5-24-2022

Chapter 28: Quantum Phase Estimation

Hiu Yung Wong
San Jose State University, hiuyung.wong@sjsu.edu

Recommended Citation
Hiu Yung Wong. "Chapter 28: Quantum Phase Estimation" *Introduction to Quantum Computing: From a Layperson to a Programmer in 30 Steps* (2022): 267-277. https://doi.org/10.1007/978-3-030-98339-0

Chapter 28
Quantum Phase Estimation

28.1 Learning Outcomes

Understand the four parameters in the general controlled unitary gate; able to describe the meaning of the qubits in the Quantum Phase Estimation (QPE) algorithm; able to explain the gates needed to construct a QPE circuit; understand mathematically how QPE works; able to implement and inspect the hardware results of QPE.

28.2 General Controlled Unitary Gate

In the previous chapter, we introduced the single-qubit arbitrary unitary gate, $\boldsymbol{U}_{\theta,\phi,\lambda}$. It describes how a single qubit rotates on the **Bloch sphere**. We have also emphasized that in order to map the qubit to the Bloch sphere, we discarded the **global phase** information. This is fine because, for a single qubit, the global phase has no physical significance. The rotation on a Bloch sphere can be described by the $\boldsymbol{U}_{\theta,\phi,\lambda}$ defined in Eq. (27.9) and is repeated here for convenience.

$$\boldsymbol{U}_{\theta,\phi,\lambda} = \begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\lambda+\phi)}\cos\frac{\theta}{2} \end{pmatrix} \tag{28.1}$$

This gate represents all possible one-qubit gates as long as we do not care about the global phase of the state. This is not a problem for a single qubit. But it is a problem when multiple qubits are considered. When more qubits are involved, while the global phase of the whole system does not matter, the "global phases" of the individual qubits matter. The global phases of the individual qubits determine the relative phase between different qubits and can result in constructive or destructive interferences that are important mechanisms in quantum computing (e.g. we have

H. Y. Wong, *Introduction to Quantum Computing*,
https://doi.org/10.1007/978-3-030-98339-0_28

seen this in QFT). Therefore, Eq. (28.1) is not enough to describe all unitary rotation *when we are not allowed to neglect the global phase of a single qubit*. We can extend the concept, so it will be able to represent any unitary rotation of a qubit by adding a phase factor, γ, as the following:

$$\boldsymbol{U_{\theta,\phi,\lambda,\gamma}} = e^{i\gamma}\begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\lambda}\sin\frac{\theta}{2} \\ e^{i\phi}\sin\frac{\theta}{2} & e^{i(\lambda+\phi)}\cos\frac{\theta}{2} \end{pmatrix} \tag{28.2}$$

The θ, ϕ, and λ still have the same meaning as in $\boldsymbol{U_{\theta,\phi,\lambda}}$. You can see that when we only have $\boldsymbol{U_{\theta,\phi,\lambda}}$, for some matrices, we are missing the $e^{i\gamma}$. This causes an error when it is applied to a vector by omitting $e^{i\gamma}$. But since for a single-qubit case, missing a phase does not matter, we were fine with that.

Example 28.1 Represent the gate $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ in the form of $\boldsymbol{U_{\theta,\phi,\lambda,\gamma}}$.

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = e^{i\pi/2}\begin{pmatrix} \cos\frac{0}{2} & -e^{i\pi}\sin\frac{0}{2} \\ e^{i0}\sin\frac{0}{2} & e^{i(\pi+0)}\cos\frac{0}{2} \end{pmatrix} \tag{28.3}$$

Therefore, $\boldsymbol{U_{0,0,\pi,\pi/2}}$ is the correct representation. When I apply this gate to $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, we get

$$\boldsymbol{U_{0,0,\pi,\pi/2}}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = i\begin{pmatrix} \alpha \\ -\beta \end{pmatrix} \tag{28.4}$$

If we use $\boldsymbol{U_{0,0,\pi}}$ instead, a phase factor of $e^{i\gamma} = e^{i\pi/2} = i$ is missing. When we apply $\boldsymbol{U_{0,0,\pi}}$ to $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, it becomes

$$\boldsymbol{U_{0,0,\pi}}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} \tag{28.5}$$

The rotated state vectors are the same except differ by the phase factor, i.

Now we want to construct a general version of a **controlled unitary gate**. Since two qubits are involved, we cannot ignore the global phase of each qubit anymore. Therefore, the controlled unitary gate must use all four parameters, and its symbol is $\boldsymbol{C - U_{\theta,\phi,\lambda,\gamma}}$. It has this matrix:

$$\boldsymbol{C - U_{\theta,\phi,\lambda,\gamma}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\gamma}\cos\frac{\theta}{2} & -e^{i(\lambda+\gamma)}\sin\frac{\theta}{2} \\ 0 & 0 & e^{i(\phi+\gamma)}\sin\frac{\theta}{2} & e^{i(\lambda+\phi+\gamma)}\cos\frac{\theta}{2} \end{pmatrix} \tag{28.6}$$

Here we assume the MSB is the control qubit and the LSB is the target qubit. We can find this matrix by using the definition. A $\boldsymbol{C-U}$ gate means that if the control qubit in the basis vector is 0, it does nothing to the target qubit, and if the control qubit is 1, it will apply the unitary gate. Therefore, the definition can be written as

$$\begin{aligned}
\boldsymbol{C-U_{\theta,\phi,\lambda,\gamma}}\left|00\right\rangle &= \boldsymbol{I}\left|0\right\rangle \otimes \boldsymbol{I}\left|0\right\rangle = \left|00\right\rangle \\
\boldsymbol{C-U_{\theta,\phi,\lambda,\gamma}}\left|01\right\rangle &= \boldsymbol{I}\left|0\right\rangle \otimes \boldsymbol{I}\left|1\right\rangle = \left|01\right\rangle \\
\boldsymbol{C-U_{\theta,\phi,\lambda,\gamma}}\left|10\right\rangle &= \boldsymbol{I}\left|1\right\rangle \otimes \boldsymbol{U_{\theta,\phi,\lambda,\gamma}}\left|0\right\rangle \\
&= \left|1\right\rangle\left(e^{i\gamma}\cos\frac{\theta}{2}\left|0\right\rangle + e^{i(\phi+\gamma)}\sin\frac{\theta}{2}\left|1\right\rangle\right) \\
&= e^{i\gamma}\cos\frac{\theta}{2}\left|10\right\rangle + e^{i(\phi+\gamma)}\sin\frac{\theta}{2}\left|11\right\rangle \\
\boldsymbol{C-U_{\theta,\phi,\lambda,\gamma}}\left|11\right\rangle &= \boldsymbol{I}\left|1\right\rangle \otimes \boldsymbol{U_{\theta,\phi,\lambda,\gamma}}\left|1\right\rangle \\
&= \left|1\right\rangle\left(-e^{i(\lambda+\gamma)}\sin\frac{\theta}{2}\left|0\right\rangle + e^{i(\lambda+\phi+\gamma)}\cos\frac{\theta}{2}\left|1\right\rangle\right) \\
&= -e^{i(\lambda+\gamma)}\sin\frac{\theta}{2}\left|10\right\rangle + e^{i(\lambda+\phi+\gamma)}\cos\frac{\theta}{2}\left|11\right\rangle
\end{aligned} \tag{28.7}$$

where we use the fact that e.g. $\left|01\right\rangle = \left|0\right\rangle \otimes \left|1\right\rangle$ and then apply the operators to each qubit before performing the tensor products on the right-hand side, and Eq. (28.2) is used in the last two terms with $\left|0\right\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $\left|1\right\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. We can show that Eq. (28.6) is correct based on the definitions on Eq. (28.7) by using Eq. (12.17).

Example 28.2 Find the element ($e_{2,2}$) of the second row and second column (counting from 0-th) of $\boldsymbol{C-U_{\theta,\phi,\lambda,\gamma}}$.

The element corresponds to $\left\langle 10\right|$ (row) and $\left|10\right\rangle$ (column). Using Eq. (28.7),

$$e_{2,2} = \left\langle 10\right|\boldsymbol{C-U_{\theta,\phi,\lambda,\gamma}}\left|10\right\rangle = e^{i\gamma}\cos\frac{\theta}{2} \tag{28.8}$$

where we apply $\left\langle 10\right|$ to line 3 in Eq. (28.7), and we use the orthonormal property of the basis vectors that $\left\langle 10|10\right\rangle = 1$ and $\left\langle 10|11\right\rangle = 0$. This is the same as in Eq. (28.6).

Finally, we may also construct the matrix in Eq. (28.6) using this equation.

$$\boldsymbol{C-U_{\theta,\phi,\lambda,\gamma}} = \left|0\right\rangle\left\langle 0\right| \otimes \boldsymbol{I} + \left|1\right\rangle\left\langle 1\right| \otimes \boldsymbol{U_{\theta,\phi,\lambda,\gamma}} \tag{28.9}$$

It is easy to see the result if we recognize that $\left|0\right\rangle\left\langle 0\right| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$ and $\left|0\right\rangle\left\langle 1\right| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$. We then perform the tensor products accordingly.

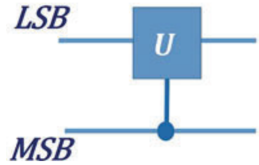

Fig. 28.1 Symbol of a $\boldsymbol{C - U_{\theta,\phi,\lambda,\gamma}}$ gate with the MSB as the control qubit

This equation says that we should perform identity operation to the target qubit if the control qubit is 0 and apply the unitary gate to the target qubit if the control qubit is 1. We will do this in the problems. Figure 28.1 shows the gate symbol.

28.3 Quantum Phase Estimation

The purpose of the **Quantum Phase Estimation (QPE)** algorithm is to estimate the phase, $2\pi\psi$, of the eigenvalue of a unitary $m \times m$ matrix, $\boldsymbol{U}$. Since it is a unitary matrix, its eigenvalue must have a magnitude of one. This is because we can always transform the matrix into a basis formed by its eigenvectors (as the basis states), and its diagonal elements are just its eigenvalues (Eq. (9.13)). And since the columns of the unitary matrix must be normalized (Eq. (9.23)), then the eigenvalues must have a magnitude of one and be in the form of $e^{i2\pi\psi}$. We choose to write its phase as $2\pi\psi$ instead of a single variable is just for convenience in the derivation.

Let us look at a QPE example for a 2×2 matrix before discussing the general algorithm.

28.3.1 QPE for a 2 × 2 Matrix

Assume we are given a phase shift gate with $\phi = \pi$, $\boldsymbol{U_{PS,\pi}}$ (Eq. (16.9)), which is just a Z-gate, $\boldsymbol{Z}$.

$$\begin{aligned} \boldsymbol{U_{PS,\pi}} &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ &= \begin{pmatrix} e^{i2\pi 0} & 0 \\ 0 & e^{i2\pi\frac{1}{2}} \end{pmatrix} \end{aligned} \tag{28.10}$$

We see that it is already in its diagonal form, and therefore, the elements are its eigenvalues, 1 and -1, which have phases of 0 and π, respectively. We also express them in the form of $e^{i2\pi\psi}$. So their ψ's are $\psi_0 = 0$ and $\psi_1 = \frac{1}{2}$, respectively. Each of the eigenvalues corresponds to an eigenvector, and they are $|e_0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ and $|e_1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$, respectively. You may refer to Chap. 9 to review how to find the eigenvectors and eigenvalues of a matrix. We can prove that they are the correct eigenvectors by showing, by definition,

$$\boldsymbol{U_{PS,\pi}}\,|e_0\rangle = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = 1\begin{pmatrix}1\\0\end{pmatrix} = 1\,|e_0\rangle$$
$$\boldsymbol{U_{PS,\pi}}\,|e_1\rangle = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = -1\begin{pmatrix}0\\1\end{pmatrix} = -1\,|e_1\rangle \quad (28.11)$$

The goal of the QPE is to find ψ_0 and ψ_1 for the given $\boldsymbol{U_{PS,\pi}}$.

Figure 28.2 shows the quantum circuit for finding the phase of the Z-gate. *To be exact, it finds ψ instead of $2\pi\psi$.* There are two groups of inputs. The less significant qubits (called the *b-register*) take the eigenvector of the Z-gate. Since the Z-gate is a 2×2 matrix, we only need 1-qubit to represent its eigenvector. In the example, we assume the input is $|e_1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. The other group of inputs (called the *c-register*) contains the more significant qubits. In this example, we use two qubits. These qubits will be used to store a value related to ψ, which is $2^n\psi$, where n is the number of the qubits in the c-register. In this case, it is $2^n\psi = 4\psi$. The inputs to the c-register are the ground state $|0\rangle_2$. This is a $2 + 1 = 3$-qubit circuit. Therefore, it starts with

$$|\xi_0\rangle = |0\rangle\,|0\rangle\,|e_1\rangle \quad (28.12)$$

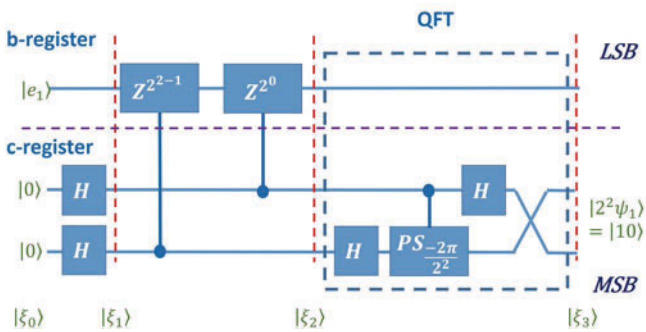

Fig. 28.2 The QPE circuit for finding the phase of the second eigenvalue of the Z-gate ($\boldsymbol{U_{PS,\pi}}$). Note that the bottom is the MSB

The circuit begins with a two-dimensional Hadamard gate ($\boldsymbol{H} \otimes \boldsymbol{H}$) to create a superposition on the c-register. That is

$$
\begin{aligned}
|\xi_1\rangle &= \boldsymbol{H} \otimes \boldsymbol{H} \otimes \boldsymbol{I}(|0\rangle\,|0\rangle\,|e_1\rangle) \\
&= \boldsymbol{H}\,|0\rangle \otimes \boldsymbol{H}\,|0\rangle \otimes \boldsymbol{I}\,|e_1\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|e_1\rangle \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|e_1\rangle \\
&= \frac{1}{2}(|00\rangle\,|e_1\rangle + |01\rangle\,|e_1\rangle + |10\rangle\,|e_1\rangle + |11\rangle\,|e_1\rangle
\end{aligned} \tag{28.13}
$$

After that, controlled gates are used. The type of controlled gate used is *related* to the Z-gate, of which we are finding the eigenvalue phase. If we were to find that of another gate/unitary matrix (e.g. the NOT gate), we need to use the controlled gate related to that new gate (e.g. CNOT gate). I say it is *related* to the Z-gate because, besides controlled-Z-gate, it also uses controlled-Z^k gates, where $k = 2^l$, with l running from 0 to $n - 1$. Again n is the number of qubits in the c-register. A controlled-Z^k gate means that, for a basis state, if the control qubit is 0, it does nothing to the target qubit. If the control qubit is 1, it will apply Z^k gate to the target qubit. The control qubit is one of the qubits in the c-register, and the target qubits are those of the b-register. Each qubit in the c-register acts as the control bit of one of the controlled gates. A Z^k gate is equivalent to applying Z-gate k times. In this case, l runs from 0 to 1 and thus k can be 1 or 2. Therefore, qubit 0 of the c-register is connected to a controlled-Z^k with $l = 0$, and qubit 1 of the c-register is connected to a controlled-Z^k with $l = 1$. In other words, qubit 0 (the less significant bit) of the c-register is the control qubit of a controlled-Z^{2^0} gate, i.e. a controlled-Z-gate. And qubit 1 (the more significant bit) of the c-register is the control qubit of a controlled-Z^{2^1} gate, i.e. a controlled-Z^2 gate.

What happens to the b-register qubit when the controlled-Z^k gates are applied? Note that the b-register has the eigenvector of Z. Therefore, the operation will give the eigenvalue of $\boldsymbol{Z}$ because of Eq. (28.11). That is, $\boldsymbol{U_{PS,\pi}}\,|e_1\rangle = \boldsymbol{Z}\,|e_1\rangle = e^{i2\pi\frac{1}{2}}\,|e_1\rangle = -1\,|e_1\rangle$. And if it is $\boldsymbol{Z}^2$, it becomes $(e^{i2\pi\frac{1}{2}})^2\,|e_1\rangle = |e_1\rangle$ as $\boldsymbol{Z}$ is applied twice. However, this only happens if the corresponding control qubit is 1. Therefore, the n controlled gates produce the following results:

$$
\begin{aligned}
|\xi_2\rangle &= \frac{1}{2}(|00\rangle\,|e_1\rangle + |01\rangle\,\boldsymbol{Z}\,|e_1\rangle + |10\rangle\,\boldsymbol{Z}^2\,|e_1\rangle + |11\rangle\,\boldsymbol{Z}^2\boldsymbol{Z}\,|e_1\rangle \\
&= \frac{1}{2}(|00\rangle\,\boldsymbol{Z}^0\boldsymbol{Z}^0\,|e_1\rangle + |01\rangle\,\boldsymbol{Z}^0\boldsymbol{Z}^1\,|e_1\rangle + |10\rangle\,\boldsymbol{Z}^2\boldsymbol{Z}^0\,|e_1\rangle + |11\rangle\,\boldsymbol{Z}^2\boldsymbol{Z}^1\,|e_1\rangle \\
&= \frac{1}{2}(|00\rangle\,\boldsymbol{Z}^{0+0}\,|e_1\rangle + |01\rangle\,\boldsymbol{Z}^{0+1}\,|e_1\rangle + |10\rangle\,\boldsymbol{Z}^{2+0}\,|e_1\rangle + |11\rangle\,\boldsymbol{Z}^{2+1}\,|e_1\rangle
\end{aligned}
$$

$$= \frac{1}{2}(|0\rangle\, \boldsymbol{Z}^0\, |e_1\rangle + |1\rangle\, \boldsymbol{Z}^1\, |e_1\rangle + |2\rangle\, \boldsymbol{Z}^2\, |e_1\rangle + |3\rangle\, \boldsymbol{Z}^3\, |e_1\rangle$$

$$= \frac{1}{2}\sum_{j=0}^{3} |j\rangle\, \boldsymbol{Z}^j\, |e_1\rangle \tag{28.14}$$

In the first line, $\boldsymbol{Z}$ is applied to the b-register if qubit 0 of the c-register is one, and $\boldsymbol{Z}^2$ is applied to the b-register if qubit 1 of the c-register is one. This is based on the definition of the controlled gates. In the second line, I also added $\boldsymbol{Z}^0$ that is just an identity gate when the control qubits are 0. In the third line, we group the $\boldsymbol{Z}$'s so we can see the sum of their exponents for each basis vector. And in the fourth line, I write the basis vectors in decimal. *Now we clearly see that the action of all controlled gates is equivalent to applying $\boldsymbol{Z}^j$ gate on the b-register if the c-register is $|j\rangle$*. This is a very important feature we use very often in other quantum computing algorithms.

And since $|e_1\rangle$ is an eigenvector of $\boldsymbol{Z}^j$, $\boldsymbol{Z}^j\, |e_1\rangle = (e^{i2\pi\frac{1}{2}})^j\, |e_1\rangle$. Therefore,

$$\begin{aligned} |\xi_2\rangle &= \frac{1}{2}\sum_{j=0}^{3} |j\rangle\, \boldsymbol{Z}^j\, |e_1\rangle \\ &= \frac{1}{2}\sum_{j=0}^{3} |j\rangle\, (e^{i2\pi\frac{1}{2}})^j\, |e_1\rangle \\ &= \frac{1}{2}\sum_{j=0}^{3} (e^{i2\pi\frac{1}{2}})^j\, |j\rangle\, |e_1\rangle \end{aligned} \tag{28.15}$$

I did not simplify $e^{i2\pi\frac{1}{2}}$, which is just -1 because I want to keep it in this form so you can appreciate the constructive and destructive interference in the following QFT step.

The next step is to apply QFT. Note that some other sources may use IQFT, and this is just because it uses a different definition of QFT than ours (see Chap. 26). What really important is that we need to use the matrix for rotating the vector instead of the basis and the matrix is shown in Eq. (25.12). The definition of QFT (Eq. (25.13)) is repeated here for convenience,

$$\boldsymbol{U_{QFT}}\, |j\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} \omega^{-kj}\, |k\rangle \tag{28.16}$$

We only apply it to the c-register and keep the b-register intact. Therefore, we will apply $\boldsymbol{U_{QFT}} \otimes \boldsymbol{I}$ to $|\xi_2\rangle$, and we have

$$
\begin{aligned}
|\xi_3\rangle &= \boldsymbol{U_{QFT}} \otimes \boldsymbol{I} \left(\frac{1}{2} \sum_{j=0}^{3} (e^{i2\pi \frac{1}{2}})^j |j\rangle |e_1\rangle \right) \\
&= \frac{1}{2} \sum_{j=0}^{3} (e^{i2\pi \frac{1}{2}})^j (\boldsymbol{U_{QFT}} |j\rangle) \otimes \boldsymbol{I} |e_1\rangle \\
&= \frac{1}{2} \sum_{j=0}^{3} (e^{i2\pi \frac{1}{2}})^j \left(\frac{1}{\sqrt{4}} \sum_{k=0}^{3} \omega^{-kj} |k\rangle \right) |e_1\rangle \\
&= \frac{1}{4} \sum_{j=0}^{3} \sum_{k=0}^{3} (e^{i2\pi \frac{1}{2}})^j \omega^{-kj} |k\rangle |e_1\rangle \\
&= \frac{1}{4} \sum_{j=0}^{3} \sum_{k=0}^{3} (e^{i \frac{2\pi}{4} 2})^j (e^{i2\pi/4})^{-kj} |k\rangle |e_1\rangle \\
&= \frac{1}{4} \sum_{j=0}^{3} \sum_{k=0}^{3} \omega^{j(2-k)} |k\rangle |e_1\rangle
\end{aligned}
\tag{28.17}
$$

Although the math looks complex, it is actually simple. The first three lines just apply $\boldsymbol{U_{QFT}}$ to the c-register in $|\xi_2\rangle$, use the linear property of quantum mechanics, and then apply Eq. (28.16), the definition of QFT. The last two lines use the definition of the n-th root of unity, ω (Chap. 25). Finally, we group the terms. Note that the b-register is no longer useful now. *It is completely disentangled with the rest of the qubit, and it can be factorized out in the tensor product.*

If we perform a measurement on the c-register, we will get one of the $|k\rangle$'s. However, if we rewrite Eq. (28.17) by shuffling the summations, we have

$$
|\xi_3\rangle = \frac{1}{4} \sum_{k=0}^{3} \left(\sum_{j=0}^{3} \omega^{j(2-k)} \right) |k\rangle |e_1\rangle \tag{28.18}
$$

We see that each $|k\rangle$ has a coefficient of $\sum_{j=0}^{3} \omega^{j(2-k)}$, and this is a summation of the n-th roots of unity. This term is 0 unless $(2-k)=0$ due to the **constructive interference** (Eq. (25.7)). Here j is the m in Eq. (25.7), and $2-k$ is the q in Eq. (25.7). Therefore, if we perform the measurement, we will only measure $|k\rangle$ if $2-k=0$. The basis state we will measure is *always*

$$
|k\rangle = |2\rangle_{10} = |10\rangle_2 \tag{28.19}
$$

Here we write the *ket* in both decimal and binary notations.

What is the meaning of $k = 2$? Let us inspect carefully how we obtain $\omega^{j(2-k)}$ in line 6 of Eq. (28.17). It came from $(e^{i2\pi\frac{1}{2}})^j\omega^{-kj}$ (line 4). The "2" in $\omega^{j(2-k)}$ is obtained by multiplying $\frac{1}{2}$ by 4 (line 5). And 4 is the $N = 2^2$ in the N-th root of unity. Note that $\frac{1}{2}$ is the ψ in the eigenvalue of the eigenvector $|e_1\rangle$, and 4 is $2^n = 2^2$, where n is the number of qubits in the c-register. Therefore, the $k = 2$ we obtained is due to the ψ ($\frac{1}{2}$) being multiplied by 2^n ($2^2 = 4$). From this, we can deduce that in a general QPE, if we measure $|k\rangle$ in a n-qubit c-register, and if the input to the b-register is the eigenvector corresponding to the eigenvalue, $e^{i2\pi\psi}$, the phase is given by

$$2\pi\psi = 2\pi k/2^n \tag{28.20}$$

28.3.2 Implementation on IBM-Q

Figure 28.3 shows the implementation on IBM-Q. $|e_1\rangle$ is created by using a NOT gate. You can see the controlled-Z-gate that is a vertical line with two dots. There is no controlled-Z^2 gate because $\boldsymbol{Z}^2 = \boldsymbol{I}$. The $\boldsymbol{I}$ gate in the circuit is there just to align the circuits. The QFT circuit is the one we used in Fig. 26.5 but only 2 qubits. You can see that the output is 100% $|100\rangle$. The first two qubits are for the c-register. Therefore, $|k\rangle = |10\rangle = |2\rangle$. That means $2\pi\psi = 2\pi k/2^n = 2\pi 2/2^2 = \pi$, which is the phase of the corresponding eigenvalue, -1. Note that we did not measure the b-register (the LSB); therefore, it is 0 by default in the classical register.

28.3.3 General QPE Circuit

Figure 28.4 shows the general QPE circuit. It is just a simple extension of the circuit we have discussed. We note that the b-register can be m-qubit that is required if we are finding the eigenvalue phase in a $m \times m$ matrix case. In that case, the controlled

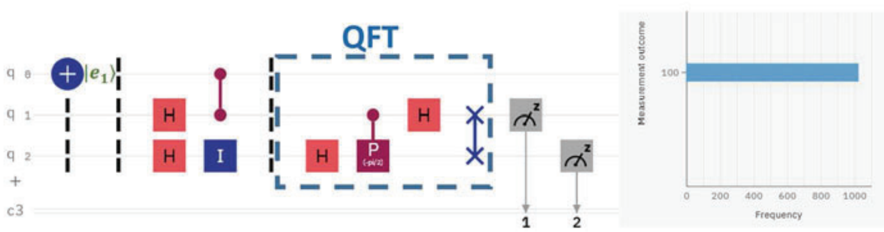

Fig. 28.3 Implementation of the QPE circuit in Fig. 28.2. Note that the bottom is the MSB

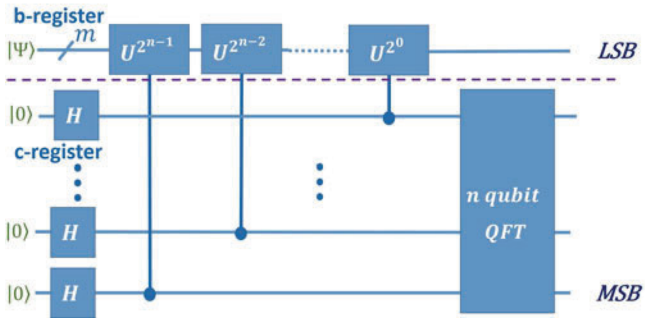

Fig. 28.4 General implementation of the QPE circuit

gate is a $m + 1$-qubit gate (including the control bit). The c-register can be n qubits. n determines the accuracy of the phase it can estimate. Referring to Eq. (28.20), larger n gives a higher resolution. The resolution is $1/2^n$, when $k = 1$. Usually, the ψ is not a fraction nor an integer as in the case we have discussed. Therefore, we cannot get the exact value, and thus it is an "estimation." In summary, the QPE has $m + n$ qubits.

We spent a lot of time discussing the controlled arbitrary unitary gate at the beginning of the chapter. It is not used so far. But it is useful if the matrix you want to study is not a simple gate. You need to use them if you want to implement the QPE for an arbitrary matrix.

The QPE seems not to be useful as we need to know the eigenvector (as input to the b-register) to find its phase. However, every vector is a linear superposition of the eigenvectors. Due to the linearity of quantum mechanics, their phases can be estimated at the same time. If we use it correctly, we can use it to solve other more important problems such as in the HHL algorithm for solving systems of linear equations.

Finally, we can derive the equation for the general QPE like what we did for the 2-qubit case. Please try so by following the steps earlier. I did not do simplification and kept ψ and n or 2^n in the derivation, so it should be relatively straightforward to generalize from 2-qubit to n-qubit. Of course, the phase estimated is given in Eq. (28.20).

28.4 Summary

In this chapter, we discussed how to construct a general controlled unitary gate. We note that it has four parameters in order not to lose the phase information of the rotation. If one wants to implement the QPE for an arbitrary matrix, we need to use it. QPE is used to estimate the phase of the eigenvalue of a matrix. We need to use its eigenvector as the input to the b-register, and the c-register will give a number related to its phase. This is achieved by using constructive and destructive interferences through the QFT.

Problems

28.1 Unitary Gate Construction

Represent the gate $\frac{1}{\sqrt{2}}\begin{pmatrix} -i & -i \\ -i & i \end{pmatrix}$ in the form of $\boldsymbol{U}_{\theta,\phi,\lambda,\gamma}$.

28.2 General Controlled Unitary Gate

Using the method in Example 28.2, show that other non-zero and non-unity elements in Eq. (28.6) are correct.

28.3 General Controlled Unitary Gate Matrix

Use matrix multiplication to prove Eq. (28.9).

28.4 QPE Calculation

In the text, we used $|e_1\rangle$ as the input to the b-register. Now, derive the QPE result for $|e_0\rangle$ of the Z-gate.

28.5 QPE on IBM-Q

Repeat what we did in the text, but use 3 qubits ($n = 3$) for the c-register. Hints: You need to create a $Z^{2^{3-1}}$ gate and its controlled version and simplify it first. The answer should be $|1000\rangle$.

28.6 Derive the General QPE Algorithm

Show that if c-register has n qubits, the answer is that in Eq. (28.20).