COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Computation: Phase estimation

Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

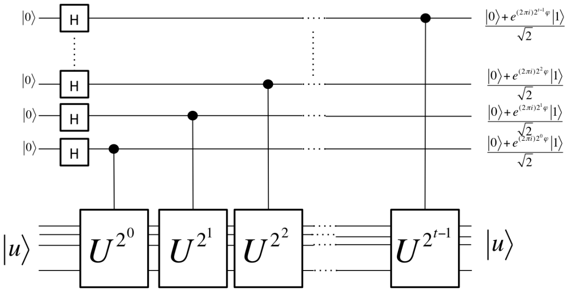
- We will use the assumption that there are black-boxes that:
  - prepare the state $|u\rangle$, and
  - perform the controlled-U^{2^j} operation.
- We will describe a phase estimation procedure that uses two registers:
  - A t-qubit register initially in state $|0...0\rangle$ (the value of t to be decided later), and
  - a register that begins in the state $|u\rangle$.

Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

- Claim 1: The final state of the first register in the circuit below is given by:

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



Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

- Claim 1: The final state of the first register in the circuit below is given by:

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

- Question: Suppose φ may be expressed exactly as $\varphi = [0 \cdot \varphi_1\varphi_2...\varphi_t]$. Suggest a way to retrieve the value of φ?

Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i \varphi}$. The goal is to estimate φ.

- Claim 1: The final state of the first register in the circuit below is given by:

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

- Question: Suppose φ may be expressed exactly as $\varphi = [0 \cdot \varphi_1 \varphi_2 \dots \varphi_t]$. Suggest a way to retrieve the value of φ?
  - Taking the inverse-fourier transform and measuring the value of the first register in the computational basis gives φ.
- In general, we will show that the inverse Fourier transform has the following behaviour:

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{(2\pi i)\varphi j} |j\rangle |u\rangle \rightarrow |\tilde{\varphi}\rangle |u\rangle$$

where $|\tilde{\varphi}\rangle$ denotes a state that is a good estimator for φ when measured.

Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

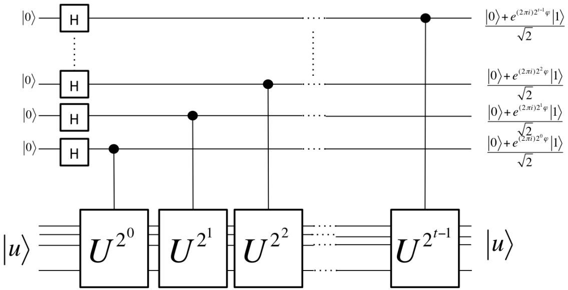
- We will use the assumption that there are black-boxes that:
  - prepare the state $|u\rangle$, and
  - perform the controlled-U^{2^j} operation.
- We will describe a phase estimation procedure that uses two registers:
  - A t-qubit register initially in state $|0...0\rangle$ (the value of t to be decided later), and
  - a register that begins in the state $|u\rangle$.

Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

- Claim 1: The final state of the first register in the circuit below is given by:

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



Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

- Claim 1: The final state of the first register in the circuit below is given by:

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

- Question: Suppose φ may be expressed exactly as $\varphi = [0 \cdot \varphi_1\varphi_2 ... \varphi_t]$. Suggest a way to retrieve the value of φ?

Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

- Claim 1: The final state of the first register in the circuit below is given by:

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

- Question: Suppose φ may be expressed exactly as $\varphi = [0 \cdot \varphi_1\varphi_2...\varphi_t]$. Suggest a way to retrieve the value of φ?
  - Taking the inverse-fourier transform and measuring the value of the first register in the computational basis gives φ.
- In general, we will show that the inverse Fourier transform has the following behaviour:

$$\frac{1}{2^{t/2}}\sum_{j=0}^{2^t-1} e^{(2\pi i)\varphi j}|j\rangle|u\rangle \rightarrow |\tilde{\varphi}\rangle|u\rangle$$

where $|\tilde{\varphi}\rangle$ denotes a state that is a good estimator for φ when measured.

- In general, we will show that the inverse Fourier transform has the following behaviour:

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{(2\pi i)\varphi j} |j\rangle |u\rangle \rightarrow |\tilde{\varphi}\rangle |u\rangle$$

where $|\tilde{\varphi}\rangle$ denotes a state that is a good estimator for φ when measured.

Claim 2

It is sufficient to run the phase estimation technique with $t = n + \log\left(2 + \frac{1}{2\varepsilon}\right)$ in order to obtain φ accurate to n bits with probability at least $(1 - \varepsilon)$.

Claim 2

It is sufficient to run the phase estimation technique with $t = n + \lceil \log \left(2 + \frac{1}{2\varepsilon}\right) \rceil$ in order to obtain φ accurate to n bits with probability at least $(1 - \varepsilon)$.

Proof sketch

- Let $0 \leq b \leq 2^t - 1$ be an integer such that $\frac{b}{2^t} = [0 \cdot b_1 \ldots b_t]$ is the best t bit approximation to φ that is less than φ. Let $\delta = \varphi - \frac{b}{2^t}$ (which implies $0 \leq \delta \leq 2^{-t}$).
- Claim 2.1: Applying the inverse Fourier transform on the first register in state $\frac{1}{2^{t/2}} \sum_{k=0}^{2^t - 1} e^{(2\pi i)\varphi k} |k\rangle$ ends in the following state:

$$\frac{1}{2^t} \sum_{k,l=0}^{2^t - 1} e^{\frac{-(2\pi i)kl}{2^t}} e^{(2\pi i)\varphi k} |l\rangle .$$

Claim 2

It is sufficient to run the phase estimation technique with $t = n + \lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \rceil$ in order to obtain φ accurate to n bits with probability at least $(1 - \varepsilon)$.

Proof sketch

- Let $0 \leq b \leq 2^t - 1$ be an integer such that $\frac{b}{2^t} = [0 \cdot b_1 \ldots b_t]$ is the best t bit approximation to φ that is less than φ. Let $\delta = \varphi - \frac{b}{2^t}$ (which implies $0 \leq \delta \leq 2^{-t}$).
- Claim 2.1: Applying the inverse Fourier transform on the first register in state $\frac{1}{2^{t/2}} \sum_{k=0}^{2^t - 1} e^{(2\pi i)\varphi k} |k\rangle$ ends in the following state: $\frac{1}{2^t} \sum_{k,l=0}^{2^t - 1} e^{\frac{-(2\pi i)kl}{2^t}} e^{(2\pi i)\varphi k} |l\rangle$.
- Claim 2.2: Let α_l be the amplitude of $|(b + l) \ mod \ 2^t\rangle$. Then $\alpha_l = \frac{1}{2^t} \left(\frac{1 - e^{(2\pi i)(2^t \varphi - (b+l))}}{1 - e^{(2\pi i)(\varphi - (b+l)/2^t)}} \right) = \frac{1}{2^t} \left(\frac{1 - e^{(2\pi i)(2^t \delta - l)}}{1 - e^{(2\pi i)(\delta - l/2^t)}} \right)$.

Claim 2

It is sufficient to run the phase estimation technique with $t = n + \lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \rceil$ in order to obtain φ accurate to n bits with probability at least $(1 - \varepsilon)$.

Proof sketch

- Let $0 \leq b \leq 2^t - 1$ be an integer such that $\frac{b}{2^t} = [0 \cdot b_1 ... b_t]$ is the best t bit approximation to φ that is less than φ. Let $\delta = \varphi - \frac{b}{2^t}$ (which implies $0 \leq \delta \leq 2^{-t}$).
- Claim 2.1: Applying the inverse Fourier transform on the first register in state $\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{(2\pi i)\varphi k} |k\rangle$ ends in the following state: $\frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{\frac{-(2\pi i)kl}{2^t}} e^{(2\pi i)\varphi k} |l\rangle$.
- Claim 2.2: Let α_l be the amplitude of $|(b+l) \ mod \ 2^t\rangle$. Then $\alpha_l = \frac{1}{2^t}\left(\frac{1-e^{(2\pi i)(2^t\varphi-(b+l))}}{1-e^{(2\pi i)(\varphi-(b+l)/2^t)}}\right) = \frac{1}{2^t}\left(\frac{1-e^{(2\pi i)(2^t\delta-l)}}{1-e^{(2\pi i)(\delta-l/2^t)}}\right)$.
- Claim 2.3: Let e be the error parameter and let m be the outcome of the measurement. Then

$$\mathbf{Pr}[|m - b| > e] \leq \frac{1}{2(e-1)}.$$

Claim 2

It is sufficient to run the phase estimation technique with $t = n + \lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \rceil$ in order to obtain φ accurate to n bits with probability at least $(1 - \varepsilon)$.

Proof sketch

- Let $0 \leq b \leq 2^t - 1$ be an integer such that $\frac{b}{2^t} = [0 \cdot b_1 \ldots b_t]$ is the best t bit approximation to φ that is less than φ. Let $\delta = \varphi - \frac{b}{2^t}$ (which implies $0 \leq \delta \leq 2^{-t}$).
- Claim 2.1: Applying the inverse Fourier transform on the first register in state $\frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{(2\pi i)\varphi k} |k\rangle$ ends in the following state: $\frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{\frac{-(2\pi i)kl}{2^t}} e^{(2\pi i)\varphi k} |l\rangle$.
- Claim 2.2: Let α_l be the amplitude of $|(b+l) \ mod \ 2^t\rangle$. Then $\alpha_l = \frac{1}{2^t}\left(\frac{1-e^{(2\pi i)(2^t\varphi-(b+l))}}{1-e^{(2\pi i)(\varphi-(b+l)/2^t)}}\right) = \frac{1}{2^t}\left(\frac{1-e^{(2\pi i)(2^t\delta-l)}}{1-e^{(2\pi i)(\delta-l/2^t)}}\right)$.
- Claim 2.3: Let e be the error parameter and let m be the outcome of the measurement. Then

$$\mathbf{Pr}[|m-b| > e] \leq \frac{1}{2(e-1)}.$$

- The claim follows by setting $t = n + p$ and $\varepsilon = \frac{1}{2(2^p-1)}$. □

Phase estimation

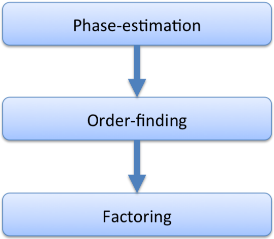
Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i\varphi}$. The goal is to estimate φ.

- The phase estimation protocol works when the second register is set to the eigenstate $|u\rangle$. In general, this may not be feasible.
- Observation: Any general state $|\psi\rangle$ may be written in terms of the eigenstates of U as $\sum_u c_u |u\rangle$.
- Exercise: The phase estimation procedure takes state $(|0\rangle)(\sum_u c_u |u\rangle)$ to $\sum_u c_u |\tilde{\varphi_u}\rangle |u\rangle$. If $t = n + \lceil \log\left(2 + \frac{1}{2\varepsilon}\right) \rceil$, then the probability of measuring φ_u accurate to n bits at the end of the phase estimation procedure is at least $|c_u|^2(1 - \varepsilon)$.

Phase estimation

Suppose a unitary operator U has an eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i \varphi}$. The goal is to estimate φ.

- Phase estimation enables us to design quantum algorithms for the order-finding and factoring problems.



Quantum Computation: Order finding

- Given integers $N > x > 0$ such that x and N have no common factors, the order of x modulo N is defined to be the least positive integer r such that $x^r = 1 \ (mod \ N)$.
- Exercise: What is the order of 5 modulo 21?

- Given integers $N > x > 0$ such that x and N have no common factors, the order of x modulo N is defined to be the least positive integer r such that $x^r = 1 \ (mod \ N)$.
- Exercise: What is the order of 5 modulo 21? 6

Order finding

Given co-prime integers $N > x > 0$, compute the order of x modulo N.

- Exercise: Is there an algorithm that computes the order of x modulo N in time that is polynomial in N?

- Given integers $N > x > 0$ such that x and N have no common factors, the order of x modulo N is defined to be the least positive integer r such that $x^r = 1 \ (mod \ N)$.
- Exercise: What is the order of 5 modulo 21? 6

Order finding

Given co-prime integers $N > x > 0$, compute the order of x modulo N.

- Exercise: Is there an algorithm that computes the order of x modulo N in time that is polynomial in N? Yes
- Exercise: Is it an efficient algorithm?

- Given integers $N > x > 0$ such that x and N have no common factors, the order of x modulo N is defined to be the least positive integer r such that $x^r = 1 \ (mod \ N)$.
- Exercise: What is the order of 5 modulo 21? 6

Order finding

Given co-prime integers $N > x > 0$, compute the order of x modulo N.

- Exercise: Is there an algorithm that computes the order of x modulo N in time that is polynomial in N? Yes
- Exercise: Is it an efficient algorithm?
- Let $L = \lceil \log n \rceil$. The number of bits needed to specify the problem is $O(L)$. So, an efficient algorithm should have running time that is polynomial in L.

Order finding

Given co-prime integers $N > x > 0$, compute the order of x modulo N.

- Consider the operator U that has the following behaviour:

$$U|y\rangle \equiv \begin{cases} |xy \ (mod \ N)\rangle & \text{if } 0 \leq y \leq N-1 \\ |y\rangle & \text{if } N \leq y \leq 2^L - 1 \end{cases}$$

- Exercise: Show that U is unitary.

Order finding

Given co-prime integers $N > x > 0$, compute the order of x modulo N.

- Consider the operator U that has the following behaviour:

$$U|y\rangle \equiv \begin{cases} |xy \ (mod \ N)\rangle & \text{if } 0 \leq y \leq N-1 \\ |y\rangle & \text{if } N \leq y \leq 2^L - 1 \end{cases}$$

- Exercise: Show that U is unitary.
- Exercise: Show that the states defined by

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-(2\pi i)\frac{sk}{r}} \left| x^k \ (mod \ N) \right\rangle$$

are the eigenstates of U. Find the corresponding eigenvalues.

Order finding

Given co-prime integers $N > x > 0$, compute the order of x modulo N.

- Consider the operator U that has the following behaviour:

$$U|y\rangle \equiv \begin{cases} |xy \ (mod \ N)\rangle & \text{if } 0 \leq y \leq N-1 \\ |y\rangle & \text{if } N \leq y \leq 2^L - 1 \end{cases}$$

- Exercise summary: Let $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-(2\pi i)\frac{sk}{r}} \left|x^k \ (mod \ N)\right\rangle$ be an eigenstate of U. Then $U|u_s\rangle = e^{(2\pi i)\frac{s}{r}} |u_s\rangle$

End