Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 467 / Phys 767
C&O 481 / C&O 681

Lecture 6 (2005)

Richard Cleve
DC 3524
cleve@cs.uwaterloo.ca

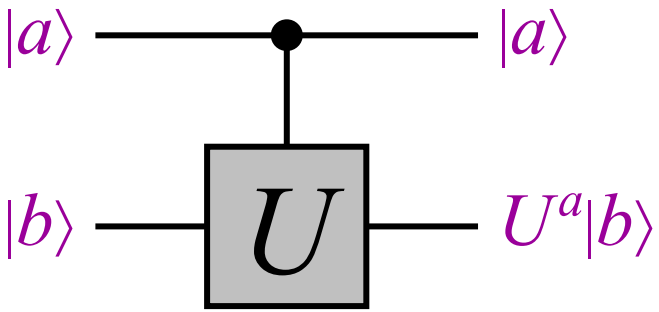
Course web site at:
http://www.cs.uwaterloo.ca/~cleve

Contents

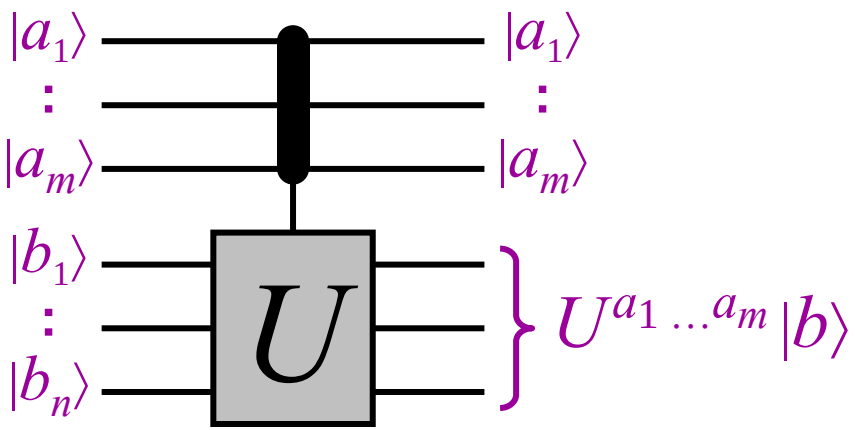
- Phase estimation problem
- Algorithm for the phase estimation problem
- Order-finding via phase estimation

- Phase estimation problem
- Algorithm for the phase estimation problem
- Order-finding via phase estimation

Generalized controlled-U gates



$$\begin{bmatrix} I & 0 \\ 0 & U \end{bmatrix}$$



$$\begin{bmatrix} I & 0 & 0 & \cdots & 0 \\ 0 & U & 0 & \cdots & 0 \\ 0 & 0 & U^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & U^{2^m-1} \end{bmatrix}$$

Example: $|1101\rangle|0101\rangle \rightarrow |1101\rangle U^{1101}|0101\rangle$

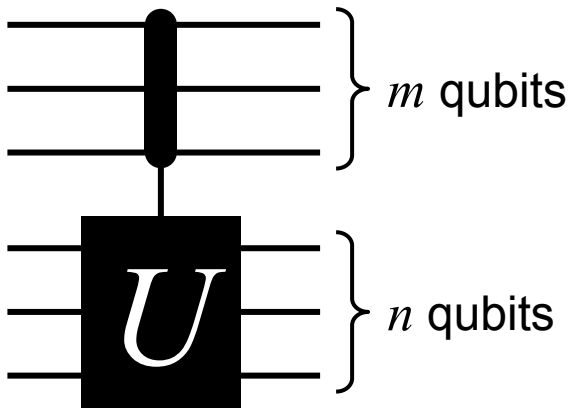
Phase estimation problem

U is a unitary operation on n qubits

$|\psi\rangle$ is an eigenvector of U, with eigenvalue $e^{2\pi i\phi}$

$(0 \leq \phi < 1)$

Input: black-box for



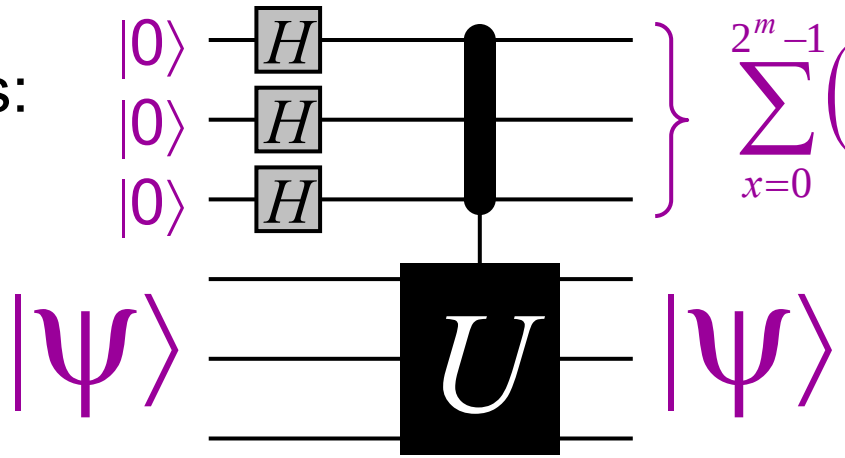
and a copy of $|\psi\rangle$

Output: ϕ (m-bit approximation)

- Phase estimation problem
- Algorithm for the phase estimation problem
- Order-finding via phase estimation

Algorithm for phase estimation (I)

Starts off as:



$$\sum_{x=0}^{2^m-1} \left(e^{2\pi i\phi}\right)^x |x\rangle$$

$|00\ldots0\rangle|\psi\rangle$

$|a\rangle|b\rangle \rightarrow |a\rangle U^a|b\rangle$

$\rightarrow (|0\rangle + |1\rangle)(|0\rangle + |1\rangle)\ldots(|0\rangle + |1\rangle)|\psi\rangle$

$= (|000\rangle + |001\rangle + |010\rangle + |011\rangle + \ldots + |111\rangle)|\psi\rangle$

$= (|0\rangle + |1\rangle + |2\rangle + |3\rangle + \ldots + |2^m - 1\rangle)|\psi\rangle$

$\rightarrow (|0\rangle + e^{2\pi i\phi}|1\rangle + (e^{2\pi i\phi})^2|2\rangle + (e^{2\pi i\phi})^3|3\rangle + \ldots + (e^{2\pi i\phi})^{2^m-1}|2^m-1\rangle)|\psi\rangle$

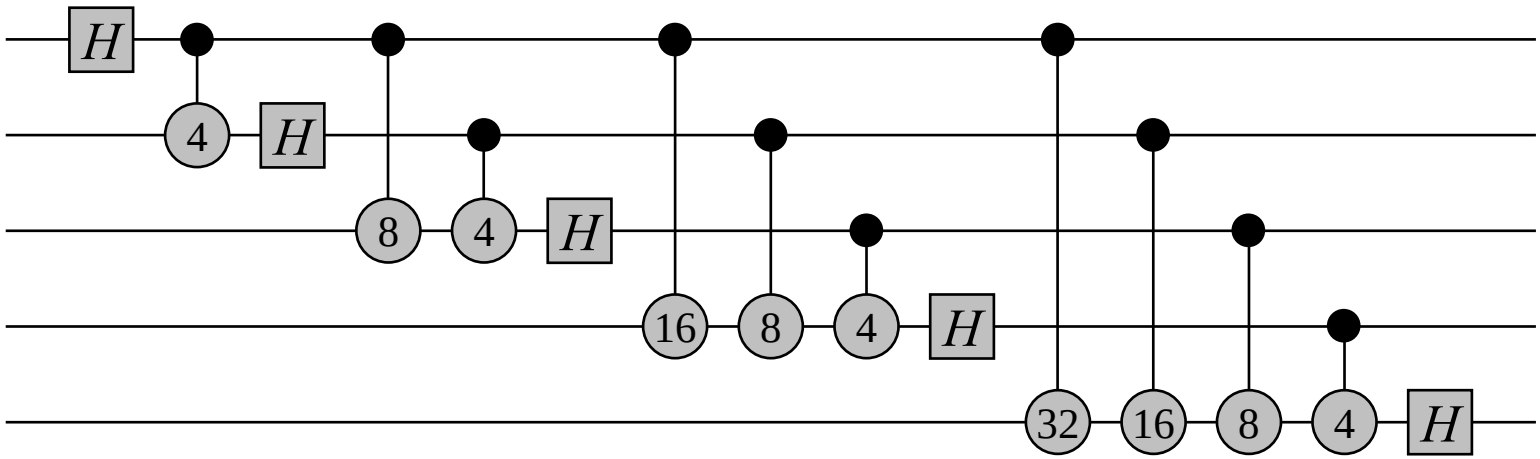
Quantum Fourier transform

$$F_N = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \omega^{3(N-1)} & \cdots & \omega^{(N-1)^2} \end{bmatrix}$$

where $\omega = e^{2\pi i/N}$ (for n qubits, $N = 2^n$)

Computing the QFT (I)

Quantum circuit for F_{32}:



reverse order

Gates: $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

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

For F_{2^n} costs $O(n^2)$ gates

Computing the QFT (II)

One way on seeing why this circuit works is to first note that

$$F_{2^n}|a_1 a_2 \ldots a_n\rangle$$

$$= (|0\rangle + e^{2\pi i \phi(0.a_n)}|1\rangle)\ldots(|0\rangle + e^{2\pi i \phi(0.a_2 \ldots a_n)}|1\rangle)(|0\rangle + e^{2\pi i \phi(0.a_1 a_2 \ldots a_n)}|1\rangle)$$

It can then be checked that the circuit produces these states (with qubits in reverse order) for all computational basis states $|a_1 a_2 \ldots a_n\rangle$

Exercise: (a) prove the above equation from the definition of the QFT; (b) confirm that the circuit produces these states

Algorithm for phase estimation (II)

$$F_{2^m}\left|a_1 a_2 \ldots a_m\right\rangle = \sum_{x=0}^{2^m-1}\left(e^{2\pi i/2^m}\right)^{(a_1 a_2 \ldots a_m)x}\left|x\right\rangle \quad = \sum_{x=0}^{2^m-1}\left(e^{2\pi i(0.\,a_1 a_2 \ldots a_m)x}\right)\left|x\right\rangle$$

Note: this is ***exactly*** the state generated by our preliminary algorithm for phase estimation when $\phi = 0.a_1 a_2 \ldots a_m$

Therefore, if $\phi = 0.a_1 a_2 \ldots a_m$ then applying $F^\dagger$ to this state yields $\left|a_1 a_2 \ldots a_m\right\rangle$ (from which ϕ can be deduced exactly)

What ϕ if is not of this nice form?

Example: $\phi = ⅓ = 0.0101010101010101\ldots$

- Phase estimation problem
- Algorithm for the phase estimation problem
- Order-finding via phase estimation

Order-finding algorithm (I)

Let M be an m-bit integer

Def: $\mathbf{Z}_M^* = \{x \in \{1,2,\ldots, M-1\} : \gcd(x,M) = 1\}$

$\mathbf{Z}_M^*$ is a ***group*** under multiplication modulo M

Example: $\mathbf{Z}_{21}^* = \{1,2,4,5,8,10,11,13,16,17,19,20\}$

For $a \in \mathbf{Z}_M^*$, consider all powers of a : a^0, a^1, a^2, a^3, …

Ex: For $a = 10$, the sequence is: 1, 10, 16, 13, 4, 19, 1, 10, 16, …

Def: $\mathrm{ord}_M(a)$ is the minimum $r > 0$ such that $a^r = 1 \pmod M$

Ex: $\mathrm{ord}_{21}(10) = 6$

Order-finding problem: given a and M, find $\mathrm{ord}_M(a)$

Order-finding algorithm (II)

Define: U (an operation on m qubits) as: $U|y\rangle = |a\,y \bmod M\rangle$

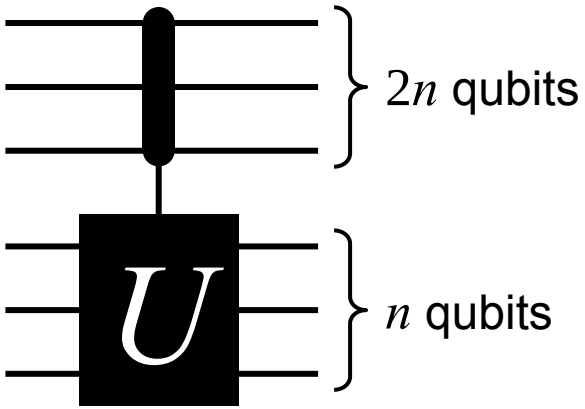
Define: $$|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} \left| a^j \bmod M \right\rangle$$

Then $$U|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} \left| a^{j+1} \bmod M \right\rangle$$

$$= \sum_{j=0}^{r-1} e^{2\pi i(1/r)} e^{-2\pi i(1/r)(j+1)} \left| a^{j+1} \bmod M \right\rangle$$

$$= e^{2\pi i(1/r)} |\psi_1\rangle$$

Order-finding algorithm (III)



corresponds to the mapping:

$|x\rangle|y\rangle \rightarrow |x\rangle|a^x y \bmod M\rangle$

Moreover, this mapping can be implemented with roughly $O(n^2)$ gates

The phase estimation algorithm yields a $2n$-bit estimate of $1/r$

From this, a good estimate of r can be calculated …

Problem: how do we construct state $|\psi_1\rangle$ to begin with?


THE END