Quantum Computation

oliverobrien111

July 2021

1 Lecture 1

1.1 Review of Shor's algoirthm/quantum period finding algorithm

Polynomial time hierarchy:// Computation with input of size n, and we are interested in the number of steps/gates (classical or quantum). When we say $O(poly(n))$ steps we regard this as an "efficent computation".

Shor's algorithm solves the factoring problem:
Given an integer N needing $O(logN)$ bits, we want to find a non-trival factor in $O(polyn)$ time.

The best known classical algorithm (number sieve): $e^{O(n^{\frac{1}{3}}(\log n)^{\frac{1}{3}})}$
Shor's alogrithm takes $O(n^3)$

1.1.1 Quantum factoring algorithm (summary)

1. First, convert factoring into periodicity determination. Given N, choose $a < N$ s.t. a is coprime (this is easy classically can be seen in part II lecture notes). Consider $f : \mathbb{Z} \to \mathbb{Z}_N$ $f(x) = a^x \mod N$. **Euler's Theorem**: if f is periodic with period r, then it is called 'order of $a \mod N$'.

2. In order to find r we need a quantum implementation of f. We are always workingon finite size registers so restricting $x \in \mathbb{Z}$ to $x \in \mathbb{Z}_M$ (for some large enough M): $f : \mathbb{Z}_M \to \mathbb{Z}_N$. f will no longer be exactly preriodic but this would have neglible effect if M is sufficently large e.g. $M = O(N^2)$

3. Using the classical theory of continued fractions. Define Hilbert spaces $\mathcal{H}_M \to \{|i\rangle\}_{i\in\mathbb{Z}_M}, \mathcal{H}_N \to \{|i\rangle\}_{i\in\mathbb{Z}_N}$.

4. $|x\rangle \to |f(x)\rangle$ is not generally a valid quantum operator, so we make it a unitary operation which can be implemented:

$$U_f : \mathcal{H}_M \otimes \mathcal{H}_N \to \mathbb{H}_M \otimes \mathbb{H}_N$$

$$U_f : |i\rangle |k\rangle \to |i\rangle |k + f(i)\rangle$$

5. if $x \to f(x)$ can be classically computed in $O(poly(m))$ time ($m = \log M$)), then U_f can be implemented in poly(m) time quantumly too

6. We will sometimes view U_f as a black box/oracle and we will count the number of times the algorithm invokes the oracle.

7. Back to facotoring to get r we'll use the quantum algorithm for periodicity determination:

8. Given an oracle U_f with the promise that f is periodic of some unknown period $r \in \mathbb{Z}_N$ so that $f(x + r) = f(x)$ and f is one-to-one in this period (for all $0 \leq x_1 < x_2 < rf(x_1) \neq f(x_2)$)

9. To find r in $O(polyn)$ with any persecribed success probability $1 - \epsilon$ we use the following alogirthm:

   - Step 1: Create the state

   $$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle |0\rangle$$

   - Step 2: Apply U_f to get

   $$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |i\rangle |f(i)\rangle$$

   - Step 3: Measure the 2nd register to get y. By the born rule the first register collapses to all those i: $f(i) = y$ i.e. $i = x_0, x_0 + r, x_o + 2r, ..., x_0 + (A-1)r$, $0 \leq x_0 < r$.

     Discard the second register to get the following state:

     $$|per\rangle = \frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle$$

     If we measure $|per\rangle$ in computation basis we will get a value of one of these states $x_0 + jr$ for uniformly random j. This only gives us a random element of $\mathbb{Z}_M$ with no information about r.

   - Step 4: Apply quantum fourier transform mod M (QFT). Lets recap what QFT does:

   $$|x\rangle \to \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \omega^{xy} |y\rangle, \forall x \in \mathbb{Z}_M, \omega = e^{2\pi i/M}$$

This can be implement in $O(m^2)$ time and gives state:

$$QFT\,|per\rangle = \frac{1}{\sqrt{MA}} \sum_{j=0}^{A-1} \sum_{y=0}^{M-1} \omega^{(x_0+jr)y}\,|y\rangle = \frac{1}{\sqrt{MA}} \sum_{y=0}^{M-1} \omega^{x_0 y} \left[\sum_{j=0}^{A-1} \omega^{jry}\,|y\rangle\right]$$

The square brackets will be:

$$\begin{cases} A & \text{if } y = KA = k\frac{M}{r}, x = 0, 1, ..., r-1 \\ 0 & \text{otherwise} \end{cases}$$

So gives final state:

$$QFT\,|per\rangle = \sqrt{\frac{A}{M}} \sum_{k=0}^{A-1} \omega^{x_0 k \frac{N}{r}}\,|k\frac{M}{r}\rangle$$

Now the random shift x_0 only appears in the phase not in the ket labels. So now the measurement probabilities will be indepedant of x_0. When we measure this we get some value $c = \frac{k_0 M}{r}$ with k_0 uniformly random in range $0 \leq k_0 < r$

$$\frac{k_0}{r} = \frac{c}{M}$$

As c and M are known, and k_0 is unknown but random in the given range. We want to find r and so we recall several classical facts.

Co-primality Theorem: The number of integers less than r that are coprime to r grows with $O(\frac{r}{\log\log r})$

Therefore, the probability of k_0 being coprime to r is $O(\frac{1}{\log\log r})$.

Lemma: If a single trial has success probability p then if one repeats it M^* times, for any $0 < 1-\epsilon < 1$. We get probability of at least one success in M^* trails is greater than $1-\epsilon$ if $M^* = \frac{-\log\epsilon}{p}$. i.e. roughly $O(1/p)$ trials suffice to achieve probability of success $> 1-\epsilon$

- After step 4 cancel $\frac{c}{M}$ down to an irredicible algorithm $\frac{a}{b}$ there is an efficent algorithm ($O(polyn)$) for this. This will give us r as denominator b if k_0 is coprime to r with probablity $O(\frac{1}{\log\log r})$. So check b value by computing $f(0)$ and $f(b)$ and $b = r \iff f(0) = f(b)$.

  By repeating this process $M^* = O(\log\log r)$ times this will give us r with any desired probability $1-\epsilon$. Since $r < M$ the whole algorithm takes $O(polym)$ time!

10. From learning the period r we can use number theory to find a factor of N

1.1.2 Further insights to QFT

Now lets think about the implications of QFT. What does applying quantum fourier transform really achieve?

Lets consider a function: $f : \mathbb{Z}_M \to \mathbb{Z}_N$ with period $r \in \mathbb{Z}_M$, $A = \frac{M}{r}$. Define:

$$R = \{0, r, 2r, 3r, ..., (A-1)r\} < \mathbb{Z}_M$$

$$|R\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |kr\rangle$$

$$|per\rangle = |x_0 + R\rangle = \frac{1}{\sqrt{A}} \sum_{k=0}^{A-1} |x_0 + rk\rangle$$

The problem was this random shift x_0 when measuring $|per\rangle$. For each $x_0 < \mathbb{Z}_M$ consider a mapping $k \to k + x_0$. "Shift by x_0". It is a 1-1 invertible map, and can define a unitary version $U(x_0)$ on $\mathcal{H}_M$: $U(x_0)\,|k\rangle = |k + x_0\rangle$.

$$|x_0 + R\rangle = U(x_0)\,|R\rangle$$

Since $(\mathbb{Z}_M, +)$ is an abelian group $U(x_0)U(x_1) = U(x_0 + x_1) = U(x_1)U(x_0)$. So all $U(x_i)$ commute as operators on $\mathcal{H}_M$. Therefore they have an orthonomal basis of common eigenvectors $\{|\chi_k\rangle\}_{k \in \mathbb{Z}_M}$. These are called shift invariant states as $U(x_0)\,|\chi_k\rangle = \omega(x_0, k)\,|\chi_k\rangle$ for all $x_0, k \in \mathbb{Z}_M$ with the important caveat that $|\omega(x_0, k)| = 1$.

Consider $|R\rangle$ written in $\{|\chi_r\rangle\}$ basis:

$$|R\rangle = \sum_{k=0}^{M-1} a_k\,|\chi_k\rangle$$

a_k only depend on r not on x_0. Then:

$$|per\rangle = U(x_0)\,|R\rangle = \sum_{k=0}^{M-1} a_k \omega(x_0, k)\,|\chi_k\rangle$$

Here it can be seen that the probability of measuring k is

$$prob(k) = |a_k \omega(x_0, k)|^2 = |a_k|^2$$

So this is all indepedant of x_0 and depends only on r. So measuring in this basis gives us some information about r. So one can think of QFT as the unitary mapping that rotates χ basis into the standard computational basis. So can define QFT as:

$$QFT\,|\chi_k\rangle = |k\rangle$$

How do these mysterious shift invariant states look?

1.1.3 Explicit form of shift invariant shapes

$$|\chi_k\rangle = \frac{1}{\sqrt{M}} \sum_{l=0}^{M-1} e^{-2\pi i l \frac{k}{M}} |l\rangle$$

$$U(x_0)|\chi_k\rangle = 1\sqrt{M} \sum_{l=0}^{M-1} e^{-2\pi i l \frac{k}{M}} |l + x_0\rangle = 1\sqrt{M} \sum_{\tilde{l}=0}^{M-1} e^{-2\pi i (\tilde{l}-x_0) \frac{k}{M}} |\tilde{l}\rangle = e^{2\pi i k \frac{x_0}{M}} |\chi_k\rangle$$

giving eigenvalue: $\omega(x_0, k) = e^{2\pi i k \frac{x_0}{M}}$. From this we could reconstruct the basis of QFT:

$$[QFT]_{kl} = \frac{1}{\sqrt{M}} e^{2\pi i \frac{kl}{M}}$$

2 Lecture 3

2.1 Hidden Subgroup Problem

Let G be a finite group of size $|G|$. We are given an oracle $f : G \to X$ with X just some set. We are promised there is a subgroup $K < G$ s.t.

f is constant on (left) cosets of K in G

f is distinct on distinct cosets

Problem: 'Determine' the 'hidden subgroup' K (e.g. output a set of generators or sample uniformly from elements of K)

We want to solve in time $O(poly(\log |G|))$ (efficent algorithm) with anuy consitent probability $1 - \epsilon$. **Examples of problems that can be cast as HSP** Periodicity finding $f : \mathbb{Z}_M \to X$ periodic, period r 1-1 in period

$$G = \mathbb{Z}_M, K = \{0, r, 2r, ..., (A-1)r\} < G$$

Discrete Logarithm Problem: p - prime number, $\mathbb{Z}_p^*$ group of integers with multiplication mod p, $g \in \mathbb{Z}_p^*$ to be a generator (or primitive root mod p). If $\mathbb{Z}_p^* = \{g^0, g^1, ..., g^{r-2}\}$ and we have $g^{p-1} = 1 \pmod p$. Fact: These always exist for p is prime. Any $x \in \mathbb{Z}_p^*$ can be written as $x = g^y$ for some $y \in \mathbb{Z}_{p-1}$, $y = \log_g x$ is called the discrete log of x to base g. Discrete log problem is given a generator g, $x \in \mathbb{Z}_p^*$ we want to compute $y = \log_g x$. To express this as the HSP:

$$f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$$

$$f(a, b) = g^a x^{-b} \mod p = g^{a-yb} \mod p$$

Can check if $f(a_1, b_1) = f(a_2, b_2) \iff (a_1, b_1) = (a_2, b_2) + \lambda(y, 1), \in \mathbb{Z}_{p-1}$:

$$G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$$

$$K = \{\lambda(y, 1) : \lambda \in \mathbb{Z}_{p-1}\} < G$$

Then f is constant and distinct on cosets of K and generator $(y, 1)$ of K gives $y = \log_g x$

Graph Problems:
So we can solve problems like those above where G is abelian, but we can also solve graph problems.

Consdier graph $A = (V, E)$, $|V| = n$ lets say that the graph is undirected and there is at most one edge between any two vertices. Vertices here are labelled by numbers from 1 to n.

Lets define an adjacency matrix M_A: $[M_a]_{ij} = \begin{cases} 1 & \iff (i,j) \\ 0 & \text{otherwise} \end{cases}$. The permuation group of $[n]$, $|P_n| = n!, \log|P_n| \sim O(n \log n)$. Define a group of automorphisms of group A which is a set of permuations with the following property: $\pi \in P_n$ s.t. $\forall i, j (i, j)$ is an edge in $A \iff (\pi(i), \pi(j))$ is also an edge in A.

An associated HSP (the case of non-abelian G):

$$G = P_n, X = \text{set of all labelled graphs on } n\text{vertices}$$

For any $A \in X$, define $f_A : G \to X$, $f_A(\pi) =$"A with vertex labels permuted by π"

$$K = Aut(A)$$

(Check $f(K)$ is constant and disctint on cosets of $Aut(A)$)

Applications:
If we can sample uniformly from K, then we can solve Graph Isomorphism problem (GI).This has a number of different applications in areas of computer science. Two labelled graphs A and B with n vertices are isomorphic if there is a 1-1 map (i.e. permutation) $\pi[n] \to [n]$ s.t. $\forall i, j \in [n](i, j)$ is an edge in $A \iff (\pi(i), \pi(j))$ is an edge in B. The GI problem is given to graphs A and B and deciding if they are isomorphic. This can be represented as a non-abealian HSP. There is no known poly(m) time classical algorithm to solve this problem, so GI is clearly in NP but not believed to be NP-complete (a class of problems such that every problem in NP can be reduced to an NP-complete problem these are the hardest NP problems). In 2017, L Babai presented a quasi-polynomial algorithm for GI runtime $n^{O}(\log n)^2)$. This ranks in between polynomial runtime and exponential algorithms.

3 Lecture 4

Quantum algorithm for finite abelian HSPs - Generalisation of period-finding algorithm
Write our abelian group $(G, +)$ additively

Construction of shift-invariant states and Fourier transform for G.
Representations of abelian G:
Consdier the mapping $\chi : G \to \mathbb{C}^* = \mathbb{C} - \{0\}$ with multiplication that satisfies:

$$\chi(g_1 + g_2) = \chi(g_1)\chi(g_2), \forall g_1, g_2 \in G$$

χ is a group homomorphism from G to $\mathbb{C}^*$. Such χ's are called irreducible representations of G. They have the following properties: **Theorem 1**:
1) any value $\chi(g)$ is a $|G|$-th root of unity ($\chi \in \to S^1$ the unit circle)
2) Schur's lemma (orthogonality): If χ_i, χ_j satisfy (HOM) then

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g)\bar{\chi_j}(g) = \delta_{ij}$$

3) There are always exactly $|G|$ different functions χ satisfying (HOM).

Examples: $\chi(g) = 1, \forall g \in G$ is an irrep/ called a trival irrep
Label the trivial irrep as χ_0, $0 \in G$. Then for any other irrep $\chi \neq \chi_0$ orthonality to χ_0 gives:

$$\sum_{g \in G} \chi(g) = 0 \text{ if } \chi \neq \chi_0$$

Going back to constructing shift-invariant states

3.0.1 Shift-invariant states

Consider a state space $\mathcal{H}_G, dim\mathcal{H}_G = |G|$ wtih basis $\{|g\rangle\}_{g \in G}$. Now introduce shift operators $U(k)$ for $k \in G$ defined as follows:

$$U(k) : |g\rangle \to |g + k\rangle \, , g, k \in G$$

All shift operators commute so there exists a simultaneous eigenbasis.
For each $\chi_k, k \in G$:

$$|\chi_k\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \bar{\chi_k}(g) \, |g\rangle$$

By thereom 1 $\{\chi_k\}$ form an orthonormal basis.

$$U(g) \, |\chi_k\rangle = \chi_k(g) \, |\chi_k\rangle$$

Proof:

$$U(g) \, |\chi_k\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \bar{\chi_k}(h) \, |h + g\rangle$$

$$\{h' = h + g\} = \frac{1}{\sqrt{|G|}} \sum_{h' \in G} \bar{\chi_k}(h' - g) \, |h'\rangle$$

using HOM $\chi_k(-g) = \chi_k(g)^{-1} = \bar{\chi}_k(g) \implies \chi_k(\bar{h'-g}) = \bar{\chi}_k(h')\bar{\chi}_k(-g) = \bar{\chi}_k(h')\chi_k(g)$. Therefore,

$$U(g)\left|\chi_k\right\rangle = \frac{1}{\sqrt{|G|}}\sum_{h'\in G}\chi_k(g)\bar{\chi}_k(h')\left|h'\right\rangle = \chi_k(g)\left|\chi_k\right\rangle$$

So $|\chi_k\rangle$'s form a common eigenbasis

Introduce Fourier transform QFT for a group G
- consider a unitary mapping on $\mathcal{H}_G$ mapping $|\chi_k\rangle$ basis to $|g\rangle$ basis

$$QFT\left|\chi_g\right\rangle = \left|g\right\rangle, \forall g \in G$$

$$QFT^{-1}\left|g\right\rangle = \left|\chi_g\right\rangle$$

k-th column of QFT^{-1} in $|g\rangle$ basis is mode of components of $|\chi_k\rangle$:

$$[QFT^{-1}]_{gk} = \frac{1}{\sqrt{|G|}}\bar{\chi_k}(g)$$

Example: $G = \mathbb{Z}_M$L
Check $\chi_a(b) = e^{\frac{2\pi iab}{M}}, a, b \in \mathbb{Z}_M$ satsifies HOM and has its irreps labelled by $a \in \mathbb{Z}_M$ with $\chi_0(b) = 1 \forall b \in \mathbb{Z}_m$.

$$G = \mathbb{Z}_{M_1} \times ... \times \mathbb{Z}_{M_r}$$

$$(a_1, ..., a_r) = g_1, (b_1, ..., b_r) = g_2$$

$$\chi_{g_1}(g_2) = e^{2\pi i(\frac{a_1b_1}{M_1}+...+\frac{a_rb_r}{M_r}}$$

This satifies HOM and our $QFT_G = QFT_{M_1} \otimes ... \otimes QFT_{M_r}$ on $\mathcal{H}_G = \mathcal{H}_{M_1} \otimes ... \otimes \mathcal{H}_{M_r}$.

This second example is exhaustive since we have a classification theroem:
Classification theorem: Any fintie abelian group G is isomorphic to a direct product of the form $G = \mathbb{Z}_{M_1} \otimes ... \otimes \mathbb{Z}_{M_r}$. So M_1 can be taken in a form $p_1^{s_1}, ...p_r^{s_r}$.

3.0.2 Quantum algorithm

$$f : G \to X$$

with hidden subgroup K and cosets $k = 0 + k, g_2 + k, ...g_m + k$, $m = \frac{|G|}{|K|}$. we will work on $\mathcal{H}_{|G|} \otimes \mathcal{H}_{|X|}$,$\{\left|g\right\rangle \left|x\right\rangle\}_{g\in G, x\in X}$.

Create a state $\frac{1}{\sqrt{|G|}}\sum_{g\in G}\left|g\right\rangle\left|0\right\rangle$
*Apply*U$_f$ and $\frac{1}{\sqrt{|G|}}\sum_{g\in G}\left|g\right\rangle\left|f(g)\right\rangle$

Measure the second register to get $f(g_0)$. The first register will not give the coset state:

$$|g_0 + k\rangle = \frac{1}{\sqrt{|k|}} \sum_{k \in K} |g_0 + k\rangle = U(g_0) |K\rangle$$

apply QFT and measure to get a result $g \in G$

4 Lecture 6

We can write $|K\rangle$ in the shift-invariant basis $\{\chi_g\}_{g \in G}$

$$|K\rangle = \sum_g a_g |\chi_g\rangle$$

$$|g_0 + K\rangle = U(g_0) |K\rangle = \sum_g a_g \chi_g(g_0) |\chi_g\rangle$$

as $QFT |\chi_g\rangle = |g\rangle$ so after we apply QFT

$$prob(g) = |a_g \chi_g(g_0)|^2 = |a_g|^2, |\chi_g(g_0)| = 1$$

$$QFT |K\rangle = \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|K|}} \sum_{l \in G} (\sum_{k \in K} \chi_l(k) |l\rangle)$$

$\sum_{k \in K} \chi_l(k) |l\rangle$ involves irreps χ_l of G restricted to subgroup $K < G$, and each such object is itself an irrep in K. Hence we have the following relation:

$$\sum_{k \in K} \chi_l(k) = \begin{cases} |k| & if \chi_l \text{ restricts to the trival irrep of K} \\ 0 & \text{otherwise} \end{cases}$$

$$QFT |K\rangle = \sqrt{\frac{|K|}{|G|}} \sum_{l \in G} |l\rangle$$

Then a measurement gives a uniformly random choice of l s.t. $\chi_l(k) = 1$.
If k has generators $k_1, ..., k_n$ where $M = O(\log(K)) = O(\log |G|)$. Then the output of a measurement gives us $\chi_l(k) = 1 \forall i$.

It can be shown that if $O(\log(|G|)$ values of l chosen uniformly at random then with probability $> \frac{2}{3}$ they will suffice to determine a generating set for k via the equations $\chi_l(k) = 1$.

Example: $G = \mathbb{Z}_{M_1} \times ... \times \mathbb{Z}_{M_l}$
$l = (l_1, ..., l_q) \in G$, $g = (b_1, ..., b_q) \in G$ gives $\chi_l(g) = e^{2\pi i (\frac{l_1 b_1}{M_1} + ... + \frac{l_q b_q}{M_q}}$
For $k = (k_1, ..., k_q) \in K$ with $\chi_l(k) = 1 \implies \frac{l_1 k_1}{M_1} + ... + \frac{l_q k_q}{M_q} = 0 mod 1$. This is a homogenous linear equation on k and $O(\log(k))$ such equations determine k as null space.

4.0.1 Remarks on HSP for non-abelian groups G

Now we will consider multiplicative shifts. As before we can generate a bunch of coset states but it is curious to investigate what breaks down.

$$|g_0 K\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 k\rangle \, , g_0 \in G \text{ is chosen randomly}$$

The real problem with QFT construction is that there is no good basis of shift invariant states. This is because $U(g_0)$ don't commute.

Construction of non-abelian QFT
Consider a d-dimensional representation of G and a group homomorphism $\chi : G \to U(d)$
χ is irreducible if no subset of $\mathbb{C}^d$ is left invariant by all matrices $\chi(g), g \in G$. (i.e. we cannot simulatenoulsy block-diagonalize all of $\chi(g)$'s by a simple basis change)
Let's define a complete set of irreps. It is a set $\chi_1, ..., \chi_m$ s.t. that any irrep is unitarily equivalent to one of them. e.g. $\chi \sim \chi' = V \chi C V^{-1}, V \in U(d)$
Example: G is abelian , all irreps have $d = 1$, since all $\chi(g)$ commute. Theorem(non-abelian analogue of Theorem 1) (consullt Fulton and Hardes "Representation Theory" fo more information)
If $d_1, ..., d_m$ are the dimensions of a complete set of irreps $\chi_1, ..., \chi_M$ then:
1) $d_1^2 + ... + d_m^2 = |G|$
2) $\chi_{i,jk}(g)$ is (j,k) th matrix entry of $\chi_i(g)$ then by Schur orthogonality:

$$\sum_g \chi_{i,jk}(g) \bar{\chi}_{i',j'k'}(g) = |G| \delta i i' \delta_{jj'} \delta k k'$$

Now if we look at the states that correspond to these irreps $\chi_{i,jk} = \sum_g \in G \bar{\chi}_{i,jk}(g) \, |g\rangle$ they form an orthonormal basis.
QFT on G is defined to be a unitary rotation between two basis of $\{\chi_{i,jk}\}$ basis $\to \{|g\rangle\}_{g \in G}$.
These takes $|\chi_{i,jk}\rangle$ are not shift-invariant for all $U(g_0)$ so this implies that measuring coset state $|g_0 k\rangle$ in the $\{|\chi\rangle\}$ basis results in an output distribution that is not independant of g_0.
A "partial" shift-invariance survives. Consider a measuremnt M_{rep} on $|g_0 k\rangle$ this measurement will only distinguish the irreps (i values) and not all (i,j,k)'s. the outcome i will be associated with d_i^2 dimensional orthogonal subspaces that are spanned by $\{\chi_{i,jk}\}_{j,k=1}^{d_i}$.
Then $\chi_i(g_1 g_2) = \chi_i(g_1)\chi_i(g_2) \implies$ the output distribution of i values is indeed independant of g_0.
So this gives us direct (but incomplete) information about k. For instance, conjugate subgroups k and $L = g_0 K g_0', g_0 \in G$. This measurement will give us the same statistics.
M_{rep} will result in the same output statistics
Not everything is lost there are some cases when this information is enough.

The reason HSP is good in the abelian case is we have an efficent QFT transform. In other words QFT can be implemented in $poly(\log(|G|)$ times. This is true for abelian groups and some non-abelian groups (e.g. P_n).
Some partial results:
For normal subgroups $gk = kgg \in G$ we have a theorem proven by Hall green, russel Ta shma in 2003 SIAM J Comp 32, p 916-934:
Suppose G has QFT that is efficently implementable. Then if a hideen subgroup k is a normal subgroup, then there is an efficent quantum HSP

Theorem(Edinsguin, Hoyer, Knill, 2004)
For general non-abelian HSP, $M = O(poly \log(|G|))$ then random coset states $|g_1 k\rangle$,..., $|g_n k\rangle$ suffice to determine k . But it is not known how to efficently determine k from the M coset states.

5 Lecture 6

5.1 Phase estimation Algorithm

- Unifying principle for quantum algorithms based on QFT
- also gives an alternative way of factoring (orginally discovered by Kitaev)
The fact the phase estimation algorithm became so wide spread and you can cast every algorithm that is tangenetially ralted to QFt in QPE
Givem a unitary operator U. and eigenstates $|v_\phi\rangle = U|v_\phi\rangle = e^{2\pi i\phi}|v_\phi\rangle$
Want to estiamte the phase ϕ $0 < \phi < 1$ (up to n bits of precision $\phi = 0.i_1 i_2, ...i_n = i_1/2 + i_2/4 + ...$ for any given n)
We will have to implement controlled unitary opearotrs and in particular we will need Controlled-U^k for integers k

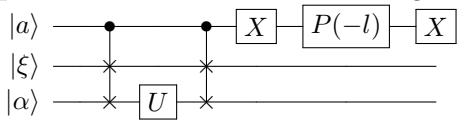
$$C - U^k |0\rangle |\xi\rangle = |0\rangle |\xi\rangle, C - U^k |1\rangle |\xi\rangle = |1\rangle U^k |\xi\rangle$$

$|\xi\rangle$ has a general dimension d:

$$U^k |v_\phi\rangle e^{2\pi ik\phi} |v\phi\rangle, C - U^k = (C - U)^k$$

If we are given U as a circuit description, we can easily implement $C - U$ by controlling each gate in U's circuit. However, if U is given as black box (e.g. a physical operation in the lab) we need further information as there is an inherent ambiguity as we have to account for local phase $e^{i\theta U}$ as it has no effect normally unless you use a controlled operation.

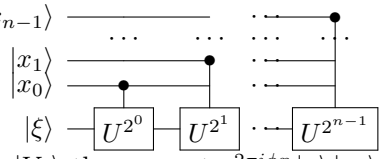
If the unitary is specified in this ambiguous way we need to figure out what to do. It suffices to have an eigenstate $|l\rangle$ with a known eigenvalue $U|l\rangle = e^{i\alpha}|l\rangle$ then $e^{i\theta}U$ will map $\alpha \to \alpha + \theta$. Consider the following circuit:



with $P(-l) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-il} \end{pmatrix}$. This correctly gives $C-U$. We'll want a "generalised controlled-U" that gives:

$$|x\rangle |\xi\rangle \rightarrow |x\rangle U^x |\xi\rangle \, x \in \mathbb{Z}_{2^n}$$

For $x = x_{n-1}...x_1x_0 = 2^0x_0 + 2^1x_1 + 2^2x_2... + 2^{n-1}x_{n-1}$:



If we input $|\xi\rangle = |V_\phi\rangle$ then we get $e^{2\pi i\phi x} |x\rangle |v_\phi\rangle$. Now superpose over all $x = 0, 1, 2, ..., 2^{n-1}$ by applying hadamards to all the qubits before applying the circuit, take $|\xi\rangle = |v_\phi\rangle$:

This gives output $|A\rangle = \frac{1}{\sqrt{2^n}} \sum_x e^{2\pi i\phi x} |x\rangle$. Applying QFT^{-1} to $|A\rangle$ and measure. We get $y_0y_1...y_{n-1}$. Then output the number $0.y_1y_2...y_{n-1} = \frac{y_0}{2} + \frac{y_1}{4} + ... + \frac{y_{n-1}}{2^n}$ as an estimate of ϕ.

Now lets assume an idealised situtation where ϕ has only n binary digits:

$$\phi = 0.z_1...z_{n-1}$$

Then $\phi = \frac{z}{2^n}$ where z is an n-bit integer in $\mathbb{Z}_{2^n}$:

$$|A\rangle = \frac{1}{\sqrt{2^n}} \sum_2 e^{2\pi i 2^n z/2^n} |x\rangle$$

is a QFT of $|z\rangle$. Applying $QFT^{-1} |A\rangle = |z\rangle$ and we get ϕ exactly with certainity.

Note the algorithm up to the final measurements is a unitary operation mapping:

$$|0\rangle |0\rangle ... |0\rangle |v_\phi\rangle \rightarrow |z_0\rangle |z_1\rangle ... |z_{n-1}\rangle |v_\phi\rangle$$

If ϕ has more than n bits $\phi = 0.z_0z_1...z_{n-1}|z_nz_{n+1}$.
Theorem (PE): If measurements in the algorithm give $y_0y_1...y_n$ and the aoutput $\Theta = 0.y_0y_1...y_{n-1}$ then :
a) Prob (Θ is closeset n-binary digit approx to ϕ) $\geq \frac{4}{\pi^2} = 0.4$
b) Prob($|\Theta - \phi| \geq \epsilon$) $\leq O(\frac{1}{2^n\epsilon}$

We will show that Prob($|\Theta - \phi| \geq \epsilon$) $\leq \frac{1}{2^{n+1}\epsilon}$)

6 Lecture 8

Today we will prove the Phase estimation theorem. We need to change the defintion of distance as we need a distance on a circle.

Define $d(\theta,\phi) = \min\{|\theta-\phi|, |1+\phi-\theta|, |1+\theta-\phi|\}$ which is the distance on the circle. Lets consider the normal binary expansion 0.999999 the closest string should be 1.

Theorem (Phase Estimation): If the output of PE algorithm with n lines (initited in as zeros) is $\theta = 0.y_0y_1...y_{m-1}$, then:
a) Prob (θ is closeset n-binary digit approx to ϕ, $d(\theta,\phi) \leq \frac{1}{2^{n+1}}) \geq \frac{4}{\pi^2} = 0.4$
b) Prob($|\theta-\phi| \geq \epsilon) \leq O(\frac{1}{2^n\epsilon})$ for ϵ fixed

Recall: the output is obtained by measuring an n-qubit state $QFT^{-1}|A\rangle$ where $|A\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1} e^{2\pi i l x}|x\rangle$

$$QFT^{-1}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{-2\pi i \frac{yx}{2^n}}|y\rangle$$

Soon we will change the notation to make sure it is not overloaded with these powers of 2^n

$$QFT^{-1}|A\rangle = \frac{1}{2^n}\sum_{y=0}\sum_{x=0} e^{2\pi i(\psi-\frac{y}{2^n})x}|y\rangle$$

Let $\{\phi = 2^n\psi\}$:

$$QFT^{-1}|A\rangle = \frac{1}{2^n}\sum_{y=0}\sum_{x=0} e^{2\pi i\frac{\phi-y}{2^n})x}|y\rangle = \frac{1}{2^n}\sum_y \frac{1-e^{2\pi i(\phi-y)}}{1-e^{2\pi i\frac{\phi-y}{2^n}}}|y\rangle$$

In the case $\phi - y \neq 0$:

$$Prob(seey) = \frac{1}{2^n}|\sum_{x=0}^{2^n-1} e^{2\pi i\frac{(\phi-y)}{2^n}x}|^2 = \frac{1}{2^{2n}}\frac{|1-e^{2\pi i(\phi-y)}|^2}{|1-e^{2\pi i\frac{\phi-y}{2^n}}|^2} = \frac{1}{2^{2n}}\frac{|1-e^{2\pi i(\psi-\frac{y}{2^n}2^n}|^2}{|1-e^{2\pi i(\psi-\frac{y}{2^n}}|^2}$$

As $\theta_y = \frac{y}{2^n}$ and observe that $|1-e^{2\pi i(\psi-\theta_y)}|^2 = |1-e^{2\pi i d(\psi,\theta_y)}|^2$ therefore:

$$Prob(see\ y) = \frac{1}{2^{2n}}\frac{|1-e^{2\pi i 2^n d(\psi,\theta_y)}|^2}{|1-e^{2\pi i d(\psi,\theta_y}|^2}$$

As $0 < d(\psi,\theta_y) \leq \frac{1}{2}$ we will ise the following bounds:
i) $|1-e^{i\alpha}| \leq 2|$
ii) $|1-e^{i\alpha}| \leq |alpha|$
iii) For $|alpha| \leq \phi$ $|1-e^{i\alpha}| = 2|sin(\frac{\alpha}{2})| \geq \frac{2|alpha|}{\pi}$

The last of thse comes from the fact that for positive α we hae $\sin(\alpha/2) \geq \frac{\alpha/\pi}{}$

When $d(\psi,\theta) \leq \frac{1}{2^{n+1}}$ implies that y is the best approxiamtion for ψ and $2\pi d(\psi,\theta_y)2^n \leq \frac{2^{n+1}}{2^{n+1}}\pi$ so:

$$Prob(yisbestapproximation) \geq \frac{1}{2^{2n}}|\frac{2}{\pi}\frac{2\pi d(\psi,\theta_y)}{2\pi d(\psi,\theta)}|^2 = \frac{4}{\pi^2}$$

The calculations for the above will be on the moodle

Further remarks:

If $C - U^{2^n}$ is implement as $(C-U)^{2^\alpha}$, then PE algorithm needs exponential time $(1 + 2 + ... + 2^{n-1} = 2^n - 1)$. But for some some U implementing $C - U^{2^k}$ requries only polynomial time so we get a poly-time PE algorithm. Harks back to the algorithm for finding powers by repeated squaring, expressing the exponent in binary and then doing repeated squaring. The number of applications of controlled unitaries does not depend on d the dimension of the space. This can be used to rpovide an alternative factoring algorithm (due to A.Kitaev) (see example sheet).

In many applications we feed an arbitary state to the last register rather than an eigenstate. If instead of $|v_\phi\rangle$ we input general state $|\xi\rangle$, expand in eigenbasis of U:

$$|\xi\rangle = \sum_j c_j |v_{\phi_j}\rangle, U |v_{\phi_j}\rangle = e^{2\pi i \phi_j} |v_{\phi_j}\rangle$$

Then we get (before the final measuremnt) a unitary process U_{PE}:

$$|00..00\rangle |\xi\rangle \rightarrow^{U_{PE}} \sum_j c_j |\psi_j\rangle |v_{\phi_j}\rangle$$

The Born rule implies that the final measurement will give a choice of ϕ_j's (or an approximation) it can be choosen with probability $|c_j|^2$. This is not some average of the ϕ_j values.

Will be elaborated more in the notes on moodle on the following:

If you want to have n-qubits and want to get m-bits correctly probablility of success $1 - \eta$, then must have :

$$n \geq m + \log \frac{1}{\eta}$$

6.1 Amplitude amplification

Much like when we multiple up to HSP we revisited shors alogrithm, in this case we revisit grovers algorithm. This is an apotheosis of technique in Grover's algorithm.

6.1.1 Background

Reflection Operators: State $|\alpha\rangle$ in $\mathcal{H}_d$, n-dim subspace L_α with $(d-1)$ dim orthogonal l_α^α

$$I_{|\alpha\rangle} = I - 2 |\alpha\rangle \langle\alpha|$$

$$I_{|\alpha\rangle} = -|\alpha\rangle$$
$$I_{|\alpha\rangle}|\beta\rangle = |\beta\rangle$$

for any $|\beta\rangle |\alpha\rangle$

For any unitary U: $UI_{|\alpha\rangle}U^\dagger = I_{U|\alpha\rangle}$, $U|\alpha\rangle\langle\alpha|U^\dagger = |\beta\rangle\langle\beta|$ for $|\beta\rangle = U|\alpha\rangle$.

Consider a k-dimensional subspace $A < \mathcal{H}_d$, any orthonormal basis $|a_1\rangle, ..., |a_k\rangle$. Lets consider a projection operator on to this subspace:

$$P_A = \sum_{i=1}^{k} |a_i\rangle\langle a_i|$$

Define a generalised projeciton operator:

$$I_A = I - 2P_A$$

$$I_A|\xi\rangle = \begin{cases} |\xi\rangle & |\xi\rangle \in A^\dagger \\ -|\xi\rangle & |\xi\rangle \in A \end{cases}$$

Now lets recall what grover does very briefly (have a look at Part II course):

Search for a unique "goal" item in unstructured database of $N = 2^n$ items.

Write B_n = set of all n-bit strings. Given an oracle for $f : B_n \to B_n$ with the promise that there is a unique element $x_0 \in B_1$ with $f(_0) = 1$. Problem is to find x_0.

Closely related to class NP and Boolean satisfiability problem. This is explained in part II lecture notes.

7 Lecture 8

Recap of grovers algorithm We are searching for a unique "good" element in an unstructured database, $N = 2^n$ items
We are given an oracle f that maps from $B_n \to B_1$
Promise: There is a unique $x_0 \in B_n$ with $f(x_0) = 1$
Problem: Find x_0

Consider Grover iteration operator on n qubits

$$Q = -H_n I_{|0\rangle} H_n I_{|x_0\rangle} = -I_{|\psi_0\rangle} I_{|x_0\rangle}$$

where $H_n = H \otimes ... \otimes H$, $|\psi_0\rangle = H_n|00.000\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in B_n} |x\rangle$

One application of Q uses 1 query of U_f

Thereom (Grover '96): In 2-dim span of $|\psi_0\rangle$ and (unknown) $|x_0\rangle$ the action of Q is rotation by angle 2α where $\sin\alpha = \frac{1}{\sqrt{N}}$. Hence grover's algorithm to find x_0 given U_f is:
Make $|\psi_0\rangle$

Apply Q m times where $m = \frac{\arccos\frac{1}{\sqrt{N}}}{2} \arcsin\frac{1}{\sqrt{N}}$ to rotate ψ_0 very close to x_0 (within the angle $\pm\alpha$

Measure to see x_0 with high probability $1 - \frac{1}{N}$ For large N $\arccos\frac{1}{\sqrt{N}} = \frac{\pi}{2}$ and $\arcsin\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{N}}$ so $m = \frac{\pi}{4}\sqrt{N}$ iteractions or queries to U_f needed.

Classically we need $O(N)$ quereies to find x_0 with any constant probability that does not depend on N, so this achieves a quadratic speed-up.

7.1 Amplitude Amplification

Let G be any subspace ('good subspace') of state space $\mathcal{H}$ G be its orthogonal complement ('bad subspace') $\mathcal{H} = G \oplus G$

Given any $|\psi\rangle \in \mathcal{H}$, we have unique decomposition with real positive coeffi-centt $|\psi\rangle = \sin\theta\,|g\rangle + \cos\theta\,|b\rangle\,, |g\rangle \in G, |b\rangle \in G$
Introduce reflection operators that flip $|\psi\rangle$ and good vectors:

$$I_{|\psi\rangle} = I - 2\,|\psi\rangle\,\langle\psi|\,, I_G = I - 2P_G$$

$\sin\theta = ||P_G\,|\psi\rangle\,||$ =length of good projection of $|\psi\rangle$
Introduce $Q = -I_{|\psi\rangle} I_G$

7.1.1 Amplitude Amplification Theorem

In the 2-dim space spanned by $|g\rangle$ and $|\psi\rangle$ Q is roation by 2θ where
$\sin\theta$ =length of good projection of $|\psi\rangle$
Proof: We have $I_G\,|g\rangle = -\,|g\rangle\,, I_G\,|b\rangle = |b\rangle$:

$$Q\,|g\rangle = I_{|\psi\rangle}\,|g\rangle\,, Q\,|b\rangle = -I_{|\psi\rangle}\,|b\rangle$$

$$I_{|\psi\rangle} = I - 2(\sin\theta\,|g\rangle + \cos\theta\,|b\rangle)(\sin\theta\,\langle g| + \cos\theta\,\langle b|)$$

using the fact that $\langle b|\,|g\rangle = 0, \langle g|\,|g\rangle = \langle b|\,|b\rangle = 1$:

$$Q\,|b\rangle = \cos 2\theta\,|b\rangle + \sin 2\theta\,|g\rangle$$

$$Q\,|G\rangle = -\sin 2\theta\,|b\rangle + \cos 2\theta\,|g\rangle$$

So

$$Q\,|g\rangle = I\,|g\rangle - 2\sin^2\theta\,|g\rangle - 2\sin\theta\cos\theta\,|b\rangle = \cos 2\theta\,|g\rangle - \sin 2\theta\,|b\rangle$$

In the $\{|b\rangle, |g\rangle\}$ basis, the Q matrix is a rotation matrix by 2θ:

$$Q = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ -\sin 2\theta & \cos 2\theta \end{pmatrix}$$

As we apply Q n $timesweget Q^n |\psi\rangle = \sin(2n+1)\theta |g\rangle + \cos(2n+1)\theta |b\rangle$. $If we measure Q^n$ in $\{|b\rangle, |g\rangle\}$ basis we have probabiliyt of seeing a good element of $\sin^2(2n+1)\theta$ so this is maximised when $(2n+1)\theta = \frac{\pi}{2}$. $So for the nearest integer to n = \pi \frac{}{4\theta - \frac{1}{2}}$ we will be within θ of the element.

Example: If we have $\theta = \frac{\pi}{6}, n = 1$ we can seee that Q^1 rotates $|\psi\rangle$ exactly onto $|g\rangle$.

Generally, for a given θ n is not an integer, so we use n = nearest integer to $\frac{4\pi}{\theta} - 1 \approx \frac{4\pi}{\theta} = O(\frac{1}{\theta}) = O(\frac{1}{\sin\theta}) = O(\frac{1}{\text{length of good projection of } |\psi\rangle}$ and then $Q|\psi\rangle$ will be witin angle θ of $|g\rangle$ so the probability of seeing a good value is: $P \geq \cos\theta = 1 - O(\theta^2)$.

All this can implement if $I_{|\psi\rangle} I_G$ can be impmeneted efficently. see ES2.

For I_G is suffices for G to be spanned by computational basis states and have an indicator funciton f.

$$f(x) = 1, x if x \text{ is good}, f(x) = 0 \text{ if} x \text{is bad}$$

For $I_{|\psi\rangle}$ we usually have $|\psi\rangle = H_n |00..000\rangle$, then $|\psi\rangle$ can be implemented in $O(n)$ time where n is the number of qubits.

In the amplitude amplification algorithm the relative amplitudes of good elements remain the same as they were in $|\psi\rangle = \sin\theta |g\rangle + \cos\theta |b\rangle$ so $|g\rangle$ remains the same just the amplitude varies. So AA amplifies overall $|g\rangle$ amplitude at the expense of reducing the amplitude of $|b\rangle$.

Second remark: Final state is generally not exactly $|g\rangle$, however, if $\sin\theta$ is known then there is a modification of this algorithm that uses a modest amount of resources t omake it exact.

The rotuine is useful for state prepation e.g.

$$\sum_{x<N, \text{x is coprime to N}} |x\rangle$$

8 Examples Class 1

Try to prove the same thing in 1(ii) in shors algorithm and it will be slightly nicer language than group theory.

For $\mathbb{Z}_2$ the irreps are $\chi_a(x) = (-1)^{ax}$ for $a, x \in \mathbb{Z}_2$ therefore $\mathbb{Z}_2^n$ has irreps $\chi_a(x) = (-1)^{a_1x_1+a_2x_2+...+a_nx_n}$ so

$$|\chi\rangle = \frac{1}{\sqrt{|G|}} \sum_g \bar{\chi}(g) |g\rangle = \frac{1}{\sqrt{|G|}} \sum_{b \in \mathbb{Z}_2^n} (-1)^{ab} |b\rangle$$

and

$$[QFT]_{ab} = \frac{1}{\sqrt{|G|}}(-1)^{ab} = \frac{1}{\sqrt{2^n}}(-1)^{a_1b_1}(-1)^{a_2b_2}...(-1)^{a_nb_n}$$

could be written using Hadmards with $QFT = H \otimes H \otimes ... \otimes H$ as $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ with the columns being a and the rows being b so it is only -1 if they are both 1 as otherwise it will have a zero in the exponent.

First part of HSP problems is generate coset states and the second part is repeation (how many times you need to repeat the process). In standard HSP we make one query to f to make the following state:

$$|y \oplus k\rangle = \frac{1}{2^k} \sum_{x \in K} |y \oplus x\rangle, y \in \mathbb{Z}_2^n$$

Apply $QFT = H^{\otimes n}$ and measure. This gives an uniformly random output $c \in \mathbb{Z}_2^n$ which is such that the irrep χ_c of G that is restricted to K is the trivial irrep of K. In other words $\chi_c(a) = 1$ for all $a \in K$. In other word, $(-1)^{ac} = 1 \implies ca = 0 \mod 2$. We know that this k viewed as a subspace of $\mathbb{Z}_2^n$ has dimension k. So we need $(n-k)$ linearly indepdendant c_i with $c_i a = 0$ to determine K.

In order to succeed with probability $1 - \epsilon$ when given a constant probability p we run the process some M times. Then you calculate the probablity of M runs failing to determine k and show that for a constant overhead we can get any accuracy. $1 - (1-p)^M > 1 - \epsilon$.

Phase gates act with $P(\alpha) : |0\rangle \to |0\rangle, |1\rangle \to e^{i\alpha} |1\rangle$. Therefore can apply a fractional phase by first preparing a register with $i_1, ..., i_n$ s.t. $y = 0.i_1...i_n$ and then by applying phase gates $P(\frac{1}{2}...P(\frac{1}{2^n}$to get the state $e^{iy} |y\rangle$.

When inventing algorithms whilst it is useful to think about eigenstates to start with make sure to run it through with a general state as you might need to uncompute at the end. e.g. need to apply an inverse controlled unitary in question 5 after computing the correct eigenvalue.

We can't just discard additoinal registers like $\sum_j \lambda_j |u_j\rangle |c_j\rangle$ to $\sum_j \lambda_j |u_j\rangle$ we need to uncompute to remove these extra stuff.