

# COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

## Quantum Computation: Phase estimation

# 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  $\varphi$ .

- 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  $|0\dots 0\rangle$  (the value of  $t$  to be decided later), and
  - a register that begins in the state  $|u\rangle$ .

# Quantum Computation

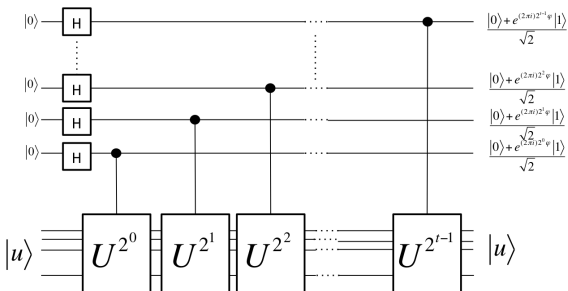
## Phase estimation

### Phase estimation

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

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

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



# 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  $\varphi$ .

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

# 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  $\varphi$ .

- 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  $\varphi$  may be expressed exactly as  $\varphi = [0 \cdot \varphi_1 \varphi_2 \dots \varphi_t]$ . Suggest a way to retrieve the value of  $\varphi$ ?
  - Taking the **inverse-fourier** transform and measuring the value of the first register in the computational basis gives  $\varphi$ .
- 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  $\varphi$  when measured.

# Quantum Computation

## Phase estimation

- 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  $\varphi$  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  $\varphi$  accurate to  $n$  bits with probability at least  $(1 - \varepsilon)$ .

# Quantum Computation

## Phase estimation

### Claim 2

It is sufficient to run the phase estimation technique with  $t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$  in order to obtain  $\varphi$  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  $\frac{b}{2^t} = [0 \cdot b_1 \dots b_t]$  is the best  $t$  bit approximation to  $\varphi$  that is less than  $\varphi$ . 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:

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



# Quantum Computation

## Phase estimation

### Claim 2

It is sufficient to run the phase estimation technique with  $t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$  in order to obtain  $\varphi$  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  $\frac{b}{2^t} = [0 \cdot b_1 \dots b_t]$  is the best  $t$  bit approximation to  $\varphi$  that is less than  $\varphi$ . 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  $\alpha_l$  be the amplitude of  $|(b+l) \bmod 2^t\rangle$ . Then 
$$\alpha_l = \frac{1}{2^t} \left( \frac{1 - e^{(2\pi i)(2^t\varphi - (b+l))}}{1 - e^{(2\pi i)(\varphi - (b+l)/2^t)}} \right) = \frac{1}{2^t} \left( \frac{1 - e^{(2\pi i)(2^t\delta - l)}}{1 - e^{(2\pi i)(\delta - l/2^t)}} \right).$$

# Quantum Computation

## Phase estimation

### Claim 2

It is sufficient to run the phase estimation technique with  $t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$  in order to obtain  $\varphi$  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  $\frac{b}{2^t} = [0 \cdot b_1 \dots b_t]$  is the best  $t$  bit approximation to  $\varphi$  that is less than  $\varphi$ . 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  $\alpha_l$  be the amplitude of  $|(b+l) \bmod 2^t\rangle$ . 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

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

# Quantum Computation

## Phase estimation

### Claim 2

It is sufficient to run the phase estimation technique with  $t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$  in order to obtain  $\varphi$  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  $\frac{b}{2^t} = [0 \cdot b_1 \dots b_t]$  is the best  $t$  bit approximation to  $\varphi$  that is less than  $\varphi$ . 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  $\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{(2\pi i)\varphi k} |k\rangle$  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  $\alpha_l$  be the amplitude of  $|(b+l) \bmod 2^t\rangle$ . 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

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

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

# 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  $\varphi$ .

- 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  $t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ , then the probability of measuring  $\varphi_u$  accurate to  $n$  bits at the end of the phase estimation procedure is at least  $|c_u|^2(1 - \varepsilon)$ .

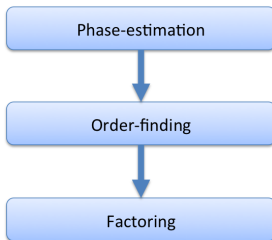
# Quantum Computation

## 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  $\varphi$ .

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



## Quantum Computation: Order finding

# Quantum Computation

Phase estimation  $\rightarrow$  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  $x^r = 1 \pmod{N}$ .
- Exercise: What is the order of 5 modulo 21?

# Quantum Computation

Phase estimation → 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  $x^r = 1 \pmod{N}$ .
- 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  $N$ ?



# Quantum Computation

Phase estimation  $\rightarrow$  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  $x^r = 1 \pmod{N}$ .
- 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?

# Quantum Computation

Phase estimation  $\rightarrow$  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  $x^r = 1 \pmod{N}$ .
- 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  $L$ .

# Quantum Computation

Phase estimation  $\rightarrow$  Order-finding

## 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:

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

- Exercise: Show that  $U$  is unitary.

# Quantum Computation

Phase estimation  $\rightarrow$  Order-finding

## 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:

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

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

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

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:

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

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

## 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:

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

- Exercise summary: Let  $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-(2\pi i) \frac{sk}{r}} |x^k \pmod{N}\rangle$  be an eigenstate of  $U$ . Then  $U|u_s\rangle = e^{(2\pi i) \frac{s}{r}} |u_s\rangle$
- Main idea for determining  $r$ : We will use **phase estimation** to get an estimate on  $\frac{s}{r}$  and then obtain  $r$  from it.

## 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:

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

- Exercise summary: Let  $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-i(2\pi) \frac{sk}{r}} |x^k \pmod{N}\rangle$  be an eigenstate of  $U$ . Then  $U|u_s\rangle = e^{i(2\pi) \frac{s}{r}} |u_s\rangle$
- Main idea for determining  $r$ : We will use **phase estimation** to get an estimate on  $\frac{s}{r}$  and then obtain  $r$  from it.
  - How do we implement controlled  $U^{2^j}$ ?
  - How do we prepare an eigenstate  $|u_s\rangle$ ?

### 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:

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

- Exercise summary: Let  $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-(2\pi i) \frac{sk}{r}} |x^k \pmod{N}\rangle$  be an eigenstate of  $U$ . Then  $U|u_s\rangle = e^{(2\pi i) \frac{s}{r}} |u_s\rangle$
- Main idea for determining  $r$ : We will use **phase estimation** to get an estimate on  $\frac{s}{r}$  and then obtain  $r$  from it.
  - How do we implement controlled  $U^{2^j}$ ? **Modular exponentiation**
  - How do we prepare an eigenstate  $|u_s\rangle$ ?



# Quantum Computation

Phase estimation  $\rightarrow$  Order-finding

## Modular exponentiation

Given  $|z\rangle |y\rangle$ , design a circuit that ends in the state  $|z\rangle |x^z y \pmod N\rangle$ .

- What we wanted to do was  $|z\rangle |y\rangle \rightarrow |z\rangle U^{z_1 2^{t-1}} \dots U^{z_1 2^0} |y\rangle$  but then this is the same as  $|z\rangle |x^z y \pmod N\rangle$ .
- Question: Suppose we work with the first register being of size  $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil = O(L)$ . What would be the size of the circuit?

# Quantum Computation

Phase estimation  $\rightarrow$  Order-finding

## Modular exponentiation

Given  $|z\rangle |y\rangle$ , design a circuit that ends in the state  $|z\rangle |x^z y \pmod N\rangle$ .

- What we wanted to do was  $|z\rangle |y\rangle \rightarrow |z\rangle U^{z_t 2^{t-1}} \dots U^{z_1 2^0} |y\rangle$  but then this is the same as  $|z\rangle |x^z y \pmod N\rangle$ .
- Question: Suppose we work with the first register being of size  $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\epsilon}) \rceil = O(L)$ . What would be the size of the circuit?  $O(L^3)$

### 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:

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

- Exercise summary: Let  $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-(2\pi i) \frac{sk}{r}} |x^k \pmod{N}\rangle$  be an eigenstate of  $U$ . Then  $U|u_s\rangle = e^{(2\pi i) \frac{s}{r}} |u_s\rangle$
- Main idea for determining  $r$ : We will use **phase estimation** to get an estimate on  $\frac{s}{r}$  and then obtain  $r$  from it.
  - How do we implement controlled  $U^{2^j}$ ? **Modular exponentiation**
  - How do we prepare an eigenstate  $|u_s\rangle$ ?
    - We work with  $|1\rangle$  as the first register since  $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$ .

# Quantum Computation

## Phase estimation $\rightarrow$ Order-finding

### 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:

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

- Exercise summary: Let  $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-(2\pi i) \frac{sk}{r}} |x^k \pmod N\rangle$  be an eigenstate of  $U$ . Then  $U|u_s\rangle = e^{(2\pi i) \frac{s}{r}} |u_s\rangle$
- Main idea for determining  $r$ : We will use **phase estimation** to get an estimate on  $\frac{s}{r}$  and then obtain  $r$  from it.
  - How do we implement controlled  $U^{2^j}$ ? **Modular exponentiation**
  - How do we prepare an eigenstate  $|u_s\rangle$ ?
    - We work with  $|1\rangle$  as the first register since  $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$ .
- So, we will argue that for each  $0 \leq s \leq r-1$ , we will obtain an estimate of  $\varphi \approx \frac{s}{r}$  accurate to  $2L+1$  bits with probability at least  $\frac{(1-\epsilon)}{r}$ .

# Quantum Computation

## Phase estimation $\rightarrow$ Order-finding

### 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:

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

- Exercise summary: Let  $|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-(2\pi i)\frac{sk}{r}} |x^k \pmod{N}\rangle$  be an eigenstate of  $U$ . Then  $U|u_s\rangle = e^{(2\pi i)\frac{s}{r}} |u_s\rangle$
- Main idea for determining  $r$ : We will use **phase estimation** to get an estimate on  $\frac{s}{r}$  and then obtain  $r$  from it.
  - How do we implement controlled  $U^{2^j}$ ? **Modular exponentiation**
  - How do we prepare an eigenstate  $|u_s\rangle$ ?
    - We work with  $|1\rangle$  as the first register since  $\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle$ .
- So, we will argue that for each  $0 \leq s \leq r-1$ , we will obtain an estimate of  $\varphi \approx \frac{s}{r}$  accurate to  $2L+1$  bits with probability at least  $\frac{(1-\epsilon)}{r}$ .
  - Question: How do we extract  $r$  from this? **Continued fractions**

# Quantum Computation

## Digression: Continued fractions

### Continued fraction

A finite simple continued fraction is defined by a collection of positive integers  $a_0, \dots, a_N$ :

$$[a_0, \dots, a_N] \equiv a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_N}}}}$$

The  $n^{\text{th}}$  convergent ( $0 \leq n \leq N$ ) of this continued fraction is defined to be  $[a_0, \dots, a_n]$ .

- Theorem: Suppose  $x \geq 1$  is a rational number. Then  $x$  has a representation as a continued fraction,  $x = [a_0, \dots, a_N]$ . This may be found by the **continued fraction algorithm**.
- Exercise: Find the continued fraction expansion of  $\frac{31}{13}$ .
- Question: What is the running time for the continued fractions algorithm for any given rational number  $\frac{p}{q} \geq 1$ ?

# Quantum Computation

## Digression: Continued fractions

### Continued fraction

A finite simple continued fraction is defined by a collection of positive integers  $a_0, \dots, a_N$ :

$$[a_0, \dots, a_N] \equiv a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_N}}}}$$

The  $n^{\text{th}}$  convergent ( $0 \leq n \leq N$ ) of this continued fraction is defined to be  $[a_0, \dots, a_n]$ .

- Question: What is the running time for the continued fractions algorithm for any given rational number  $\frac{p}{q} \geq 1$ ?
- Theorem: Let  $a_0, \dots, a_N$  be a sequence of positive numbers. Then  $[a_0, \dots, a_n] = \frac{p_n}{q_n}$ , where  $p_n$  and  $q_n$  are real numbers defined inductively by  $p_0 \equiv 0$ ,  $q_0 \equiv 1$ ,  $p_1 \equiv 1 + a_0 a_1$ ,  $q_1 \equiv a_1$ , and for  $2 \leq n \leq N$ ,

$$p_n \equiv a_n p_{n-1} + p_{n-2}$$

$$q_n \equiv a_n q_{n-1} + q_{n-2}$$

In the case when  $a_j$  are positive integers, so too are  $p_j$  and  $q_j$  and moreover  $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$  for  $n \geq 1$  which implies that  $\gcd(p_n, q_n) = 1$ .

End