Chapter 7: Quantum Gates and Circuits

INTRODUCTION TO QUANTUM PHYSICS AND INFORMATION PROCESSING

Radhika Vathsan
BITS Pilani K.K. Birla Goa Campus
India

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

Chapter 7

Quantum Gates and Circuits

We are now ready to see how computing with qubits can be done. In this book, we will mainly use the circuit model for computation which was first introduced by Deutsch [25]. We will represent by quantum "wires," the qubits upon which manipulations. The length of the wire is to be interpreted as the time axis. Manipulations on qubits can be done using basic unitary operators that are the equivalents of logic "gates." An algorithm, or a complete set of steps for achieving a processing task, is a combination of wires and gates representing a quantum circuit. This circuit must be thought of as a time sequence of events with every wire a way of representing qubit states, and with gates representing processing of those states.

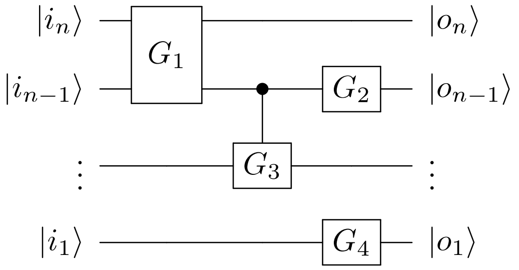
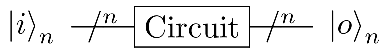


FIGURE 7.1: Illustrating a quantum circuit with n qubits.

This notation is based on one by Richard Feynman, with the convention that time flows from left to right.

Sometimes, an n-qubit state is represented by a wire with a $/^n$ decoration on it, that is referred to as a **register**.



In practice the circuit is effectively a unitary operator acting on the input qubits. A few major differences between classical circuits and quantum ones are:

- Quantum circuits never contain loops or feedbacks: they are *acyclic*
- Quantum wires are never fanned out: since arbitrary quantum states cannot be cloned

- Though the action of a circuit can be analyzed using classical states, the effect on superpositions is what gives it true quantum power.

The fact that quantum evolution is unitary results in quantum gates (and circuits) being reversible. This means that any manipulation of quantum information can be undone, unless an irreversible process such as measurement or decoherence happens on the system. This, and the peculiar features of qubits discussed in Chapter 4, makes for startling differences in the way we must think about quantum algorithms.

Mathematically a gate can be represented as a matrix. Classical reversible gates can have only ones and zeros as elements: reversibility implies that they can only perform a permutation of the inputs. For example, a reversible XOR gate is given by y' output in the truth table of what has sometimes been called a Feynman gate:

x	y	x'	y'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

$$\Longrightarrow \quad \begin{array}{c} \\ 00 \\ 01 \\ 10 \\ 11 \end{array} \begin{array}{c} \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array} \tag{7.1}$$

Such a gate is also implementable as a quantum gate, but the most generic quantum gate is represented by a complex matrix.

7.1 Single Qubit Gates

Classically, there exists only one reversible single bit gate: the NOT gate which effects $0 \to 1, 1 \to 0$. However, any unitary operation on the qubits $|0\rangle$ and $|1\rangle$ is a valid single qubit gate. As we will see, such a gate can always be regarded as a linear combination of the Pauli gates X, iY, Z and the identity.

In circuit notation, a gate G that acts on state $|i\rangle$ to produce state $|o\rangle$ is represented as

$$|i\rangle \; - \boxed{G} - \; |o\rangle$$

The matrix representation of G is found by computing its action on the computational basis states:

$$G_{ij} = \langle i|G|j\rangle \tag{7.2}$$

The full power of the quantum gate emerges when it acts on superposition states. Consider for example the action of NOT, defined in the computational basis by

$$\begin{aligned} X|0\rangle &= \ |1\rangle \\ X|1\rangle &= \ |0\rangle \end{aligned} \quad ; \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \sigma_x \tag{7.3}$$

When X acts on a generic quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we get $X|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$. This represents interchanged probabilities of the state being in $|0\rangle$ or $|1\rangle$.

Other useful quantum single-qubit gates, that have no classical analogue, are described below.

1. Phase Flip (Z) gate:

$$\begin{aligned} Z|0\rangle &= \ |0\rangle \\ Z|1\rangle &= \ -|1\rangle \end{aligned} \quad ; \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \sigma_z \tag{7.4}$$

This gate gives the state $|1\rangle$ a negative sign, an operation that is meaningless in classical logic, but is relevant when it acts on superposition states of a qubit. For instance, the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ changes to the orthogonal state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

2. Hadamard (H) gate:

$$\begin{aligned} H|0\rangle &= \ \tfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right); \\ H|1\rangle &= \ \tfrac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right); \end{aligned} \qquad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(\sigma_x + \sigma_z\right) \tag{7.5}$$

This is an invaluable gate in quantum information processing: it produces equal superpositions of the basis states. Its action can be expressed algebraically as

$$H|x\rangle = \frac{1}{\sqrt{2}}(|x\rangle + (-1)^x|\bar{x}\rangle) = \frac{1}{\sqrt{2}} \sum_{y=0,1} (-1)^{xy}|y\rangle. \tag{7.6}$$

3. Phase (Φ) gate:

$$\begin{aligned} \Phi|0\rangle &= \ |0\rangle; \\ \Phi|1\rangle &= \ e^{i\varphi}|1\rangle \end{aligned} \quad ; \qquad \Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \tag{7.7}$$

Exercise 7.1. Show that the Z, H, and Φ matrices are all unitary.

Exercise 7.2. Calculate the output of each of these gates when the input is a general qubit state $\alpha|0\rangle + \beta|1\rangle$.

Exercise 7.3. What is the action of the Pauli Y gate?

It is useful to visualize the action of single qubit gates by looking at their action on the Bloch sphere. A gate must take any point on the Bloch sphere to another, and can be a rotation about an arbitrary axis through the center of the Bloch sphere. Inversions about the center are also allowed.

Example 7.1.1. To see the effect of the Pauli X matrix on a qubit state on the Bloch sphere,

$$
\begin{aligned}
X\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right) &= \cos\frac{\theta}{2}|1\rangle + e^{i\phi}\sin\frac{\theta}{2}|0\rangle \\
&= e^{i\phi}\left[\cos\left(\frac{\pi}{2}-\frac{\theta}{2}\right)|0\rangle + e^{-i\phi}\sin\left(\frac{\pi}{2}-\frac{\theta}{2}\right)|1\rangle\right] \qquad (7.8)
\end{aligned}
$$

This is a state for which $\theta \to \pi - \theta$ and $\phi \to -\phi$. The transformation is illustrated in Figure 7.2.

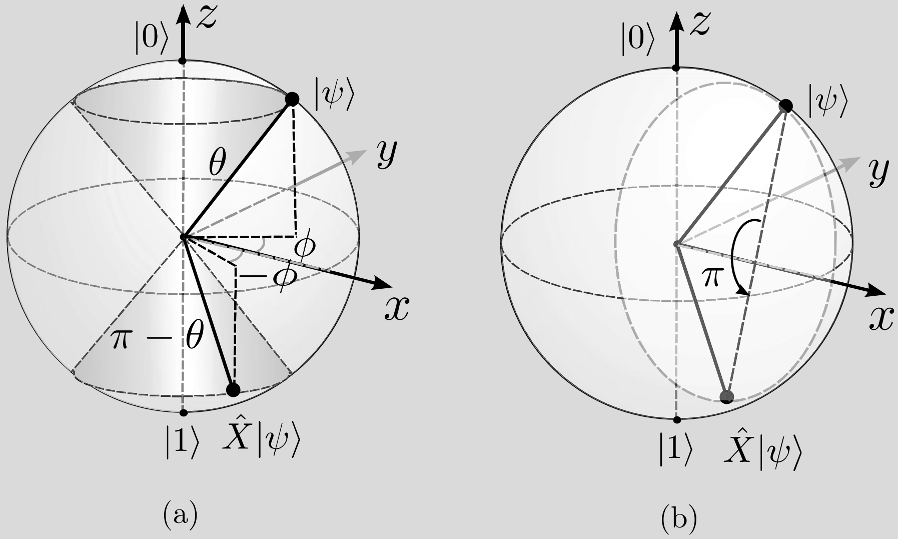


FIGURE 7.2: Action of $\hat{X}$ on the Bloch sphere.(a) The θ and $\pi - \theta$ cones are indicated to show you how the transformation works. (b) The result is equivalent to a rotation about $\hat{\boldsymbol{x}}$ by π.

Exercise 7.4. Show that the Pauli gates Y and Z gates rotate a state on the Bloch sphere by π about the $\hat{\boldsymbol{y}}$ and $\hat{\boldsymbol{z}}$ axes, respectively.

Exercise 7.5. The effect of the H gate on the Bloch sphere can also be regarded as a rotation by π about some axis. Find that axis.

Exercise 7.6. What is the effect of the phase gate Φ on a state located at (θ, ϕ) on the Bloch sphere?

A general rotation can always be constructed as combinations of rotations about the $\hat{\boldsymbol{x}}, \hat{\boldsymbol{y}}$, and $\hat{\boldsymbol{z}}$ axes. Hence a very useful set of gates is the rotation gates, expressed as functions of the Pauli matrices as follows:

$$R_x(\theta) \equiv e^{-i\theta\sigma_x/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{7.9a}$$

$$R_y(\theta) \equiv e^{-i\theta\sigma_y/2} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{7.9b}$$

$$R_z(\theta) \equiv e^{-i\theta\sigma_z/2} = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} \tag{7.9c}$$

Exercise 7.7. Show by using the series expansion of e^x that if A is a matrix such that $A^2 = \mathbb{1}$ then $e^{iA\theta} = \cos(\theta)\mathbb{1} + i\sin(\theta)A$.

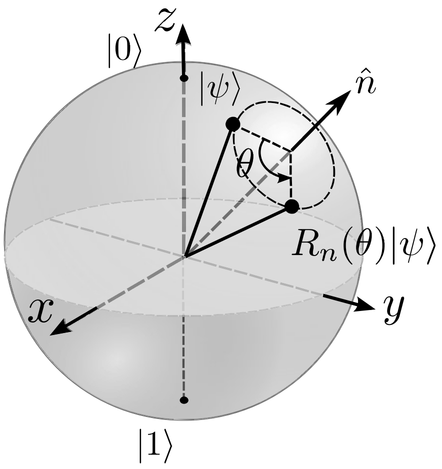


FIGURE 7.3: Rotation of a qubit by $R_n(\theta)$ on the Bloch sphere.

You can now see that a rotation about an axis $\hat{\boldsymbol{n}} = n_x\hat{\boldsymbol{\imath}} + n_y\hat{\boldsymbol{\jmath}} + n_y\hat{\boldsymbol{k}}$ by an angle θ is given by

$$R_{\hat{\boldsymbol{n}}}(\theta) = e^{-i\theta\hat{\boldsymbol{n}}\cdot\vec{\boldsymbol{\sigma}}/2} = \cos\left(\frac{\theta}{2}\right)\mathbb{1} - i\sin\left(\frac{\theta}{2}\right)(n_x\sigma_x + n_y\sigma_y + n_z\sigma_z). \tag{7.10}$$

The action of this gate is illustrated in Figure 7.3.

Exercise 7.8. Verify that gate $R_{\hat{\boldsymbol{n}}}(\theta)$ takes a state with Bloch vector $\hat{\boldsymbol{a}}$ to one rotated by θ about the $\hat{\boldsymbol{n}}$ axis.

Box 7.1: Useful Representations of Single Qubit Gates

The Pauli matrices, along with the 2×2 identity matrix, are said to form a basis for the space of 2×2 matrices. So any single qubit gate A can be expressed as a linear combination

$$A = a_0 \mathbb{1} + \vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}}.$$

1. Since A is unitary, it can be expressed up to an overall phase as

$$U = u_0 \mathbb{1} + i\vec{\boldsymbol{u}} \cdot \vec{\boldsymbol{\sigma}}, \tag{7.11}$$

   for *real* u_0, u_1, u_2, u_3 s.t. $u_0^2 + \vec{\boldsymbol{u}} \cdot \vec{\boldsymbol{u}} = 1$.

2. This can be re-expressed as

$$U = e^{i\alpha} e^{i\beta \hat{\boldsymbol{n}} \cdot \vec{\boldsymbol{\sigma}}}, \tag{7.12}$$

   where α is a phase, $\hat{\boldsymbol{n}}$ is a unit vector parallel to $\vec{\boldsymbol{u}}$ and β is an angle, which turns out to be half the angle of rotation of the initial state about the axis $\hat{\boldsymbol{n}}$.

Successive action of gates

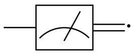
Two successive operations are two unitary gates, say A and B, acting one after another. Algebraically, we represent the resultant by the action of the usual matrix product of the two gates:

$$|\psi\rangle \xrightarrow{A} A|\psi\rangle \xrightarrow{B} BA|\psi\rangle. \tag{7.13}$$

Note that the order of the gates is important. Operators do not in general commute. The circuit representation of this process is like a time sequence, and the order of gates is obvious:

$$|\psi\rangle \;—\boxed{A}—\boxed{B}—$$

7.1.1 Measurement gate

At the end of a computation we need to measure the output in order to read out the result of the computation. This leads to obtaining classical information (in bits) out of the quantum system. One sets up an experiment that measures an appropriate physical quantity to give one of its eigenvalues as the result (recall Section 3.3 and the nature of measurements in quantum mechanics). We denote this process generically by a *measurement gate* . The double line for the output state is to emphasize that it is a classical state. By default the measurement is assumed to be in the computational basis. The state just prior to measurement encodes the probabilities of its collapsing to $|0\rangle$ or $|1\rangle$.

7.2 Multi-Qubit Gates

Two qubits together can be represented as 4-column vectors in Hilbert space. The most general 2-qubit gate is therefore a 4×4 unitary. An operation on two qubits that acts independently on each of the two can be expressed as a direct product of two single-qubit operations as defined in Equation 3.31:

$$O = O_1 \otimes O_2.$$

For example, the 2-qubit H gate is represented by the action

$$H^{\otimes 2}|x\rangle|y\rangle = H|x\rangle \otimes H|y\rangle, \tag{7.14}$$

with matrix representation

$$\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{7.15}$$

You need to distinguish between the different possibilities shown in Figure 7.4. The circuit diagrams for these gates will clarify the difference.

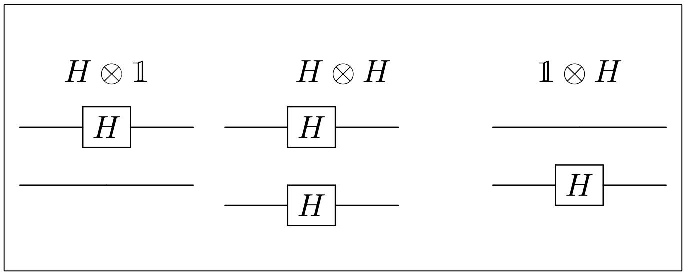


FIGURE 7.4: H gates acting in different ways on two qubits.

These sort of gates can easily be generalized to any dimensions.

Exercise 7.9. Construct the matrix representations for the operators shown in Figure 7.4.

Exercise 7.10. Find the matrix representing $X \otimes Z$.

The interesting thing about multi-qubit gates is that in general, they would not act independently on the individual qubits, but entangle them. This is the hallmark of quantum information processing that gives the most crucial advantage over classical processing. For example, consider the most famous 2-qubit gate, the controlled-NOT or CNOT gate whose classical version we saw in Chapter 6. This gate flips the target qubit when the control qubit is set to 1. The truth table of the CNOT is used to define the action of the quantum gate on the computational basis states:

$$U_{\text{CNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \equiv \begin{bmatrix} \mathbb{1} & 0 \\ 0 & X \end{bmatrix} \tag{7.16}$$

Notice that the truth table for the second output corresponds to the well-known XOR operation on the inputs. The operation is, however, completely reversible. We denote the action of this gate by

$$U_{\text{CNOT}}|x\rangle|y\rangle = |x\rangle|x \oplus y\rangle. \tag{7.17}$$

Note that when we use letters x and y to label quantum states, they refer to the computational basis states. This gate is represented by the circuit of Figure 7.5. An important caveat here: though the control qubit seems to come out of the gate unchanged when it is in a computational basis state, the output will in general be entangled with the state of the target qubit, as we will see in the next example.

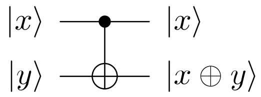


FIGURE 7.5: CNOT gate.

Example 7.2.1. As an illustration of how a controlled gate acts on superposition states, consider

$$\begin{aligned} CNOT(\alpha|0\rangle + \beta|1\rangle)|0\rangle &= CNOT(\alpha|00\rangle + \beta|10\rangle) \\ &= \alpha|00\rangle + \beta|11\rangle \end{aligned} \tag{7.18}$$

which is an entangled state. Figure 7.6 gives the circuit for this process.

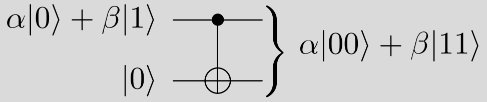

$\alpha|0\rangle + \beta|1\rangle$
$|0\rangle$
$\alpha|00\rangle + \beta|11\rangle$

FIGURE 7.6: CNOT producing entanglement.

This example also illustrates the No-cloning theorem of Chapter 4. The CNOT gate appears as a cloner if the target qubit is $|0\rangle$:

$$U_{\text{CNOT}}|x\rangle|0\rangle = |x\rangle|x\rangle. \tag{7.19}$$

However, this is true iff $|x\rangle$ is a computational basis state. If the control qubit is a generic quantum state $|\psi\rangle$, the output of this gate is an *entangled* state. If our gate were a cloner, then the output ought to have been $|\psi\rangle \otimes |\psi\rangle$, which is a separable state.

The notion of a conditional or controlled gate can be extended to any unitary single-qubit operation U by defining

$$U_{CU}|x\rangle|y\rangle = |x\rangle U^x|y\rangle \tag{7.20}$$

The notation makes it obvious that the operator U acts on the target qubit $|y\rangle$ only if the control qubit is set to 1. Figure 7.7 shows the circuit representation for this action.

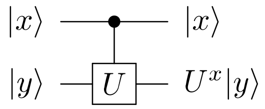


FIGURE 7.7: Circuit representing a controlled-U gate.

The matrix representation of such a gate is

$$U_{CU} = \begin{bmatrix} \mathbb{1} & 0 \\ 0 & U \end{bmatrix}. \tag{7.21}$$

You can prove that U_{CU} is unitary if U is.

One can use either of the input qubits as the control or the target. We will use the notation C_{ij} to denote the i^{th} bit as the control bit and the j^{th} bit as the target.

Exercise 7.11. Show that $(H \otimes H)C_{12}(H \otimes H) = C_{21}$, i.e., if you change basis from computational basis to the X basis $\{|+\rangle, |-\rangle\}$, then the control and target bits get interchanged. The circuit for the problem looks like Figure 7.8.

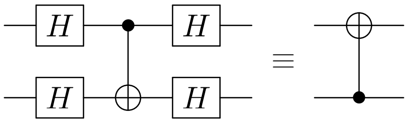


FIGURE 7.8: CNOT with second qubit as control and first as target.

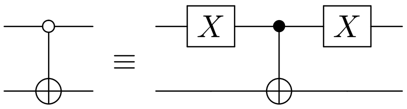


FIGURE 7.9: A 0-controlled gate.

The control action can be conditioned on the control bit set to 0 instead of 1. Such a gate is represented in Figure 7.9.

For more than one qubit, a variety of control possibilities are illustrated in Figure 7.10.

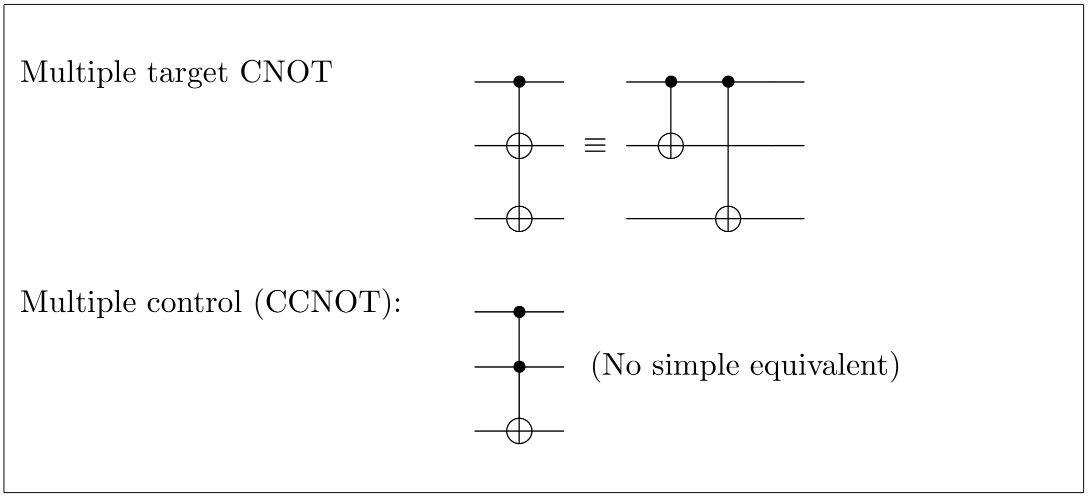


FIGURE 7.10: Different control operations

Example 7.2.2. Creating Bell states

Prototype entangled states are the Bell states of Equation 4.10, and they can be produced using CNOT gates. For example,

$$|0\rangle \otimes |0\rangle \xrightarrow{H\otimes\mathbb{1}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \xrightarrow{C_{12}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{7.22}$$

producing the first Bell state $|\beta_{00}\rangle$. It's easy to deduce that the general Bell state is produced by the simple circuit given in Figure 7.11:

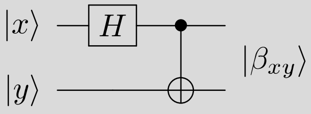


FIGURE 7.11: Circuit for preparing Bell States

Exercise 7.12. Verify that the operation depicted in circuit 7.11 is reversible.

Exercise 7.13. Verify that the Bell states can be written as

$$|\beta_{xy}\rangle = \frac{1}{\sqrt{2}}\left(|0y\rangle + (-1)^x|1\bar{y}\rangle\right).$$

The reverse of the circuit 7.11 can be used to convert the Bell basis to the computational one. Making a measurement after that can tell us which of the Bell states we started with. This is called a *Bell Measurement*, depicted in Figure 7.12.

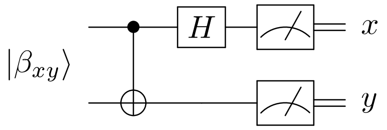


FIGURE 7.12: Circuit for Bell measurement.

Example 7.2.3. Let us analyze the output of the circuit shown in Figure 7.13. $|\psi\rangle$ is a generic unknown qubit $\alpha|0\rangle+\beta|1\rangle$. A Bell measurement is performed on this qubit and one of an entangled pair prepared in the state $|\beta_{00}\rangle$ (Equation 4.10).

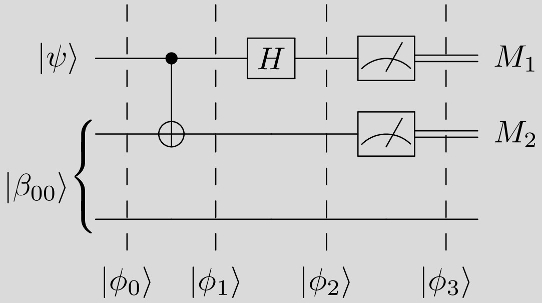


FIGURE 7.13: Bell measurement on part of an entangled state.

We will algebraically analyze the output at each stage of the circuit:

$$\begin{aligned}
|\phi_0\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right). \\
|\phi_1\rangle &= C_{12} \otimes \mathbb{1}|\phi_0\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right). \\
|\phi_2\rangle &= H \otimes \mathbb{1} \otimes \mathbb{1}|\phi_1\rangle \\
&= \frac{\alpha}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)(|00\rangle + |11\rangle)\right] \\
&\quad +\frac{\beta}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right].
\end{aligned}$$

Now $|\phi_3\rangle$ is a single-qubit state of the last wire, obtained after measuring the first two qubits of $|\phi_2\rangle$. So let's regroup the terms in $|\phi_2\rangle$ separating out the states of the first two qubits from the third:

$$\begin{aligned} |\phi_2\rangle &= \frac{1}{2}\left[\alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle)\right. \\ &\quad \left.+\beta\left(|010\rangle + |001\rangle - |110\rangle - |101\rangle\right)\right] \\ &= \frac{1}{\sqrt{2}}|00\rangle\left[\frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)\right] \\ &+ \frac{1}{\sqrt{2}}|01\rangle\left[\frac{1}{\sqrt{2}}(\alpha|1\rangle + \beta|0\rangle)\right] \\ &+ \frac{1}{\sqrt{2}}|10\rangle\left[\frac{1}{\sqrt{2}}(\alpha|0\rangle - \beta|1\rangle)\right] \\ &+ \frac{1}{\sqrt{2}}|11\rangle\left[\frac{1}{\sqrt{2}}(\alpha|1\rangle - \beta|0\rangle)\right] \end{aligned}$$

When the first two qubits are measured, $|\phi_2\rangle$ collapses to the state corresponding to the output. This leaves the third qubit in a corresponding state, that is closely related to $|\psi\rangle$as tabulated in Table 7.1.

TABLE 7.1: Resulting state after measurement.

Measurement result	$|\psi_3\rangle$
00	$|\psi\rangle$
01	$X|\psi\rangle$
10	$Z|\psi\rangle$
11	$XZ|\psi\rangle$

The idea behind this circuit is quantum state teleportation, which will be further discussed in Section 9.1.1.

Example 7.2.4. Measuring an operator

Consider a unitary operator $\hat{U}$ that can be used as a quantum gate. If $\hat{U}$ happens to be an observable as well, then it must be Hermitian. So its eigenvalues must be ±1. The Pauli operators are examples of such operators. Now we'll show that the circuit in Figure 7.14 effects a measurement of $\hat{U}$ on the state $|\psi\rangle$ input in the lower register.

Remember, this means that at the end of the circuit, the meter reads 0 or 1 corresponding to the eigenvalues $+1$ or -1, and the state on the bottom wire must be the corresponding eigenstate $|u_+\rangle$ or $|u_-\rangle$ of $\hat{U}$.

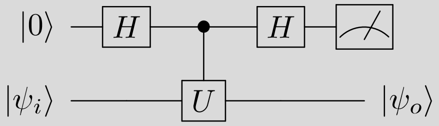


FIGURE 7.14: Circuit for measuring an operator

We have

$$\hat{U}|u_+\rangle = |u_+\rangle, \qquad \hat{U}|u_-\rangle = -|u_-\rangle.$$

We can expand the initial state in the U-basis:

$$|\psi_i\rangle = a|u_+\rangle + b|u_-\rangle.$$

Working through the circuit,

$$\begin{aligned}
|0\rangle \otimes |\psi_i\rangle \quad & \xrightarrow{H_1} \quad \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \otimes \big(a|u_+\rangle + b|u_-\rangle\big) \\
& = \frac{1}{\sqrt{2}}\big(a|0\rangle|u_+\rangle + a|1\rangle|u_+\rangle + b|0\rangle|u_-\rangle + b|1\rangle|u_-\rangle\big) \\
& \xrightarrow{CU_{12}} \quad \frac{1}{\sqrt{2}}\big(a|0\rangle|u_+\rangle + a|1\rangle\hat{U}|u_+\rangle + b|0\rangle|u_-\rangle + b|1\rangle\hat{U}|u_-\rangle\big) \\
& = a\frac{\big(|0\rangle + |1\rangle\big)}{\sqrt{2}}|u_+\rangle + b\frac{\big(|0\rangle - |1\rangle\big)}{\sqrt{2}}|u_-\rangle.
\end{aligned}$$

On measuring the first qubit, in the X basis, we get 0 with probability $|a|^2$ and 1 with probability $|b|^2$ with the second qubit left in the corresponding eigenstate of $\hat{U}$. The circuit thus implements a measurement of the observable U. If the input state were an exact eigenstate of U then the corresponding eigenvalue is measured with probability 1.

7.3 Quantum Function Evaluation

We've taken the circuit analogy for quantum computation up to gates. Can we go further? Can we identify a set of universal gates, as we did for classical computation?

Since a computation is essentially the evaluation of a function of the inputs, let's first fix what we mean by a quantum function evaluation. Consider a function $f : \{0,1\}^n \mapsto \{0,1\}^m$ that takes an n-bit input x and produces an m-bit output $f(x)$. A reversible implementation of this function would have an $n + m$-bit input and the same number of bits in the output. We will use this to define the unitary operator implementing $f(x)$.

Definition 7.1. A quantum function evaluator *is a unitary operator* U_f, *for* $f : \{0,1\}^n \mapsto \{0,1\}^m$, *such that*

$$U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle. \tag{7.23}$$

This is essentially an f-controlled XOR gate (which is like an f-controlled NOT gate if $m = 1$), expressed in the circuit of Figure 7.15.

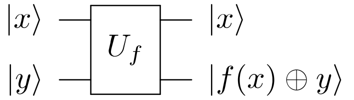


FIGURE 7.15: Quantum function evaluator.

Here, $|x\rangle$ is an n-qubit basis state while $|y\rangle$ is an m-qubit one. Note that U_f will be represented by an $n + m$ square matrix. If the input lower register $y = 0$, then the output on the register is just $f(x)$.

Exercise 7.14. Show that U_f as defined in Equation 7.23 is unitary and therefore reversible.

The important feature of a unitary transformation is not only that it admits an inverse, but also that it is linear. So it acts on superpositions thus:

$$U_f\left(c_1|x_1\rangle + c_2|x_2\rangle\right)|y\rangle = c_1 U_f\left(|x_1\rangle|y\rangle\right) + c_2 U_f\left(|x_2\rangle|y\rangle\right). \tag{7.24}$$

For instance, if the input is the uniform superposition of two qubits, the linearity of U_f means that

$$U_f \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle\right).$$

The output is an entangled superposition state of both registers, containing both $f(0)$ as well as $f(1)$. This generalizes to multiple qubits as well. A uniform superposition of n qubits is the normalized sum of all 2^n possible n-qubit basis states $|0\rangle, |1\rangle \ldots |2^n - 1\rangle$. So we have

$$U_f \frac{1}{\sqrt{2^n}}\left(\sum_{x=0}^{2^n-1} |x\rangle_n\right)|0\rangle_m = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_m \tag{7.25}$$

where the subscripts on the states indicate the dimensionality. The function has been evaluated in parallel on all inputs. This has been referred to as **quantum parallelism**. The catch is, however, that this superposition does not mean much to our classical minds, until we measure the output, upon which **one** of the answers is selected! We can never know all the $f(x)$'s at once, nor can we clone the output and hope to learn $f(x)$ by making repeated measurements of the output state.

Nevertheless, this feature is enormously useful in designing quantum algorithms. One has to additionally choose clever modifications of the output such that the state containing the answer occurs with high amplitude. We will see this in action in the next chapters.

7.4 Universal Quantum Gates

We now wish to push the circuit analogy further and explore the possibility of universal quantum gates. Let's start with single-qubit gates. We've seen that these are 2×2 unitary matrices, which take a point on the Bloch sphere to another. It is easy to see that there are infinitely many possible 1-qubit gates. These however cannot form a universal set since controlled operations cannot be implemented by taking direct products of 1-qubit gates. How do we implement controlled gates in general?

7.4.1 Controlled-U gate

Working toward a general construction for a controlled U gate for arbitrary U makes use of the following representation for U:

Theorem 7.1. *Any unitary 2×2 matrix can be decomposed as*

$$U = e^{i\theta}\ A\ \sigma_x\ B\ \sigma_x\ C, \quad s.t \qquad A\ B\ C = \mathbb{1}, \tag{7.26}$$

where $A, B,$ and C are also unitary.

Proof. The proof hinges on the fact that any unitary matrix implements a rotation on the Bloch sphere, up to an over-all phase factor $e^{i\theta}$. Suppose V is some unitary matrix. The matrix $V\sigma_x V^\dagger$ is also unitary, so that it can be represented (see Equation 7.11) as

$$V\sigma_x V^\dagger = a_0\mathbb{1} + \vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}}, \quad a_0^2 + \vec{\boldsymbol{a}} \cdot \vec{\boldsymbol{a}} = 1.$$

But $V\sigma_x V^\dagger$ is a similarity transformation of σ_x. So it must preserve its trace, which is zero. Therefore $a_0 = 0$ and

$$V\sigma_x V^\dagger = \hat{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}} \text{ for a real unit } \hat{\boldsymbol{a}}.$$

Note that $\sigma_x = \hat{\boldsymbol{x}} \cdot \vec{\boldsymbol{\sigma}}$. Then $V\sigma_x V^\dagger$ must be rotating $\hat{\boldsymbol{x}}$ to a new direction $\hat{\boldsymbol{a}}$. Similarly, another unitary W will achieve

$$W\sigma_x W^\dagger = \hat{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}} \text{ for a real unit } \hat{\boldsymbol{b}}.$$

Thus we have

$$\begin{aligned} V\sigma_x V^\dagger\ W\sigma_x W^\dagger &= (\hat{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}})\ (\hat{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}}) \\ &= \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{b}}\mathbb{1} + i\ \hat{\boldsymbol{a}} \times \hat{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}}. \end{aligned}$$

(Refer to Equation 3.34 you proved in one of the problems of Chapter 3.) We can now think of $\hat{\boldsymbol{a}}$ and $\hat{\boldsymbol{b}}$ as directions with an angle γ between them so that

$$\hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{b}} = \cos\gamma, \qquad \hat{\boldsymbol{a}} \times \hat{\boldsymbol{b}} = \sin\gamma\hat{\boldsymbol{n}}, \text{ which is perpendicular to } \hat{\boldsymbol{a}} \text{ and } \hat{\boldsymbol{b}}.$$

Then we can construct

$$\begin{aligned} U &= e^{i\theta} V\sigma_x V^\dagger \; W\sigma_x W^\dagger \\ &= e^{i\theta}\left(\cos\gamma\mathbb{1} + i\sin\gamma\hat{\boldsymbol{n}}\cdot\vec{\boldsymbol{\sigma}}\right) \\ &= e^{i\theta} e^{i\gamma\hat{\boldsymbol{n}}\cdot\vec{\boldsymbol{\sigma}}}, \end{aligned}$$

which is a valid representation for a unitary operator! If we identify

$$V = A, \quad V^\dagger \; W = B \text{ and } W^\dagger = C,$$

then we have the requisite representation for U. □

We can implement C-$V\sigma_x V^\dagger \; W\sigma_x W^\dagger$ by the circuit of Figure (7.16).

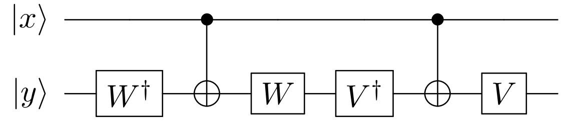


FIGURE 7.16: Circuit to evaluate C-U up to the phase factor

It is straightforward to see that when $x = 0$, the output is $VV^\dagger WW^\dagger y = y$, and when $x = 1$, the output is $V\sigma_x V^\dagger \; W\sigma_x W^\dagger y = Uy$ up to the phase. So this gives C-U up to the phase factor. We need to additionally implement the controlled phase C-Θ where

$$\Theta = \begin{bmatrix} e^{i\theta} & 0 \\ 0 & e^{i\theta}. \end{bmatrix}$$

Now check that

$$\text{C}{-}\Theta = \begin{bmatrix} \mathbb{1} & 0 \\ 0 & \Theta \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \otimes \mathbb{1}.$$

We then have the implementation of the full C-U illustrated in Figure (7.17), that uses only CNOT gates and single-qubit gates.

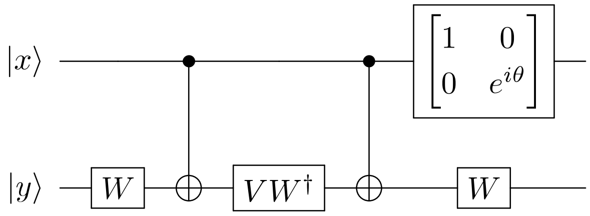


FIGURE 7.17: Implementation of controlled U gate.

Here, V and W are arbitrary unitaries. We are now half-way through in our quest for universal quantum gates, of which one set is given in the following theorem:

Theorem 7.2. ***Universal Quantum Gates:*** *the CNOT gate along with single-qubit gates is universal.*

How do we prove this? Now classically, the Toffoli gate, which is a C-C-NOT gate, is universal. We'll now show that given our construction for C-U gates, we can build doubly controlled C-C-U gates as follows. Consider a unitary Q such that $Q^2 = U$. Then we can build a C-C-U by the circuit in Figure 7.18. Let's work through this circuit algebraically to show that it works as expected:

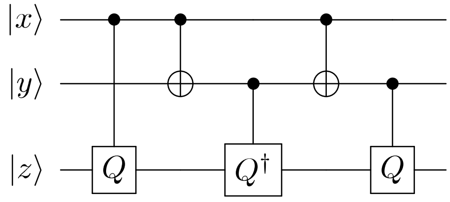


FIGURE 7.18: Implementation of C-C-U gate.

$$\begin{aligned}
|x\rangle|y\rangle|z\rangle &\rightarrow |x\rangle|y\rangle\ Q^x|z\rangle \\
&\rightarrow |x\rangle|x \oplus y\rangle\ Q^x|z\rangle \\
&\rightarrow |x\rangle|x \oplus y\rangle\ (Q^\dagger)^{x\oplus y}\ Q^x|z\rangle \\
&\rightarrow |x\rangle|y\rangle\ (Q^{-1})^{x\oplus y}\ Q^x|z\rangle \\
&\rightarrow |x\rangle|y\rangle\ Q^y\ Q^{-x\oplus y}\ Q^x|z\rangle
\end{aligned}$$

The power of Q that acts on $|z\rangle$ in the end is

$$y - (x \oplus y) + x = y - (x + y - 2xy) + x = 2xy.$$

So the effect of this circuit is

$$|z\rangle \rightarrow Q^{2xy}|z\rangle = U^{xy}|z\rangle,$$

which is exactly what we want. We can for instance construct a quantum Toffoli gate by using $Q^2 = X$. One such "square root of NOT" gate is

$$\sqrt{X} = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}. \tag{7.27}$$

Example 7.4.1. A useful question to ask in designing circuits is how to minimize the number of basic gates required for a given implementation. In our construction for the C-C-U gate given above, we require 2 CNOTs plus 2 CNOTs for each C-Q gate, that is a total of 8 CNOTs. Can we be more frugal? Here is an example from Mermin [48] of a construction for a Toffoli gate using only 4 CNOT gates. Consider two unitaries A and B such that $A^2 = \mathbb{1} = B^2$. This means that

$$A = V^\dagger X V, \qquad B = W^\dagger X W.$$

Thus each C-A and C-B gate requires only one CNOT gate and two single-qubit gates.

You should be able to work out that the circuit of Figure 7.19 implements a doubly controlled $(BA)^2$ gate, up to a phase α.

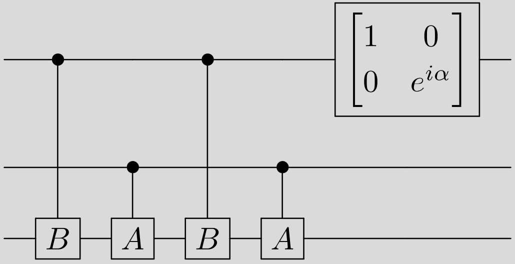


FIGURE 7.19: Efficient implementation of a Toffoli gate.

Now

$$\begin{aligned} AB &= V^\dagger X V W^\dagger X W = (\hat{\boldsymbol{a}} \cdot \vec{\boldsymbol{\sigma}})(\hat{\boldsymbol{b}} \cdot \vec{\boldsymbol{\sigma}}) \\ &= \hat{\boldsymbol{a}} \cdot \hat{\boldsymbol{b}} \mathbb{1} + i(\hat{\boldsymbol{a}} \times \hat{\boldsymbol{b}}) \cdot \vec{\boldsymbol{\sigma}}. \end{aligned}$$

If we choose the angle between $\hat{\boldsymbol{a}}$ and $\hat{\boldsymbol{b}}$ to be $\pi/4$, and also let $\hat{\boldsymbol{a}} \times \hat{\boldsymbol{b}}$ point along $\hat{\boldsymbol{x}}$, then we have

$$\begin{aligned} AB &= \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\sigma_x = \frac{1}{\sqrt{2}}(\mathbb{1} + iX) \\ (AB)^2 &= \frac{1}{2}(\mathbb{1} + 2iX + (-X)^2) = iX. \end{aligned}$$

Thus we can regard AB as the square-root of X up to a phase of i. This phase can be cancelled if we choose $\alpha = -\pi/2$ and this circuit implements a Toffoli gate with just 4 CNOTs and single-qubit gates.

One can construct multiply controlled U gates, a C^n-U gate, by a cascading circuit using n control bits, Toffoli gates and $n-1$ auxiliary bits, as in Figure 7.20.

Verify that this works! The use of the Toffoli gates performs an "AND" of all the control bits, which finally controls the U gate. Also note that all the auxiliaries can be returned to their original state of $|0\rangle$ by adding the reverse of each of the actions after obtaining C^n-U.

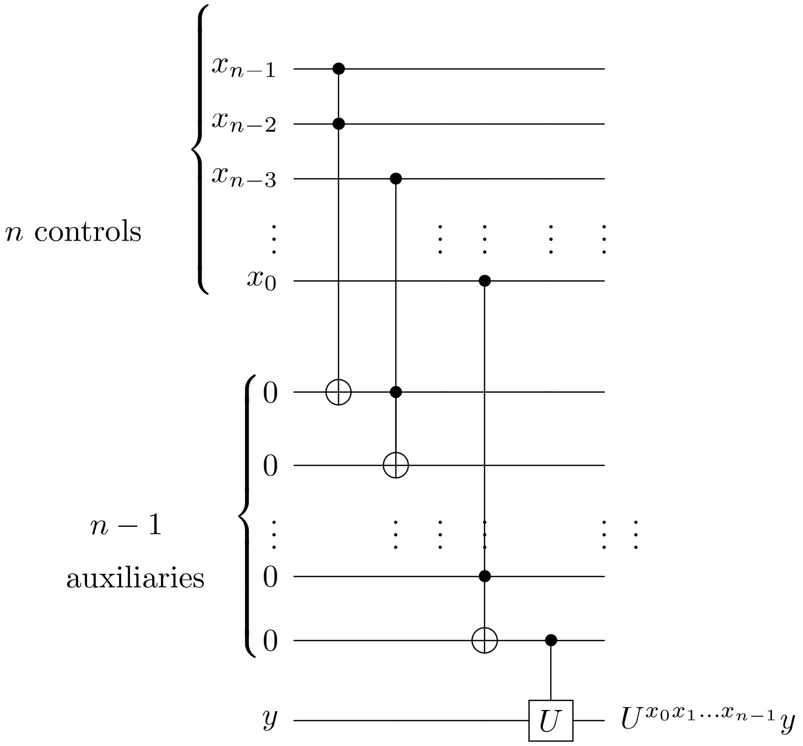


FIGURE 7.20: Implementation of C^n-U gate

7.4.2 Universal gates

We've proved that the CNOT gate along with all possible single-qubit gates form a universal set. But this set is still infinite. We'd like to do better: to get a finite set of gates as in the classical case. Of course we must realize that the set of possible single qubit gates is itself infinite as opposed to the finite number of gates in classical computation. Yet it is surprising that there exist more rigorous theorems (e.g., the Solovay–Kitaev Theorem [23]) confirming the universality of a smaller set of gates, such as for example, H, CNOT, $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ or the Toffoli and H gates. But these sets of gates cannot be used to construct arbitrary gates to infinite precision. So the theorems actually prove that one can *approximate* arbitrary unitary gates, to *any* degree of accuracy, by using a finite set of gates. We will not dwell on these theorems or their proofs here.

7.5 Comments on Measurement

Some issues regarding measurement in quantum circuits are to be noted here, which you can prove for yourself with some thought:

1. **Deferred measurement**: when measurements are made in a circuit and after that further gates are implemented (whether controlled by the measurement or no), it can always be assumed that the measurement is made at the very end of the circuit. This is saying that measurement can always be assumed to have been *deferred* to the end of the computation without any effect on the results.
2. **Implicit measurement**: any quantum wires that are left at the end of the circuit can be assumed to have been measured: their states will anyway have collapsed when other wires are measured for the purpose of readout.
3. **Irreversibility**: quantum measurement is in general an irreversible process, and if included in a circuit, will make it irreversible. However, if the measurement reveals no information about the state being measured (refer for instance to the teleportation protocol of Example 7.2) then the circuit is still reversible!

Many of the results in this chapter are discussed in the paper by Barenco et al. [3], and in the book by Mermin [48].

Problems

7.1. Show that the n-qubit Hadamard gate acts as

$$H^{\otimes n}|x\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{y=1}^{2^n-1} (-1)^{x\cdot y}|y\rangle. \tag{7.28}$$

where $x \cdot y$ is the bitwise product of x and y:

$$x \cdot y = x_0y_0 \oplus x_1y_1 \oplus \ldots x_{n-1}y_{n-1}. \tag{7.29}$$

7.2. Often it helps to simplify circuits when we can identify equivalences between some combinations of gates. Prove, for example, the following circuit identities:

(a) $HXH = Z$

(b) $HYH = -Y$

(c) $HZH = X$

7.3. Show the following relations concerning rotation matrices:

(a) $R_n(\theta_1)R_n(\theta_2) = R_n(\theta_1 + \theta_2)$

(b) $XR_n(\theta)X = R_n(-\theta)$

7.4. The "SWAP" gate S interchanges two inputs, defined by

$$S|xy\rangle = |yx\rangle.$$

(a) Give the matrix representing this gate.

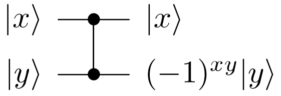
(b) Show that it can be implemented by 3 CNOT gates as

$$S_{12} = C_{12}C_{21}C_{12}.$$

(c) Show that the matrix is equivalent to

$$S_{12} = \frac{1}{2}\left(\mathbb{1} + X_1X_2 + Y_1Y_2 + Z_1Z_2\right)$$

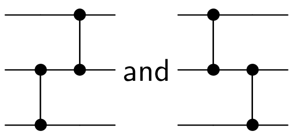
7.5. The controlled phase-flip gate takes $|11\rangle$ to $-|11\rangle$ while leaving the other basis states unchanged. It is sometimes represented as follows, since its action is symmetric in the inputs:



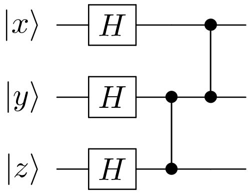
(a) Construct the matrix for this gate.

(b) Build a CNOT gate using controlled phase-flip gates an another single-qubit gate.

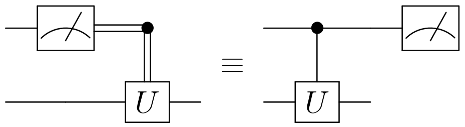
(c) What is the difference in the outputs of the following two circuits?



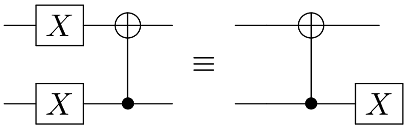
(d) Evaluate the output of the circuit

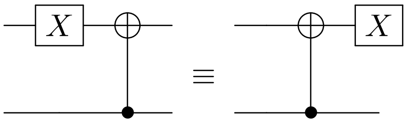


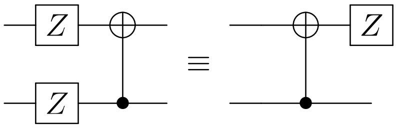
7.6. Show that classical conditional operations are equivalent to quantum control, i.e., show that the following two circuits are equivalent:

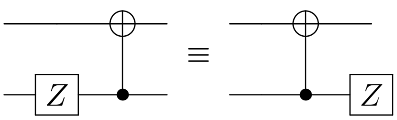


7.7. Verify the following circuit identities:

(a)


(b)


(c)


(d)


7.8. Consider the four possible 1-bit functions

$$\begin{aligned} f_0 : 0 &\to 0 \\ 1 &\to 0 \end{aligned}, \qquad \begin{aligned} f_1 : 0 &\to 0 \\ 1 &\to 1 \end{aligned}, \qquad \begin{aligned} f_2 : 0 &\to 1 \\ 1 &\to 0 \end{aligned}, \qquad \begin{aligned} f_3 : 0 &\to 1 \\ 1 &\to 1 \end{aligned}.$$

Construct the matrix representation of U_f for each. Also give a simple circuit to implement each using basic 1-qubit gates.

7.9. Consider 1-bit integer addition. Write down the truth tables for sum and carry bits. Then construct a quantum half-adder by implementing the truth tables, using only CNOT gates.

7.10. Examine the following circuit and analyze the final output. Here, the input is an unknown entangled state

$$\begin{aligned} |\psi\rangle &= \alpha|01\rangle + \beta|10\rangle \\ \text{and } |GHZ\rangle &= \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right). \end{aligned}$$