An Introduction to Quantum Computing

Lecture 09:

The Quantum Fourier Transform and Phase Estimation - Towards Shor's Algorithm (I)

Paolo Zuliani

Dipartimento di Informatica
Università di Roma "La Sapienza", Rome, Italy

Agenda

- Discrete Fourier Transform
- Quantum Fourier Transform
- Quantum Algorithm for Phase Estimation

The Discrete Fourier Transform

It maps N complex numbers $x_0, \ldots, y_{N-1}$ to N complex numbers $y_0, \ldots, y_{N-1}$:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$$

where i is the imaginary unit.

- The Fourier Transform is much used for signal processing (*e.g.*, speech recognition, audio compression)
- It is sometimes easier to study a signal in a different domain (*e.g.*, frequency instead of time)
- The Discrete Fourier Transform[1] "filters" the input sequence through a sinusoidal wave of frequency k/N.

[1] For a deeper and clear treatment of the DFT see Chapter 7 of "The Design and Analysis of Computer Algorithms" by Aho, Hopcroft, and Ullman.

The Quantum Fourier Transform

Definition

The QFT maps each basis state $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ as follows

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

Equivalently, for a generic vector:

$$\sum_{j=0}^{N-1} x_j |j\rangle \to \sum_{k=0}^{N-1} y_k |k\rangle$$

where $y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$.

The Quantum Fourier Transform

The QFT maps each basis state $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ as follows

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

so it can be written as

$$QFT = \sum_{j=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \right) \langle j|$$

The Quantum Fourier Transform

The QFT maps each basis state $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ as follows

$$|j\rangle \xrightarrow{QFT} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle$$

so it can be written as

$$QFT = \sum_{j=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \right) \langle j|$$

Proposition

The QFT is a unitary operator, i.e., $QFT\ QFT^{\dagger} = QFT^{\dagger}\ QFT = I$.

$$QFT^{\dagger} = \sum_{j=0}^{N-1} |j\rangle \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{-2\pi ijk/N} \langle k| \right)$$

The Quantum Fourier Transform: Unitarity

Let us show that the QFT is unitary:

$$QFT^\dagger \; QFT = \sum_{j=0}^{N-1} |j\rangle \left(\frac{1}{\sqrt{N}} \sum_{r=0}^{N-1} e^{-2\pi ijr/N} \langle r| \right) \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} e^{2\pi isk/N} |s\rangle \right) \langle k|$$

The Quantum Fourier Transform: Unitarity

Let us show that the QFT is unitary:

$$
\begin{aligned}
QFT^{\dagger}\ QFT &= \sum_{j=0}^{N-1} |j\rangle \left(\frac{1}{\sqrt{N}} \sum_{r=0}^{N-1} e^{-2\pi i j r/N} \langle r| \right) \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} e^{2\pi i s k/N} |s\rangle \right) \langle k| \\
&= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{-2\pi i j r/N} \langle r| \right) \left(\sum_{s=0}^{N-1} e^{2\pi i s k/N} |s\rangle \right) \langle k|
\end{aligned}
$$

The Quantum Fourier Transform: Unitarity

Let us show that the QFT is unitary:

$$
\begin{aligned}
QFT^{\dagger}\ QFT &= \sum_{j=0}^{N-1} |j\rangle \left(\frac{1}{\sqrt{N}} \sum_{r=0}^{N-1} e^{-2\pi i jr/N} \langle r| \right) \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} e^{2\pi i sk/N} |s\rangle \right) \langle k| \\
&= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{-2\pi i jr/N} \langle r| \right) \left(\sum_{s=0}^{N-1} e^{2\pi i sk/N} |s\rangle \right) \langle k| \\
&= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r,s=0}^{N-1} e^{2\pi i(-jr+ks)/N} \langle r|s\rangle \right) \langle k|
\end{aligned}
$$

The Quantum Fourier Transform: Unitarity

Let us show that the QFT is unitary:

$$
\begin{aligned}
QFT^\dagger \; QFT &= \sum_{j=0}^{N-1} |j\rangle \left(\frac{1}{\sqrt{N}} \sum_{r=0}^{N-1} e^{-2\pi i jr/N} \langle r| \right) \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{s=0}^{N-1} e^{2\pi i sk/N} |s\rangle \right) \langle k| \\
&= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{-2\pi i jr/N} \langle r| \right) \left(\sum_{s=0}^{N-1} e^{2\pi i sk/N} |s\rangle \right) \langle k| \\
&= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r,s=0}^{N-1} e^{2\pi i(-jr+ks)/N} \langle r|s\rangle \right) \langle k| \\
&= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k| \qquad [\text{recall } \langle r|s\rangle = \delta_{rs}]
\end{aligned}
$$

The Quantum Fourier Transform: Unitarity

$$= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k|$$

The Quantum Fourier Transform: Unitarity

$$= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k|$$

$$= \frac{1}{N} \sum_{j=k;j=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} 1 \right) \langle k| + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k|$$

The Quantum Fourier Transform: Unitarity

$$= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k|$$

$$= \frac{1}{N} \sum_{j=k;j=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} 1 \right) \langle k| + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k|$$

$$= \sum_{j=0}^{N-1} |j\rangle\langle j| + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i(k-j)/N})^r \right) \langle k|$$

The Quantum Fourier Transform: Unitarity

$$
\begin{aligned}
&= \frac{1}{N} \sum_{j,k=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k| \\
&= \frac{1}{N} \sum_{j=k;j=0}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} 1 \right) \langle k| + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} e^{2\pi i r(k-j)/N} \right) \langle k| \\
&= \sum_{j=0}^{N-1} |j\rangle\langle j| + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i(k-j)/N})^r \right) \langle k| \\
&= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i(k-j)/N})^r \right) \langle k|
\end{aligned}
$$

The Quantum Fourier Transform: Unitarity

$$= I + \frac{1}{N} \sum_{j,k=0; j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i (k-j)/N})^r \right) \langle k|$$

The Quantum Fourier Transform: Unitarity

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i(k-j)/N})^r \right) \langle k|$$

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\frac{1 - (e^{2\pi i(k-j)/N})^N}{1 - e^{2\pi i(k-j)/N}} \right) \langle k| \qquad \text{[recall } \sum_{i=0}^{N-1} \rho^i = \frac{1-\rho^N}{1-\rho} \text{ for } \rho \neq 1\text{]}$$

The Quantum Fourier Transform: Unitarity

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i(k-j)/N})^r \right) \langle k|$$

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\frac{1 - (e^{2\pi i(k-j)/N})^N}{1 - e^{2\pi i(k-j)/N}} \right) \langle k| \qquad \text{[recall } \sum_{i=0}^{N-1} \rho^i = \frac{1-\rho^N}{1-\rho} \text{ for } \rho \neq 1\text{]}$$

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \frac{1 - e^{2\pi i(k-j)}}{1 - e^{2\pi i(k-j)/N}} \langle k|$$

The Quantum Fourier Transform: Unitarity

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i(k-j)/N})^r \right) \langle k|$$

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\frac{1-(e^{2\pi i(k-j)/N})^N}{1-e^{2\pi i(k-j)/N}} \right) \langle k| \qquad \left[\text{recall } \sum_{i=0}^{N-1} \rho^i = \frac{1-\rho^N}{1-\rho} \text{ for } \rho \neq 1\right]$$

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \frac{1-e^{2\pi i(k-j)}}{1-e^{2\pi i(k-j)/N}} \langle k| \qquad [\forall j \neq k \in \{0,\ldots,N-1\}, e^{2\pi i(k-j)} = 1]$$

$$= I$$

The Quantum Fourier Transform: Unitarity

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\sum_{r=0}^{N-1} (e^{2\pi i(k-j)/N})^r \right) \langle k|$$

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \left(\frac{1 - (e^{2\pi i(k-j)/N})^N}{1 - e^{2\pi i(k-j)/N}} \right) \langle k| \qquad \left[\text{recall } \sum_{i=0}^{N-1} \rho^i = \frac{1-\rho^N}{1-\rho} \text{ for } \rho \neq 1\right]$$

$$= I + \frac{1}{N} \sum_{j,k=0;j\neq k}^{N-1} |j\rangle \frac{1 - e^{2\pi i(k-j)}}{1 - e^{2\pi i(k-j)/N}} \langle k| \qquad [\forall j \neq k \in \{0, \ldots, N-1\}, e^{2\pi i(k-j)} = 1]$$

$$= I$$

Exercise: prove $QFT\ QFT^{\dagger} = I$.

The Quantum Fourier Transform: Quantum Circuit

An **equivalent** QFT definition (assuming $N = 2^n$, hence n qubits):

$$|j_1 \dots j_n\rangle \xrightarrow{QFT} \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle)}{2^{n/2}}$$

where $j_1, \dots, j_n$ are bits, and the **binary fraction**

$$0.j_l j_{l+1} j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \cdots + \frac{j_m}{2^{m-l+1}}$$

The Quantum Fourier Transform: Quantum Circuit

An **equivalent** QFT definition (assuming $N = 2^n$, hence n qubits):

$$|j_1 \ldots j_n\rangle \xrightarrow{QFT} \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle)}{2^{n/2}}$$

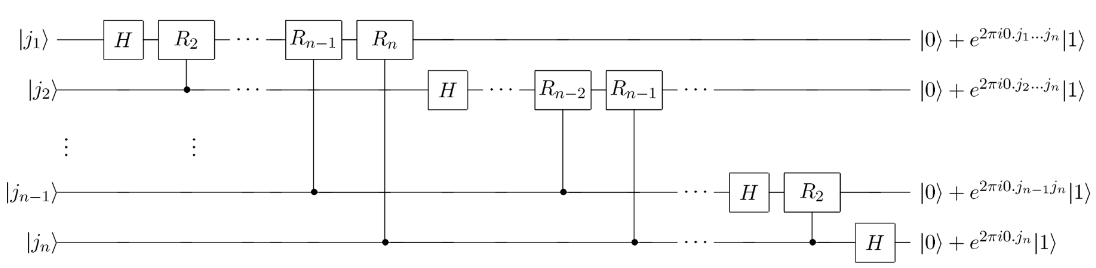
where $j_1, \ldots, j_n$ are bits, and the **binary fraction**

$$0.j_l j_{l+1} j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \cdots + \frac{j_m}{2^{m-l+1}}$$

Example:

$$0.1101 = \frac{1}{2} + \frac{1}{4} + \frac{1}{2^4}$$

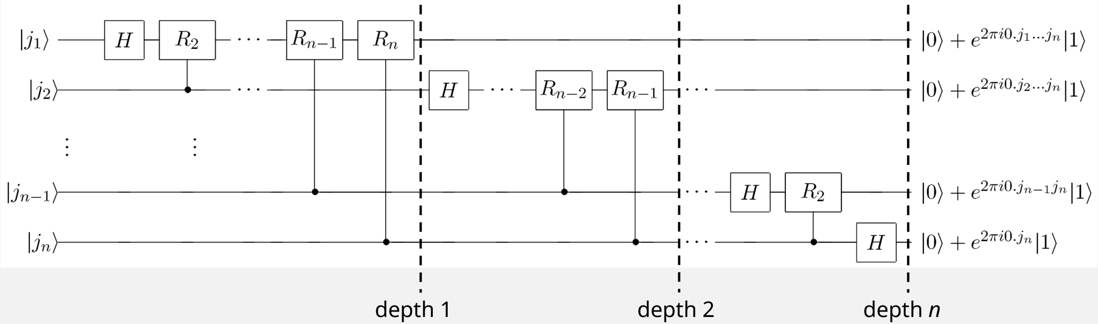
The Quantum Fourier Transform: Quantum Circuit



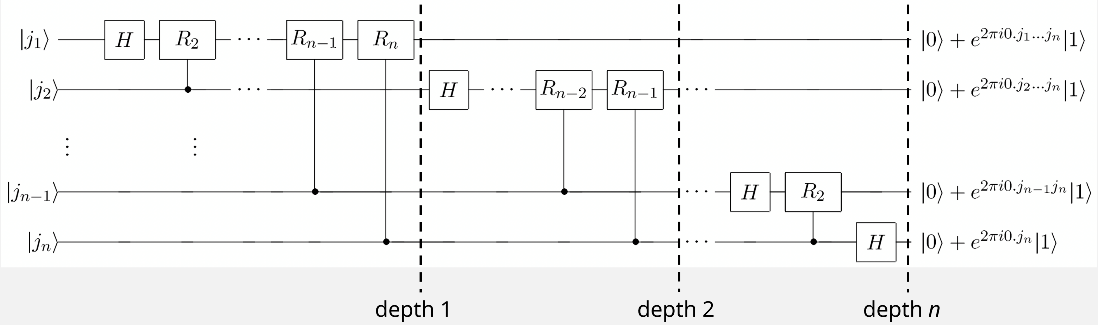
where H is the usual Hadamard and the controlled-R_k gates are defined on

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

The Quantum Fourier Transform: Quantum Circuit

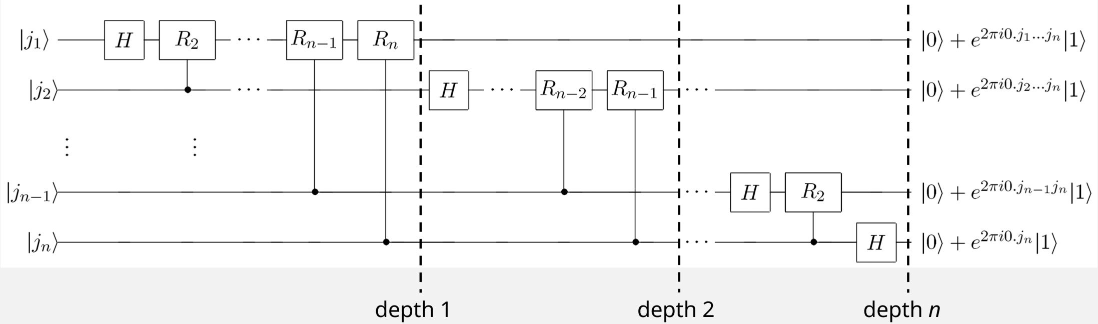


The Quantum Fourier Transform: Quantum Circuit



State at depth 1: $\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle)|j_2 \dots j_n\rangle$

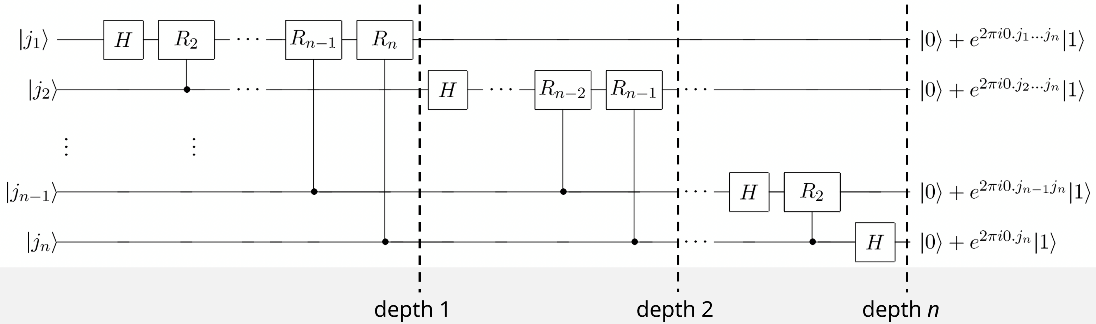
The Quantum Fourier Transform: Quantum Circuit



State at depth 1: $\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle)|j_2 \ldots j_n\rangle$

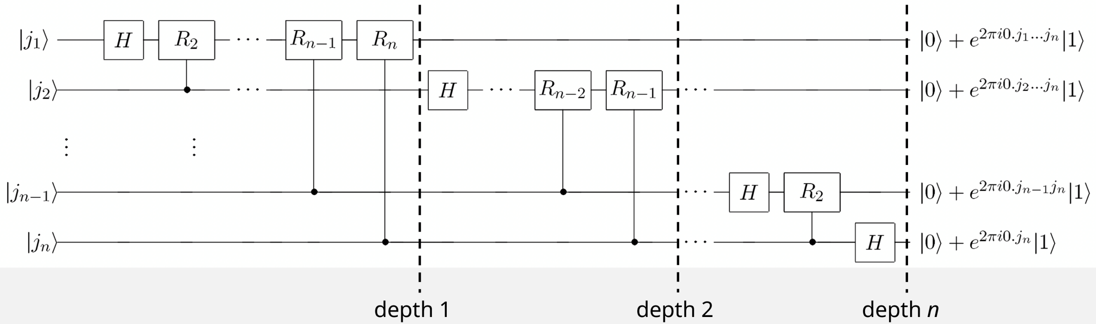
State at depth 2: $\frac{1}{2^{2/2}}(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.j_2 \cdots j_n}|1\rangle)|j_3 \ldots j_n\rangle$

The Quantum Fourier Transform: Quantum Circuit



The state at depth n has the correct terms, but in the wrong order! (Remember the tensor product is NOT commutative.)

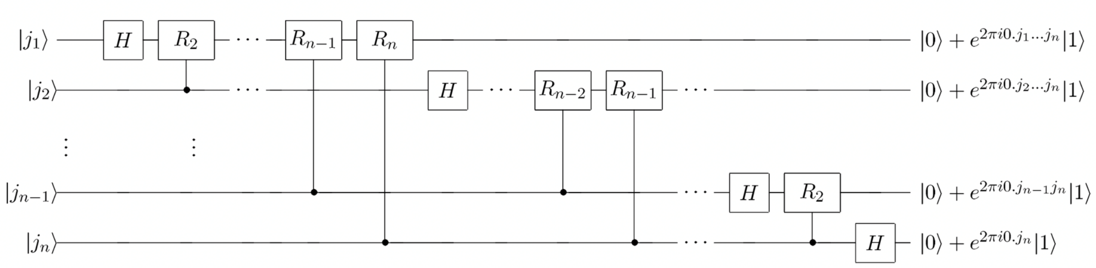
The Quantum Fourier Transform: Quantum Circuit



The state at depth n has the correct terms, but in the wrong order! (Remember the tensor product is NOT commutative.)

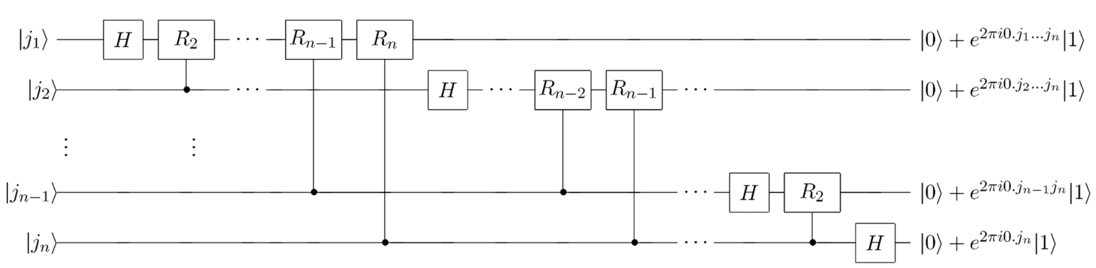
We need to **swap** the qubits, which can be done unitarily, of course.

The Quantum Fourier Transform: Complexity



- Quantum circuit has $O(n^2)$ gates
- Best classical circuit needs $O(n2^n)$ gates
- Looks great! Is it?

The Quantum Fourier Transform: Complexity



- Quantum circuit has $O(n^2)$ gates
- Best classical circuit needs $O(n2^n)$ gates
- Looks great! Is it?

$$\sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{QFT} \sum_{k=0}^{N-1} y_k |k\rangle \qquad (\text{where } y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N})$$

- We want the DFT coefficients y_k's, but they are encoded in the amplitudes!

Phase Estimation

Let's see an application of the QFT.

A previous exercise: the eigenvalues of a unitary operator are complex numbers of **modulus 1**.

This means that any eigenvalue of a unitary operator can be written as $e^{2\pi i\varphi}$ for some real $\varphi \in [0, 1]$.

Phase Estimation

Let's see an application of the QFT.

A previous exercise: the eigenvalues of a unitary operator are complex numbers of **modulus 1**.

This means that any eigenvalue of a unitary operator can be written as $e^{2\pi i \varphi}$ for some real $\varphi \in [0, 1]$.

Definition (Phase Estimation Problem)

Let $\lambda = e^{2\pi i \varphi}$ be an eigenvalue of a unitary operator U. Find φ.

Phase Estimation

Let's see an application of the QFT.

A previous exercise: the eigenvalues of a unitary operator are complex numbers of **modulus 1**.

This means that any eigenvalue of a unitary operator can be written as $e^{2\pi i\varphi}$ for some real $\varphi \in [0, 1]$.

Definition (Phase Estimation Problem)

Let $\lambda = e^{2\pi i\varphi}$ be an eigenvalue of a unitary operator U. Find φ.

This problem can be solved quite easily with the QFT.

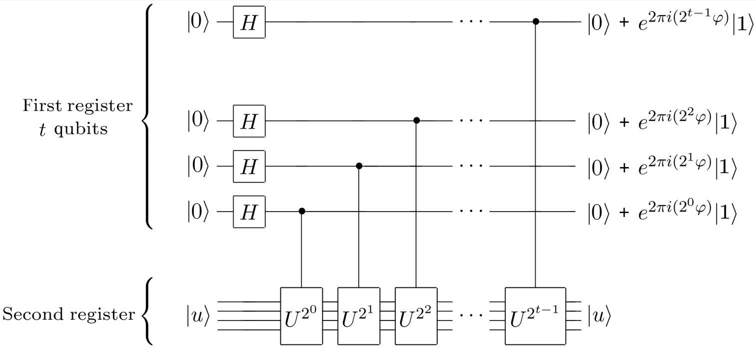
Quantum Phase Estimation Algorithm

Let u be an eigenvector associated to the unknown eigenvalue $e^{2\pi i\varphi}$ of a unitary operator U, *i.e.*, $U|u\rangle = e^{2\pi i\varphi}|u\rangle$.

Quantum Phase Estimation Algorithm

Let u be an eigenvector associated to the unknown eigenvalue $e^{2\pi i\varphi}$ of a unitary operator U, *i.e.*, $U|u\rangle = e^{2\pi i\varphi}|u\rangle$.

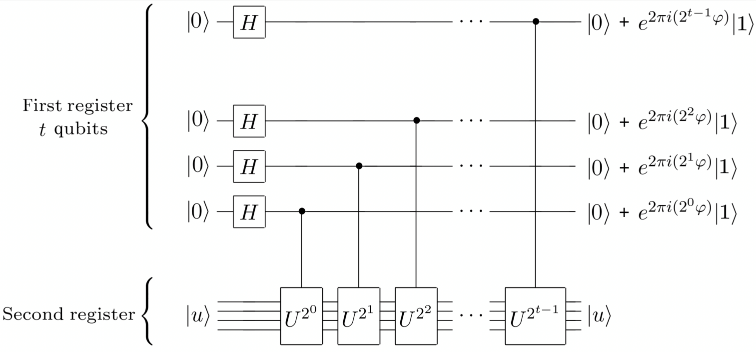
Consider the circuit below for some natural $t > 0$:



Quantum Phase Estimation Algorithm

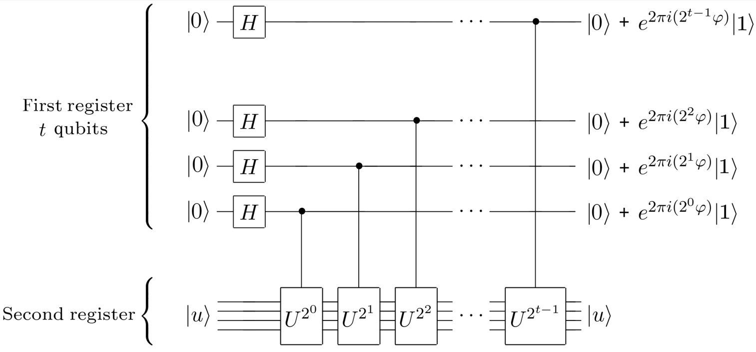
Let u be an eigenvector associated to the unknown eigenvalue $e^{2\pi i\varphi}$ of a unitary operator U, *i.e.*, $U|u\rangle = e^{2\pi i\varphi}|u\rangle$.

Consider the circuit below for some natural $t > 0$:



A control-U^{2^k} gate conditionally applies $U^{2^k} = \underbrace{U \cdots U}_{2^k \textit{ times}}$ to the second qubit register.

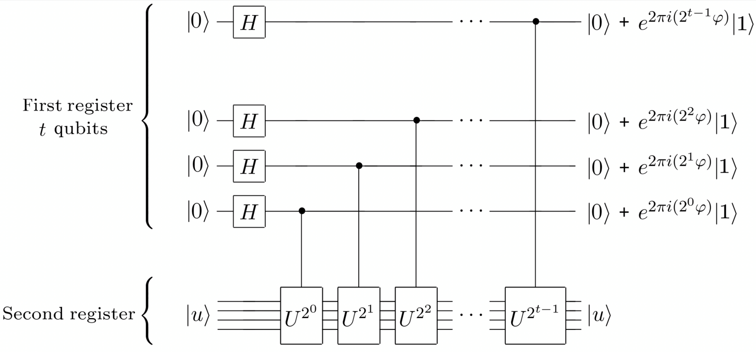
Quantum Phase Estimation Algorithm



The state of the t qubits at the end of the QPE circuit is:

$$\frac{1}{2^{t/2}}(|0\rangle+e^{2\pi i 2^{t-1}\varphi}|1\rangle)\otimes(|0\rangle+e^{2\pi i 2^{t-2}\varphi}|1\rangle)\otimes\cdots\otimes(|0\rangle+e^{2\pi i 2^{0}\varphi}|1\rangle)$$

Quantum Phase Estimation Algorithm



The state of the t qubits at the end of the QPE circuit is:

$$\frac{1}{2^{t/2}}(|0\rangle+e^{2\pi i 2^{t-1}\varphi}|1\rangle)\otimes(|0\rangle+e^{2\pi i 2^{t-2}\varphi}|1\rangle)\otimes\cdots\otimes(|0\rangle+e^{2\pi i 2^{0}\varphi}|1\rangle) = \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i k\varphi}|k\rangle$$

Quantum Phase Estimation Algorithm

Suppose now that φ can be written exactly with t bits:

$$\boxed{\varphi = 0.\varphi_1 \dots \varphi_t}$$

Quantum Phase Estimation Algorithm

Suppose now that φ can be written <u>exactly</u> with t bits:

$$\boxed{\varphi = 0.\varphi_1 \dots \varphi_t}$$

Then, the state at the end of the QPE circuit is:

$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\dots\varphi_t}|1\rangle)$$

which is *precisely* the final state of the QFT circuit (after the swap)!

Quantum Phase Estimation Algorithm

Suppose now that φ can be written exactly with t bits:

$$\boxed{\varphi = 0.\varphi_1 \dots \varphi_t}$$

Then, the state at the end of the QPE circuit is:

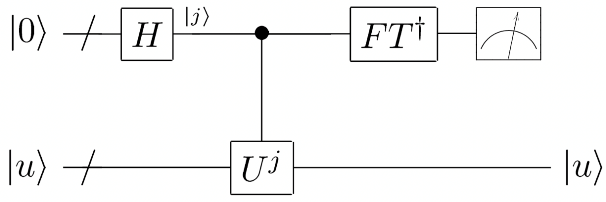
$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle) \otimes (|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle) \otimes \cdots \otimes (|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2\dots\varphi_t}|1\rangle)$$

which is *precisely* the final state of the QFT circuit (after the swap)!

Therefore, we apply the inverse QFT circuit at the end of the QPE circuit and then measure to obtain the sought phase $|\varphi_1 \dots \varphi_t\rangle$ with probability 1!

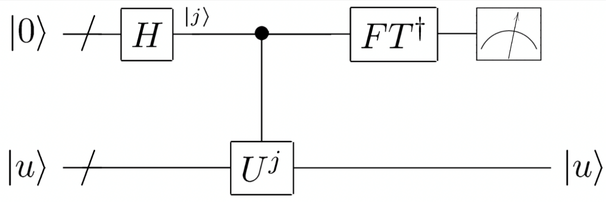
Quantum Phase Estimation Algorithm

The final quantum circuit for solving phase estimation is thus:



Quantum Phase Estimation Algorithm

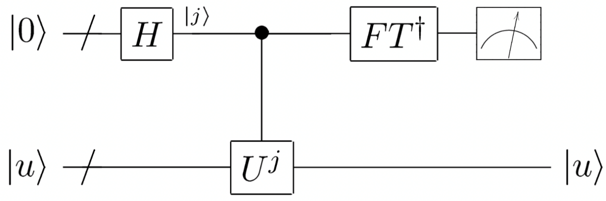
The final quantum circuit for solving phase estimation is thus:



What if φ is not expressible in exactly t bits?

Quantum Phase Estimation Algorithm

The final quantum circuit for solving phase estimation is thus:



What if φ is not expressible in exactly t bits?

Proposition

To estimate φ with n bits of precision *and* success probability *at least* $1 - \epsilon$, *it is sufficient to use the QPE circuit with r qubits*

$$r = n + \left\lceil \log\left(2 + \frac{1}{2\epsilon}\right) \right\rceil$$