Quantum Computation

October 18, 2018

Contents

0 Introduction

asdasd

Exercise classes: Sat 3 Nov 11am MR4, Sat 24 Nov 11am MR4, early next term (tba).
Thursday 8 November lecture is moved to Saturday 10 November 11am (still MR4).

—Lecture 2—

1 1

Recall that we have an oracle U_f for $f : \mathbb{Z}_M \to \mathbb{Z}_\mathbb{N}$ periodic, with period r, $A = M/r$. We want to find r in $O(poly(m))$ time where $m = \log M$.

1.1 The quantum algorithm

Work on state space $\mathcal{H}_M \otimes \mathcal{N}$ with basis $\{|i\rangle|k\rangle\}_{i\in\mathbb{Z}_M, k\in\mathbb{Z}_N}$.
• Step 1. Make staet $\frac{1}{\sqrt{M}}\sum_{i=0}^{M-1}|i\rangle|0\rangle$.
• 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 a result y. By Born rule, the first register collapses to all those i's (and only those) with $f(i)$ equal to the seen y, i.e. $i = x_0, x_0+r, ..., x_0+(A-1)r$, where $0 \le x_0 < r$ in 1st period has $f(m) = y$. Discard 2nd register to get $|per\rangle = \frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0+jr\rangle$.
Note: each of the r possible function values y occurs with same probability $1/r$, so $0 \le x_0 < r$ has been chosen uniformly at random.
If we now measure $|per\rangle$, we'd get a value $x_0 + jr$ for uniformly random j, i.e. random element (x_0^{th}) of a random period (j^{th}), i.e. random element of $\mathbb{Z}_m$, so we could get no information about r.
• Step 4. Apply quantum Fourier transform mod M (QFT) to $|per\rangle$. Recall the definition of QFT: $QFT : |x\rangle \to \sum_{y=0}^{M-1}\omega^{xy}|y\rangle$ for all $x \in \mathbb{Z}_M$ where $\omega = e^{2\pi i/M}$ is the Mth root of unity. The existing result is that QFT mod M can be implemented in $O(M^2)$ time.
Then we get

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

where we group all the terms with the same $|y\rangle$ together. One good thing is that the sum inside the square bracket is a geometric series, with ratio $\alpha = \omega^{ry} = e^{2\pi i r y/M} = (e^{2\pi i/A})^y$.
Hence term inside bracket $= A$ if $\alpha = 1$, i.e. $y = kA = k\frac{M}{r}$, $k = 0, 1, ..., (r-1)$, and equals 0 otherwise when $\alpha \ne 1$. Now

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

The random shift x_0 now appears only in phase, so measurement probabilities are now independent of x_0!

Measuring $QFT|per\rangle$ gives a value c, where $c = k_0\frac{M}{r}$ with $0 \leq k_0 \leq r-1$ chosen uniformly at random. Thus $\frac{k_0}{r} = \frac{c}{M}$, note that c, M are known, r is unknown (what we want), and k_0 is unknown but uniformly random.

So note that if we are lucky and get a k_0 that is coprime to r then we could just simplify $\frac{c}{M}$ to get r. Obviously we cannot be always lucky every time, but by theorem in number theory, the number of integers $< r$ coprime to r grows as $O(r/\log\log r)$ for large r, so we know probability of k_0 coprime to r is $O(\frac{1}{\log\log r})$.

Then by some probability calculation we know that $O(1/p)$ trials are enough to achieve $1-\varepsilon$ probability of success.

So afer Step 4, cancel c/M to the lowest terms a/b, giving r as denominator b (if k_0 is coprime to r). Check b value by computing $f(0)$ and $f(b)$, since $b = r$ iff $f(0) = f(b)$.

Repeating $K = O(\log\log r)$ times gives r with any desired probability.

Further insights into utility of QFT here:
Write $R = \{0, r, 2r, ..., (A-1)r\} \subseteq \mathbb{Z}_M$. $|R\rangle = \frac{1}{\sqrt{A}}\sum_{k=0}^{A-1}|kr\rangle$, and $|per\rangle = |x_0 + R\rangle = \frac{1}{\sqrt{A}}\sum_{k=0}^{A-1}|x_0 + br\rangle$ where x_0 is the random shift that caused problem previously.
For each $x_0 \in \mathbb{Z}_M$, consider mapping $k \to k + x_0$ (shift by x_0) on $\mathbb{Z}_M$, which is a 1-1 invertible map.

So linear map $U(x_0)$ on $\mathcal{H}_M$ defined by $U(x_0) : |k\rangle \to |k + x_0\rangle$ is unitary, and $|x_0 + R\rangle = U(x_0)|R\rangle$.

Since $(\mathbb{Z}_M, +)$ is abelian, $U(x_0)U(x_1) = U(x_0 + x_1) = U(x_1)U(x_0)$ i.e. all $U(x_0)$'s commute as operators on $\mathcal{H}_M$.
So we have orthonormal basis of common eigenvectors $|\chi_k\rangle\}_{k\in\mathbb{Z}_M}$, called *shift invariant states.*

$U(x_0)|\chi_k\rangle = \omega(x_0, k)|\chi_k\rangle$ for all $x_0, k \in \mathbb{Z}_M$ with $|\omega(x_0, k)| = 1$. Now consider $|R\rangle$ written in $|\chi\rangle$ basis,
$|R\rangle = \sum_{k=0}^{M-1} a_k|\chi_k\rangle$ where a_k's depending on r (not x_0).
Then $|per\rangle = U(x_0)|R\rangle = \sum_{k=0}^{M-1} a_k\omega(x_0, k)|\chi_k\rangle$, and measurement in the χ-basis has $prob(k) = |a_k\omega(x_0, k)|^2 = |a_k|^2$ which is independent of x_0, i.e. giving information about r!

—Lecture 3—

Recall last time we had $\mathcal{H}_M$: shift operations $U(x_0)|y\rangle = |y + x_0\rangle$ for $x_0, y \in$

$\mathbb{Z}_M$, which all permute, so have a common eigenbasis (shift invariant states) $\{|\chi_k\rangle\}_{k\in\mathbb{Z}_M}$, $U(x_0)|x_k\rangle = \omega(x_0,k)|\chi_k\rangle$.
Measurement of $|x_0+R\rangle = \frac{1}{\sqrt{A}}\sum_{l=0}^{A-1}|x_0+l_r\rangle = U(x_0)|R\rangle$ in $|\chi\rangle$ basis has output distribution independent of x_0, therefore gives information about r.

Introduce QFT as the unitary mapping that rotates χ-basis to standard basis, i.e. define $QFT|\chi_k\rangle = |k\rangle$. So QFT followed by measurement implements χ-basis measurement.

Explicit form of $|\chi_k\rangle$ eigenspaces (!): consider

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

Then

$$\begin{aligned}U(x_0)|\chi_k\rangle &= \frac{1}{\sqrt{M}}\sum_{l=0}^{M-1} e^{-2\pi ikl/M}|l+x_0\rangle\\ &= \frac{1}{\sqrt{M}}\sum_{\tilde{l}=0}^{M-1} e^{-2\pi ik(\tilde{l}-x_0)/M}|\tilde{l}\rangle \text{ where } \tilde{l} = l+x_0\\ &= e^{2\pi ikx_0/M}\cdot|\chi_k\rangle\end{aligned}$$

i.e. these are the shift invariant staets, eigenvalues $\omega(x_0,k) = e^{2\pi ikx_0/M}$.

Matrix of QFT: So

$$[QFT^{-1}]_{lk} = \frac{1}{\sqrt{M}}e^{-2\pi ilk/M}$$

(componets of $|\chi_k\rangle = QFT^{-1}|k\rangle$ as k^{th} column). So

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

as expected.

2 The hidden subgroup problem (HSP)

Let G be a finite group of size $|G|$. Given (oracle for) function $f : G \to X$ (X is some set), and promise that there is a subgroup $K < G$ such that f is constant on (left) cosets of K in G, and f is distinct on distinct cosets.
The problem: determine the *hidden subgroup* K (e.g. output a set of generators, or sample uniformly from K).
We want to solve in time $O(poly(\log |G|))$ (an efficient algorithm) with any constant probability $1 - \varepsilon$.

Examples of problems that can be cast(?) as HSPs:
(i) periodicity: $f : \mathbb{Z}_M \to X$, periodic with period r. Let $G = (\mathbb{Z}_m, +)$, the hidden subgroup is $K = \{0, r, 2r, ...\} < G$, cosets $x_0 + K = \{x_0, x_0 + r, x_0 + 2r, ...\}$. The period r is generator of K.
(ii) discrete logarithm: for prime p, $\mathbb{Z}_p^* = \{1, 2, ..., p-1\}$ with multiplication mod p. $g \in \mathbb{Z}_p^*$ is a generator (or primitive root mod p). If powers generate all of $\mathbb{Z}_p^*$, $\mathbb{Z}_p^* = \{g^0 = 1, g^1, ..., g^{p-2}\}$, then also $g^{p-1} \equiv 1 \pmod p$ (easy number theory).
Fact: the generator always exists if p is prime. So any $x \in \mathbb{Z}_p^*$ can be written $x = g^y$ for some $y \in \mathbb{Z}_{p-1}$, write $y = \log_g x$ called the discrete log of x to base g.

Discrete log problem: given a generator g and $x \in \mathbb{Z}_p^*$, compute $y = \log_g x$ (classically hard).
To express as HSP, consider $f : \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$: $f(a, b) = g^a x^{-b} \ mod \ p = g^{a-yb} \ mod \ p$.
Then check: $f(a_1, b_1) = f(a_2, b_2)$ iff $(a_2, b_2) = (a_1, b_1) + \lambda(y, 1)$ where $\lambda \in \mathbb{Z}_{p-1}$.

So if $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, $K = \{\lambda(y, 1) : \lambda \in \mathbb{Z}_{p-1}\} < G$. Then f is constant and distinct on the cosets of K in G, and generator $(y, 1)$ gives $y = \log_g x$.

(iii) graph problems (G non-abelian now): consider undirected graph $A = \{V, E\}$, $|V| = n$, with at most one edge between any two vertices. Label vertices by $[n] = \{1, 2, ..., n\}$.
Introduce the permutation group $\mathcal{P}_n$ of $[n]$. Define $Aut(A)$ to be the group of automorphisms of A, which is a subgroup of $\mathcal{P}_n$, containing exactly the permutations $\pi \in \mathcal{P}_n$ such that for all $i, j \in [n]$, $(i, j) \in E \iff (\pi(i), \pi(j)) \in E$, i.e. the labelled graph $\pi(A)$ obtained by permuting labels of A by π is the same *labelled* graph as A.

Associated HSP: Take $G = \mathcal{P}_n$. Let X be set of all labelled graphs on n vertices. Given A, consider $f_A : \mathcal{P}_n \to X$ by $f_A(\pi) = \pi(A)$, A with labels permuted by π. The associated hiiden subroup is $Aut(A) = K$.

Application: if we can sample uniformly from this K, then we can solve graph isomorphism problem (GI): two labelled graphs A, B are isomorphic if there is 1-1 map $\pi : [n] \to [n]$ such that for all $i, j \in [n]$, i, j is an edge in A iff $\pi(i), \pi(j)$ is an edge in B, i.e. A and B are the same graph but just labelled differently.

—Lecture 4—

Let's come back to the graph isomorphism problem.

Problem: given A, B, decide if $A \cong B$ or not. This can be expressed as anon-abelian HSP (on example sheet), no known classical polynomial time algorithm. However it is in NP, but it is not believed to be NP-complete.
Recent result (2017): a quasi-poly time classical algorithm (L.Babai).

Quantum algorithm for finite *abelian* HSP:
Write group $(G, +)$ additively.

Construction of shift invariant states and FT for G:
Let's introduce some representation theory for abelian group G. Consider mapping $\chi : G \to \mathbb{C}^* = (\mathbb{C} \setminus \{0\}, \cdot)$ satisfying $\chi(g_1 + g_2) = \chi(g_1)\chi(g_2)$, i.e. χ is a group homomorphism. Such χ's are called *irreducible* representations of G.
We have the following properties (without proof), which we'll call Theorem A later when we refer to it:
(i) any value $\chi(g)$ is a $|G|^{th}$ root of unity (so χ: $G \to S^1$ = unit circle in $\mathbb{C}$);
(ii) (Schur's lemma, orthogonality): If χ_i and χ_j are representations, then $\sum_{g \in G} \chi_i(g)\bar{\chi}_j(g) = \delta_{ij}|G|$;
(iii) there are always exactly $|G|$ different representations χ (well, this is a special case of general representation theory).

By (iii), we can label χ's as χ_g for $g \in G$. For example, $\chi(g) = 1$ for all $g \in G$ is always an irreducible representation (the trivial representation), labelled χ_0;
Then by orthogonality (ii) for any $\chi \neq \chi_0$ gives $\sum_{g \in G} \chi(g) = 0$.

Shift invariant states: in space $\mathcal{H}_{|G|}$ with basis $\{|g\rangle\}_{g \in G}$, introduce *shift operators* $U(k)$ for $k \in G$ defined by $U(k) : |g\rangle \to |g + k\rangle$. Clearly these all commute, so there is simultaneous eigenbasis:
For each χ_k, $k \in G$, consider state $|\chi_k\rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} \bar{\chi}_k(g)|g\rangle$. Then theorem A(ii) implies these form orthonormal basis, and $U(g)|\chi_k\rangle = \chi_k(g)|\chi_k\rangle$.

Proof.

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

This implies that

$$\chi_k * -g) = (\chi_k(g))^{-1} = \bar{\chi_k}(g),$$
$$\chi_k(\overline{h'} - g) = \bar{\chi_k}(h')\bar{\chi_k}(-g) = \chi_k(h')\chi_k(g)$$

So

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

□

So $|\chi_k\rangle$'s are common eigenspaces, called *shift-invariant states.*
Introduce (define) Fourier transform QFT for group G as the unitary that

$QFT|\chi_g\rangle = |g\rangle$ for all $g \in G$.
In $|g\rangle-$basis matrices, k^{th} column of (QFT^{-1}) =components of $|\chi_k\rangle$, i.e. $\frac{1}{\sqrt{|G|}}\bar{\chi_k}(g) = [QFT^{-1}]_{gk}$.
So $[QFT]^\dagger_{kg} = \frac{1}{\sqrt{|G|}}\chi_k(g)$, and so $QFT|g\rangle = \frac{1}{\sqrt{|G|}}\sum_{k\in G}\chi_k(g)|k\rangle$.

Example. $G = \mathbb{Z}_M$. Check $\chi_a(b) = e^{2\pi iab/M}$, $a, b \in \mathbb{Z}_M$ is a representation.
Similarly, for $G = \mathbb{Z}_{M_1} \times ... \times \mathbb{Z}_{M_r}$, $(a_1, ..., a_r) = g_1, (b_1, ..., b_r) = g_2$ where $g_1, g_2 \in G$,

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

is a representation of G. And we get

$$QFT_G = QFT_{M_1} \otimes ... \otimes QFT_{M_r}$$

on $\mathcal{H}_{|G|} = \mathcal{H}_{M_1} \otimes ... \otimes \mathcal{H}_{M_r}$.
This is exhaustive, since by classification theorem, every finite abelian group G is isomorphic to a direct product of the form $G \cong \mathbb{Z}_{M_1} \times ... \times \mathbb{Z}_{M_r}$. Furthermore, we can insist that M_i are prime powers $p_i^{s_i}$, where p_i are not necessarily distinct.

Quantum algorithm for finite abelian HSP:
Let $f : G \to X$, hidden subgroup $K < G$. We have cosets $K = 0 + K, g_2 + K, ..., g_m+K$, where $m = |G|/|K|$. State space as usual, with basis $\{|g\rangle, |x\rangle\}_{g\in G, x\in X}$.
• make the state $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|0\rangle$;
• Apply oracle U_f, get $\frac{1}{\sqrt{|G|}}\sum_{g\in G}|g\rangle|f(g)\rangle$;
measure second register to see a value $f(g_0)$.
Then first register gives coset state (remember the function is constant on each coset). $|g_0 + K\rangle = \frac{1}{\sqrt{|K|}}\sum_{k\in K}|g_0 + K\rangle = U(g_0)|K\rangle$.
Apply QFT and measure to obtain result $g \in G$.

—Lecture 5—

Last time we disccused how to solve the abelian HSP problem. Now how does the output g related to K?
• the output distribution of g is independent of g_0, so same as that obtained from $QFT|K\rangle$ (i.e. $g_0 = 0$) since:
write $|K\rangle$ in shift invariant basis $|\chi_g\rangle$'s, $|K\rangle = \sum_g a_g|\chi_g\rangle$, then $|g_0 + K\rangle = U(g_0)|K\rangle = \sum a_g \underbrace{\chi_g(g_0)|\chi_g\rangle}_{=U(g_0)|\chi_g\rangle}$; but $QFT|\chi_g\rangle = |g\rangle$, so $Prob(g) = |a_g\chi_g(g_0)|^2 = |a_g|^2$ as $\chi_g(g_0)| = 1$.

Thus look at $QFT|K\rangle$. Recall $QFT|k\rangle = \frac{1}{\sqrt{|G|}}\sum_{l\in G}\chi_l(k)|l\rangle$, so $QFT|K\rangle = \frac{1}{\sqrt{|G|}}\frac{1}{\sqrt{|K|}}\sum_{l\in G}\left[\sum_{k\in K}\chi_l(k)\right]|l\rangle$.
The terms in [...] involves irreducible representation χ_l of G restricted to subgroup $K < G$, which is an irreducible representation of K. Hence

$$\sum_{k\in K}\chi_l(k) = \begin{cases} |K| & \chi_l \text{ restricts to trivial irreducible representation on } K \\ 0 & \text{otherwise} \end{cases}$$

and

$$QFT|K\rangle = \sqrt{\frac{|K|}{|G|}} \sum_{l \in G \text{ with } \chi_l \text{ reducing to trivial irreducible representation of } K} |l\rangle$$

So measurement gives a uniformly random choice of l such that $\chi_l(k) = 1$ for all $k \in K$.
e.g. If K has generators $k_1, k_2, ..., k_M$, $M = O(\log |K|) = O(\log |G|)$, then output has $\chi_l(k_i) = 1$ for all i.

It can be shown that if $O(\log |G|)$ such l's are chosen uniformly at random, then with probability $> 2/3$ they suffice to determine a generating set for K via equations $\chi_l(k) = 1$.
(see example sheet 1 for particular examples).

Example. If $G = \mathbb{Z}_{M_1} \times ... \times \mathbb{Z}_{M_q}$.
We had for $l = (l_1, ..., l_q)$, $g \in (b_1, ..., b_q) \in G$,

$$\chi_l(g) = e^{2\pi i(\frac{l_1 k_1}{M_1} + ... + \frac{l_q b_q}{M_q})}$$

So for $k = (k_1, ..., k_q)$, $\chi_l(k) = 1$ becomes

$$\frac{l_1 k_1}{M_1} + ... + \frac{l_q k_q}{M_q} \equiv 0 \pmod 1$$

(i.e. is an integer), a homogeneous linear equation on K, and $O(\log |K|)$ is independent such that equations determine K as null space.

Some remarks on HSP for non-abelian groups G (write multiplicatively):
As before, can easily generate coset states

$$|g_0 K\rangle = \frac{1}{\sqrt{|K|}} \sum_{k \in K} |g_0 K\rangle$$

where g_0's are randomly chosen. But problems arise with QFT construction, because now there's no basis of shift-invariant states exists! (this is since $U(g_0)$'s don't commute anymore, so no common full eigenbasis).

Construction of non-abelian Fourier Transform (some more representation theory):
• d-dimensional representation of G is a group homomorphism $\chi : G \to U(d)$ where $U(d)$ is the space of $d \times d$ unitary matrices acting on $\mathbb{C}^d$, by $\chi(g_1 g_2)\chi(g_1)\chi(g_2)$. (see part II representation theory for the general form)
• χ is irreducible representation if no subspace of $\mathbb{C}^d$ is left invariant under $\chi(g)$ for all $g \in G$ (i.e. cannot simultaneously block diagonalise all $\chi(g)$'s by a basis change).
• a complete set of irreducible representation: set $\chi_1, ..., \chi_m$ such that any irreducible representation is unitarily equivalent to one of them (equivalence $\chi \to \chi' = V\chi V^T$).

Theorem. (non-abelian version of theorem A – properties of representations)
If $d_1, ..., d_m$ are dimensions of a complete set of irreducible representations

$\chi_1, ..., \chi_m$, then:
(i) $d_1^2 + ... + d_m^2 = |G|$;
(ii) Write $\chi_i(g)_{jk}$ for the $(j,k)^{th}$ entry of matrix $\chi_i(g)$, where $j,k = 1, ..., d_i$. Then (Schur orthogonality):

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

Hence states

$$|\chi_{i,jk}\rangle \equiv \frac{1}{\sqrt{|G|}}\sum_{g\in G}\bar{\chi}_i(g)_{jk}|g\rangle$$

is an orthonomal basis.

• QFT on G *defined* to be the unitary that rotates $\{|\chi_{ijk}\rangle\}$ basis into standard basis $\{|g\rangle\}$. However, $|\chi_{ijk}\rangle$ are *not* shift invariant for all $U(g_0)$'s, and consequently measurement of coset state $|g_0K\rangle$ in $|\chi\rangle$-basis gives an output distribution *not* independent of g_0.

However, *partial* shift invariance survives: Consider the incomplete measurement M_{rep} on $|g_0K\rangle$ that distinguishes only the irreducible representations (i.e. i values) and not all (i,j,k)'s.
i.e. with measurement outcome i associated to d_i^2-dimensional orthogonal subspaces spanned by $\{|\chi_{(i),jk}\rangle\}_{j,k=1,...,d_i}$.
Then $\chi_i(g_1, g_2) = \chi_i(g_1)\chi_i(g_2)$ implies output distribution of i values is independent of g_0, giving direct, albeit imcomplete, information about K.
E.g. conjugate subgroups K and $= g_0Kg_0^{-1}$ for some $g_0 \in G$ give *same* output distribution.