Introduction to Quantum Information Processing

Lecture 10

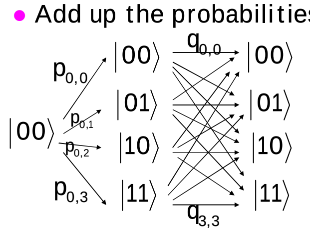
Michele Mosca

Overview

- Classical Randomized vs. Quantum Computing
- Deutsch-Jozsa and Bernstein-Vazirani algorithms
- The quantum Fourier transform and phase estimation

A classical randomised algorithm

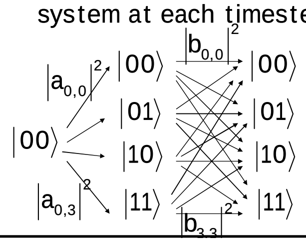
- Several computational paths leading to the same outcome.
- Add up the probabilities.



$$\Pr(00) = \sum_j p_{0,j} q_{j,0}$$

A classical randomised algorithm

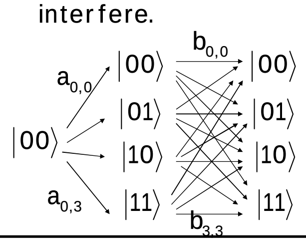
- The probabilities could correspond to the square of a probability amplitude (due to measuring they quantum system at each timestep)



$$\Pr(00) = \sum_j \left| a_{0,j} b_{j,0} \right|^2$$

A quantum algorithm

- If we don't measure at each time step, only at the end, the probability amplitudes first have a chance to interfere.



$$\Pr(00) = \left| \sum_j a_{0,j} b_{j,0} \right|^2$$

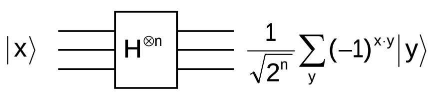
Decoherence

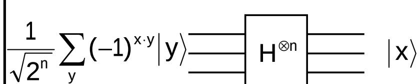
- A quantum system that is continually measured (or interacts with an external system) will behave like a classical randomized system
- Partial measurements will give a probability distribution somewhere in between the two extremes
- Error-correcting codes will allow a quantum system interacting with the environment to maintain "coherence".

Quantum Algorithms

- Quantum Algorithms should exploit quantum parallelism and quantum interference.
- We have already seen the Deutsch, Deutsch-Jozsa, Bernstein-Vazirani and Simon's algorithms.

Multi-qubit Hadamard





Quantum Algorithms

- These algorithms have been computing essentially classical functions on quantum superpositions
- This encoded information in the phases of the basis states: measuring basis states would provide little useful information
- But a simple quantum transformation translated the phase information into information that was measurable in the computational basis

Quantum Phase Estimation

- Suppose we wish to estimate a number $\omega \in [0,1)$ given the quantum state

$$\sum_{y=0}^{2^n-1} e^{2\pi i \omega y}|y\rangle$$

- Note that in binary we can express

$$\omega = 0.x_1 x_2 x_3 \ldots$$

$$2\omega = x_1.x_2 x_3 \ldots$$

$$2^{n-1}\omega = x_1 x_2 x_3 \ldots x_{n-1}.x_n x_{n+1} \ldots$$

Quantum Phase Estimation

- Since $e^{2\pi i k} = 1$ for any integer k, we have

$$e^{2\pi i(2\omega)} = e^{2\pi i(x_1.x_2 x_3 \ldots)} = e^{2\pi i x_1} e^{2\pi i(0.x_2 x_3 \ldots)} = e^{2\pi i(0.x_2 x_3 \ldots)}$$

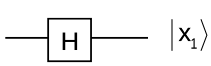
$$e^{2\pi i(2^k \omega)} = e^{2\pi i(0.x_{k+1} x_{k+2} \ldots)}$$

Quantum Phase Estimation

- If $\omega = 0.x_1$ then we can do the following

$$\frac{|0\rangle + e^{2\pi i(0.x_1)}|1\rangle}{\sqrt{2}}$$

$$= \frac{|0\rangle + (-1)^{x_1}|1\rangle}{\sqrt{2}}$$



Useful identity

- We can show that

$$\sum_{y=0}^{2^n-1} e^{2\pi i\omega y}|y\rangle$$

$$= \left(|0\rangle + e^{2\pi i(2^{n-1}\omega)}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i(2^{n-2}\omega)}|1\rangle\right)\otimes \cdots \otimes \left(|0\rangle + e^{2\pi i(\omega)}|1\rangle\right)$$

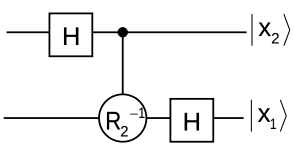
$$= \left(|0\rangle + e^{2\pi i(0.x_n x_{n+1}\ldots)}|1\rangle\right)\otimes\left(|0\rangle + e^{2\pi i(0.x_{n-1}x_n x_{n+1}\ldots)}|1\rangle\right)\otimes \cdots \otimes \left(|0\rangle + e^{2\pi i(0.x_1 x_2\ldots)}|1\rangle\right)$$

Quantum Phase Estimation

- So if $\omega = 0.x_1x_2$ then we can do the following

$$\frac{|0\rangle + e^{2\pi i(0.x_2)}|1\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + e^{2\pi i(0.x_1x_2)}|1\rangle}{\sqrt{2}}$$



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

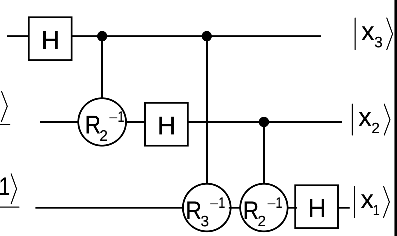
Quantum Phase Estimation

- So if $\omega = 0.x_1x_2x_3$ then we can do the following

$$\frac{|0\rangle + e^{2\pi i(0.x_3)}|1\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + e^{2\pi i(0.x_2x_3)}|1\rangle}{\sqrt{2}}$$

$$\frac{|0\rangle + e^{2\pi i(0.x_1x_2x_3)}|1\rangle}{\sqrt{2}}$$



Quantum Phase Estimation

- Generalizing this network (and reversing the order of the qubits at the end) gives us a network with $O(n^2)$ gates that implements

$$\sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle \rightarrow |x\rangle$$

Discrete Fourier Transform

- The discrete Fourier transform maps vectors of dimension N by transforming the x^{th} elementary vector according to

$$(0,0,\ldots,0,1,0,\ldots 0) \rightarrow (1, e^{2\pi i \frac{x}{N}}, e^{2\pi i \frac{2x}{N}}, \ldots, e^{2\pi i \frac{(N-1)x}{N}})$$

- The quantum Fourier transform maps vectors in a Hilbert space of dimension N according to

$$|x\rangle \rightarrow \sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y} |y\rangle$$

Discrete Fourier Transform

- Thus we have illustrated how to implement (the inverse of) the quantum Fourier transform in a Hilbert space of dimension 2^n

Estimating arbitrary $\omega \in [0,1)$

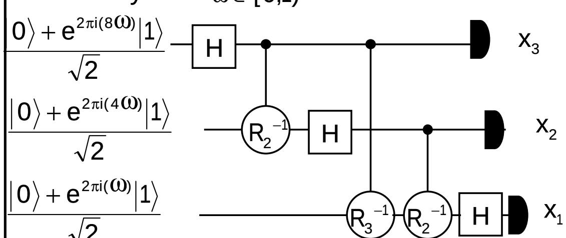
- What if ω is not necessarily of the form $\frac{x}{2^n}$ for some integer x?
- The QFT will map $\sum_{x=0}^{2^n-1} e^{2\pi i \omega z}|z\rangle$ to a superposition $|\tilde{\omega}\rangle = \sum_y \alpha_y |y\rangle$

where

$$\mathrm{Prob}\left(\left|\frac{y}{N} - \omega\right| \le \frac{1}{N}\right) \ge \frac{8}{\pi^2} \qquad |\alpha_y| \in O\left(\frac{1}{\left|\frac{y}{N} - \omega\right|}\right)$$

Quantum Phase Estimation

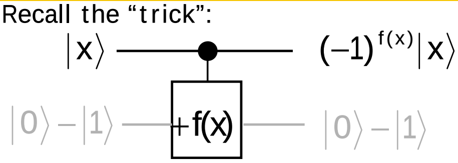
- For any real $\omega \in [0,1)$



- With high probability $\frac{4x_1+2x_2+x_3}{8} \approx \omega$

Eigenvalue kick-back

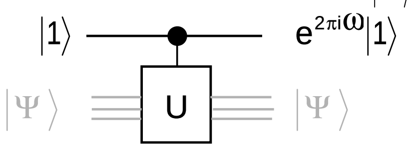
- Recall the "trick":



$$|x\rangle(|0\rangle - |1\rangle) \rightarrow |x\rangle(|f(x)\rangle - |f(x) \oplus 1\rangle)$$
$$= |x\rangle(-1)^{f(x)}(|0\rangle - |1\rangle)$$
$$= (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

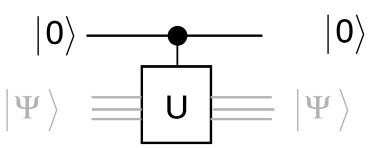
Eigenvalue kick-back

- Consider a unitary operation U with eigenvalue $e^{2\pi i\omega}$ and eigenvector $|\Psi\rangle$



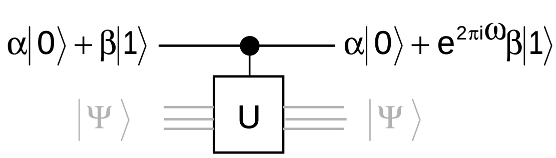
$$|1\rangle|\Psi\rangle \rightarrow |1\rangle U|\Psi\rangle = |1\rangle e^{2\pi i\omega}|\Psi\rangle$$
$$= e^{2\pi i\omega}|1\rangle|\Psi\rangle$$

Eigenvalue kick-back



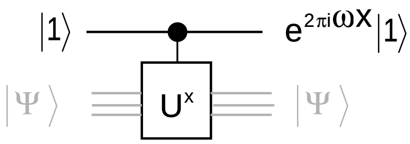
Eigenvalue kick-back

- As a relative phase, $e^{2\pi i\omega}$ becomes measurable

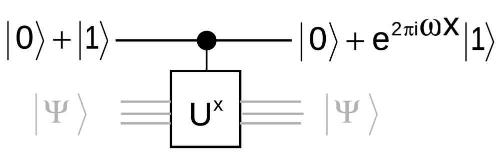


Eigenvalue kick-back

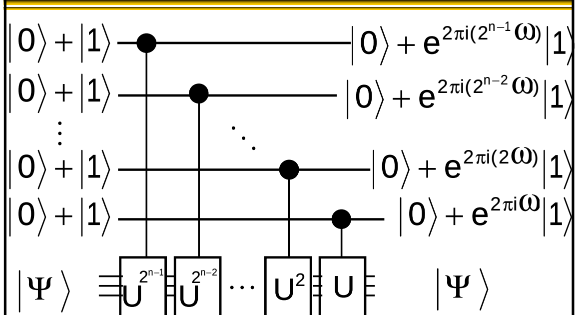
- If we exponentiate U, we get multiples of ω



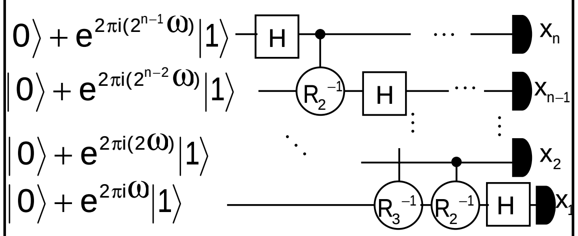
Eigenvalue kick-back



Eigenvalue kick-back

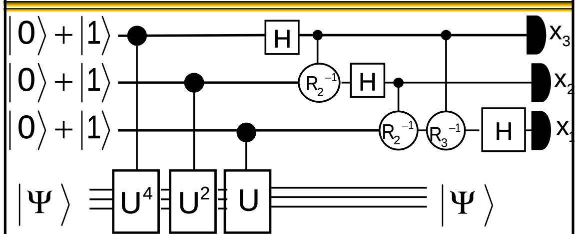


Phase estimation

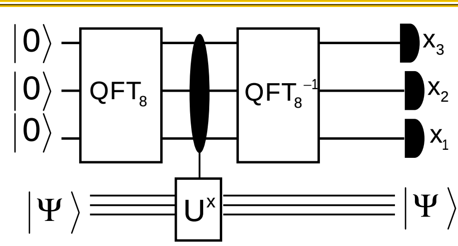


$$\frac{2^{n-1}x_1 + 2^{n-2}x_2 + \cdots x_n}{2^n} \approx \omega$$

Eigenvalue estimation



Eigenvalue estimation



Eigenvalue kick-back

- Given U with eigenvector $|\Psi\rangle$ and eigenvalue $e^{2\pi i\omega}$ we thus have an algorithm that maps

$$|0\rangle|\Psi\rangle \rightarrow |\tilde{\omega}\rangle|\Psi\rangle$$

Eigenvalue kick-back

- Given U with eigenvectors $|\Psi_k\rangle$ and respective eigenvalues $e^{2\pi i\omega_k}$ we thus have an algorithm that maps

$$|0\rangle|\Psi_k\rangle \rightarrow |\tilde{\omega}_k\rangle|\Psi_k\rangle$$

and therefore

$$|0\rangle\sum_k \alpha_k|\Psi_k\rangle = \sum_k \alpha_k|0\rangle|\Psi_k\rangle \rightarrow \sum_k \alpha_k|\tilde{\omega}_k\rangle|\Psi_k\rangle$$

Eigenvalue kick-back

- Measuring the first register of

$$\sum_k \alpha_k|\tilde{\omega}_k\rangle|\Psi_k\rangle$$

is equivalent to measuring $|\tilde{\omega}_k\rangle$ with probability $|\alpha_k|^2$

Example

- Suppose we have a group G and we wish to find the order of $a \in G$ (I.e. the smallest positive r such that $a^r \equiv 1$)
- If we can efficiently do arithmetic in the group, then we can realise a unitary operator U_a that maps $|x\rangle \rightarrow |ax\rangle$
- Notice that $U_a{}^r = U_{a^r} = I$
- This means that the eigenvalues of U_a are of the form $e^{2\pi i \frac{k}{r}}$ where k is an integer