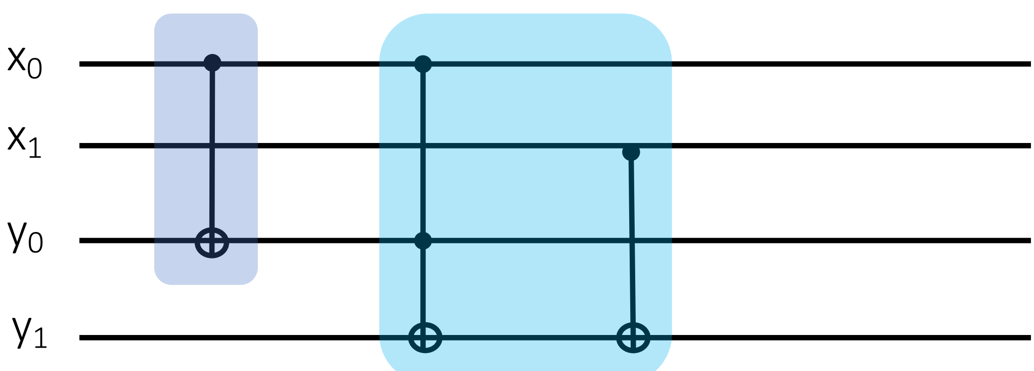
$x_1 \rightarrow x_1$

$y_0 \rightarrow x_0 \oplus y_0$ This is implemented by a CNOT gate

$y_1 \rightarrow x_1 \oplus y_1 \oplus (x_0 y_0)$ $y_1 \oplus (x_0 y_0)$ is implemented by a CCNOT gate

the rest by a CNOT gate

The circuit then is



Universal Quantum Gates

Like in the classical case, there exist a **universal set of quantum gates**.

We will now show that

- Single qubit gates
- CNOT gate

are universal for quantum computation.

Two-level unitary matrix

We will prove the following Lemma before stating the main theorem. Let us start with a definition. A **two-level unitary matrix** is a unitary matrix which acts non-trivially only on two vector components. Suppose V is a two-level unitary matrix. Then V has the same matrix elements as those of the unit matrix except for certain four elements V_{aa}, V_{ab}, V_{ba} and V_{bb}. An example of a two-level unitary matrix is

$$V = \begin{pmatrix} \alpha^* & 0 & 0 & \beta^* \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -\beta & 0 & 0 & \alpha \end{pmatrix}, \quad (|\alpha|^2 + |\beta|^2 = 1),$$

where $a = 1$ and $b = 4$.

LEMMA 4.1 Let U be a unitary matrix acting on $\mathbb{C}^d$. Then there are $N \leq d(d-1)/2$ two-level unitary matrices $U_1, U_2, \ldots, U_N$ such that

$$U = U_1 U_2 \ldots U_N. \tag{4.46}$$

Proof of lemma: d = 3

Proof. The proof requires several steps. It is instructive to start with the case $d = 3$. Let

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix}$$

be a unitary matrix. We want to find two-level unitary matrices U_1, U_2, U_3 such that

$$U_3 U_2 U_1 U = I.$$

Then it follows that

$$U = U_1^\dagger U_2^\dagger U_3^\dagger.$$

(Never mind the daggers! If U_k is two-level unitary, $U_k^\dagger$ is also two-level unitary.) We prove the above decomposition by constructing U_k explicitly.

(i) Let

$$U_1 = \begin{pmatrix} \frac{a^*}{u} & \frac{b^*}{u} & 0 \\ -\frac{b}{u} & \frac{a}{u} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

where $u = \sqrt{|a|^2 + |b|^2}$. Verify that U_1 is unitary. Then we obtain

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{pmatrix},$$

where $a', \ldots, j'$ are some complex numbers, whose details are not necessary. Observe that, with this choice of U_1, the first component of the second row vanishes.

(ii) Let

$$U_2 = \begin{pmatrix} \frac{a'^*}{u'} & 0 & \frac{c'^*}{u'} \\ 0 & 1 & 0 \\ -\frac{c'}{u'} & 0 & \frac{a'}{u'} \end{pmatrix} = \begin{pmatrix} a'^* & 0 & c'^* \\ 0 & 1 & 0 \\ -c' & 0 & a' \end{pmatrix},$$

where $u' = \sqrt{|a'|^2 + |c'|^2} = 1$. Then

$$U_2 U_1 U = \begin{pmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix},$$

where the equality $d'' = g'' = 0$ follows from the fact that $U_2 U_1 U$ is unitary, and hence the first row must be normalized.

(iii) Finally let

$$U_3 = (U_2 U_1 U)^\dagger = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix}.$$

Then, by definition, $U_3 U_2 U_1 U = I$ is obvious. This completes the proof for $d = 3$.

The moral of the lemma is that with N two-level unitary matrices there are enough degrees of freedom to play with, to reproduce any unitary matrix of dimension d.

Proof of lemma: any d

Suppose U is a unitary matrix acting on $\mathbb{C}^d$ with a general dimension d. Then by repeating the above arguments, we find two-level unitary matrices $U_1, U_2, \ldots, U_{d-1}$ such that

$$U_{d-1} \ldots U_2 U_1 U = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & * & * & \ldots & * \\ 0 & * & * & \ldots & * \\ & & \ldots\ldots & & \\ 0 & * & * & \ldots & * \end{pmatrix},$$

namely the $(1,1)$ component is unity and other components of the first row and the first column vanish. The number of matrices $\{U_k\}$ to achieve this form is the same as the number of zeros in the first column, hence $(d-1)$.

We then repeat the same procedure to the $(d-1) \times (d-1)$ block unitary matrix using $(d-2)$ two-level unitary matrices. After repeating this, we finally decompose U into a product of two-level unitary matrices

$$U = V_1 V_2 \ldots V_N,$$

where $N \leq (d-1) + (d-2) + \ldots + 1 = d(d-1)/2$. ∎

Exercise

EXERCISE 4.12 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 4.13 Let

$$U = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}. \tag{4.47}$$

Decompose U into a product of two-level unitary matrices. Esercizio 4.37 del Nielsen Chuang

Universality theorem

THEOREM 4.2 (Barenco *et al.*) The set of single qubit gates and CNOT gate are universal. Namely, any unitary gate acting on an n-qubit register can be implemented with single qubit gates and CNOT gates.

Proof. Thanks to the previous lemma, it suffices to prove the theorem for a **two-level unitary matrix**, acting non trivially on two qubits s and t.

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}, \quad (a, b, c, d \in \mathbb{C})$$

In the example (2^3 dim matrix):
s = 000 and t = 111

$$s = s_{n-1}2^{n-1} + \ldots + s_1 2 + s_0 \qquad t = t_{n-1}2^{n-1} + \ldots + t_1 2 + t_0$$

Step 1. The two-level unitary matrix U can be reduced to a 2x2 unitary matrix.

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \Rightarrow \tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}$$

Define the **Gray code** connecting s and t. It is a sequence of binary numbers such that adjacent numbers differ only by one bit. In our case s = 000 and t = 111; an example of Gray code is

$$\begin{array}{rccc} & q_1 & q_2 & q_3 \\ g_1 = & 0 & 0 & 0 \\ g_2 = & 1 & 0 & 0 \\ g_3 = & 1 & 1 & 0 \\ g_4 = & 1 & 1 & 1 \end{array}$$

If s and t differ in p bits, the shortest Gray code is made of p+1 elements

The strategy now is to find gates providing the sequence of state changes

$$|s\rangle = |g_1\rangle \rightarrow |g_2\rangle \rightarrow \ldots \rightarrow |g_{m-1}\rangle$$

Then g_{m-1} and g_m differ only in one bit, which is identified with the single qubit on which U acts. After having applied the U gate, we bring things back. In our example:

$$|s\rangle = \underbrace{|000\rangle \longrightarrow |100\rangle \longrightarrow |110\rangle}_{\text{DO the Gary code}} = |11\rangle \otimes \boxed{|0\rangle}$$

$$|t\rangle \qquad |11\rangle \otimes \boxed{|1\rangle}$$

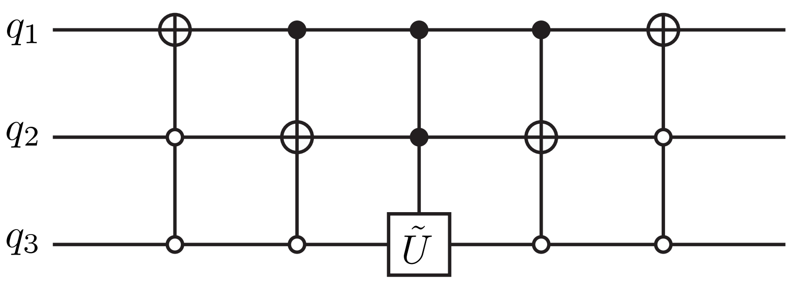
Act with the 2x2 gate $\tilde{U}$

UNDO the Gary code

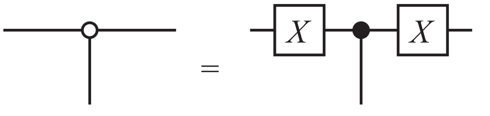
Universality theorem: d = 3 example

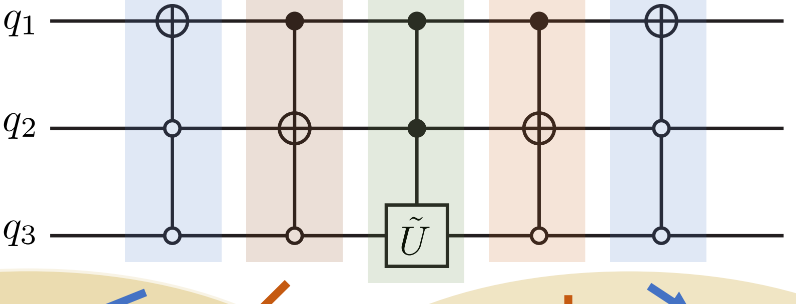
$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}$$

$=$



Where we defined





$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}$$

It changes
$|x00\rangle \rightarrow |\bar{x}00\rangle$

It changes
$|1x0\rangle \rightarrow |1\bar{x}0\rangle$

DO

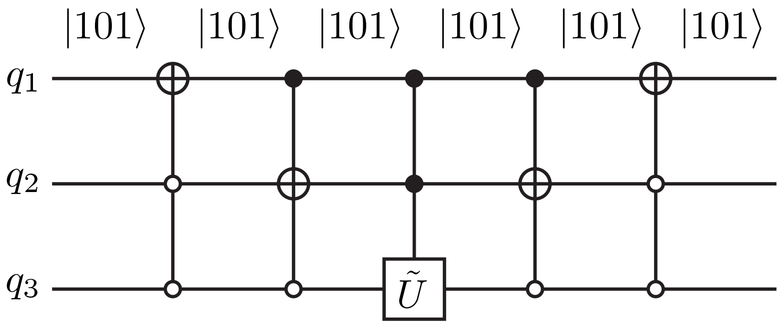
It changes
$|1x0\rangle \rightarrow |1\bar{x}0\rangle$

It changes
$|1x0\rangle \rightarrow |1\bar{x}0\rangle$

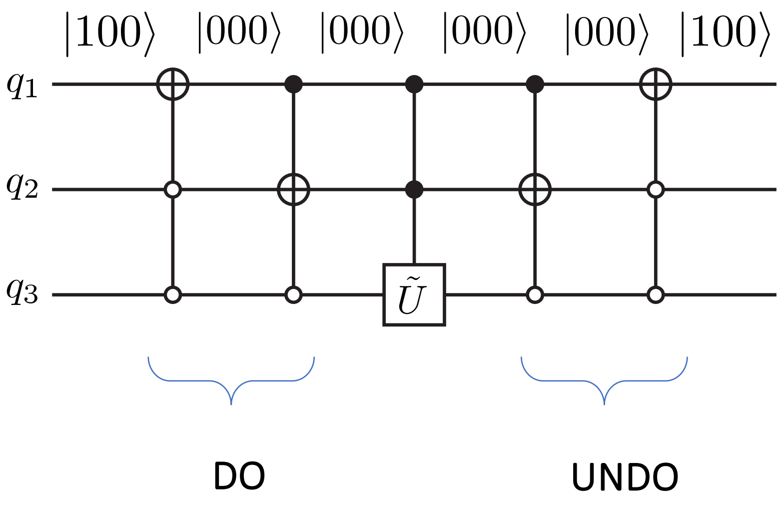
UNDO

	q_1	q_2	q_3
$g_1 =$	0	0	0
$g_2 =$	1	0	0
$g_3 =$	1	1	0
$g_4 =$	1	1	1

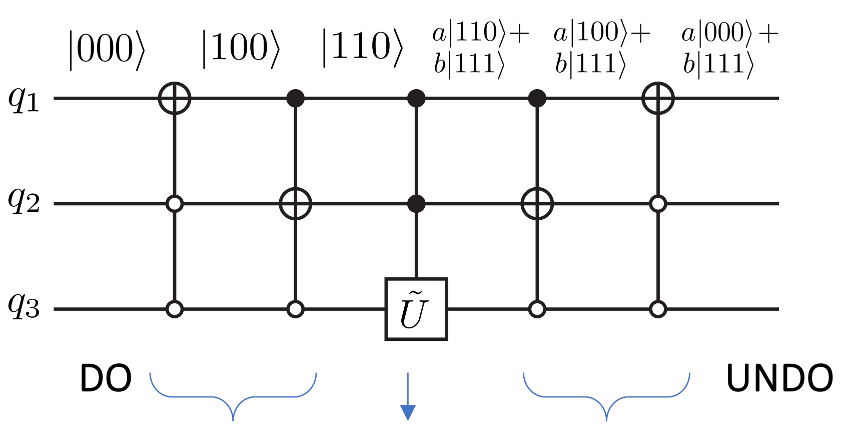
Let us consider the effect on a qubit different from |s> and |t>, for example the qubit |101>



Or the qubit |100>



While on |000>



The gate acts only on the third qubit

Exercises

EXERCISE 4.14 (1) Find the shortest Gray code which connects 000 with 110.
(2) Use this result to find a quantum circuit, such as Fig. 4.5, implementing a two-level unitary gate

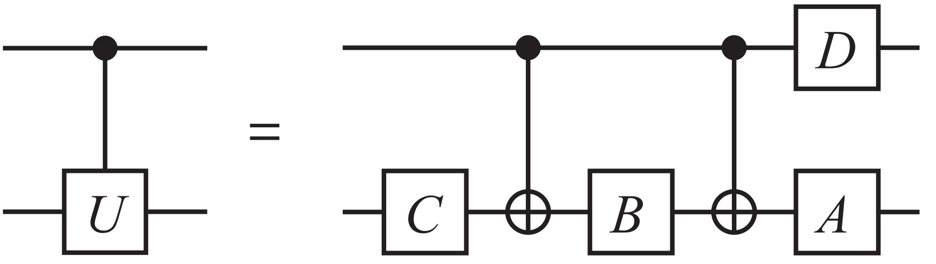
$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & c & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & d & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \tilde{U} \equiv \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in U(2).$$

Exercise 4.39: Find a quantum circuit using single qubit operations and CNOTs to implement the transformation

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}, \tag{4.60}$$

It will be shown next that all the gates in the above circuit can be implemented with single-qubit gates and CNOT gates, which proves the universality of these gates.

Step 2. The controlled-U gate is decomposed in the CNOT gate and single qubit gates



LEMMA 4.2 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

$$R_z(\alpha)R_y(\beta)R_z(\gamma) = \begin{pmatrix} e^{i(\alpha+\gamma)/2}\cos(\beta/2) & e^{i(\alpha-\gamma)/2}\sin(\beta/2) \\ -e^{i(-\alpha+\gamma)/2}\sin(\beta/2) & e^{-i(\alpha+\gamma)/2}\cos(\beta/2) \end{pmatrix}. \tag{4.53}$$

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

$$U = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} = \begin{pmatrix} \cos\theta e^{i\lambda} & \sin\theta e^{i\mu} \\ -\sin\theta e^{-i\mu} & \cos\theta e^{-i\lambda} \end{pmatrix}, \tag{4.54}$$

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

$$\theta = \frac{\beta}{2}, \lambda = \frac{\alpha+\gamma}{2}, \mu = \frac{\alpha-\gamma}{2}. \tag{4.55}$$

∎

LEMMA 4.3 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 4.2 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. ∎

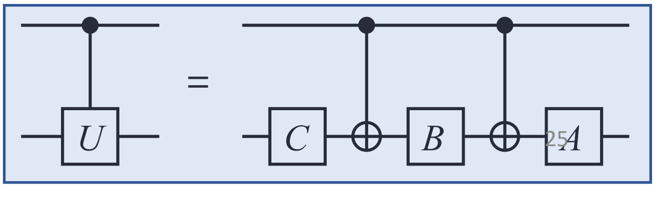
LEMMA 4.4 Let $U \in \mathrm{SU}(2)$ be factorized as $U = AXBXC$ as in the previous Lemma. Then the controlled-U gate can be implemented with at most three single-qubit gates and two CNOT gates (see Fig. 4.8).

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 bit is 1, we have

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



From SU(2) to (2)

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 4.5 Let

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

and

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

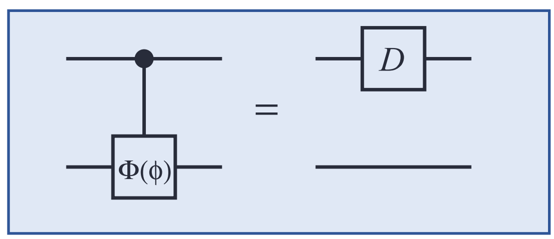
Then the controlled-$\Phi(\phi)$ gate is expressed as a tensor product of single qubit gates as

$$U_{\mathrm{C}\Phi(\phi)} = D \otimes I. \tag{4.56}$$

.

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. ∎

EXERCISE 4.15 Let us consider the controlled-V_1 gate $U_{\mathrm{C}V_1}$ and the controlled-V_2 gate $U_{\mathrm{C}V_2}$. Show that the controlled-V_1 gate followed by the controlled-V_2 gate is the controlled-V_2V_1 gate $U_{\mathrm{C}(V_2V_1)}$ as shown in Fig. 4.10.

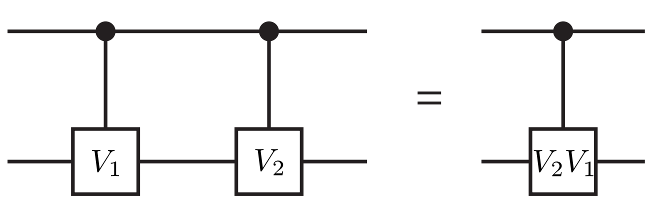


FIGURE 4.10
Equality $U_{\mathrm{C}V_2}U_{\mathrm{C}V_1} = U_{\mathrm{C}(V_2V_1)}$.

Controlled-U gate with U in U(2)

PROPOSITION 4.1 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 exercise above, the controlled-U gate is written as a product of the controlled-$\Phi(\phi)$ gate and the controlled-$AXBXC$ gate. Moreover, Lemma 4.5 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 4.3. Therefore we have the following decomposition:

$$U_{\mathrm{CU}} = (D \otimes A)U_{\mathrm{CNOT}}(I \otimes B)U_{\mathrm{CNOT}}(I \otimes C), \tag{4.57}$$

where

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

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

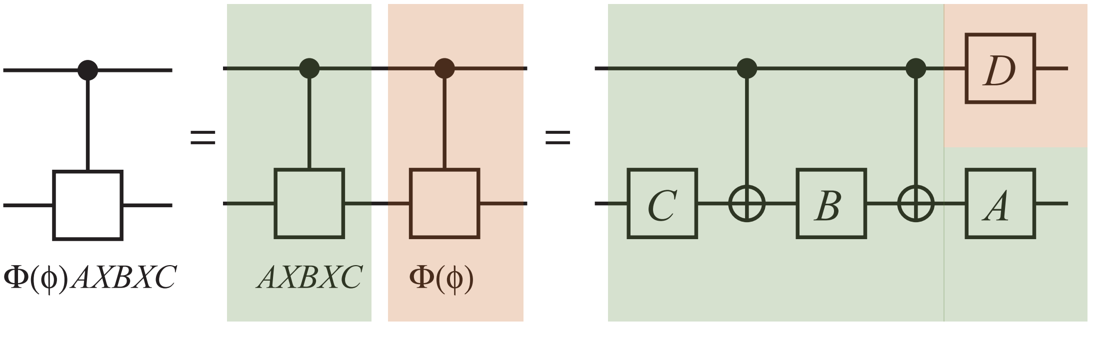
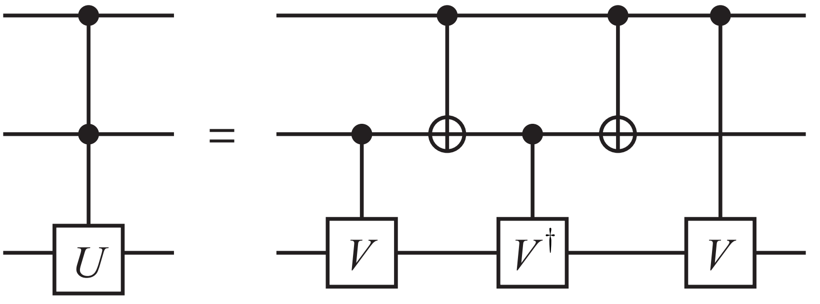


FIGURE 4.11
Controlled-U gate is implemented with at most four single-qubit gates and two CNOT gates.

Step 3. The CCNOT gate and its variants are implemented with CNOT gates and its variants

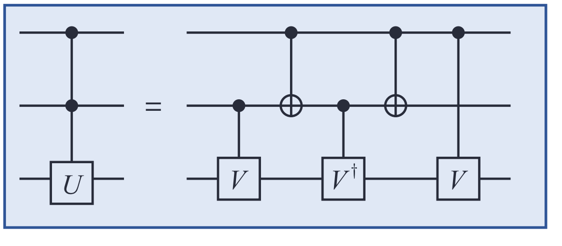


LEMMA 4.6 The two quantum circuits in Fig. 4.12 are equivalent, where $U = V^2$.

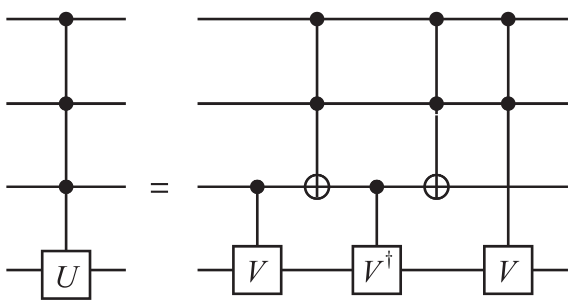
Proof. If both the first and the second qubits are 0 in the RHS, all the gates are ineffective and the third qubit is unchanged; the gate in this subspace acts as $|00\rangle\langle 00| \otimes I$. In case the first qubit is 0 and the second is 1, the third qubit is mapped as $|\psi\rangle \mapsto V^\dagger V|\psi\rangle = |\psi\rangle$; 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. 4.12 is

$$(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes U, \tag{4.58}$$

namely the controlled-controlled-U gate. ∎



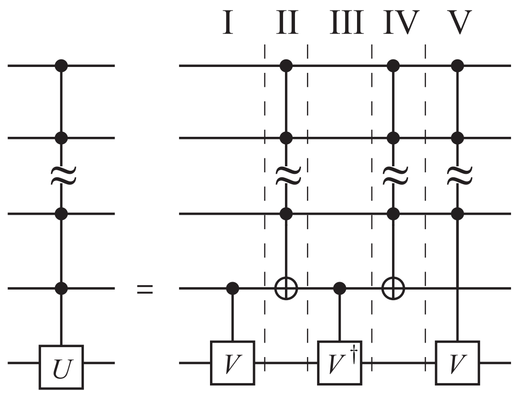
EXERCISE 4.17 Show that the circuit in Fig. 4.13 is a controlled-U gate with three control bits, where $U = V^2$.



PROPOSITION 4.2 The quantum circuit in Fig. 4.14 with $U = V^2$ is a decomposition of the controlled-U gate with $n - 1$ control bits.

The proof of the above proposition is very similar to that of Lemma 4.6 and Exercise 4.17 and is left as an exercise to the readers.

Theorem 4.2 has been now proved. ∎



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 to construct the gate in Fig. 4.14 by $C(n)$. Construction of layers I and III requires elementary gates whose number is independent of n. It can be shown the number of the elementary gates required to construct the controlled NOT gate with $(n-2)$ control bits 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 bits, requires $C(n-1)$ basic gates by definition. Thus we obtain a recursion relation

$$C(n) - C(n-1) = \Theta(n). \tag{4.59}$$

The solution to this recursion relation is

$$C(n) = \Theta(n^2). \tag{4.60}$$

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