Introduction to Quantum Computing
Fall 2023, Peking University

Lecturer: Tongyang, scribed by Shuo Zhou, Yexin Zhang
Date: October 20, 2023

Lecture 7

Order Finding and Shor's Algorithm

- Order finding
- Shor's algorithm

1 Recap & Preview

Our course so far:

- Basics: Quantum states, dynamics(circuits), measurements...
- Introduction to quantum algorithms:

First idea : Use uniform superposition, i.e., Hadamard transform

$$|x\rangle \overset{H^{\otimes n}}{\longmapsto} \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle$$

Deutsch-Jozsa
$f : \{0,1\}^n \longmapsto \{0,1\}$
constant or balanced.

Q: 1 query;
C: $2^{n-1}+1$ queries. or $(O(\log\frac{1}{\epsilon}))$ randomly.

Simon's problem
$f : \{0,1\}^n \longmapsto X$.
$f(x) = f(y)$ iff $x = y$ or $x = y \otimes s$.

Q: $O(n)$ query (w.h.p.);
C: $\Theta(2^{n/2})$ queries. even with randomized algorithm.
Less requirement than Deutsch-Jozsa but still structured.

Phase estimation
$U|\psi\rangle = e^{i\theta}|\psi\rangle$.
Find θ.

$O(1/\epsilon)$ queries, w.p. $\geq \frac{8}{\pi^2}$.
Techinque: Quantum Fourier transform.

Now, having a new tool: QFT^{-1}. What can we do?
In mathematics, Fourier transform is applied to periodic functions:

Technique		Problem		Applications
Quantum Fourier transform(QFT)	$\longmapsto$	Period finding		
		(in number theroy)		
		$\downarrow$		
		Order finding	$\longmapsto$	Shor's algorithm

2 Order finding

Order definition: The order of an integer a modulo N is the smallest integer such that:

$$a^r \equiv 1 \pmod N.$$

For example: $N = 15, a = 2$: $2^1 \equiv 2 \pmod{15}, 2^2 \equiv 4 \pmod{15}, 2^3 \equiv 8 \pmod{15}, 2^4 \equiv 1 \pmod{15}$ thus $r = 4$.

The order only exists if $\gcd(a, N) = 1$. gcd= greatest common divisor

Proof. When gcd > 1: $\exists$ prime p, $p|a$, $p|N$. $p|a^r - N \Rightarrow p|1$. On the other hand, by Euler's theorem: if $\gcd(\mathrm{a,N}) = 1$, $\exists\, r$, $a^r \equiv 1 \pmod N$. □

Consider the multiplication-by-a map: $U\,|x\rangle = |ax\rangle$ for $x \in \mathbb{Z}_N$.
$\gcd(a, N) = 1 \Rightarrow \exists\, b \in \mathbb{Z}_N$ s.t.$a \cdot b \equiv 1 \pmod N$. We can do this efficiently:

$$|x, 0\rangle \overset{\text{mutiply by a}}{\longmapsto} |x, ax\rangle \overset{\text{swap}}{\longmapsto} |ax, x\rangle \overset{\text{substract 2nd register by } b \text{ times 1st}}{\longmapsto} |ax, 0\rangle$$

What are the eigenvectors/eigenvalues of U?
Let P be a cyclic shift modulo $r(\mathbb{Z}_r)$: $P\,|x\rangle = |x + 1 \bmod r\rangle$.
Isomorphism: $x \bmod r \longleftrightarrow a^x \bmod N$
addition $\longleftrightarrow$ multiplication
Eigenvectors of P: $\forall k \in \{0, \cdots, r-1\}$

$$|\tilde{k}\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{\frac{2\pi i k x}{r}} |x\rangle \quad P|\tilde{k}\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{\frac{2\pi i k x}{r}} |x+1\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{\frac{2\pi i k}{r}(x-1)} |x\rangle = e^{-\frac{2\pi i k}{r}} |\tilde{k}\rangle.$$

About U: Therefore, $|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{x=0}^{r-1} e^{\frac{2\pi i k x}{r}} \mid a^x \bmod N\rangle$ is an eigenvector of U with eigenvalue $e^{\frac{-2\pi i k}{r}}$.
Applying phase estimation of U on $|u_k\rangle$, we get an estimation of $\frac{k}{r}$.

Problems:

1. We don't know r, and as a result, how can we make $|u_k\rangle$?
2. We only get an approximation of $\frac{k}{r}$; which precise fraction it is?
3. What if k and r have common factors? Since we don't know r, can confuse with factor cancellation.

Issue(intuition)	Issue(precise)	Solution
Don't know which state to use	How to make $\lvert u_k\rangle$	Apply phase estimation on uniform superposition $\Rightarrow$ uniformally random k
Output is imprecise	How to recover $\frac{k}{r}$ by its approximation	continous fraction expansion (CFE) with sufficiently procision
Not being coprime ruins the algorithms	Need to have $\gcd(k, v) = 1$	promised by the property of Euler's totient function

2.1 Estimate $\frac{k}{r}$ in superposition

For any $n \geqslant 2$, if $w = e^{\frac{2\pi i}{n}}$, $\quad 1 + w + \cdots + w^{n-1} = \frac{w^n - 1}{w-1} = 0$.

Consider

$$\begin{aligned}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle &= \frac{1}{r}\sum_{k=0}^{r-1}\sum_{x=0}^{r-1} e^{\frac{2\pi i k x}{r}} \mid a^x \bmod N\rangle \\ &= \frac{1}{r}\sum_{x=0}^{r-1}\sum_{k=0}^{r-1} e^{\frac{2\pi i k x}{r}} \mid a^x \bmod N\rangle \\ &= \frac{1}{r}\cdot r \mid a^0 \bmod N\rangle \ = |1\rangle\end{aligned}$$

Phase estimation (with precision n):

$$|0^n\rangle \otimes |1\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|0^n\rangle \otimes |u_k\rangle \overset{\text{phase estimation}}{\longmapsto} \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\widetilde{k|r}\rangle \otimes |u_k\rangle$$

Measuring the first register gives an estimate of $\frac{k}{r}$, where k is chosen uniformly at random.
Note: $c - U^{2^n}$ can be implemented in time poly (n) by square-and-multiply.

2.2 Reconstructing $\frac{k}{r}$ from the approximation

Main idea: We can have an integer y close to $k \cdot \frac{2^n}{r}$ (either $\left\lfloor k \cdot \frac{2^n}{r}\right\rfloor$ or $\left\lceil k \cdot \frac{2^n}{r}\right\rceil$ with probability $\geqslant \frac{8}{\pi^2}$).
Compute the continuous fraction expansion (CFE) : $\frac{y}{2^n} = \frac{1}{a_1 + \frac{1}{a_2 + \cdots}} \quad a_1, a_2 \in \mathbb{N}$

For example: $\frac{5}{8} = \frac{1}{1.6} = \frac{1}{1+0.6} = \frac{1}{1+\frac{1}{5/3}} = \frac{1}{1+\frac{1}{1+2/3}} = \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{2}}}} = \frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+1}}}}$

Each time, deleting the term in $(0,1]$, get: $\frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}$. End when we reach 1 .
Consider the sequence $\frac{1}{a_1}, \frac{1}{a_1+\frac{1}{a_2}}, \ldots$ (truncate the CFE).
Since $\frac{y}{2^n}$ is rational, this must ends finally. Denote the sequence of fractions we get ane $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$
Can prove: $q_{i+2} \geqslant 2q_i \quad \forall i \in [n]$. This implies that the length $\leqslant 2n$.
Furthermove, CFE has very strong convengence property:
Fact. If we estimate x by CFE, then $\left|x - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2}$.
In our case, we know $\left|y - k \cdot \frac{2^n}{r}\right| \leq 1 \Leftrightarrow \left|\frac{y}{2^n} - \frac{k}{r}\right| \leq \frac{1}{2^n}$.
Taking n such that $2^n > 2r^2$ and using CFE theory, we can prove that $\frac{k}{r}$ must appear in the CFE. Also due to the CFE has $O(n)$ terms and whether $a^r \equiv 1 \pmod N$ or not can be verified in poly $(\log N)$ time using square-and-multiply.

As a result, taking $n = C \cdot \log N$ for a large enough C, $2^n > 2r^2$ can be satisfied the overall cost is poly $(\log N)$.

2.3 Common factors

Although phase estimation works for any $k \in \{0, 1, \cdots, r-1\}$, only when $\gcd(k,r) = 1$. the denominator of $\frac{k}{r}$ is directly r.

Euler's totient function: If $N = p_1^{\alpha_1} \ldots p_l^{\alpha_l}$ for different primes $p_1, \cdots, p_l, \alpha_1, \cdots, \alpha_l \in \mathbb{N}$, then $\phi(N) := \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_N}\right) N$ is the number of integers in [N] that has gcd $= 1$ with N.

Fact: $\frac{\phi(r)}{r} = \Omega\left(\frac{1}{\log(\log r)}\right)$. (Also by Fermat's Little Theorem, $a^{\phi(N)} \equiv 1 \pmod N$)

Therefore, $O(\log \log r)$ repititions suffice.

Conclusion: Quantum computing can solve order finding with cost $\operatorname{poly} \log(N)$ with high probability.

Finally, it comes to Shor's algorithm:

3 Shor's algorithm

3.1 Factorization(N)

Input: N (WLOG, N is composite). Output: A non-trivial factoe of N.

1. If N is even, return factor 2 ;
2. If $N=p^{\alpha}$ for a prime $p \geq 3$ and $\alpha \geqslant 2$, compute the 2nd (square) root, 3rd, $\cdots$, $\lceil\log_2 N\rceil$ root, and return one of them being an integer;
3. Uniformly randomly choose x in $\{1,2,\ldots,N-1\}$. If $\gcd(x, N)>1$, then return factor $\gcd(x, N)$;
4. Use the order-finding subroutine to find the order r of x, modulo N;
5. If r is even and $x^{r/2} \neq -1 \pmod N$, compute $\gcd\left(x^{r/2}-1, N\right)$ and $\gcd\left(x^{r/2+1}, N\right)$. If one of them >1, return that. Otherwise, start over.