Quantum Phase Estimation

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

Table of Contents

Quantum Phase Estimation

The Problem

Unitary operator on n qubits

Eigenvector with eigenvalue $\lambda = e^{i2\pi\phi}$ $(0 \leq \phi < 1)$

Find out ϕ

↓

Eigenvalues of unitaries are always of form above

Quantum Phase Estimation

The Problem

Unitary operator on n qubits

Eigenvector with eigenvalue $\lambda = e^{i2\pi\phi}$ $(0 \leq \phi < 1)$

Find out ϕ

Eigenvalues of unitaries are always of form above

This problem occurs in diverse tasks

- Shor's algorithm
- Determining n^{o} of solutions in unstructured search

A Certain Subroutine

Previous problem uses an important subroutine called

Quantum Fourier Transform (QFT)

Essentially a change-of-basis operation which encodes information of computational basis states in local phases

Table of Contents

QFT: 1 Qubit

$$QFT_1 \, |0\rangle = \frac{1}{\sqrt{2}}\big(\, |0\rangle + 1 \, |1\rangle \, \big) \qquad QFT_1 \, |1\rangle = \frac{1}{\sqrt{2}}\big(\, |0\rangle + (-1) \, |1\rangle \, \big)$$

QFT: 1 Qubit

$$QFT_1 \, |0\rangle = \frac{1}{\sqrt{2}} \big(\, |0\rangle + 1 \, |1\rangle \, \big) \qquad QFT_1 \, |1\rangle = \frac{1}{\sqrt{2}} \big(\, |0\rangle + (-1) \, |1\rangle \, \big)$$

Hence $QFT_1 = H$. Operation H^{-1} allows to extract information encoded in local phases

$= H$

QFT: 1 Qubit

$$QFT_1 |0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + 1 |1\rangle \big) \qquad QFT_1 |1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + (-1) |1\rangle \big)$$

Hence $QFT_1 = H$. Operation H^{-1} allows to extract information encoded in local phases

$= H$

Exercise

Let $\omega_1 = e^{i2\pi\frac{1}{2}}$. Show that $QFT_1 |x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + \omega_1^{1\cdot x} |1\rangle \Big)$

angle of π radians

QFT: 2 Qubits

Let $\omega_2 = e^{i2\pi\frac{1}{4}}$

$$QFT_2\,|00\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{2\cdot 0}\,|1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{1\cdot 0}\,|1\rangle\,\big)$$

$$QFT_2\,|01\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{2\cdot 1}\,|1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{1\cdot 1}\,|1\rangle\,\big)$$

$$QFT_2\,|10\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{2\cdot 2}\,|1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{1\cdot 2}\,|1\rangle\,\big)$$

$$QFT_2\,|11\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{2\cdot 3}\,|1\rangle\,\big) \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle + \omega_2^{1\cdot 3}\,|1\rangle\,\big)$$

QFT: 2 Qubits

Let $\omega_2 = e^{i2\pi\frac{1}{4}}$

$$QFT_2 \, |00\rangle = \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2\cdot 0} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{1\cdot 0} \, |1\rangle \, \big)$$

$$QFT_2 \, |01\rangle = \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2\cdot 1} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{1\cdot 1} \, |1\rangle \, \big)$$

$$QFT_2 \, |10\rangle = \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2\cdot 2} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{1\cdot 2} \, |1\rangle \, \big)$$

$$QFT_2 \, |11\rangle = \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2\cdot 3} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{1\cdot 3} \, |1\rangle \, \big)$$

Exercise

Use Bloch sphere to study $QFT_2 \, |x\rangle$. Specifically note that

- previously, info. of $|x\rangle$ encoded by vectors pointing to the poles; now is encoded by vectors in the *xz*-plane
- for every ω_2-rotation on the second qubit there are *two* such rotations on the first qubit

QFT: 2 Qubits

In order to derive a circuit for QFT_2, we calculate

$$
\begin{aligned}
QFT_2 \, |x\rangle &= \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2\cdot x} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{1\cdot x} \, |1\rangle \, \big) \\
&= \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2(2x_1+x_2)} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2x_1+x_2} \, |1\rangle \, \big) \\
&= \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{4x_1+2x_2} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2x_1+x_2} \, |1\rangle \, \big) \\
&= \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{4x_1}\omega_2^{2x_2} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2x_1}\omega_2^{x_2} \, |1\rangle \, \big) \\
&= \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2x_2} \, |1\rangle \, \big) \otimes \tfrac{1}{\sqrt{2}}\big(\, |0\rangle + \omega_2^{2x_1}\omega_2^{x_2} \, |1\rangle \, \big) \\
&= \underbrace{\tfrac{1}{\sqrt{2}}\big(\, |0\rangle + (-1)^{x_2} \, |1\rangle \, \big)}_{H|x2\rangle} \otimes \underbrace{\tfrac{1}{\sqrt{2}}\big(\, |0\rangle + (-1)^{x_1}\omega_2^{x_2} \, |1\rangle \, \big)}_{\text{some controlled rot. on } H|x1\rangle}
\end{aligned}
$$

QFT: 2 Qubits

Take $R_2 \left|0\right\rangle = \left|0\right\rangle$ and $R_2 \left|1\right\rangle = \omega \left|1\right\rangle$. Intuitively, R_2 rotates a vector in the xz-plane $\frac{\pi}{2}$ radians

QFT: 2 Qubits

Take $R_2 |0\rangle = |0\rangle$ and $R_2 |1\rangle = \omega |1\rangle$. Intuitively, R_2 rotates a vector in the xz-plane $\frac{\pi}{2}$ radians

It yields a controlled-R_2 operation defined by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_2 |x\rangle |1\rangle$. Equivalently

$$|0\rangle |x_2\rangle \mapsto |0\rangle |x_2\rangle \qquad |1\rangle |x_2\rangle \mapsto \omega^{x_2} |1\rangle |x_2\rangle$$

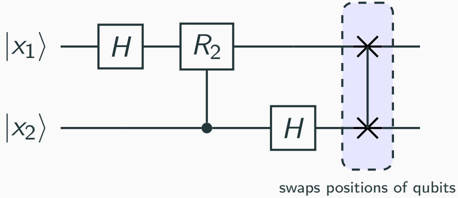
QFT: 2 Qubits

Take $R_2 |0\rangle = |0\rangle$ and $R_2 |1\rangle = \omega |1\rangle$. Intuitively, R_2 rotates a vector in the xz-plane $\frac{\pi}{2}$ radians

It yields a controlled-R_2 operation defined by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_2 |x\rangle |1\rangle$. Equivalently

$$|0\rangle |x_2\rangle \mapsto |0\rangle |x_2\rangle \qquad |1\rangle |x_2\rangle \mapsto \omega^{x_2} |1\rangle |x_2\rangle$$

Putting all pieces together we derive the QFT circuit for 2 qubits



QFT: 3 Qubits

Let $\omega_n = e^{i2\pi \cdot \frac{1}{2^n}}$ (division of the unit circle in 2^n slices)

$$QFT_3 |x\rangle = (|0\rangle + \omega_3^{4 \cdot x} |1\rangle) \otimes (|0\rangle + \omega_3^{2 \cdot x} |1\rangle) \otimes (|0\rangle + \omega_3^{1 \cdot x} |1\rangle)$$

QFT: 3 Qubits

Let $\omega_n = e^{i2\pi \cdot \frac{1}{2^n}}$ (division of the unit circle in 2^n slices)

$$QFT_3 |x\rangle = (\,|0\rangle + \omega_3^{4 \cdot x} |1\rangle\,) \otimes (\,|0\rangle + \omega_3^{2 \cdot x} |1\rangle\,) \otimes (\,|0\rangle + \omega_3^{1 \cdot x} |1\rangle\,)$$

Actually, it is now easy to extrapolate the general defn. of QFT

$$QFT_n |x\rangle = (\,|0\rangle + \omega_n^{2^{n-1} \cdot x} |1\rangle\,) \otimes \cdots \otimes (\,|0\rangle + \omega_n^{2^0 \cdot x} |1\rangle\,)$$

N.B. In both equations above we drop the normalisation factor $\frac{1}{\sqrt{2}}$ in each state to make notation easier on the eyes

QFT: 3 Qubits

In order to derive a circuit for QFT_3, we observe

$$\omega_n^2 = \omega_{n-1} \text{ and thus } \omega_n^{2^{n-1}} = e^{i\pi} = -1$$

and recall that a binary number $x_1 \dots x_n$ represents the natural number $2^{n-1} \cdot x_1 + \cdots + 2^0 \cdot x_n$.

QFT: 3 Qubits

In order to derive a circuit for QFT_3, we observe

$$\omega_n^2 = \omega_{n-1} \text{ and thus } \omega_n^{2^{n-1}} = e^{i\pi} = -1$$

and recall that a binary number $x_1 \dots x_n$ represents the natural number $2^{n-1} \cdot x_1 + \dots + 2^0 \cdot x_n$. We then calculate

$$\begin{aligned}
& QFT_3 \, |x\rangle \\
&= \left(|0\rangle + \omega_3^{4 \cdot x} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{2 \cdot x} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{1 \cdot x} |1\rangle \right) \\
&= \left(|0\rangle + (-1)^{x} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{2 \cdot x} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{1 \cdot x} |1\rangle \right) \\
&= \left(|0\rangle + (-1)^{x_3} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{2 \cdot x} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{1 \cdot x} |1\rangle \right) \\
&= H \, |x_3\rangle \otimes \left(|0\rangle + \omega_3^{2 \cdot (4x_1 + 2x_2 + x_3)} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{1 \cdot x} |1\rangle \right) \\
&= H \, |x_3\rangle \otimes \left(|0\rangle + \omega_3^{2 \cdot (4x_1 + 2x_2)} \omega_3^{2 \cdot x_3} |1\rangle \right) \otimes \left(|0\rangle + \omega_3^{1 \cdot x} |1\rangle \right)
\end{aligned}$$

QFT: 3 Qubits

$\cdots\cdots$

$$= H\,|x_3\rangle \otimes \big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_3^{4x_1+2x_2+x_3}\,|1\rangle\,\big)$$

$$= H\,|x_3\rangle \otimes \big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_3^{4x_1+2x_2}\omega_3^{x_3}\,|1\rangle\,\big)$$

$$= H\,|x_3\rangle \otimes \big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_3^{2\cdot(2x_1+x_2)}\omega_3^{x_3}\,|1\rangle\,\big)$$

$$= H\,|x_3\rangle \otimes \underbrace{\big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_2^{2x_1+x_2}\omega_3^{x_3}\,|1\rangle\,\big)}_{\text{some controlled-rotations on } QFT_2|x_1x_2\rangle}$$

QFT: 3 Qubits

$$
\begin{aligned}
&\cdots\cdots \\
&= H\,|x_3\rangle \otimes \big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_3^{4x_1+2x_2+x_3}\,|1\rangle\,\big) \\
&= H\,|x_3\rangle \otimes \big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_3^{4x_1+2x_2}\omega_3^{x_3}\,|1\rangle\,\big) \\
&= H\,|x_3\rangle \otimes \big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_3^{2\cdot(2x_1+x_2)}\omega_3^{x_3}\,|1\rangle\,\big) \\
&= H\,|x_3\rangle \otimes \underbrace{\big(\,|0\rangle + \omega_2^{2\cdot(2x_1+x_2)}\omega_2^{x_3}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + \omega_2^{2x_1+x_2}\omega_3^{x_3}\,|1\rangle\,\big)}_{\text{some controlled-rotations on } QFT_2|x_1x_2\rangle}
\end{aligned}
$$

Calculation easily extends to QFT_n (*in lieu* of QFT_3) which suggests a recursive defn. for the general QFT circuit

QFT: 3 Qubits

Take $R_n |0\rangle = |0\rangle$ and $R_n |1\rangle = \omega_n |1\rangle$. Intuitively, R_n rotates a vector in the xz-plane 'one 2^n-th of the unit circle'

It yields a controlled-R_n operation defined by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_n |x\rangle |1\rangle$. Equivalently

$$|0\rangle |y\rangle \mapsto |0\rangle |y\rangle \text{ and } |1\rangle |y\rangle \mapsto \omega_n^y |1\rangle |y\rangle$$

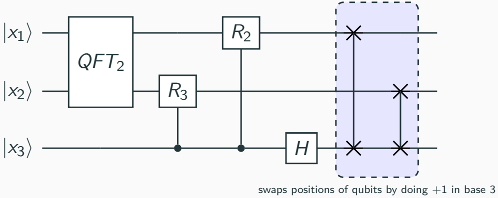
QFT: 3 Qubits

Take $R_n |0\rangle = |0\rangle$ and $R_n |1\rangle = \omega_n |1\rangle$. Intuitively, R_n rotates a vector in the xz-plane 'one 2^n-th of the unit circle'

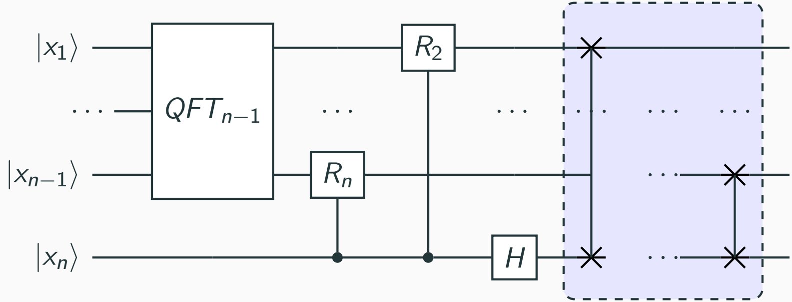
It yields a controlled-R_n operation defined by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_n |x\rangle |1\rangle$. Equivalently

$$|0\rangle |y\rangle \mapsto |0\rangle |y\rangle \text{ and } |1\rangle |y\rangle \mapsto \omega_n^y |1\rangle |y\rangle$$

Putting all pieces together we derive the QFT circuit for 3 qubits



General QFT Circuit



swaps positions of qubits by doing $+1$ in base n

Complexity of QFT

How many gates does the QFT circuit require?

Complexity of QFT

How many gates does the QFT circuit require?

$$\text{nº gates } QFT_n = \text{nº gates } QFT_{n-1} \; + \; \underbrace{1}_{\text{Hadamard}} \; + \; \underbrace{n-1}_{\text{Rotations } R_n} \; + \; \underbrace{n-1}_{\text{nº of swap gates}}$$

Complexity of QFT

How many gates does the QFT circuit require?

nº gates $QFT_n =$ nº gates $QFT_{n-1} \; + \; 1 \; + \; n-1 \; + \; n-1$

Hadamard — Rotations R_n — nº of swap gates

We then calculate,

$$\begin{aligned} \text{nº gates } QFT_n &= \text{nº gates } QFT_{n-1} + n + n - 1 \\ &= \textstyle\sum_{i=1}^{n} i + \sum_{i=0}^{n-1} i \\ &= \frac{(n+1)n}{2} + \frac{n(n-1)}{2} \\ &\approx \frac{n^2}{2} + \frac{n^2}{2} \\ &= n^2 \end{aligned}$$

Thus complexity of QFT is polynomial

An Equivalent Formulation of QFT

Previously we saw that

$$QFT_n \left|x\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \omega_n^{2^{n-1} \cdot x} \left|1\right\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(\left|0\right\rangle + \omega_n^{1 \cdot x} \left|1\right\rangle)$$

An Equivalent Formulation of QFT

Previously we saw that

$$QFT_n \left| x \right\rangle = \tfrac{1}{\sqrt{2}}(\left|0\right\rangle + \omega_n^{2^{n-1} \cdot x} \left|1\right\rangle) \otimes \cdots \otimes \tfrac{1}{\sqrt{2}}(\left|0\right\rangle + \omega_n^{1 \cdot x} \left|1\right\rangle)$$

Equivalent and useful definition given by

$$QFT_n \left| x \right\rangle = \tfrac{1}{\sqrt{2^n}} \textstyle\sum_{k=0}^{2^n-1} \omega_n^{x \cdot k} \left| k \right\rangle$$

An Equivalent Formulation of QFT

Previously we saw that

$$QFT_n |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega_n^{2^{n-1}\cdot x} |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + \omega_n^{1\cdot x} |1\rangle)$$

Equivalent and useful definition given by

$$QFT_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_n^{x\cdot k} |k\rangle$$

Examples with $n = 1$ and $n = 2$

$$QFT_1 |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega_1^{x} |1\rangle)$$

$$QFT_2 |x\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle + \omega_2^{x} |01\rangle + \omega_2^{2\cdot x} |10\rangle + \omega_2^{3\cdot x} |11\rangle)$$

Exercises

Exercise 1

Show that both definitions of QFT coincide when $n = 2$

Exercise 2

Can you show that both definitions coincide for arbitrary n?

Table of Contents

Quantum Phase Estimation

The Problem

Unitary operator on n qubits

Eigenvector with eigenvalue $\lambda = e^{i2\pi\phi}$ $(0 \leq \phi < 1)$

Find out ϕ

Eigenvalues of unitaries are always of form above

A Simple Example

Take a unitary U with an eigenvector $|\psi\rangle$ whose eigenvalue is $e^{i2\pi\phi}$

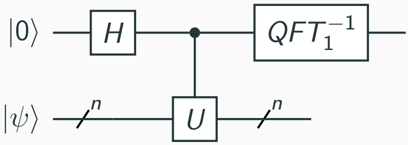
ϕ is equal to one of the values $\{0 \cdot \frac{1}{2}, 1 \cdot \frac{1}{2}\}$. Find out ϕ

A Simple Example

Take a unitary U with an eigenvector $|\psi\rangle$ whose eigenvalue is $e^{i2\pi\phi}$

ϕ is equal to one of the values $\{0 \cdot \frac{1}{2}, 1 \cdot \frac{1}{2}\}$. Find out ϕ

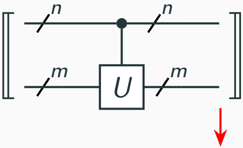
This is obtained via the circuit



Multi-Controlled Operations

Take a unitary U on n qubits

It gives rise to a multi-controlled operation



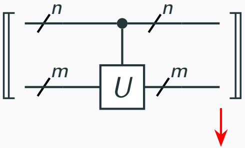
$= |x\rangle\, |y\rangle \mapsto |x\rangle\, U^{x}\, |y\rangle$

decimal representation of x

Intuitively it applies U to $|y\rangle$ a number of times equal to x

Take a unitary U on n qubits

It gives rise to a multi-controlled operation



$$= |x\rangle\, |y\rangle \mapsto |x\rangle\, U^{x}\, |y\rangle$$

decimal representation of x

Intuitively it applies U to $|y\rangle$ a number of times equal to x

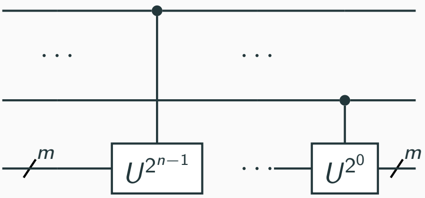
Examples

$|10\rangle\, |y\rangle \mapsto |10\rangle\, (UU\, |y\rangle)$ and $|00\rangle\, |y\rangle \mapsto |00\rangle\, |y\rangle$

Multi-Controlled Operations

Recall that a binary number $x_1 \ldots x_n$ corresponds to the natural number $2^{n-1}x_1 + \cdots + 2^0 x_n$

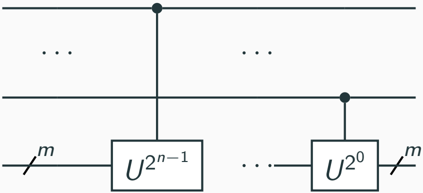
We use this to build the previous multi-controlled operation in terms of simpler operations



Multi-Controlled Operations

Recall that a binary number $x_1 \dots x_n$ corresponds to the natural number $2^{n-1}x_1 + \cdots + 2^0 x_n$

We use this to build the previous multi-controlled operation in terms of simpler operations



Note that the multi-controlled operation uses n 'simply'-controlled rotations U^{2^i}

Another Example

Take a unitary U with an eigenvector $|\psi\rangle$ whose eigenvalue is $e^{i2\pi\cdot\phi}$

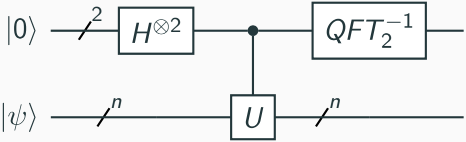
ϕ is equal to one of the following values $\left\{0 \cdot \frac{1}{4}, 1 \cdot \frac{1}{4}, 2 \cdot \frac{1}{4}, 3 \cdot \frac{1}{4}\right\}$

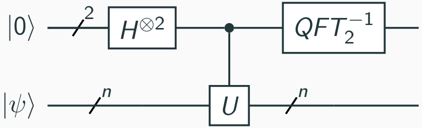
Another Example

Take a unitary U with an eigenvector $|\psi\rangle$ whose eigenvalue is $e^{i2\pi\cdot\phi}$

ϕ is equal to one of the following values $\left\{0 \cdot \frac{1}{4}, 1 \cdot \frac{1}{4}, 2 \cdot \frac{1}{4}, 3 \cdot \frac{1}{4}\right\}$

In order to discover ϕ we use the circuit





$$|0\rangle\,|0\rangle$$
$$\overset{H^{\otimes 2}}{\longmapsto}\ \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$
$$\overset{\text{ctrl. } U}{\longmapsto}\ \frac{1}{\sqrt{2^2}}(|00\rangle + e^{i2\pi\phi}\,|01\rangle + e^{i2\pi\phi\cdot 2}\,|10\rangle + e^{i2\pi\phi\cdot 3}\,|11\rangle)$$
$$= \frac{1}{\sqrt{2^2}}(|00\rangle + e^{i2\pi x\cdot\frac{1}{4}}\,|01\rangle + e^{i2\pi x\cdot\frac{1}{4}\cdot 2}\,|10\rangle + e^{i2\pi x\cdot\frac{1}{4}\cdot 3}\,|11\rangle)$$
$$= \frac{1}{\sqrt{2^2}}(|00\rangle + \omega_2^{x}\,|01\rangle + \omega_2^{x\cdot 2}\,|10\rangle + \omega_2^{x\cdot 3}\,|11\rangle)$$
$$\overset{QFT_2^{-1}}{\longmapsto}\ |x\rangle$$

Yet Another Example

Take a unitary U with eigenvector $|\psi\rangle$ whose eigenvalue is $e^{i2\pi\phi}$

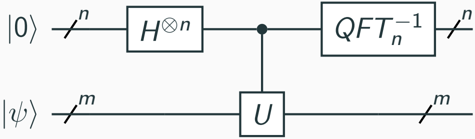
ϕ is equal to one of the following values $\left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$

Yet Another Example

Take a unitary U with eigenvector $|\psi\rangle$ whose eigenvalue is $e^{i2\pi\phi}$

ϕ is equal to one of the following values $\left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$

In order to discover ϕ we use the following circuit



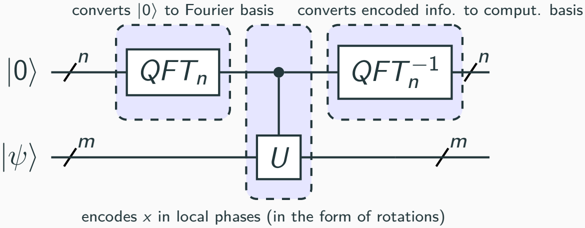
Exercise

Prove that the circuit returns x with $\phi = x \cdot \frac{1}{2^n}$

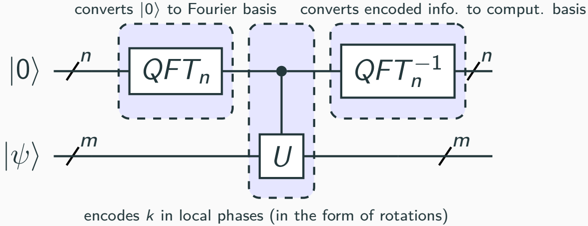
Yet Another Example

Exercise

Show that $QFT_n |0\rangle = H^{\otimes n} |0\rangle$. Note that this allows to rewrite the previous circuit in the one below

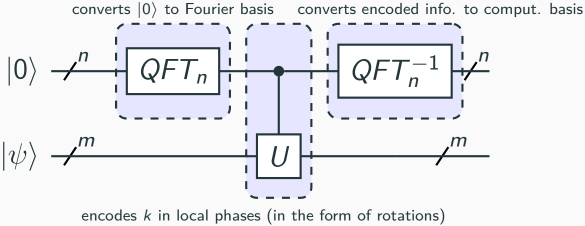


Complexity of Quantum Phase Estimation



How many gates does the circuit above use?

Complexity of Quantum Phase Estimation



How many gates does the circuit above use?

n 'Hadamards' $+$ n 'simply'-controlled gates $+$ n^2 gates for QFT_n^{-1}

Table of Contents

Precision is Limited

We assumed $0 \leq \phi < 1$ takes a value from $\left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$

Assumption arose from having only *n* qubits to estimate

What to do if ϕ takes none of these values?

Precision is Limited

We assumed $0 \leq \phi < 1$ takes a value from $\left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$

Assumption arose from having only n qubits to estimate

What to do if ϕ takes none of these values?

Return the n-bit number k with $k \cdot \frac{1}{2^n}$ the value above closest to ϕ

Precision is Limited

We assumed $0 \leq \phi < 1$ takes a value from $\left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$

Assumption arose from having only n qubits to estimate

What to do if ϕ takes none of these values?

Return the n-bit number k with $k \cdot \frac{1}{2^n}$ the value above closest to ϕ

Is the QPE circuit up to this task?

Setting the Stage

Let $\omega_n = e^{i2\pi \cdot \frac{1}{2^n}}$ $\underbrace{\text{(division of the unit circle in } 2^n \text{ slices)}}_{\text{a.k.a. the n roots of unity}}$

To answer the previous question, we will use the following explicit defn. of QFT^{-1}

$$QFT_n^{-1} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_n^{-x \cdot k} |k\rangle$$

Setting the Stage

Let $\omega_n = e^{i2\pi \cdot \frac{1}{2^n}}$ $\underbrace{\text{(division of the unit circle in } 2^n \text{ slices)}}_{\text{a.k.a. the n roots of unity}}$

To answer the previous question, we will use the following explicit defn. of QFT^{-1}

$$QFT_n^{-1} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_n^{-x \cdot k} |k\rangle$$

Exercise

Prove that QFT_n^{-1} is indeed the inverse of QFT_n

Setting the Stage pt. II

Let $k \cdot \frac{1}{2^n}$ be the value in $\left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$ closest to ϕ

$\exists \epsilon$ s.t. $0 \leq |\epsilon| \leq \frac{1}{2^n}$ and $k \cdot \frac{1}{2^n} + \epsilon = \phi$

The difference ϵ decreases when the number of qubits increases

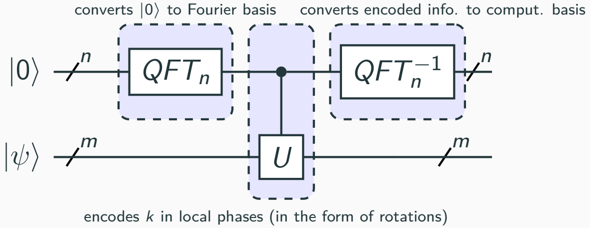
Setting the Stage pt. II

Let $k \cdot \frac{1}{2^n}$ be the value in $\left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$ closest to ϕ

$\exists \epsilon$ s.t. $0 \leq |\epsilon| \leq \frac{1}{2^n}$ and $k \cdot \frac{1}{2^n} + \epsilon = \phi$

The difference ϵ decreases when the number of qubits increases

Recall the QPE circuit



Computing again the Output

$$|0\rangle$$

$$\overset{H^{\otimes n}}{\longmapsto} \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle)$$

$$\overset{\text{ctrl.}\ U}{\longmapsto} \frac{1}{\sqrt{2^n}}\Big(|0\rangle + e^{i2\pi\phi\cdot 1}\,|1\rangle + \cdots + e^{i2\pi\phi\cdot 2^{n-1}}\,|2^n - 1\rangle \Big)$$

$$= \frac{1}{\sqrt{2^n}}\Big(|0\rangle + e^{i2\pi(k\cdot\frac{1}{2^n}+\epsilon)\cdot 1}\,|1\rangle + \cdots + e^{i2\pi(k\cdot\frac{1}{2^n}+\epsilon)\cdot 2^{n-1}}\,|2^n - 1\rangle \Big)$$

$$= \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} e^{i2\pi(k\cdot\frac{1}{2^n}+\epsilon)\cdot j}\,|j\rangle$$

$$= \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} e^{i2\pi k\cdot\frac{1}{2^n}\cdot j} e^{i2\pi\epsilon\cdot j}\,|j\rangle$$

$$\overset{QFT^{-1}}{\longmapsto} \frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1} e^{i2\pi k\cdot\frac{1}{2^n}\cdot j} e^{i2\pi\epsilon\cdot j}\Big(\frac{1}{\sqrt{2^n}}\sum_{l=0}^{2^n-1} e^{-i2\pi j\cdot\frac{1}{2^n}\cdot l}\,|l\rangle\Big)$$

$$= \frac{1}{2^n}\sum_{j=0}^{2^n-1} e^{i2\pi k\cdot\frac{1}{2^n}\cdot j} e^{i2\pi\epsilon\cdot j}\Big(\sum_{l=0}^{2^n-1} e^{-i2\pi j\cdot\frac{1}{2^n}\cdot l}\,|l\rangle\Big)$$

$$= \frac{1}{2^n}\sum_{j=0}^{2^n-1}\sum_{l=0}^{2^n-1} e^{i2\pi\epsilon\cdot j} e^{i2\pi j\cdot\frac{1}{2^n}\cdot(k-l)}\,|l\rangle$$

An Analysis of the Final State

The amplitude of $|k\rangle$ is $\frac{1}{2^n}\sum_{j=0}^{2^n-1} e^{i2\pi\epsilon\cdot j}$

It is a finite geometric series and therefore

$$\frac{1}{2^n}\sum_{j=0}^{2^n-1} e^{i2\pi\epsilon j} = \begin{cases} 1 & \text{if } \epsilon = 0 \\ \frac{1}{2^n}\frac{1-e^{i2\pi\epsilon 2^n}}{1-e^{i2\pi\epsilon}} & \text{if } \epsilon \neq 0 \end{cases}$$

An Analysis of the Final State

The amplitude of $|k\rangle$ is $\frac{1}{2^n}\sum_{j=0}^{2^n-1} e^{i2\pi\epsilon\cdot j}$

It is a finite geometric series and therefore

$$\frac{1}{2^n}\sum_{j=0}^{2^n-1} e^{i2\pi\epsilon j} = \begin{cases} 1 & \text{if } \epsilon = 0 \\ \frac{1}{2^n}\frac{1-e^{i2\pi\epsilon 2^n}}{1-e^{i2\pi\epsilon}} & \text{if } \epsilon \neq 0 \end{cases}$$

We proceed with the assumption $\epsilon \neq 0$

A Detour Through Geometry

$|1 - e^{i\theta}|$ for some angle θ is the Euclidean distance between 1 and $e^{i\theta}$ (length of the straight line segment between both points)

Consider also arc length θ between 1 and $e^{i\theta}$ (distance between the two points by running along the unit circle)

A Detour Through Geometry

$|1 - e^{i\theta}|$ for some angle θ is the Euclidean distance between 1 and $e^{i\theta}$ (length of the straight line segment between both points)

Consider also arc length θ between 1 and $e^{i\theta}$ (distance between the two points by running along the unit circle)

Theorem

Let d^E and d^a be respectively the Euclidean distance and arc length between 1 and $e^{i\theta}$. Then (a) $d^E \leq d^a$ and (b) if $0 \leq \theta \leq \pi$ we have $\frac{d^a}{d^E} \leq \frac{\pi}{2}$

Finally!

Recall $\left|\frac{1}{2^n}\frac{1-e^{i2\pi\epsilon 2^n}}{1-e^{i2\pi\epsilon}}\right|^2$ is the probability of measuring $|k\rangle$

$$
\begin{aligned}
\left|\frac{1}{2^n}\frac{1-e^{i2\pi\epsilon 2^n}}{1-e^{i2\pi\epsilon}}\right|^2 &= \left(\frac{1}{2^n}\right)^2 \frac{\left|1-e^{i2\pi\epsilon 2^n}\right|^2}{\left|1-e^{i2\pi\epsilon}\right|^2} \\
&\geq \left(\frac{1}{2^n}\right)^2 \frac{\left|1-e^{i2\pi\epsilon 2^n}\right|^2}{(2\pi\epsilon)^2} && \{\text{Prev. Thm. (a)}\} \\
&\geq \left(\frac{1}{2^n}\right)^2 \frac{\left(\frac{2}{\pi}\cdot 2\pi\epsilon 2^n\right)^2}{(2\pi\epsilon)^2} && \{\text{Prev. Thm. (b)}\} \\
&= \left(\frac{1}{2^n}\right)^2 \frac{(4\epsilon 2^n)^2}{(2\pi\epsilon)^2} \\
&= \left(\frac{1}{2^n}\right)^2 \frac{(2\cdot 2^n)^2}{\pi^2} = \frac{2^2}{\pi^2} = \frac{4}{\pi^2}
\end{aligned}
$$

Table of Contents

From an Eigenvector to a Superposition of Eigenvectors

Recall: QPE requires an eigenvector as input

Sometimes highly difficult to build such a vector

Paradoxically (but not really :-)) often easier to feed instead a superposition of eigenvectors

From an Eigenvector to a Superposition of Eigenvectors

Recall: QPE requires an eigenvector as input

Sometimes highly difficult to build such a vector

Paradoxically (but not really :-)) often easier to feed instead a superposition of eigenvectors ↓

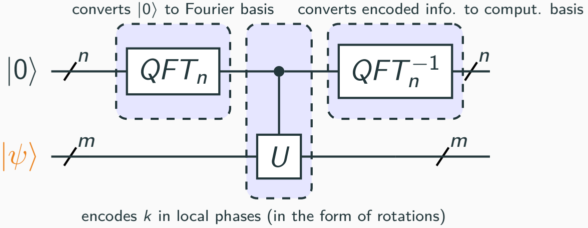
Recall the Spectral Theorem

How does QPE behave in this setting?

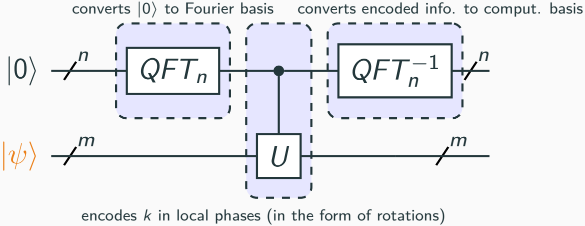
QPE + Superposition of eigenvectors

Take a unitary U with eigenvectors $|\psi_1\rangle, \ldots, |\psi_N\rangle$ and associated eigenstates $e^{i2\pi\phi_1}, \ldots, e^{i2\pi\phi_N}$

Define $|\psi\rangle = \frac{1}{\sqrt{N}}(|\psi_1\rangle + \cdots + |\psi_N\rangle)$ and consider the circuit



QPE + Superposition of eigenvectors

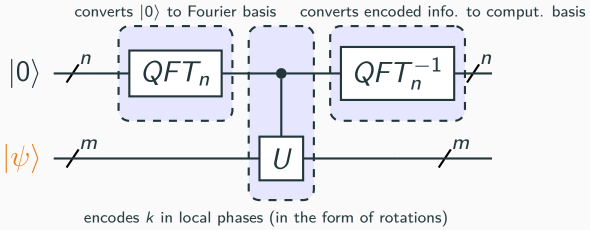


Exercise 1

Show that if $\forall i \leq N.\phi_i \in \left\{0 \cdot \frac{1}{2^n}, \ldots, 2^n - 1 \cdot \frac{1}{2^n}\right\}$ then the circuit's output is

$$\frac{1}{\sqrt{N}}\Big(|k_1\rangle\,|\psi_1\rangle + \cdots + |k_N\rangle\,|\psi_N\rangle \Big) \qquad \left(\phi_i = k_i \cdot \frac{1}{2^n}\right)$$

QPE + Superposition of eigenvectors



Exercise 2

Show that in general the circuit's output is

$$\frac{1}{\sqrt{N}}\left(\left|\tilde{\phi_1}\right\rangle |\psi_1\rangle + \cdots + \left|\tilde{\phi_N}\right\rangle |\psi_N\rangle \right)$$

where each $\tilde{\phi}_i$ is the best n-bit approximation of ϕ_i with probability $\geq \frac{4}{\pi^2}$