Introduction to Quantum Information Processing
QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 8 (2017)

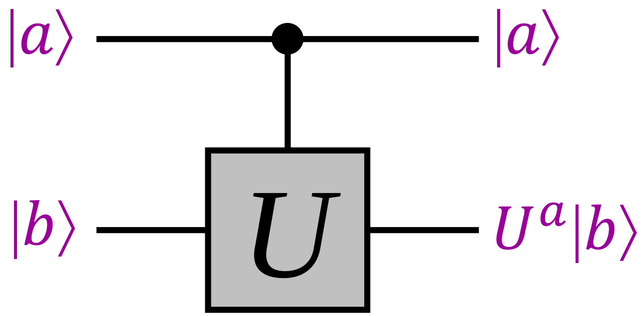
Jon Yard
QNC 3126
jyard@uwaterloo.ca
http://math.uwaterloo.ca/~jyard/qic710

Recap of:

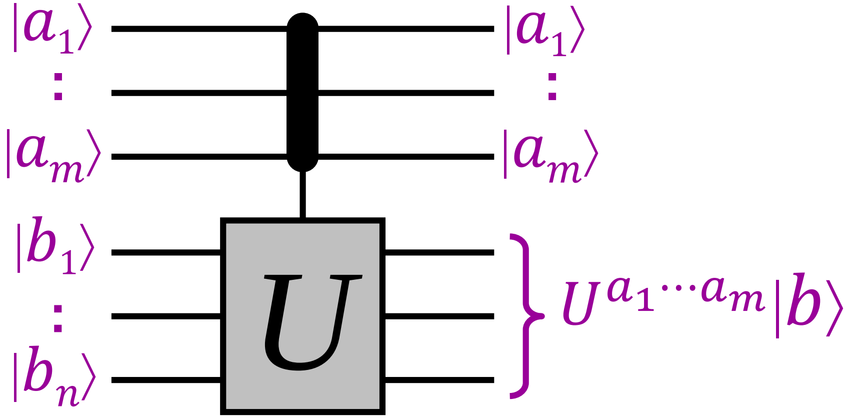
Eigenvalue estimation problem

(a.k.a. phase estimation)

Generalized controlled-U gates



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



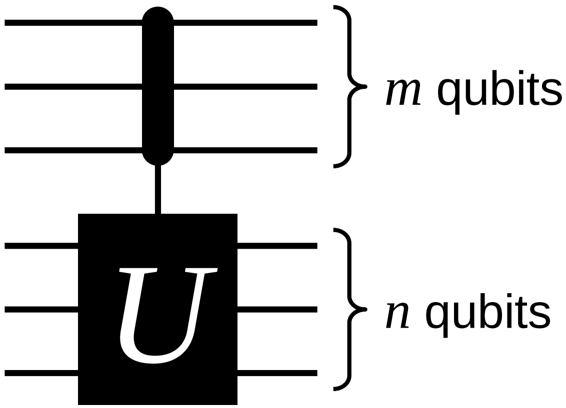
$$\begin{bmatrix} I & 0 & 0 & \cdots & 0 \\ 0 & U & 0 & \cdots & 0 \\ 0 & 0 & U^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & U^{2^m-1} \end{bmatrix}$$

Example: $|1101\rangle|0101\rangle \;\mapsto\; |1101\rangle U^{13}|0101\rangle$

Eigenvalue 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:
- one query to generalized controlled-U gate
- $O(n^2)$ auxiliary gates
- Success probability $4/\pi^2 \approx 0.4$

Note: with **$2m$-qubit** control gate, error probability is exponentially small

Order-finding via eigenvalue estimation

Order-finding problem

Let m be an n-bit integer

Def: $\mathbb{Z}_m^\times = \{x \in \{1,2,\ldots,m-1\} : \gcd(x,m) = 1\}$ a group (mult.)

Def: $\mathrm{ord}_m(a)$ is the minimum $r > 0$ such that $a^r \equiv 1 \bmod m$

Order-finding problem: given m and $a \in \mathbb{Z}_m^\times$ find $\mathrm{ord}_m(a)$

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

The powers of 5 are: $1, 5, 4, 20, 16, 17, 1, 5, 4, 20, 16, 17, 1, 5, \ldots$

Therefore, $\mathrm{ord}_{21}(5) = 6$

Note: no ***classical*** polynomial-time algorithm is known for this problem—it turns out that this is as hard as factoring

Order-finding algorithm (1)

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

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

Then

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

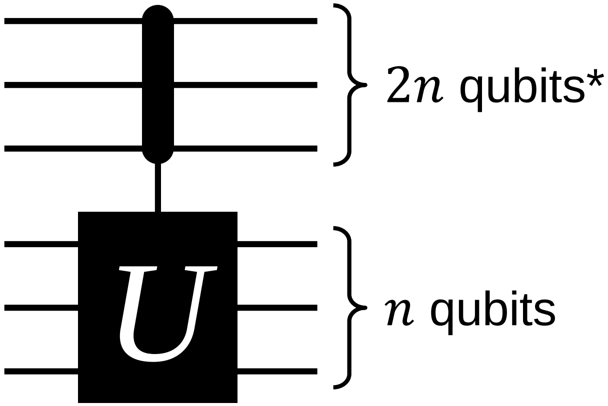
$$= \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi i(1/r)} e^{-2\pi i(1/r)(j+1)} |a^{j+1} \bmod m\rangle$$

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

Therefore $|\psi_1\rangle$ is an eigenvector of U.

Knowing the eigenvalue is equivalent to knowing $1/r$, from which r can be determined.

Order-finding algorithm (2)



Corresponds to the mapping $|x\rangle|y\rangle \mapsto |x\rangle|a^x y \bmod m\rangle$.

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

The eigenvalue estimation algorithm yields a $2n$-bit estimate of $1/r$ (using the above mapping and the state $|\psi_1\rangle$).

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?

Big problem: how do we construct $|\psi_1\rangle$ to begin with?

* We're now using m for the modulus and setting the number of control qubits to $2n$.

Bypassing the need for $|\psi_1\rangle$ (1)

Note: If we let

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

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

$$\vdots$$

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

$$\vdots$$

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

then ***any*** one of these could be used in the previous procedure, giving an estimate of k/r. Then $r = k(k/r)^{-1}$.

What if k is chosen randomly and kept secret?

Bypassing the need for $|\psi_1\rangle$ (2)

What if k is chosen randomly and kept secret?

Can ***still*** uniquely determine k and r from a $2n$-bit estimate of k/r, provided they have no common factors, using the ***continued fractions algorithm*.***

Note: If k and r have a common factor, it is impossible because, for example, $2/3$ and $34/51$ are indistinguishable

So this is fine as long as k and r are relatively prime …

* For a discussion of the *continued fractions algorithm*, please see Appendix A4.4 in [Nielsen & Chuang]

Bypassing the need for $|\psi_1\rangle$ (3)

What is the probability that k and r are relatively prime?

Recall that k is randomly chosen from $\{1, \ldots, r\}$.

The probability that this occurs is $\phi(r)/r$, where ϕ is ***Euler's totient function*** (defined as the cardinality of $\mathbb{Z}_r^\times$).

It is known that $\phi(r) = \Omega(r/\log\log(r))$, which implies that this probability is at least $\Omega(1/\log\log(r)) = \Omega(1/\log(n))$.

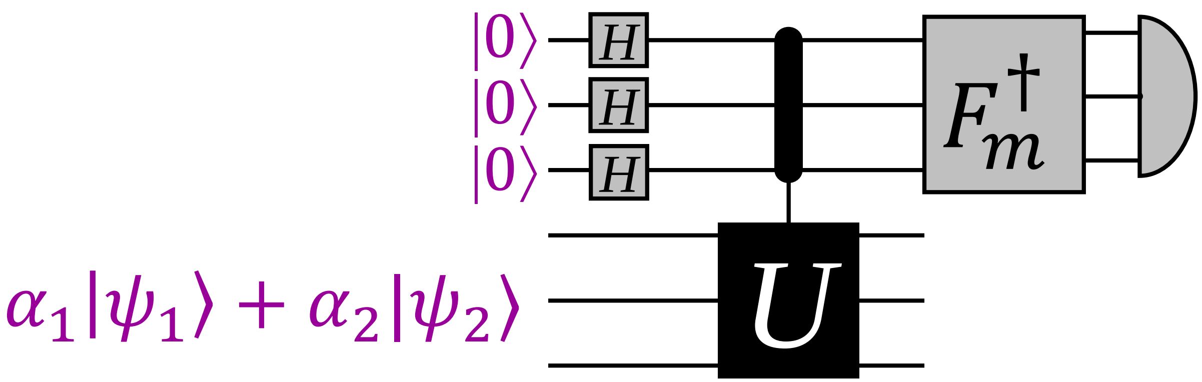
Therefore, the success probability is at least $\Omega(1/\log(n))$.

Is this good enough? Yes, because it means that the success probability can be amplified to any constant < 1 by repeating $O(\log n)$ times (so still polynomial in n).

But we'd still need to generate a random $|\psi_k\rangle$ here …

Bypassing the need for $|\psi_1\rangle$ (4)

Returning to the phase estimation problem, suppose that $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal, with 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 eigenvector:



What will the outcome of the measurement be?

It can be shown* that the outcome will be an estimate of

$$\begin{cases} \phi_1 \text{ with probability } |\alpha_1|^2 \\ \phi_2 \text{ with probability } |\alpha_2|^2 \end{cases}$$

* Showing this is straightforward, but not entirely trivial.

Bypassing the need for $|\psi_1\rangle$ (5)

Along these lines, the state $\frac{1}{\sqrt{r}}\sum_{k=1}^{r}|\psi_k\rangle$

yields the same outcome as using a random $|\psi_k\rangle$ (but not being given k), where each $k \in \{1, \ldots, r\}$ occurs with probability $1/r$.

This is a case that we've already solved.

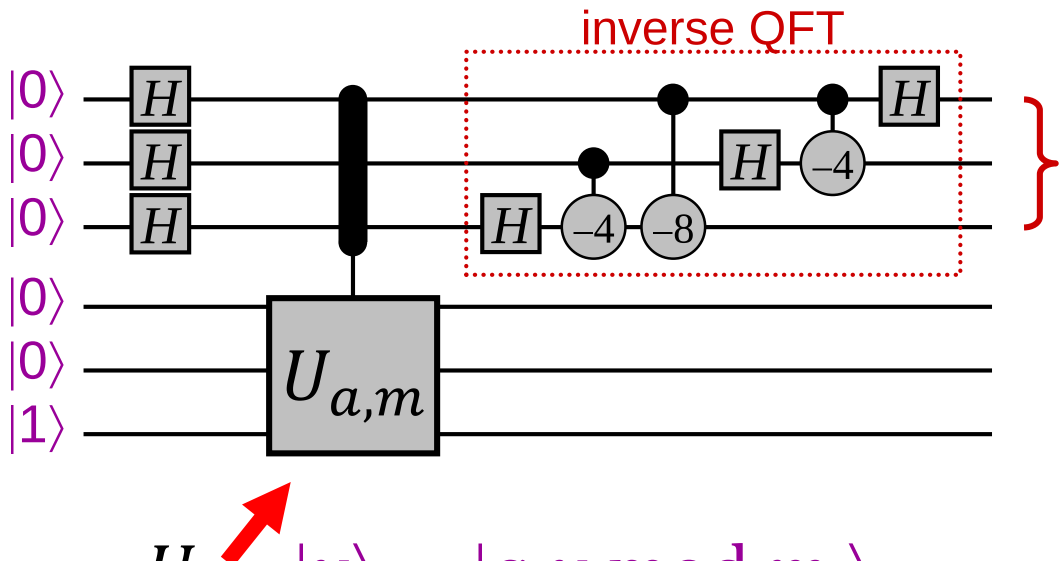
So now all we have to do is construct the state.

In fact, ***this*** is something that is easy, since

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

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

Quantum algorithm for order-finding



measure these qubits and apply continued fractions algorithm to determine a quotient, whose denominator divides r

$$U_{a,m}|y\rangle = |a\, y \bmod m\rangle$$

Number of gates for $\Omega(1/\log n)$ success probability is: $O(n^2 \log(n) \log\log(n))$

For ***constant*** success probability, repeat $O(\log n)$ times and take the smallest resulting r such that $a^r \equiv 1 \bmod m$

Reducing factoring to order finding

The integer factorization problem

Input: m (n-bit integer; we can assume it is composite)

Output: $h, h' > 1$ such that $hh' = m$.

Note 1: no efficient (polynomial-time) classical algorithm is known for this problem.

Note 2: given any efficient algorithm for the above, we can recursively apply it to fully factor m into primes efficiently.

Note 3: $\exists$ polynomial-time classical algorithms for primality testing:

- Miller-Rabin - randomized
- Agrawal–Kayal–Saxena (AKS) - deterministic, but slower
- `sage: is_prime(m)` uses PARI implementation of ECPP (Elliptic Curve Primality Proving) - randomized and faster

Factoring prime-powers

There is a straightforward efficient ***classical*** algorithm for recognizing and factoring numbers of the form $m = p^k$, for some (unknown) prime p.

What is this algorithm?

Hint: If in fact $m = p^k$, then $k \leq \log_2 m \leq n$.

Therefore, the interesting remaining case is where m has at least two distinct prime factors.

Numbers other than prime-powers

Problem. Given odd composite $m \neq p^k$, compute nontrivial divisor h of m.

Proposed quantum algorithm (repeatedly do):

1. randomly choose $a \in \{2, 3, \dots, m-1\}$
2. compute $h = \gcd(a, m)$
3. **if** $h > 1$ **then**
   output $h, m/h$
   else
   compute $r = \text{ord}_m(a)$ (quantum part)
   if r is even **then**
   compute $x = a^{r/2} - 1 \bmod m$
   compute $h = \gcd(x, m)$
   if $h > 1$ **then** output $h, m/h$

Analysis

Assume we find an a with $r = \text{ord}_m(a)$ even.

This means $m \mid a^r - 1$.

So $m \mid (a^{r/2} + 1)(a^{r/2} - 1)$.

Thus, either $m | a^{r/2} + 1$ or $\gcd(a^{r/2} - 1, m)$ is a nontrivial divisor of m.

At least half (actually a $1 - 2^{-\#\text{odd prime factors of } m}$ fraction) of the $a \in \{2, 3, \dots, m-1\}$ have $\text{ord}_m(a)$ even and result in $\gcd(a^{r/2} - 1, m)$ being a nontrivial divisor of m (see Shor's 1995 paper for details).