Introduction to Quantum Information Processing

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

Lecture 7 (2005)

Richard Cleve
DC 3524
cleve@cs.uwaterloo.ca

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

Contents

- Recap of phase estimation problem/algorithm
- How the algorithm works for general phases
- Recap of the order-finding problem/algorithm
- How to bypass the need for an eigenstate

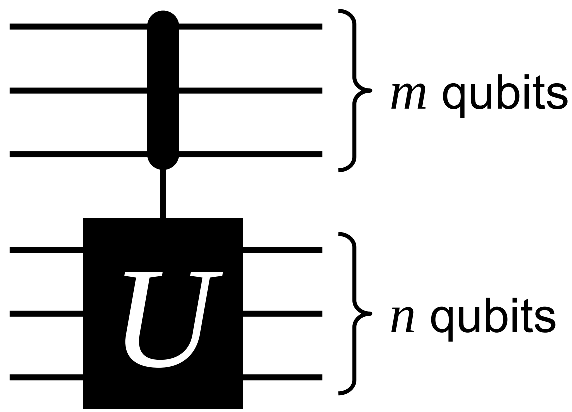
- Recap of phase estimation problem/algorithm
- How the algorithm works for general phases
- Recap of the order-finding problem/algorithm
- How to bypass the need for an eigenstate

Phase estimation problem

U is a unitary operation on n qubits

$|\psi\rangle$ is an eigenvector of U, with eigenvalue $e^{2\pi i\phi}$ $(0 \leq \phi < 1)$

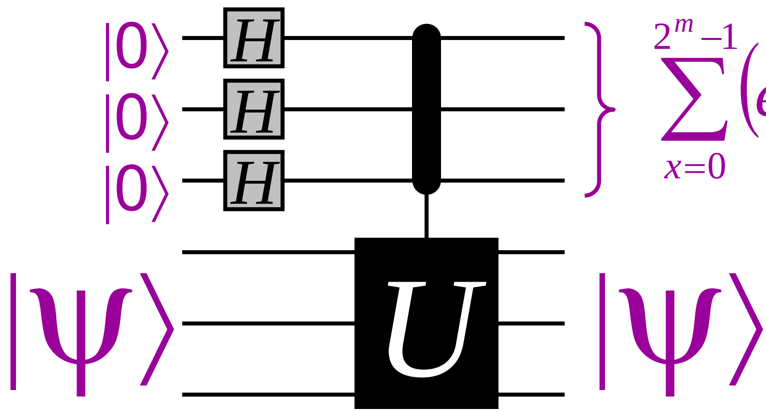
Input: black-box for



and a copy of $|\psi\rangle$

Output: ϕ (m-bit approximation)

Algorithm for phase estimation



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

When $\phi = 0.a_1a_2\ldots a_m$: $F_M|a_1a_2\ldots a_m\rangle = \sum_{x=0}^{2^m-1}\left(e^{2\pi i\phi}\right)^x|x\rangle$

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

Therefore, applying the ***inverse*** of F_M yields the digits of ϕ

- Recap of phase estimation problem/algorithm
- How the algorithm works for general phases
- Recap of the order-finding problem/algorithm
- How to bypass the need for an eigenstate

Arbitrary phases (I)

What if ϕ is not of the nice form $\phi = 0.a_1 a_2 \ldots a_m$?

Example: $\phi = ⅓ = 0.\underline{0101010101}010101\ldots$

Let's calculate what the previously-described procedure does:

Let $a/2^m = 0.a_1 a_2 \ldots a_m$ be an m-bit approximation of ϕ, in the sense that $\phi = a/2^m + \delta$, where $|\delta| \le 1/2^{m+1}$

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

$$= \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} e^{-2\pi i xy/2^m} e^{2\pi i\left(\frac{a}{2^m}+\delta\right)x} |y\rangle$$

$$= \frac{1}{2^m} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^m-1} e^{2\pi i(a-y)x/2^m} e^{2\pi i\delta x} |y\rangle$$

What is the amplitude of $|a_1 a_2 \ldots a_m\rangle$?

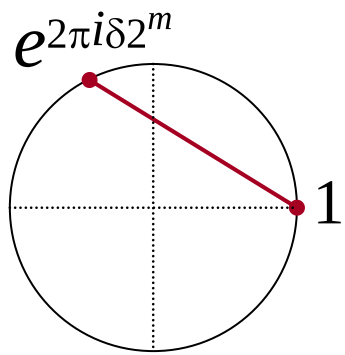
Arbitrary phases (II)

State is: $\frac{1}{2^m}\sum_{y=0}^{2^m-1}\sum_{x=0}^{2^m-1} e^{2\pi i(a-y)x/2^m} e^{2\pi i\delta x}|y\rangle$

geometric series!

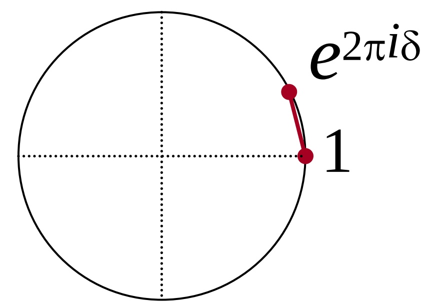
The amplitude of $|y\rangle$, for y = a is $\frac{1}{2^m}\sum_{x=0}^{2^m-1} e^{2\pi i\delta x} = \frac{1}{2^m}\frac{1-\left(e^{2\pi i\delta}\right)^{2^m}}{1-e^{2\pi i\delta}}$

Numerator:



lower bounded by $2\pi i\delta 2^m(2/\pi) > 4\delta 2^m$

Denominator:



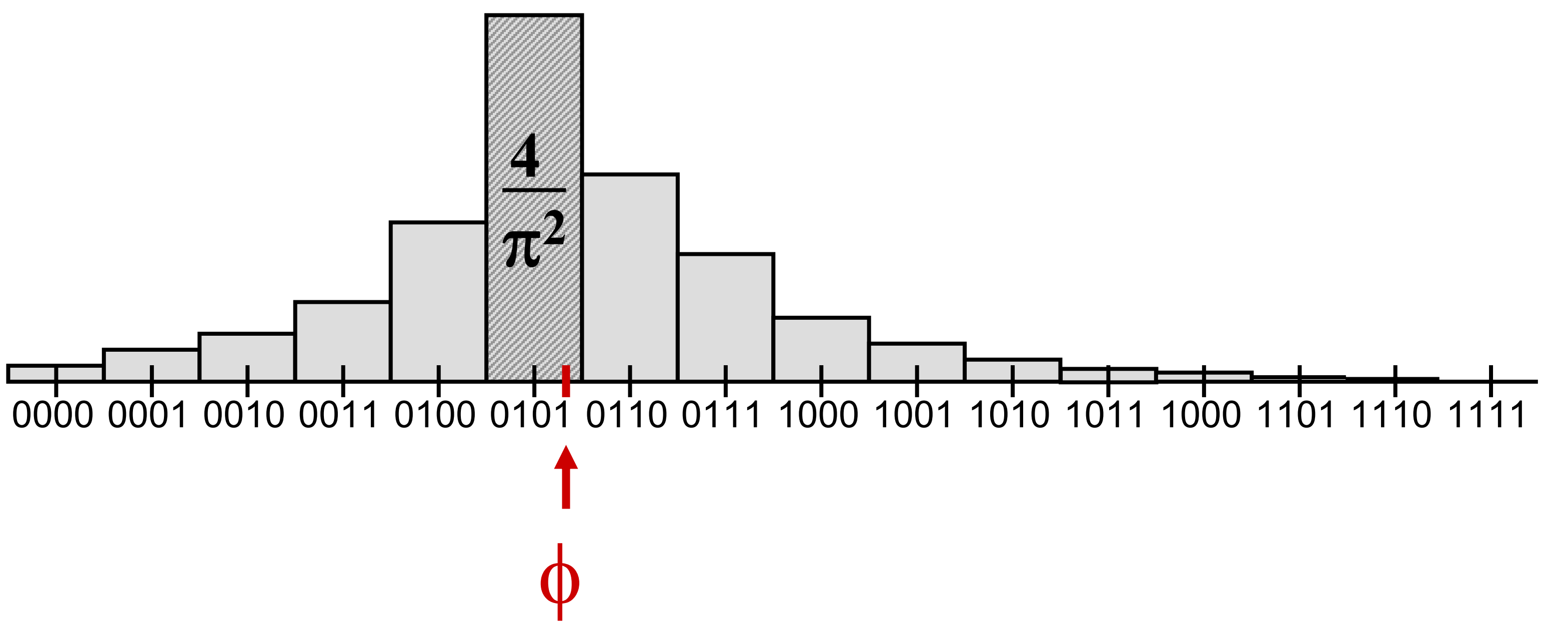
upper bounded by $2\pi\delta$

Therefore, the absolute value of the amplitude of $|y\rangle$ is at least the quotient of $(1/2^m)$(numerator/denominator), which is $2/\pi$

Arbitrary phases (III)

Therefore, the probability of measuring an m-bit approximation of ϕ is always at least $4/\pi^2 \approx 0.4$

For example, when $\phi = ⅓ = 0.\underline{0101}0101010101\ldots$, the outcome probabilities look roughly like this:



- Recap of phase estimation problem/algorithm
- How the algorithm works for general phases
- Recap of the order-finding problem/algorithm
- How to bypass the need for an eigenstate

Order-finding problem

Let M be an m-bit integer

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

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

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

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

The powers of 10 are: $1, 10, 16, 13, 4, 19, 1, 10, 16, \ldots$

Therefore, $\mathrm{ord}_{21}(10) = 6$

Order-finding algorithm (I)

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

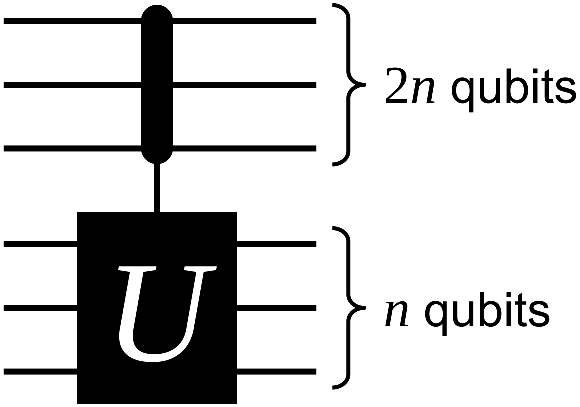
Define: $$|\psi_1\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(1/r)j} \left| a^j \bmod M \right\rangle$$

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 (II)



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 by taking the reciprocal, and rounding off to the nearest integer

Exercise: why are $2n$ bits necessary and sufficient for this?

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

- Recap of phase estimation problem/algorithm
- How the algorithm works for general phases
- Recap of the order-finding problem/algorithm
- How to bypass the need for an eigenstate

Bypassing the need for $|\psi_1\rangle$ (I)

Let

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

$$|\psi_2\rangle = \sum_{j=0}^{r-1} e^{-2\pi i(2/r)j} |a^j \bmod M\rangle$$

$$\vdots$$

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

$$\vdots$$

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

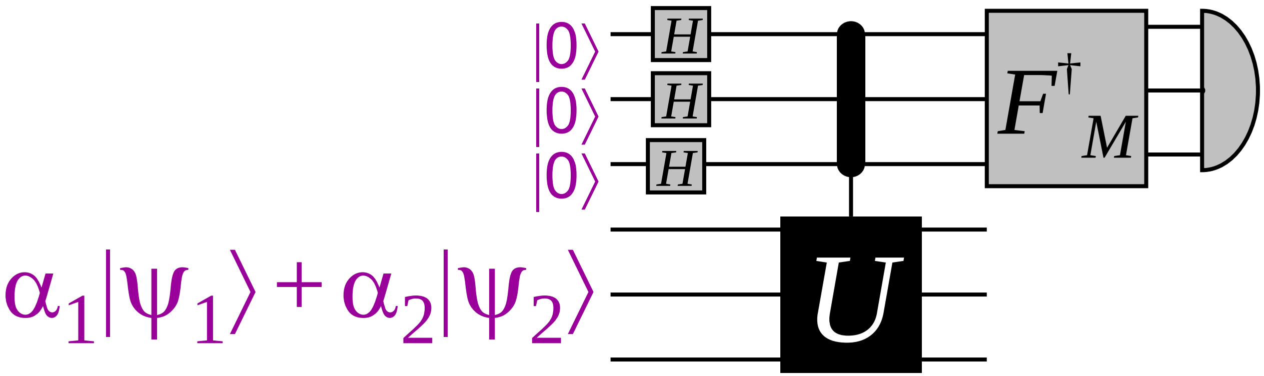
Can still uniquely determine k and r, provided they have no common factors (and $O(\log n)$ trials suffice for this)

Any one of these could be used in the previous procedure, to yield an estimate of k/r, from which r can be extracted

What if k is chosen randomly and kept secret?

Bypassing the need for $|\psi_1\rangle$ (II)

Returning to the phase estimation problem, suppose that $|\psi_1\rangle$ and $|\psi_2\rangle$ have respective eigenvalues $e^{2\pi i \phi_1}$ and $e^{2\pi i \phi_2}$, and that $\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle$ is used in place of an eigenvalue:



What will the outcome be?

It will be an estimate of $\begin{cases} \phi_1 \text{ with probability } |\alpha_1|^2 \\ \phi_2 \text{ with probability } |\alpha_2|^2 \end{cases}$

Bypassing the need for $|\psi_1\rangle$ (III)

Using the state

yields results equivalent to choosing a $|\psi_k\rangle$ at random

Is it hard to construct the state $\frac{1}{\sqrt{r}}\sum_{k=1}^{r}|\psi_k\rangle$?

In fact, it's easy, since

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

This is how the previous requirement for $|\psi_1\rangle$ is bypassed

THE END