5.3 Applications: order-finding and factoring

Phase estimation is useful! (5.2.1)

Recall: 'Spose unitary operator U has eigenvector $|u\rangle$ with eigenvalue $e^{2\pi i \varphi}$ where φ unknown. Goal of Phase est. is to estimate φ.

Algo: Quantum Phase Estimation

Input: (1) Black box performing controlled U^j operation for $j \in \mathbb{Z}$,
(2) eigenstate $|u\rangle$ of U with eigenvalue $e^{2\pi i \varphi_u}$, and
(3) $t = n + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ qubits initialized to $|0\rangle$
(depends on # of digits of accuracy, and with what probability our estimation will be successful)

Output: n-bit approximation of $\tilde{\varphi}_u$ to φ_u.

Runtime: $O(t^2)$ operations + one call to U^j black box. Succeeds w/ prob. $\geq 1 - \varepsilon$.

(1) $|0\rangle|u\rangle$ initialize state

(2) $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t - 1} |j\rangle|u\rangle$ create superposition

(3) $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j |u\rangle$ apply black box

$$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \boxed{\varphi_u}} |j\rangle |u\rangle$$

(4.) $\rightarrow |\tilde{\varphi}_u\rangle |u\rangle$ apply inverse fourier transform

(5.) $\rightarrow \tilde{\varphi}_u$ measure first register

Exciting part is the applications!

Carrying on with 5.3 ...

Can use phase estimation for order-finding problem and for factoring problem. (They're equivalent)

Step Back for a moment. Why does this matter?

- Serious evidence that quantum more powerful than classical, and potentially credible case against Church-Turing thesis.
- Just intrinsically worthy problems anyways.
- Practically, can break RSA encryption

Order Finding: For positive $x, N \in \mathbb{Z}$, $x < N$, with no common factors, the problem is to find the order of x in $\mathbb{Z}_n$ (ring). In other words, what is the least positive r s.t. $x^r = 1 \pmod N$?

Classical: Hard problem, requiring polynomial resources in the $O(L)$ bits needed to specify problem where $L \equiv \lceil \log(N) \rceil$ is # of bits needed to specify N.

Ex.) What's the order of 5 in $\mathbb{Z}_{21}$? $5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5$

Quantum: Just phase estimation algo with unitary operator:

$$U|y\rangle \equiv |xy \pmod N\rangle$$

A little bit of work shows us that the states defined by

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^k \bmod N\rangle,$$

for integer $0 \le s \le r-1$ are eigenstates of U, since

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left[\frac{-2\pi i s k}{r}\right] |x^{k+1} \bmod N\rangle$$

$$= \exp\left[\frac{2\pi i s}{r}\right] |u_s\rangle$$ → which can give us r out of $\exp(2\pi i s/r)$ with minimal work from there,

(using phase estimation procedure)

To do that though, we have 2 requirements:

1.) Must efficiently implement controlled-U^{2^j} operation for any $j \in \mathbb{Z}$,

2.) Must efficiently prepare eigenstate $|u_s\rangle$ with nontrivial eigenvalue

For 1.) $\rightarrow$ can do "modular exponentiation" using $O(L^3)$ gates

(see pg 228 if interested)

For 2.) $\rightarrow$ trickier, since preparing $|u_s\rangle$ requires we know r.

However, it must be that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle.$$

Then, we can use phase estimation with first register as

$t = 2L+1+\lceil \log(2+\frac{1}{2\epsilon}) \rceil$ and second register as just $|1\rangle$,

Can estimate the phase $\varphi \approx s/r$ accurate to $2L+1$ bits w/

prob. $\geq (1-\epsilon)/r$

This gives an estimate $\varphi \approx s/r$, but φ is just an estimate.

But we know that φ is rational. Thus, if we can compute nearest

fraction to φ, we might obtain r.

Can do this with continued fractions algorithm!

So, <u>cont'd fractions algo:</u>

Goal is to describe real #'s using integers alone, using expressions of the form $\underbrace{[a_0, \dots, a_m]}$ = $\underbrace{a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{a_m}}}}}$

Spose we try $\boxed{31/13.}$

Just split 'em up!

$$\frac{31}{13} = 2 + \frac{5}{13}$$

$$= 2 + \frac{1}{\frac{13}{5}}$$

$$= 2 + \underbrace{\frac{1}{2 + \frac{3}{5}}} = 2 + \underbrace{\frac{1}{2 + \frac{1}{\frac{5}{3}}}} = 2 + \underbrace{\frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}}}$$

$$= \underbrace{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{2}}}}}.$$

$L = \lceil \log N \rceil$

→ uses $O(L^3)$ operations
- $O(L)$ "split & invert", using $O(L^2)$ gates for basic arithmetic.

Can the quantum order-finding algo fail?

No. It's complicated, but no. see pg $\boxed{229, 231}$ for the nitty gritty details of it all.

At long last: $x^r \equiv 1 \bmod N$ what's r?

Quantum Order Finding Algorithm:

In: (1) Black box $U_{x,N}$ performing $|j\rangle|k\rangle \to |j\rangle|x^j k \bmod N\rangle$, for x co-prime to L-bit number N.

(2) $t = 2L + 1 + \lceil \log(2 + \frac{1}{2\varepsilon}) \rceil$ qubits initialized to $|0\rangle$

(3) L qubits initialized to $|1\rangle$.

Out: The least integer $r > 0$ s.t. $x^r \equiv 1 \pmod N$.

Runtime: $O(L^3)$ operations, succeeds w/ probability $O(1)$.

1.) $|0\rangle|1\rangle$ initial state.

2.) $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|1\rangle$ create superposition.

3.) $\to \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|x^j \bmod N\rangle$ apply $U_{x,N}$

$\approx \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi i s j/r} |j\rangle|u_s\rangle$

4.) $\to \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\widetilde{s/r}\rangle |u_s\rangle$ apply inverse fourier transform

5.) $\to \widetilde{s/r}$ measure 1st register

6.) $\to r$ measure 2nd register

Factoring: turns out to be equivalent to order-finding

Reduction: 1.) We can compute factor of N if we can find non-trivial $x \not\equiv \pm 1 \bmod N$ solution to $x^2 = 1 \bmod N$.

2.) randomly chosen y co-prime with N has order r (likely to be even) and s.t. $y^{r/2} \not\equiv 1 \bmod N$ and thus $x \equiv y^{r/2} \bmod n$ is non-trivial soln to $x^2 = 1 \bmod N$.

Reduction Algo:

In: composite number N

Out: non-trivial factor of N.

Runtime: $O((\log N)^3)$ operations, succeeds w/ probability $O(1)$.

Algo:

1.) If N even, return 2

2.) If $N = a^b$ for $a \geq 1$ and $b \geq 2$, return a

3.) Randomly choose x in range 1 to $N-1$.
If $GCD(x, N) > 1$, return $GCD(x, N)$

4.) Use order-finding subroutine to find order r of $x \bmod N$

5.) if r is even and $x^{r/2} \neq -1 \pmod N$ then compute $\gcd(x^{r/2}-1, N)$ and $\gcd(x^{r/2}+1, N)$. If one of these is non-trivial factor, return it.

Else, algorithm fails.

(pf on pg 234 if helpful)

5.4 Additional Applications

Hidden Subgroup Problem - encompasses all known 'exponentially fast' applications of quantum fourier transform.

Generalization of finding unknown period of a periodic function, where structure of domain & range may be intricate.

Specific instances:

- Period-finding of a 1-Dim. function
- Discrete logarithms

Period-finding:

'Spose f is a periodic function producing a single bit as output s.t. $f(x+r) = f(x)$ for unknown $0 < r < 2^L$, where $x, r \in \{0, 1, 2, \ldots\}$.

Given a quantum black box U performing $U|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$ (where $\oplus$ denotes + mod 2), how many black box queries and other operations needed to determine r?

Algo that does it in one query with $O(L^2)$ operations otherwise.

Period finding Algo:

Inputs: (1) a black box performing operation $U|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$,

(2) a state to store function evaluation, initialized to $|0\rangle$

(3) $t = O(L + \log(1/\varepsilon))$ qubits initialized to 0.

Out: The least integer $r > 0$ s.t. $f(x+r) = f(x)$

Runtime: One use of U, $O(L^2)$ operations. Succeeds w/ probability $O(1)$.

Procedure:

1.) $|0\rangle|0\rangle$ initial state

2.) $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|0\rangle$ create superposition

3.) $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{x=0}^{2^t-1} |x\rangle|f(x)\rangle$ apply U.

$$\approx \frac{1}{\sqrt{r2^t}} \sum_{l=0}^{r-1} \sum_{x=0}^{2^t-1} e^{2\pi i l x/r} |x\rangle|\hat{f}(l)\rangle$$

4.) $\rightarrow \frac{1}{\sqrt{r}} \sum_{l=0}^{r-1} |\widetilde{l/r}\rangle|\hat{f}(l)\rangle$ apply inverse Fourier to 1st register.

5.) $\rightarrow \widetilde{l/r}$ measure 1st register

6.) r rational $\frac{31}{13}$ apply cont'd fractions algo.

5.4.2 Discrete Logarithms

What happens when function is more complex?

Take $f(x_1, x_2) = a^{sx_1 + x_2} \bmod N$, and find r s.t. $a^r \bmod N = 1$

- Periodic since $f(x_1 + l, x_2 - ls) = f(x_1, x_2)$
- Period is 2-tuple $(l, -ls)$ for $l \in \mathbb{Z}$.
- Useful in cryptography
- Solvable in only one query of a quantum black box U and $O(\lceil \log r \rceil^2)$ other operations.
- Algorithm is messy and complicated, but takes exact same general form as before.

1.) Initialize 3 qubits to $|0\rangle$
2.) Create superposition with 2 of them
3.) Apply U (complicated) and find some meaningful equality for inverse Fourier transform
4.) Apply inverse Fourier transform to first two registers
5.) Measure first two registers
6.) Apply generalized cont'd fractions algo.

5.4.3 The Hidden Subgroup Problem

A pattern is emerging - if given a periodic function, even a complicated one, can use quantum algos like the above to efficiently determine the period. But not all periods of periodic functions can be determined.

General problem:

Let f be a function from finitely generated group G to a finite set X such that f is constant on the cosets of a subgroup K, and distinct on each coset. Given a quantum black box performing the unitary $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$ for $g \in G$, $h \in X$, and $\oplus$ the appropriate binary operation on X, Find a generating set for K.

Takeaways of Chapter 5:

1] When $N = 2^n$, the quantum Fourier transform

$$|j\rangle = |j_1, \ldots, j_n\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{N}} |k\rangle$$

can be written

$$|j\rangle \to \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle\right) \ldots$$

$$\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n} |1\rangle\right)$$ & is implementable with $\Theta(n^2)$ gates.

2.) Phase Estimation: Let $|u\rangle$ be an eigenstate of operator U w/ eigenvalue $e^{2\pi i \varphi}$. Starting from $|0\rangle^{\otimes t}|u\rangle$ & given ability to perform U^{2^k} for $k \in \mathbb{Z}$, one can obtain $|\tilde{\varphi}\rangle|u\rangle$, an accurate estimation of φ. (Up to $\lceil \log(2 + \frac{1}{2\epsilon}) \rceil$ bits with probability $\geq 1 - \varepsilon$.

3.) Order Finding: Order x modulo N is least positive r s.t. $x^r \bmod N = 1$. computable in $O(L^3)$ operations using Q.P.E. for L-bit integers x and N.

4.) Factoring: Prime factor of L-bit integer N can be found in $O(L^3)$ operations by reducing problem to find order of random number x co-prime with N.

5.) Hidden subgroup: Generalizes all of these fast quantum algos.