Contents

List of Figures

Chapter 1

Quantum circuits

Classical computers use bits to represent information for computation. A bit can take on only one value at a time from a choice of two permitted values. For example, a bit 1 may be used to encode the information "turned on" while the bit 0 may be used to represent "turned off." A string of bits can be used to represent large chunks of information for computation. The study of computer architecture begins with a botton-up approach in which bits are studied first, followed by bit operations leading to more complicated circuitry for manipulating bits. We follow a similar approach here. We will explain the most fundamental components of a quantum computer starting with the most basic element, the qubit.

1.1 The qubit

Qubits are the most fundamental elements of a quantum computer. They correspond to their classical computer counterparts known as bits. The most important difference between qubits and classical bits is the idea of quantum superposition – while a bit is limited to two values (say 0 and 1), a qubit can be in a state that consists of some component of either 0 and 1.

The appropriate notation for a qubit is through the use of bras and kets in Dirac notation. The wave function of a qubit is given by

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1.1}$$

where $|0\rangle$ and $|1\rangle$ are the *computational basis states*. These two states are essentially the quantum analogues of classical bits. In (1.1), α and β are complex numbers.

Classical bits can be measured for their information content without any effect on that information. A classical bit with a value of 1 can be measured to indicate this value. Following the measurement, the bit will remain in the same *state* before measurement. A qubit differs from this significantly. Since the state of a qubit is described by a wave function as shown in (1.1), its measured value is predicted by quantum mechanics to be either $|0\rangle$ or $|1\rangle$ with probability $|\alpha|^2$ or $|\beta|^2$. For that reason, the coefficients α and β are the *probability amplitudes* of $|\psi\rangle$.

Despite this strange behavior of qubits, they exist in nature and can be implemented using several methods. For instance, in chapter 3 we realize qubits using photons. Active areas of research in qubit implementation study several schemes including ion traps, electron spins and NMR [6].

1.2 Bloch sphere interpretation of the qubit

We have discussed the meaning of the probability amplitudes in the qubit wave function defined in (1.1). Because the probabilities must sum to one, we have the following constraint.

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.2}$$

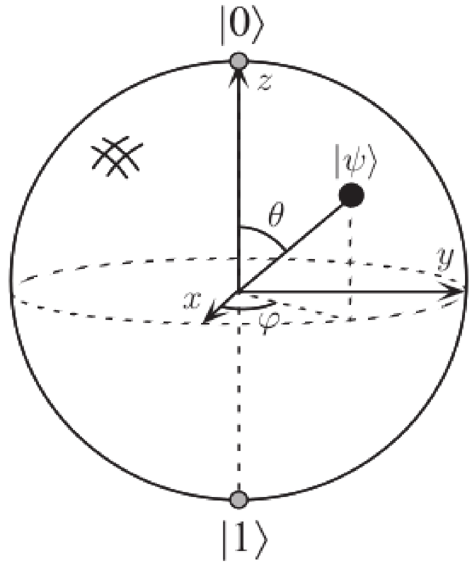

Figure 1.1: Bloch sphere interpretation of a qubit

This results in a geometrical interpretation of the qubit. Because α and β are complex numbers, the wave function of a qubit may be rewritten as

$$|\psi\rangle = e^{i\gamma}\cos\frac{\theta}{2}|0\rangle + e^{i(\gamma+\varphi)}\sin\frac{\theta}{2}|1\rangle \tag{1.3}$$
$$= e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{1.4}$$

for some real numbers γ, θ and φ. Here, note that there is a global phase shift which produces no observable effects. We will ignore it and instead write the qubit as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{1.5}$$

This representation of a qubit results in a mapping with the unit sphere. The qubit in (1.5) is located at the point $(1, \theta, \varphi)$ on the unit sphere in spherical coordinates. This unit sphere is named the *Bloch sphere* after the name of its discoverer. The Bloch sphere is an excellent way of visualizing single qubit states. It is shown in figure 1.1. Sadly, it cannot be used to visualize multiple qubit systems. However, in section 1.3, we introduce operations on single qubits and visualize the changes that they cause with the help of the Bloch sphere.

1.3 Single qubit operations

Operations on a qubit must preserve the norm of the qubit, i.e., given an operation O on a single qubit and two qubits $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\psi'\rangle = O|\psi\rangle = a'|0\rangle + b'|1\rangle$, the normalization conditions

$$a^2 + b^2 = a'^2 + b'^2 = 1 \tag{1.6}$$

must hold. For this reason, operators on single qubits are 2x2 unitary matrices. A unitary matrix U has the defining property $U^\dagger U = UU^\dagger = I$ where $U^\dagger$ is the adjoint of U.

The most common single qubit operations are represented by the Pauli matrices. The Pauli matrices are shown below.

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} ; Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} ; Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{1.7}$$

Three other matrices that are commonly used in quantum computing are the Hadamard (H), $\pi/8$ (T) and phase (S) gates. These are shown below.

$$H \equiv \frac{X+Z}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} ; T \equiv \begin{bmatrix} 1 & 0 \\ 0 & exp(i\pi/4) \end{bmatrix} ; S \equiv T^2 = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{1.8}$$

Incidentally, the Hadamard gate is also known as the "square root of NOT" gate because it maps $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|0\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$, both of which are "halfway" between $|0\rangle$ and $|1\rangle$. We can visualize the operation of the Hadamard gate in two steps:

1. Rotate the qubit vector in the Bloch sphere about the y axis by 90° and

2. Rotate the new qubit vector in the Bloch sphere about the x axis by 180°

The final vector represents the output of the Hadamard gate.

In Appendix A, we have shown how to exponentiate matrices. Using these results, we now introduce three additional unitary matrices known as *rotation matrices* corresponding to the Pauli matrices. These are shown below.

$$R_x(\theta) \equiv \exp(-i\theta X/2) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{1.9}$$

$$R_y(\theta) \equiv \exp(-i\theta Y/2) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix} \tag{1.10}$$

$$R_z(\theta) \equiv \exp(-i\theta Z/2) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right) Z = \begin{bmatrix} \exp(-i\theta/2) & 0 \\ 0 & \exp(i\theta/2) \end{bmatrix} \tag{1.11}$$

In general, the rotation by θ about an axis defined by the real unit vector $\hat{n} = (n_x, n_y, n_z)$ is applied using the following matrix.

$$R_{\hat{n}}(\theta) \equiv \exp\left(-i\theta\frac{n_x X + n_y Y + n_z Z}{2}\right) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z) \tag{1.12}$$

The rotation matrices R_x, R_y and R_z result in rotations about the x, y, and z axes respectively on the Bloch sphere.

We present a very useful way of representing unitary operator matrices below. Any unitary operator U can be represented by a matrix which is a product of rotations in the y and z axes plus a global phase. Appendix B proves this relation.

$$\begin{aligned}
U &= \exp(i\alpha)\, R_z(\beta) R_y(\gamma) R_z(\delta) && (1.13)\\
&= e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} && (1.14)
\end{aligned}$$

Yet another representation of a unitary operator matrix which follows from above is shown below.

$$U = \exp(i\alpha)\, AXBXC \qquad (1.15)$$

The proof follows from (1.13) by making the following substitutions.

$$\begin{aligned}
A &\equiv R_z(\beta)\, R_y\left(\frac{\gamma}{2}\right) && (1.16)\\
B &\equiv R_y\left(-\frac{\gamma}{2}\right) R_z\left(-\frac{\delta+\beta}{2}\right) && (1.17)\\
C &\equiv R_z\left(\frac{\delta-\beta}{2}\right) && (1.18)
\end{aligned}$$

In the above representation, A, B and C are unitary themselves and $ABC = I$. These representations will be important as we define controlled operations using multiple qubits in the next section. One additional set of identities that we need to keep in mind is the following. The proofs for these are straightforward substitutions and are not shown here.

$$HXH = Z \; ; \; HYH = -Y \; ; \; HZH = X \qquad (1.19)$$

Figure 1.2 summarizes all the single qubit gates and shows their circuit notations.

Hadamard	$-\boxed{H}-$	$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli-X	$-\boxed{X}-$	$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli-Y	$-\boxed{Y}-$	$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli-Z	$-\boxed{Z}-$	$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Phase	$-\boxed{S}-$	$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$
$\pi/8$	$-\boxed{T}-$	$\begin{bmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{bmatrix}$

Figure 1.2: Single-qubit gates and their circuit notations

1.4 Multiple qubits and controlled operations

So far, we have talked about operations on single qubits. We now discuss a class of families on multiple qubits known as *controlled operations*. In particular, we will discuss two-qubit controlled operations. These discussions can intuitively be generalized for larger numbers of qubits.

1.4.1 Multiple qubits

Before discussing the operations, let us introduce the concept of multiple qubits. We introduced single qubits by discussing their classical counterparts. We saw that given the computational basis composed of two states, the general qubit wavefunction in (1.1) is a superposition of these states with the appropriate probability amplitudes. We will introduce multiple qubits in a similar fashion. Consider two classical qubits. They can be combined to form four classical possibilities: 00, 01, 10 and 11. Measurement will reveal one of these four possible states. Given two qubits, the wave function of their combination is given by

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{1.20}$$

such that

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \tag{1.21}$$

Following measurement, the wave function will collapse to one of the four states with its respective probability.

Generally, given n qubits, there are 2^n states in the computational basis with 2^n corresponding probability amplitudes. Therefore, using 500 qubits, we can theoretically encode the state of all atoms in the universe!

1.4.2 Controlled operations

The simplest controlled operation is the controlled version of the classical NOT gate, known as the CNOT gate. It operates on two qubits known as the *control qubit* and the *target qubit*. Its operation is described as follows: if the control qubit is set (to $|1\rangle$), then the target qubit is inverted (from $|0\rangle$ to $|1\rangle$ and vice versa). The shorthand notation for the CNOT gate is given below.

$$\text{CNOT: } |control\rangle|target\rangle \rightarrow |control\rangle|control \oplus target\rangle \tag{1.22}$$

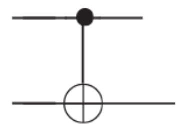

Figure 1.3: Circuit notation for a CNOT gate

The matrix representation for the CNOT operator can be determined as follows from the above shorthand notation.

$$\text{CNOT: } |0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \tag{1.23}$$

$$\text{CNOT: } |0\rangle|1\rangle \rightarrow |0\rangle|1\rangle \tag{1.24}$$

$$\text{CNOT: } |1\rangle|0\rangle \rightarrow |1\rangle|1\rangle \tag{1.25}$$

$$\text{CNOT: } |1\rangle|1\rangle \rightarrow |1\rangle|0\rangle \tag{1.26}$$

In the computational basis $\{|0\rangle, |1\rangle\}$, the CNOT gate acts on two qubits and is therefore 4x4. The columns of the CNOT matrix are the outputs of $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ and $|1\rangle|1\rangle$ respectively. Hence,

$$\text{CNOT} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.27}$$

The circuit notation for the CNOT operator is shown in figure 1.3. In general, a controlled-U operator can be represented by a matrix by noting how it affects combinations of input qubits. The shorthand notation is shown below.

$$\text{controlled-U: } |control\rangle|target\rangle \rightarrow |control\rangle U^{control}|target\rangle \tag{1.28}$$

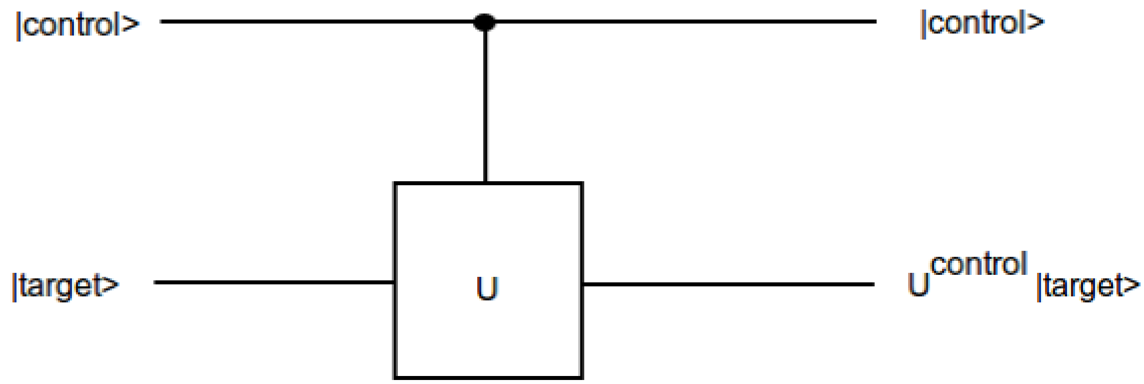

Figure 1.4: A controlled-U operator. Note the control and target qubits

This general notation leads to a general form for the matrix of a controlled-U operator, which is shown below.

$$\text{controlled-U} \equiv \begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix} \tag{1.29}$$

Note that the above matrix is 4x4 because both I and U are 2x2. Also note that the CNOT operator has the same matrix representation as a controlled-X operator. Notationally,

$$\text{CNOT} \equiv \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} \tag{1.30}$$

The commonly used circuit notation for a controlled-U operation is shown in figure 1.4.

Recall from equation 1.15 that we can represent unitary operators by elementary operators. Therefore, for a controlled-U gate, we have the following: when the control is disabled, the identity matrix is applied to the target qubit. Otherwise,

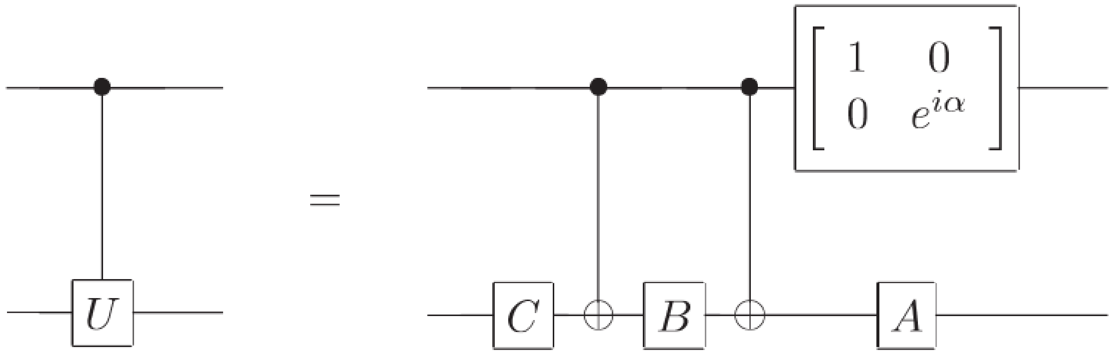

Figure 1.5: A controlled-U gate decomposed into elementary single-qubit gates

$U = \exp(i\alpha)\, AXBXC$ is applied to the target qubit. Also recalling the constraints on A, B and C such that $ABC = I$, this implies that the control qubit affects the X operators, turning them into CNOT gates.

Also note the following.

$$\exp(i\alpha):\ |0\rangle|0\rangle \rightarrow |0\rangle|0\rangle \tag{1.31}$$

$$\exp(i\alpha):\ |0\rangle|1\rangle \rightarrow |0\rangle|1\rangle \tag{1.32}$$

$$\exp(i\alpha):\ |1\rangle|0\rangle \rightarrow |1\rangle\exp(i\alpha)(|0\rangle) = \exp(i\alpha)(|1\rangle)|0\rangle \tag{1.33}$$

$$\exp(i\alpha):\ |1\rangle|1\rangle \rightarrow |1\rangle\exp(i\alpha)(|1\rangle) = \exp(i\alpha)(|1\rangle)|1\rangle \tag{1.34}$$

From the above equations, we observe that the effect of the global phase can be applied to the control or target qubits. Since it only applies when the control qubit is set, we will apply it there, giving the circuit diagram in figure 1.5.

The above discussion easily applies when there are multiple control and target qubits. Given a unitary operator U applied on n control qubits $\{x_1, x_2, \ldots, x_n\}$ and k target qubits $\{y_1, y_2, \ldots, y_k\}$, we have the following shorthand notation.

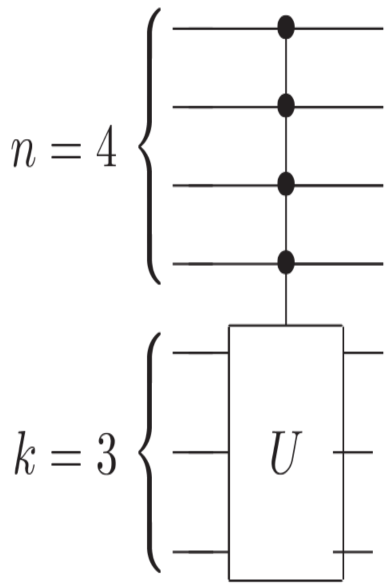

Figure 1.6: A multiple-control multiple-target controlled-U operator with 4 control and 3 target qubits

$$\text{controlled-U: } |x_1\rangle|x_2\rangle \ldots |x_{n-1}\rangle|x_n\rangle|y_1\rangle|y_2\rangle \ldots |y_{k-1}\rangle|y_k\rangle \rightarrow \tag{1.35}$$

$$|x_1\rangle|x_2\rangle \ldots |x_{n-1}\rangle|x_n\rangle U^{x_1 x_2 \ldots x_{n-1} x_n}|y_1\rangle|y_2\rangle \ldots |y_{k-1}\rangle|y_k\rangle \tag{1.36}$$

This shorthand notation is shown in circuit notation in figure 1.6.

1.5 Summary

In this chapter, we have introduced the two-state quantum system used in quantum computation known as the qubit. We have indicated its wavefunction and used the Bloch sphere as a means of visualizing qubits. The Bloch sphere is particularly important when we consider single qubit gates. It helps us visualize the effects of the unitary operators that we normally encounter in matrix form.

We have also discussed the fundamental single-qubit gates – the Pauli gates, their derived rotation operators, the Hadamard, phase and $\pi/8$ gates.

After introducing single-qubit gates, we showed how they can be controlled using additional qubits to form multiple-qubit gates. We showed how to derive the matrices corresponding to these operators and derived general controlled operations in terms of elementary single-qubit gates. The method of control was shown to be applicable even when the number of control and target qubits increases.

For additional reading, including topics such as universal gates and operator approximations, the interested reader is referred to chapter 4 of [6].

Chapter 2

Quantum Mechanical Analysis of the Harmonic Oscillator

2.1 Motivation

This chapter will provide the necessary background for understanding optical implementations of quantum gates. We introduce relevant operators such as annihilators and creators based on a quantum mechanical description of the harmonic oscillator. The material in this chapter is based on analysis of the harmonic oscillator provided in [2] and [3]. Additional material concerned with annihilators and creators can be found in [5].

2.2 Creation and Annihilation Operators

In quantum mechanics, physical observables are represented by Hermitian operators that have real eigenvalues. We represent operators with boldface symbols throughout the chapter. The Hamiltonian of a one-dimensional harmonic oscillator is given below.

$$\boldsymbol{H} = \frac{\boldsymbol{p}^2}{2m} + \frac{1}{2}K\boldsymbol{x}^2 \tag{2.1}$$

In addition, the commutator relationship $[\boldsymbol{x}, \boldsymbol{p}]$ relates the two physical observables in the above equation. The first term in the Hamiltonian is the kinetic energy, and the second is the potential energy. Thus, the Hamiltonian is the total energy of the system. The normalized position and momentum operators are

$$\boldsymbol{X} = \sqrt{\frac{K}{\hbar\omega_0}}\boldsymbol{x} \tag{2.2}$$

$$\boldsymbol{P} = \frac{\boldsymbol{p}}{\sqrt{m\hbar\omega_0}} \tag{2.3}$$

where $\omega_0 = \sqrt{\frac{K}{m}}$. The Hamiltonian expressed in terms of these normalized operators becomes

$$\boldsymbol{H} = \frac{\hbar\omega_0}{2}\left(\boldsymbol{P}^2 + \boldsymbol{X}^2\right) \tag{2.4}$$

with a new commutator relationship $[\boldsymbol{X}, \boldsymbol{P}] = j$. We introduce the non-Hermitian annihilator $\boldsymbol{a}$ and its adjoint $\boldsymbol{a}^\dagger$ as

$$\boldsymbol{a} = \frac{1}{\sqrt{2}}(\boldsymbol{X} + j\boldsymbol{P}) \tag{2.5}$$

$$\boldsymbol{a}^\dagger = \frac{1}{\sqrt{2}}(\boldsymbol{X} - j\boldsymbol{P}) \tag{2.6}$$

with a commutator $[\boldsymbol{a}, \boldsymbol{a}^\dagger] = 1$. We are also interested in the anti-commutator $\{\boldsymbol{a}, \boldsymbol{a}^\dagger\}$ of the annihilator and its adjoint. Note that

$$\boldsymbol{a}\boldsymbol{a}^\dagger = \frac{1}{2}\left(\boldsymbol{X}^2 + \boldsymbol{P}^2 + 1\right) \tag{2.7}$$

$$\boldsymbol{a}^\dagger\boldsymbol{a} = \frac{1}{2}\left(\boldsymbol{X}^2 + \boldsymbol{P}^2 - 1\right) \tag{2.8}$$

Hence, $\{\boldsymbol{a}, \boldsymbol{a}^\dagger\} = \boldsymbol{a}\boldsymbol{a}^\dagger + \boldsymbol{a}^\dagger\boldsymbol{a} = \boldsymbol{P}^2 + \boldsymbol{X}^2$. The Hamiltonian can now be expressed in terms of this anti-commutator.

$$\boldsymbol{H} = \frac{\hbar\omega_0}{2}\left(\boldsymbol{P}^2 + \boldsymbol{X}^2\right) = \frac{\hbar\omega_0}{2}\left(\boldsymbol{a}^\dagger\boldsymbol{a} + \boldsymbol{a}\boldsymbol{a}^\dagger\right) \tag{2.9}$$

$$= \hbar\omega_0\left(\boldsymbol{a}^\dagger\boldsymbol{a} + \frac{1}{2}\right) \tag{2.10}$$

We introduce an additional Hermitian operator known as the number operator $\boldsymbol{N}$ such that

$$\boldsymbol{N} = \boldsymbol{a}^\dagger\boldsymbol{a} \tag{2.11}$$

that counts the number of energy quanta excited in the harmonic oscillator. The eigenvectors $|n\rangle$ of $\boldsymbol{N}$ are known as *Fock* states and the corresponding eigenvalues are denoted as N_n such that

$$\boldsymbol{N}|n\rangle = N_n|n\rangle \tag{2.12}$$

Since $\boldsymbol{N}$ is Hermitian, it has orthonormal eigenvectors and real eigenvalues. In other words, for two eigenvectors $|n\rangle, |m\rangle$ of $\boldsymbol{N}$,

$$\langle m|n\rangle = \delta_{mn} \tag{2.13}$$

The annihilation operator and its adjoint have special effects on the Fock states [3].

$$\boldsymbol{a}|n\rangle = \sqrt{n}|n-1\rangle \tag{2.14}$$

$$\boldsymbol{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle \tag{2.15}$$

We define $\boldsymbol{a}|0\rangle = 0$ for the ground state of the harmonic oscillator. Note that the application of $\boldsymbol{a}$ leads to one less quantum while that of $\boldsymbol{a}^\dagger$ leads to an additional quantum. For this reason, the two operators are usually called the annihilation and creation operators respectively. Starting from the ground state, we can reach a Fock state $|n\rangle$ by repeated application of the creation operator followed by normalization.

$$|n\rangle = \frac{\boldsymbol{a}^\dagger|n-1\rangle}{\sqrt{n}} = \frac{\left(\boldsymbol{a}^\dagger\right)^2|n-2\rangle}{\sqrt{n}\sqrt{n-1}} = \dots \tag{2.16}$$

$$= \frac{1}{\sqrt{(n)!}}\left(\boldsymbol{a}^\dagger\right)^n|0\rangle \tag{2.17}$$

Since the ground state has energy $\frac{\hbar\omega_0}{2}$ with each additional quantum contributing the same energy, the eigenvalues of the Hamiltonian of the harmonic oscillator are related to the Hamiltonian as

$$\boldsymbol{H}|n\rangle = E_n|n\rangle = \hbar\omega_0\left(n+\frac{1}{2}\right) \tag{2.18}$$

where E_n is the energy eigenvalue corresponding to the Fock state $|n\rangle$.

2.3 Matrix Elements of the Creation and Annihilation Operators

In this section, we will investigate the elements of the matrices that represent the annihilation and creation operators. From (2.5), we have

$$\boldsymbol{X} = \frac{1}{\sqrt{2}}\left(a^\dagger + a\right) \tag{2.19}$$

$$\boldsymbol{P} = \frac{j}{\sqrt{2}}\left(a^\dagger - a\right) \tag{2.20}$$

For Fock states $|m\rangle$ and $|n\rangle$, we now derive a series of relations that reveal the matrix elements of the annihilation and creation operators. Note that for an operator O,

$\langle m|O|n\rangle$ is the element O_{mn} of the matrix representation of O.

$$\langle m|\boldsymbol{a}|n\rangle = \sqrt{n}\,\langle m|n-1\rangle = \sqrt{n}\,\delta_{m,n-1} \tag{2.21}$$

$$\langle m|\boldsymbol{a}^\dagger|n\rangle = \sqrt{n+1}\,\langle m|n+1\rangle = \sqrt{n+1}\,\delta_{m,n+1} \tag{2.22}$$

$$\langle m|\boldsymbol{a}^\dagger\boldsymbol{a}|n\rangle = n\langle m|n\rangle = n\delta_{m,n} \tag{2.23}$$

$$\langle m|\boldsymbol{a}\boldsymbol{a}^\dagger|n\rangle = (n+1)\,\langle m|n\rangle = (n+1)\,\delta_{m,n} \tag{2.24}$$

$$\langle m|\boldsymbol{X}|n\rangle = \langle m|\frac{1}{\sqrt{2}}\left(a^\dagger + a\right)|n\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{n+1}\,\delta_{m,n+1} + \sqrt{n}\,\delta_{m,n-1}\right) \tag{2.25}$$

$$\langle m|\boldsymbol{P}|n\rangle = \langle m|\frac{j}{\sqrt{2}}\left(a^\dagger - a\right)|n\rangle = \frac{j}{\sqrt{2}}\left(\sqrt{n+1}\,\delta_{m,n+1} - \sqrt{n}\,\delta_{m,n-1}\right) \tag{2.26}$$

$$\langle m|\boldsymbol{a}^2|n\rangle = \sqrt{n}\,\langle m|\boldsymbol{a}|n-1\rangle = \sqrt{n(n-1)}\,\langle m|n-2\rangle = \sqrt{n(n-1)}\,\delta_{m,n-2} \tag{2.27}$$

$$\langle m|\left(\boldsymbol{a}^\dagger\right)^2|n\rangle = \sqrt{n+1}\,\langle m|\boldsymbol{a}^\dagger|n+1\rangle = \sqrt{(n+1)(n+2)}\,\langle m|n+2\rangle \tag{2.28}$$

$$= \sqrt{(n+1)(n+2)}\,\delta_{m,n+2} \tag{2.29}$$

$$\langle m|\boldsymbol{X}^2|n\rangle = \langle m|\frac{1}{2}\left(\left(\boldsymbol{a}^\dagger\right)^2 + \boldsymbol{a}^\dagger\boldsymbol{a} + \boldsymbol{a}\boldsymbol{a}^\dagger + \boldsymbol{a}^2\right)|n\rangle \tag{2.30}$$

$$= \frac{1}{2}\left(\sqrt{(n+1)(n+2)}\,\delta_{m,n+2} + n\delta_{m,n} + (n+1)\delta_{m,n} + \sqrt{n(n-1)}\,\delta_{m,n-2}\right) \tag{2.31}$$

$$= \frac{1}{2}\left(\sqrt{(n+1)(n+2)}\,\delta_{m,n+2} + (2n+1)\delta_{m,n} + \sqrt{n(n-1)}\,\delta_{m,n-2}\right) \tag{2.32}$$

$$\langle m|\boldsymbol{P}^2|n\rangle = \langle m| - \frac{1}{2}\left(\left(\boldsymbol{a}^\dagger\right)^2 - \boldsymbol{a}^\dagger\boldsymbol{a} - \boldsymbol{a}\boldsymbol{a}^\dagger + \boldsymbol{a}^2\right)|n\rangle \tag{2.33}$$

$$= -\frac{1}{2}\left(\sqrt{(n+1)(n+2)}\,\delta_{m,n+2} - n\delta_{m,n} - (n+1)\delta_{m,n} + \sqrt{n(n-1)}\,\delta_{m,n-2}\right) \tag{2.34}$$

$$= -\frac{1}{2}\left(\sqrt{(n+1)(n+2)}\,\delta_{m,n+2} - (2n+1)\delta_{m,n} + \sqrt{n(n-1)}\,\delta_{m,n-2}\right) \tag{2.35}$$

$$= \frac{1}{2}\left(-\sqrt{(n+1)(n+2)}\,\delta_{m,n+2} + (2n+1)\delta_{m,n} - \sqrt{n(n-1)}\,\delta_{m,n-2}\right) \tag{2.36}$$

$$\tag{2.37}$$

Chapter 3

Optical Implementations

3.1 What makes a good quantum computer?

3.2 Optical devices for quantum computing

3.3 Quantum gates using optical devices

3.3.1 Single qubit gates

3.3.2 Multiple qubit gates

3.4 Drawbacks of the optical scheme

Appendix A

Exponentiating Matrices

In this appendix, we prove the following.

$$\exp(iAx) = cos(x)I + isin(x)A \tag{A.1}$$

for a real number x and matrix A such that $A^2 = I$ and $A^0 = I$. Recall the power series expansion for the exponential $\exp(x)$ for all x.

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \tag{A.2}$$

We now rewrite this power series expansion for $\exp(x)$ after replacing x by iAx.

$$\begin{align}
\exp(iAx) &= \sum_{n=0}^{\infty} \frac{(iAx)^n}{n!} \tag{A.3}\\
&= \frac{I}{0!} + \frac{iAx}{1!} + \frac{(iAx)^2}{2!} + \frac{(iAx)^3}{3!} + \ldots \tag{A.4}\\
&= \frac{A^2}{0!} + \frac{iAx}{1!} + \frac{(iAx)^2}{2!} + \frac{(iAx)^3}{3!} + \ldots \tag{A.5}
\end{align}$$

Noting that even powers of A reduce to identity and $i^2 = -1$, we now rearrange the terms in the above equation as follows.

$$\exp\left(iAx\right) = \frac{A^2}{0!} + \frac{iAx}{1!} + \frac{(iAx)^2}{2!} + \frac{(iAx)^3}{3!} + \dots \tag{A.6}$$

$$= \left(\frac{x^0}{0!} - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots\right) I + i\left(\frac{x^1}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots\right) A \tag{A.7}$$

$$\tag{A.8}$$

The power series expansions for the sine and cosine functions appear in the above equation. We will state the power series expansions for these two functions below.

$$sin(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n+1}}{(2n+1)!} = \left(\frac{x^1}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots\right) \tag{A.9}$$

$$cos(x) = \sum_{n=0}^{\infty} (-1)^n \frac{x^{2n}}{(2n)!} = \left(\frac{x^0}{0!} - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots\right) \tag{A.10}$$

Therefore,

$$\exp\left(iAx\right) = \left(\frac{x^0}{0!} - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots\right) I + i\left(\frac{x^1}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots\right) A \tag{A.11}$$

$$= cos(x)I + isin(x)A \quad \square \tag{A.12}$$

Appendix B

Decomposing Unitary Matrices into Rotations

In this appendix, we prove that any unitary 2x2 matrix U can be decomposed into rotations as defined in (1.13), which we repeat here for convenience.

$$\begin{aligned} U &= \exp(i\alpha)\, R_z(\beta) R_y(\gamma) R_z(\delta) && \text{(B.1)} \\ &= e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix} && \text{(B.2)} \end{aligned}$$

Consider the unitary matrix below. It is formed by carrying out the product above.

$$U = \begin{bmatrix} e^{i\left(\alpha-\frac{\beta}{2}-\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} & -e^{i\left(\alpha-\frac{\beta}{2}+\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} \\ e^{i\left(\alpha+\frac{\beta}{2}-\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} & e^{i\left(\alpha+\frac{\beta}{2}+\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} \end{bmatrix} \tag{B.3}$$

We claim that this is a unitary matrix for real numbers α, β, γ and δ. In order to prove this, we first find the adjoint of U, which is simply the conjugate transpose.

$$U^\dagger = \begin{bmatrix} e^{-i\left(\alpha-\frac{\beta}{2}-\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} & e^{-i\left(\alpha+\frac{\beta}{2}-\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} \\ -e^{-i\left(\alpha-\frac{\beta}{2}+\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} & e^{-i\left(\alpha+\frac{\beta}{2}+\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} \end{bmatrix} \tag{B.4}$$

Now, we compute $UU^\dagger$.

$$UU^\dagger = \begin{bmatrix} e^{i\left(\alpha-\frac{\beta}{2}-\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} & -e^{i\left(\alpha-\frac{\beta}{2}+\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} \\ e^{i\left(\alpha+\frac{\beta}{2}-\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} & e^{i\left(\alpha+\frac{\beta}{2}+\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} \end{bmatrix} \begin{bmatrix} e^{-i\left(\alpha-\frac{\beta}{2}-\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} & e^{-i\left(\alpha+\frac{\beta}{2}-\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} \\ -e^{-i\left(\alpha-\frac{\beta}{2}+\frac{\delta}{2}\right)}\sin\frac{\gamma}{2} & e^{-i\left(\alpha+\frac{\beta}{2}+\frac{\delta}{2}\right)}\cos\frac{\gamma}{2} \end{bmatrix} \tag{B.5}$$

$$= \begin{bmatrix} \cos^2\frac{\gamma}{2}+\sin^2\frac{\gamma}{2} & e^{-i\beta}\cos\frac{\gamma}{2}\sin\frac{\gamma}{2} - e^{-i\beta}\sin\frac{\gamma}{2}\cos\frac{\gamma}{2} \\ e^{i\beta}\sin\frac{\gamma}{2}\cos\frac{\gamma}{2} - e^{i\beta}\cos\frac{\gamma}{2}\sin\frac{\gamma}{2} & \sin^2\frac{\gamma}{2}+\cos^2\frac{\gamma}{2} \end{bmatrix} \tag{B.6}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{B.7}$$

$$= I \tag{B.8}$$

Hence, $UU^\dagger = I$. In other words, $U^\dagger = U^{-1}$. This is exactly the definition of a unitary matrix. Recalling that U was made up of the three smaller matrices with a global phase in (B.1) we have shown that any 2x2 unitary matrix can be written as a product of rotations in the z and y axes plus a global phase shift.

More generally, for two non-parallel real unit vectors $\hat{m}$ and $\hat{n}$, one may write

$$U = e^{i\alpha}R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta) \tag{B.9}$$

for some α, β, γ and δ.

Appendix C

The Baker-Campbell-Hausdorf Formula

The Baker-Campbell-Hausdorf formula for a complex number λ and operators A, G and C_n is given by

$$e^{\lambda G} A e^{-\lambda G} = \sum_{n=0}^{\infty} \frac{\lambda^n}{n!} C_n \tag{C.1}$$

where C_n is defined recursively such that $C_0 = A$ and $C_n = [G, C_{n-1}]$. Several references on Lie Algebras such as [4], [1] and [7] provide interesting proofs of the formula.

Here, we are interested in applying the Baker-Campbell-Hausdorf formula to the unitary matrix which represents the operation of an optical beamsplitter. In particular, for a beamsplitter B of angle θ, the unitary matrix representation is

$$B = \exp\left(\theta(a^\dagger b - ab^\dagger)\right) \tag{C.2}$$

For such a beamsplitter, we will compute $BaB^\dagger$ and $BbB^\dagger$ for annihilation operators a and b and creation operators $a^\dagger$ and $b^\dagger$. Recall from 2.2 that for annihilation operators α and β, $[\alpha, \alpha^\dagger] = [\beta, \beta^\dagger] = 1$ and $[\alpha, \beta] = [\alpha^\dagger, \beta] = [\alpha, \beta^\dagger] = [\alpha^\dagger, \beta^\dagger] = 0$. Setting G

in (C.1) to $a^\dagger b - ab^\dagger$, we have

$$\begin{aligned}
[G,a] &= (a^\dagger b - ab^\dagger)a - a(a^\dagger b - ab^\dagger) \\
&= a^\dagger ba - ab^\dagger a - aa^\dagger b + aab^\dagger \\
&= a^\dagger ba - aa^\dagger b + aab^\dagger - ab^\dagger a \\
&= [a^\dagger b, a] + a\cancelto{0}{[a, b^\dagger]} \\
&= [a^\dagger b, a] \\
&= a^\dagger ba - a^\dagger ab + a^\dagger ab - aa^\dagger b \\
&= a^\dagger \cancelto{0}{[b, a]} - [a, a^\dagger]b \\
&= -b
\end{aligned}$$

Similarly, we can prove that $[G, b] = a$. We summarize these results below.

$$[G,a] = -b \tag{C.3}$$

$$[G,b] = a \tag{C.4}$$

We can now generalize the terms of C_n. Setting $C_0 = a$, $C_1 = [G,a] = -b$, $C_2 = [G, C_1] = -a$, $C_3 = [G, C_2] = b, \ldots$ and generally,

$$C_n = i^n a \text{ for even n}$$

$$C_n = i^{n+1} b \text{ for odd n}$$

Hence,

$$BaB^\dagger = e^{\theta G} a e^{-\theta G} \tag{C.5}$$

$$= \sum_{n=0}^{\infty} \frac{\theta^n}{n!} C_n \tag{C.6}$$

$$= \sum_{n=even} \frac{(i\theta)^n}{n!} a + i \sum_{n=odd}^{\infty} \frac{(i\theta)^n}{n!} b \tag{C.7}$$

$$= a\cos\theta + b\sin\theta \tag{C.8}$$

Similarly, $BbB^\dagger = -a\sin\theta + b\cos\theta$. $\square$

Bibliography

[1] Gustav W. Delius. Introduction to Quantum Lie Algebras. 1996.

[2] Herbert Goldstein, Charles P. Poole, and John Safko. Classical mechanics, 2002.

[3] David Griffiths. *Introduction to Quantum Mechanics*. 2nd edition edition, 2005.

[4] James E. Humphreys. Introduction to lie algebras and representation theory. 1972.

[5] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409, 2001.

[6] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*. Cambridge University Press, 2004.

[7] A. Sagle and R. Walde. Introduction to Lie Groups and Lie Algebras. 1973.