Quantum Computing (CST Part II)

Lecture 9: Quantum Fourier Transform & Quantum Phase Estimation

If computers that you build are quantum,
Then spies everywhere will all want 'em.
Our codes will all fail,
And they'll read our email,
Till we get the crypto that's quantum, and daunt'em.
Jennifer and Peter Shor

The Fourier transform

In the early 1800s French mathematician Joseph Fourier discovered (or invented if you prefer) the Fourier transform. It allows frequency components of signals to be extracted, and is still at the heart of modern day signal processing.

In particular, the discrete Fourier transform (DFT) is still widely used, which takes an input vector x and transforms of it an output vector y as follows:

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

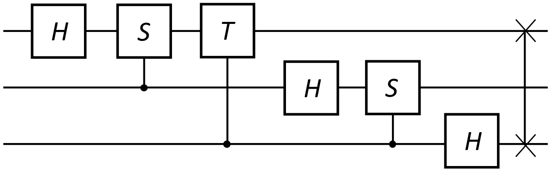
(where both x and y have N elements).

Significance of the quantum Fourier transform

- The QFT on n qubits requires n Hadamard gates, $\frac{n(n-1)}{2}$ 2-qubit conditional rotation gates and $\frac{n}{2}$ SWAP gates: $\mathcal{O}(n^2)$ gates in total.
- This means that it can be efficiently implemented (i.e., in time polynomial in n) using gates from a finite universal gate-set.
- By contrast, classically the Fourier transform requires $\Theta(n2^n)$ gates.
- The QFT cannot be used to speed-up signal processing tasks...
- ...but it is at the heart of many applications of quantum computing and simulation that demonstrate exponential speed-ups compared to the best-known classical counterparts. In particular, as part of the *quantum phase estimation* sub-routine.
- In some sense, the QFT can be thought of as playing the role of "interference" at the end of the quantum algorithm, that we argued in the previous lecture is a necessity.

The three-qubit quantum Fourier transform

The three-qubit quantum Fourier transform is as follows (we now use $|j\rangle = |j_1 j_2 j_3\rangle$ rather than $|x\rangle$ for the general quantum state).



Prior to the SWAP gate we have:

$$|j_1\rangle \rightarrow \frac{|0\rangle + e^{\pi i j_1}|1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle + e^{\pi i j_1} e^{\pi i j_2/2}|1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle + e^{\pi i j_1} e^{\pi i j_2/2} e^{\pi i j_3/4}|1\rangle}{\sqrt{2}}$$

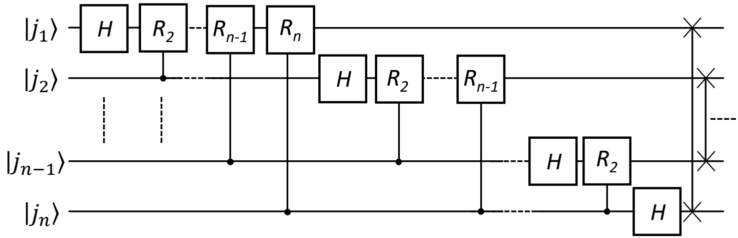
$$|j_2\rangle \rightarrow \frac{|0\rangle + e^{\pi i j_2}|1\rangle}{\sqrt{2}} \rightarrow \frac{|0\rangle + e^{\pi i j_2} e^{\pi i j_3/2}|1\rangle}{\sqrt{2}}$$

$$|j_3\rangle \rightarrow \frac{|0\rangle + e^{\pi i j_3}|1\rangle}{\sqrt{2}}$$

We can thus express the state after the SWAP gate:

$$\frac{1}{2\sqrt{2}}\Big(|0\rangle + e^{\pi i j_3}|1\rangle\Big)\Big(|0\rangle + e^{\pi i (j_2 + (j_3/2))}|1\rangle\Big)\Big(|0\rangle + e^{\pi i (j_1 + (j_2/2) + (j_3/4))}|1\rangle\Big)$$

The quantum Fourier transform circuit



Where $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$ is a single qubit unitary *rotation* gate.

The quantum Fourier transform

We can see that the general quantum Fourier transform is thus (where $N = 2^n$):

$$\frac{1}{\sqrt{N}}\left(|0\rangle + e^{\pi i j_n}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{\pi i (j_2+(j_3/2)+\cdots+(j_n/(2^{n-2})))}|1\rangle\right)$$
$$\otimes\left(|0\rangle + e^{\pi i (j_1+(j_2/2)+\cdots+(j_n/(2^{n-1})))}|1\rangle\right)$$

To rearrange further, we will use binary decimals (also termed binary fractions, that is we can express: $\frac{a_1}{2}+\frac{a_2}{4}+\cdots+\frac{a_n}{2^n}$ as the binary decimal $0.a_1a_2\cdots a_n$. So we can thus express the QFT:

$$\frac{1}{\sqrt{N}}\left(|0\rangle + e^{2\pi i(0.j_n)}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i(0.j_2j_3\cdots j_n)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.j_1j_2\cdots j_n)}|1\rangle\right)$$

Furthermore, as $e^{2m\pi i} = 1$ for any integer m, this equals:

$$\frac{1}{\sqrt{N}}\bigotimes_{l=1}^{n}\left(|0\rangle + e^{2\pi i j 2^{-l}}|1\rangle\right)$$

The quantum Fourier transform (continued)

We now rearrange the quantum Fourier transform into standard form:

$$
\begin{aligned}
\frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right) &= \frac{1}{\sqrt{N}} \bigotimes_{l=1}^{n} \left(\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right) \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j (\sum_{l=1}^{n} k_l 2^{-l})} |k_1 \cdots k_n\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle
\end{aligned}
$$

Comparing the QFT to the DFT

From the analysis on the previous slides we have that the QFT performs the transformation:

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

If we now consider an arbitrary state, by linearity:

$$\begin{aligned} \sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{j=0}^{N-1} x_j \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \\ = \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N} \right) |k\rangle \\ = \sum_{k=0}^{N-1} y_k |k\rangle \end{aligned}$$

i.e., using the previously stated definition of the DFT:

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

The inverse quantum Fourier transform

To invert the QFT, we must run the circuit in reverse, with the inverse of each gate in place to achieve the transform:

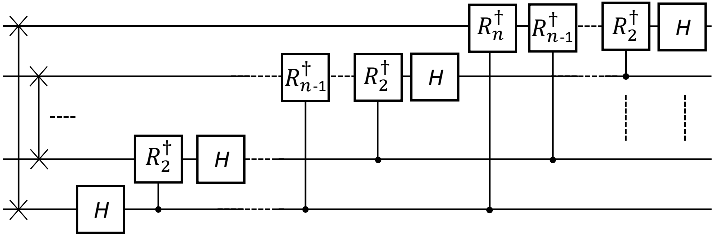
$$\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle \to |j\rangle$$

We have already seen that the Hadamard gate is self-inverse, and the same is clearly true for the SWAP gate; the inverse of the rotations gate R_k is given by:

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

The inverse quantum Fourier transform circuit

Thus we can express the inverse QFT circuit:



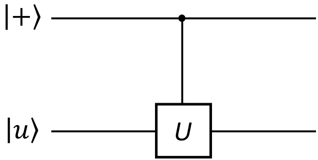
Quantum phase estimation

Quantum phase estimation addresses the following problem:

- We have a n-qubit oracle function U, encoded in the form of a controlled-U unitary.
- U has an eigenvalue $e^{2\pi i\phi}$, associated with an eigenvector $|u\rangle$ which we can prepare.
- We wish to estimate the phase, ϕ, of the eigenvalue to t bits of precision.

The action of the oracle on $|+\rangle$

We can express the result when $|+\rangle$ is used to control U:

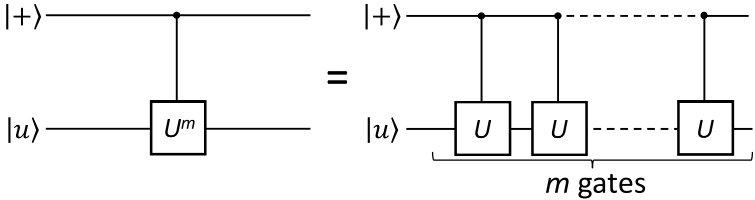


Which is the transformation:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|u\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle + |1\rangle e^{2\pi i\phi}|u\rangle\right)$$
$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\phi}|1\rangle\right)|u\rangle$$

The action of the oracle on $|+\rangle$ (continued)

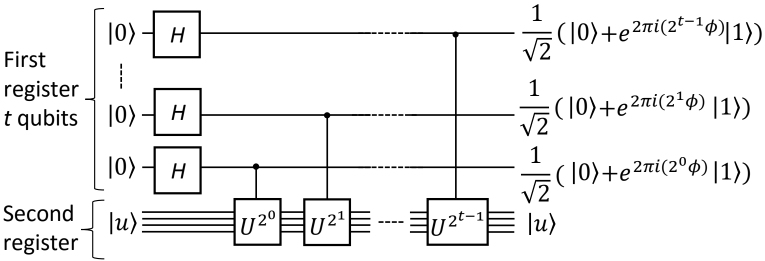
In QPE we have to apply U repeatedly:



Which is the transformation:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|u\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2m\pi i\phi}\,|1\rangle\right)|u\rangle$$

Using the oracle to prepare the state



Using the previous analysis, the final state can be expressed:

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i \phi j} |j\rangle |u\rangle$$

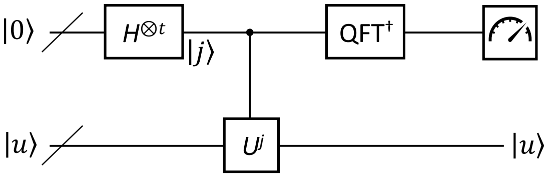
Using the inverse QFT to estimate the eigenvalue phase

We now perform an inverse QFT on the first register: by definition, the effect of the inverse QFT on the first register is the transformation:

$$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i \phi j} |j\rangle |u\rangle \rightarrow |\tilde{\phi}\rangle |u\rangle$$

Thus measuring the first register, whose state is now $|\tilde{\phi}\rangle$, gives a t-bit approximation, $\tilde{\phi}$, of the eigenvalue phase, ϕ.

In summary, the entire QPE circuit can be expressed:



Quantum phase estimation example

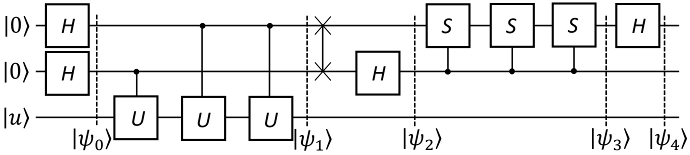
Typically QPE is applied to large unitaries, but for the example we'll consider the single-qubit unitary

$$U = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Which we know has eigenvector $|u\rangle = \begin{bmatrix} 1 \\ -i \end{bmatrix}$ associated with eigenvalue -1, i.e., $\phi = \frac{1}{2}$ (from exercise sheet 1 question 3).

We will estimate the eigenvalue to two bits of precision (i.e., $t = 2$).

Quantum phase estimation example: circuit



$$|\psi_0\rangle = \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\,|u\rangle$$

$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + e^{2\pi i}\,|1\rangle)(|0\rangle + e^{\pi i}\,|1\rangle)\,|u\rangle$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|0\rangle\,|u\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|0\rangle\,|u\rangle$$

$$|\psi_4\rangle = |1\rangle\,|0\rangle\,|u\rangle$$

So we measure 10 which corresponds to the binary fraction $1 \times \frac{1}{2} + 0 \times \frac{1}{4} = \frac{1}{2}$ as expected.

Significance of quantum phase estimation

- QPE enables the phase of an eigenvalue to be estimated to an arbitrary number of bits of precision.
- It can be shown that the estimate is good even when the phase cannot be exactly expanded as a binary fraction.
- QPE is at the heart of quantum chemistry and many quantum computing algorithms.
- As QPE uses the oracle U and the prepared state $|u\rangle$ it should be thought of as a subroutine that can be called, rather than an entire algorithm in and of itself.

Summary

In this lecture we have looked at:

- **Quantum Fourier transform**: which performs the transformation:

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

  Using $\mathcal{O}(n^2)$ gates.

- **Quantum phase estimation**: which is a subroutine at the heart of quantum chemistry and many important quantum algorithms.