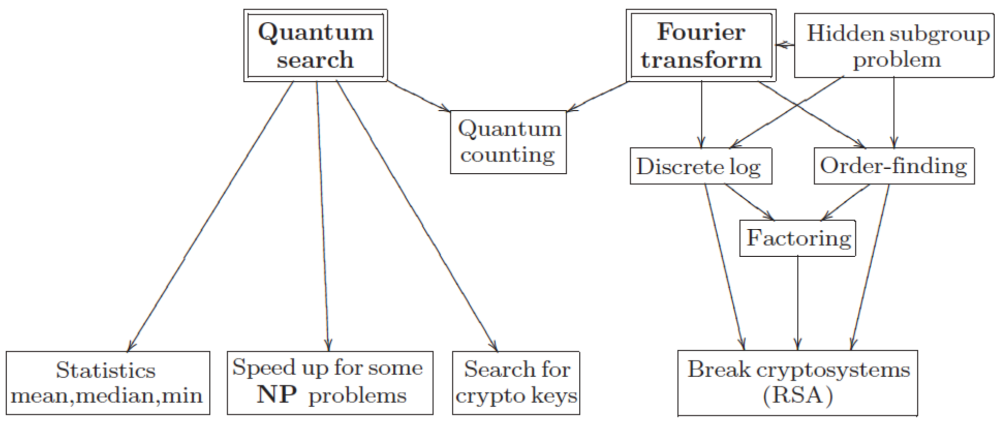
Quantum

Lecture 12

- Quantum algorithms
- Quantum search
- The quantum Fourier transform
- Quantum simulation



Quantum algorithms

$$\mathcal{O}(g_n) = \{f_n : 0 \leq f_n \leq c g_n \text{ for } n \geq n_0\}$$
$$\text{for some } c > 0 \text{ and integer } n_0 > 0$$

"Complexity $\mathcal{O}(g_n)$" $\iff$ true complexity $c_n \in \mathcal{O}(g_n)$

Quantum Search

Generic search problem

For $x \in [0 : N-1]$ assume that $f(x) = 1$ for $x \in \mathcal{M} \subset [0 : N-1]$, $|\mathcal{M}| = M < N$ ($M \ll N$), and $f(x) = 0$ o.w.

$\mathcal{M}$ is the set of solutions to $f(x)$

The problem is to find *one* solution, i.e. one $x \in \mathcal{M}$

Assume that we have an oracle that can check the value $f(x)$ for one given x at low cost

In general (i.e. not only for search)

$\mathbb{P} = \{$can be *solved* with complexity $\mathcal{O}$(a polynomial)$\}$

$\mathbb{NP} = \{$has an *oracle* of complexity $\mathcal{O}$(a polynomial)$\}$

Not known if $\mathbb{NP} = \mathbb{P}$

For a basis $\{|x\rangle\}_{x=0}^{N-1}$ the quantum oracle O is the operator

$$O|x\rangle = (-1)^{f(x)}|x\rangle$$

The Grover operator

$G|x\rangle = (2|\psi\rangle\langle\psi| - I)O|x\rangle$

Assume $N = 2^n$ and let

$$|\psi\rangle = 2^{-\frac{n}{2}} \sum_{x=0}^{N-1} |x\rangle$$

where each $|x\rangle$ corresponds to n qubits ($|0\rangle = |00\cdots 0\rangle$ etc.)

Let $\mathcal{N} = [0 : N-1] \setminus \mathcal{M}$ and

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in \mathcal{N}} |x\rangle, \quad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x \in \mathcal{M}} |x\rangle$$

If we define

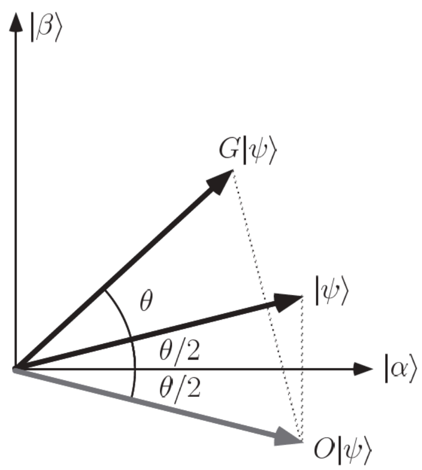
$$\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}} \Rightarrow \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$$

then

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

and

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$



Each time G is applied, the initial state $|\psi\rangle$ is taken closer to $|\beta\rangle$

Quantum search (for $M < N/2$): Prepare the state $|\psi\rangle$

Iterate the Grover operator K times

Measure $\Rightarrow$ a state $|x\rangle' \in \{|x\rangle : x \in \mathcal{M}\}$ with high probability

For $M \ll N$ choosing $K = \lceil \sqrt{N/M} \rceil$ gives a probability of success of at least $1 - M/N$

The Quantum Fourier Transform

Assume $\mathcal{H}$ is N-dimensional, and let $\{|k\rangle\}_{k=0}^{N-1}$ be a basis. For an arbitrary state $|\psi\rangle = \sum_k x_k |k\rangle$, let $\mathcal{F}$ be the operator defined by

$$\mathcal{F}|\psi\rangle = \sum_k y_k |k\rangle$$

where

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$$

is the discrete Fourier transform of $\{x_j\}$

$\mathcal{F}|\psi\rangle$ is the quantum Fourier transform of $|\psi\rangle$

$\mathcal{F}$ is a unitary transformation

Assume that $N = 2^n$ for some integer n, and for $j \in [0 : N-1]$ let

$$j = \sum_{\ell=1}^{n} j_\ell 2^{n-\ell}$$

be the binary expansion of j in terms of $\{j_\ell\}$, $j_\ell \in \{0, 1\}$

Define the notation

$$j = j_1 j_2 \cdots j_n = \sum_{\ell=1}^{n} j_\ell 2^{n-\ell} \in [0 : N-1]$$

and, for $1 \le k \le \ell \le n$,

$$0.j_k j_{k+1} \cdots j_\ell = \sum_{i=k}^{\ell} j_i 2^{k-i-1} \in [0, 1)$$

Identify $\{|j\rangle\}$ with an n-fold qubit basis via $|j\rangle \leftrightarrow |j_1 \cdots j_n\rangle$

Then we can write $\mathcal{F}|j_1 \cdots j_n\rangle =$

$$2^{-\frac{n}{2}} \left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.j_1 \cdots j_{n-1}j_n}|1\rangle\right)$$

Phase estimation

Assume we wish to estimate the eigenvalue $\lambda = e^{2\pi i \phi}$ corresponding to the eigenvector $|u\rangle$ of a unitary operator U

Assume ϕ has an exact t-bits expansion, $\phi = 0.f_1 \cdots f_t$

If we, without knowing ϕ, can compute the state

$$2^{-\frac{t}{2}} \Big(|0\rangle + e^{2\pi i 0.f_t}|1\rangle\Big)\Big(|0\rangle + e^{2\pi i 0.f_{t-1}f_t}|1\rangle\Big) \cdots \Big(|0\rangle + e^{2\pi i 0.f_1 \cdots f_{t-1}f_t}|1\rangle\Big)$$

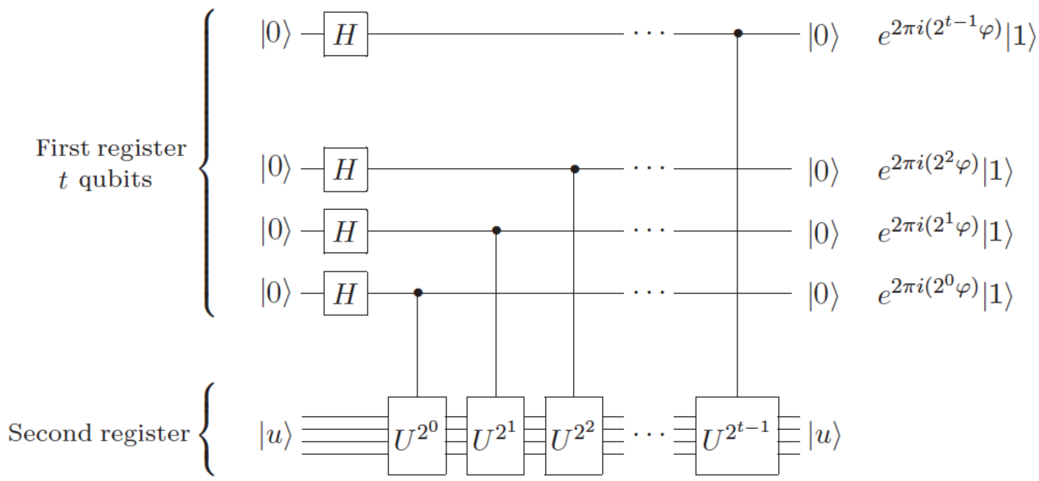
then an inverse Fourier transform will result in $|f_1 f_2 \cdots f_t\rangle$

A measurement in the qubit basis then gives ϕ

If ϕ is not on the form $0.f_1 \cdots f_t$ for some t, then using

$$t = n + \left\lceil \log\left(2 + \frac{1}{2\varepsilon}\right)\right\rceil$$

qubits will give n bits accuracy and error probability $\leq \varepsilon$



Phase estimation: Need to prepare the state $|u\rangle$; Need to implement the U^j mappings; Complexity $\mathcal{O}(t^2)$

Order finding

Greatest common divisor of a set A of integers $=$ biggest integer that divides all numbers in the set, notation gcd(A)

Two integers q_1 and q_2 are relatively prime (coprime) if gcd$(q_1, q_2) = 1$

The order r of an integer x modulo a prime number p is the smallest integer r such that $x^r = 1 \bmod p$

Finding r is believed to be hard on a classical computer, in the sense that the complexity is at least linear in p,

Fermat's little theorem: $x^{p-1} = 1 \bmod p \Rightarrow r < p$

Order of x modulo a non-prime M: $x^{\varphi(M)} = 1 \bmod M$ where

$$\varphi(M) = |\{y : 1 \leq y \leq M, \text{ gcd}(y, M) = 1\}|$$

i.e., the complexity is still linear in M

Defining the unitary operation U as $U|y\rangle = |xy \text{ mod } M\rangle$, we have with

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi isk/r} |x^k \text{ mod } M\rangle$$

for $0 \leq s \leq r-1$, that

$$U|u_s\rangle = e^{2\pi is/r}|u_s\rangle$$

Phase estimation $\Rightarrow \{e^{2\pi is/r}\} \Rightarrow r$ with complexity $\mathcal{O}((\log M)^3)$

We need r to prepare $|u_s\rangle$: Can use $|1\rangle$ instead of $|u_s\rangle$, since

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

Factoring

Prime factoring: Given a (large) positive integer q, find a prime number p that divides q

Believed to be hard on a classical computer, with complexity $\mathcal{O}(\sqrt{q})$ — The factoring problem being "hard" is a crucial assumption in *public key encryption*

Assume q is odd (otherwise 2 is a trivial factor)

For $x \in [2 : q-2]$ suppose $x^2 = 1 \bmod q$. Then at least one of gcd$(x-1, q)$ and gcd$(x+1, q)$ is a factor in q

Suppose q has m different prime factors and let x be an integer chosen uniformly in $[1 : q-1] \cap \{s : s$ and q relatively prime$\}$, then

$$\Pr\left(r \text{ is even and } x^{\frac{r}{2}} \neq -1 \bmod q\right) \geq 1 - \frac{1}{2^m}$$

where r is the order of x mod q

Algorithm: Given an odd number $q > 1$

Check if $q = a^b$ for some prime a and integer b

Choose x at random in $[1 : q-1]$; if gcd$(x, q) > 1$ return gcd(x, q)

Use *quantum order finding* to find the order r of x mod q

If r is even and $x^{r/2} \neq -1$ mod q then compute gcd$(x^{r/2} - 1, q)$ and gcd$(x^{r/2} + 1, q)$ and check if one of these is a factor

Otherwise terminate with an error

The steps performed using classical computing have complexity $\mathcal{O}((\log q)^3)$, so the overall complexity relies on the order finding

Quantum Simulation

Classical system with state in $\mathbb{R}^d$: In general, complexity of simulation grows as $\mathcal{O}(d)$

N quantum particles with states in $\mathcal{H}$ of dimension d, complexity of simulating the combined system is in general $\mathcal{O}(d^N)$

Assume N interacting sub-systems such that the evolution of the joint system is described by

$$i\frac{d}{dt}|\psi\rangle = H|\psi\rangle \Rightarrow |\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

with H of the form

$$H = \sum_{\ell=1}^{L} H_\ell$$

where $L = \mathcal{O}(N)$ and each H_ℓ acts only on few subsystems

Assume the action of each H_ℓ, $\exp(-iH_\ell t)$, can be simulated efficiently on a quantum computer

We get

$$|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$$

where we can use the Trotter formula

$$\lim_{n\to\infty}(e^{\frac{iAt}{n}}e^{\frac{iBt}{n}})^n = e^{i(A+B)t}$$

(for A and B self-adjoint/Hermitian)

Quantum simulation:

For subsystems of dimension $\mathcal{O}(d)$, the total dimension is $\mathcal{O}(d^N)$

Approximate each H_ℓ at resolution $\mathcal{O}(N^k)$ (some $k \geq 1$) qubits

Simulate each subsystem on a quantum computer

Combine using Trotter's formula, or similar