Lecture 10

Oct 29, 2024

Problem (Abelian Hidden Subgroup)

given an abelian group G and $H \leq G$ and a fn f hiding H, find a generating set for H.

A q. algorithm for solving AHSP exists* and it will be a generalization of Simon's algorithm.

Requires quantum Fourier transform for an abelian group.

$H = QFT(\mathbb{Z}_2)$ and $H^{\otimes n} = QFT(\mathbb{Z}_2^n)$.

What is QFT? A unitary finding a different basis for $\mathbb{C}^{|G|}$.

Illustrative to understand $G = \mathbb{Z}_N$. Let $\omega = e^{\frac{2\pi \hat{i}}{N}}$. ← imaginary i

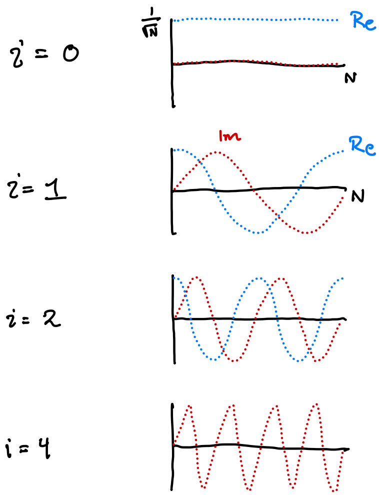
For $i \in \{0, \dots, N-1\}$,

$$QFT|i\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{i \cdot j} |j\rangle$$

or $QFT_{ij} = \langle j | QFT | i \rangle = \frac{1}{\sqrt{N}} \omega^{i \cdot j} = \frac{1}{\sqrt{N}} \left(\cos \frac{2\pi i j}{N} + \hat{i} \sin \frac{2\pi i j}{N} \right)$

Visualizing $QFT|i\rangle$ (for large N).

Plot QFT_{ij} as a fn of j: (For large N)



Curves are discrete approximations of sine and cosine fns.

For a general abelian group G, in order to define $QFT(G)$, we need the notion of a character from group theory.

For now, $\chi : G \times G \to \mathbb{C} \setminus \{0\}$ s.t.

① $\chi(g,h) = \chi(h,g) \quad \forall\, g,h \in G$

② $\chi(g, h_1 + h_2) = \chi(g,h_1)\,\chi(g,h_2). \quad \forall\, g, h_1, h_2 \in G$

③ $\sum_{h \in G} \chi(g,h)^* \chi(g',h) = |G|\, \mathbb{1}_{\{g = g'\}} \quad \forall\, g, g' \in G.$

Then $QFT(G) \in \mathbb{C}^{|G| \times |G|}$ defined by

$$QFT\,|g\rangle = \frac{1}{\sqrt{|G|}} \sum_{h \in G} \chi(g,h)\,|h\rangle.$$

or $$QFT = \frac{1}{\sqrt{|G|}} \sum_{g,h \in G} \chi(g,h)\,|h\rangle\langle g|.$$

Pf QFT is unitary:

$$\langle g_1|\, QFT^{+} QFT\, |g_2\rangle$$

$$= \frac{1}{|G|} \sum_{h_1,h_2 \in G} \langle h_1|\, \chi(g_1,h_1)^* \, \chi(g_2,h_2)\,|h_2\rangle$$

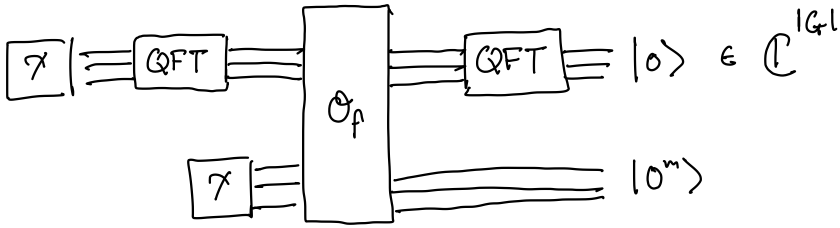
$$= \frac{1}{|G|} \sum_{h \in G} \chi(g_1,h)^* \chi(g_2,h)$$

$$= \frac{1}{|G|} \cdot |G|\, \mathbb{1}_{\{g=g'\}} = \mathbb{1}_{\{g=g'\}}.$$

Let's use QFT to solve AHSP and then get to writing an efficient q. circuit for QFT — for all we know it could be hard to implement.

Idea: Subroutine to learn random element of $H^\perp$

where $H^\perp$ is the subgroup $\{ g \mid \chi(g,h) = 1 \ \forall\ h \in H \}$.



Alternatively, we can ignore the second measurement like in Simon's problem.

Before O_f query: $\displaystyle \frac{1}{\sqrt{|G|}} \sum_{g \in G} \chi(0,g)\, |g\rangle\, |0^m\rangle$

$$= \frac{1}{\sqrt{|G|}} \sum_{g} |g\rangle |0^m\rangle$$

since $\chi(0,g)\chi(h,g) = \chi(0+h,g) \Rightarrow \chi(0,g) = 1$

After O_f query and measurement. For some $z \in \{0,1\}^m$,

$$\propto \sum_{g:\, f(g) = z} |g\rangle$$

$$\{ g : f(g) = z \} = g_0 + H = \{ g_0 + h \mid h \in H \} \text{ for some } g_0.$$

So state equals $\displaystyle \frac{1}{\sqrt{|H|}} \sum_{h \in H} |g_0 + h\rangle$

Apply QFT : $\displaystyle \frac{1}{\sqrt{|G| \cdot |H|}} \sum_{h \in H} \sum_{g \in G} \chi(g_0 + h, g) |g\rangle$

$$= \frac{1}{\sqrt{|G| \cdot |H|}} \sum_{h \in H} \sum_{g \in G} \chi(g_0, g) \chi(h, g) |g\rangle$$

$$= \frac{1}{\sqrt{|G| \cdot |H|}} \sum_{g \in G} \chi(g_0, g) \Big(\underbrace{\sum_{h \in H} \chi(h, g)}_{|H| \, \mathbb{1}_{\{g \in H^\perp\}} \quad (*)} \Big) |g\rangle$$

$$= \sqrt{\frac{|H|}{|G|}} \sum_{g \in H^\perp} \chi(g_0, g) |g\rangle = \frac{1}{\sqrt{|H^\perp|}} \sum_{g \in H^\perp} \chi(g_0, g) |g\rangle$$

Measuring gives $g \in H^\perp$ uniformly randomly. ∎

Pf of $(*)$: Write $g \in G$ as $g_1 + g_2$, $g_1 \in H$, $g_2 \in H^\perp$

$$\sum_{h \in H} \chi(h, g) = \sum_{h \in H} \chi(h, g_1) \underbrace{\chi(h, g_2)}_{1}$$

$$= \sum_{h \in H} \chi(h, g_1) \cdot 1$$

$$= \sum_{h \in H} \chi(h, g_1)\, \chi(h, 0)$$

$$= |H| \cdot \mathbb{1}_{\{g_1 = 0\}}$$

$$= |H| \cdot \mathbb{1}_{\{g \in H^\perp\}}.$$

Ok, learning samples from $H^\perp$ can be used to calculate a generating set for H using Gaussian elimination.

For Simon's problem, $H = \{0, s\}$ so $H^\perp = \{y : y \cdot s = 0\}$.

Solving AHSP when $G = \mathbb{Z}_Q$, r divides Q

$f(x) = f(x')$ iff $x' - x$ is a multiple of r :

When $G = \mathbb{Z}_Q$, $\chi(g, h) = \omega^{g \cdot h}$ where $\omega = e^{2\pi i / Q}$

Each sample gives y s.t. $\chi(y, r) = 1 \iff yr \equiv 0 \bmod Q$

or $yr = kQ$. Since r divides Q, $\frac{Q}{r}$ is an int.

Each sample $y_i = k_i \cdot \frac{Q}{r}$ is an integer.

$$GCD(\{y_i\}) = \frac{Q}{r}$$ with high probability with

$O(\log Q)$ samples. Next lecture, we will review Euclid's algorithm for efficiently calculating GCD.

But...

We still need to create a q. circuit for QFT.

When $G = \mathbb{Z}_Q$, $\chi(g,h) = \omega^{g \cdot h}$ where $\omega = e^{2\pi i/Q}$

And for groups G_1, G_2

$$\chi_{G_1 \times G_2}((g_1,g_2),(h_1,h_2)) = \chi_{G_1}(g_1,h_1) \cdot \chi_{G_2}(g_2,h_2).$$

equiv. $QFT(G_1 \times G_2) = QFT(G_1) \otimes QFT(G_2)$.

Note that all abelian groups are isomorphic to

$$\mathbb{Z}_{Q_1} \times \ldots \times \mathbb{Z}_{Q_k}.$$

We know how to produce $H = QFT(\mathbb{Z}_2)$

and $H^{\otimes n} = QFT(\mathbb{Z}_2^n)$

We will show how to produce $QFT(\mathbb{Z}_N)$ for $N = 2^n$.

Note: $\mathbb{Z}_{2^N} \neq \mathbb{Z}_2^n$. Turns out sufficient for Shor's.

For $x \in N$, write $x = x_1 \ldots x_n$ as a binary number,

<u>Claim</u> $$QFT|x\rangle = \bigotimes_{j=1}^{n} \frac{1}{\sqrt{2}}\left(|0\rangle + \omega^{x 2^{n-j}} |1\rangle\right) =: \bigotimes_{j=1}^{n} |\psi_j^{(x)}\rangle$$

<u>Pf</u>. $$\langle y| \bigotimes_{j=1}^{n} \frac{1}{\sqrt{2}}\left(|0\rangle + \omega^{x 2^{n-j}} |1\rangle\right)$$

$$= \prod_{j : y_j = 1} \omega^{x 2^{n-j}}$$

$$= \omega^{\left(\sum_{j:\, y_j=1} x\, 2^{n-j}\right)}$$

$$= \omega^{\left(x \cdot \underbrace{\sum_{j=1}^{n} y_j\, 2^{n-j}}_{\text{binary decomposition of } y}\right)}$$

$$= \omega^{x \cdot y}. \qquad \blacksquare$$

Notice $\omega^{x\,2^{n-j}} = \omega^{(x\,2^{n-j} \bmod N)}$

$$x \cdot 2^{n-j} \bmod N = \sum_{k=1}^{n} x_k\, 2^{n-k} \cdot 2^{n-j} \bmod N$$

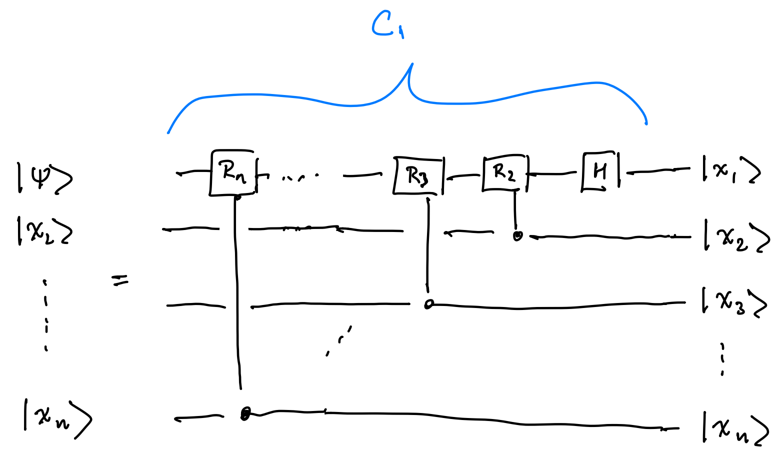
$$= \sum_{k \geq n-j}^{n} x_k\, 2^{2n-k-j}.$$

Using this, let's write a q. circuit for QFT.

gates: H, $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$ and $CR_k = \begin{pmatrix} \mathbb{1}_2 & \\ & R_k \end{pmatrix}$

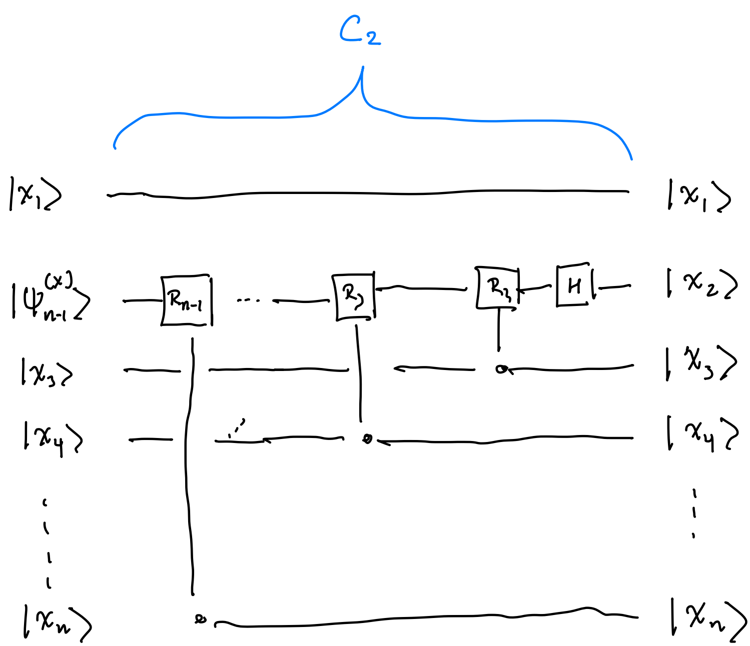
$$e^{2\pi i/2^k} = \omega^{(2^{n-k})}$$

Subcircuit:

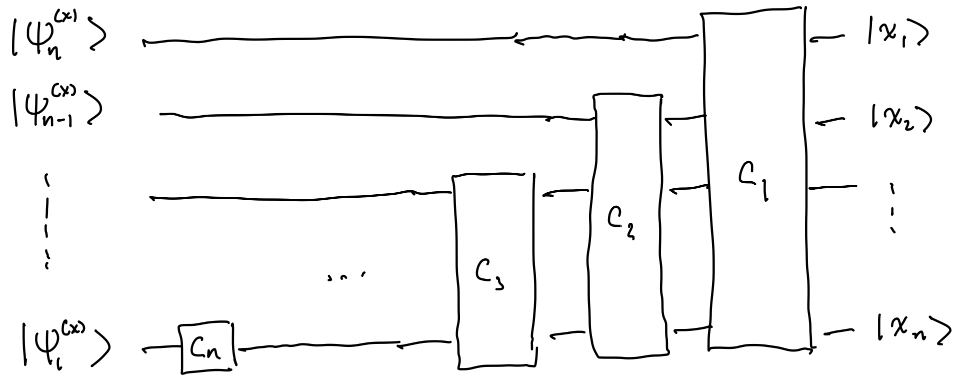


$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \omega^{\left(\sum_{k\geq 1}^{n} 2^{n-k} x_k\right)} |1\rangle\right) = |\psi_n^{(x)}\rangle$$

Similarly,



So,



Correct up to permutation of gates.

Need to append $SWAP_{1,n}\ SWAP_{2,n-1}, \ldots\ SWAP_{\frac{n}{2},\frac{n}{2}+1}$.

This produces QFT transform for any fixed $N = 2^n$.

C_1 has n gates, C_2 has $n-1$ gates, ...

total $O(n^2)$ gates + n swap gates.

There is still a fundamental issue: $C\text{-}R_k$ gates may be expensive to apply.

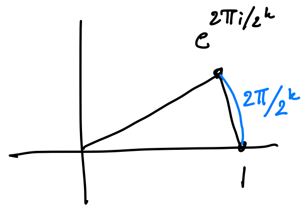
Not all $C\text{-}R_k$ gates may be necessary.

Consider replacing gate g in ckt with g' s.t.

$$\|g - g'\| \le \epsilon.$$

By unitarity, total change in output POVM is also ϵ.

$$C\text{-}R_k = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & e^{2\pi i/2^k} \end{pmatrix}$$ so



$$\| C\text{-}R_k - \mathbb{1}_4 \| = |e^{2\pi i/2^k} - 1| \le \frac{2\pi}{2^k}.$$

Notice $C\text{-}R_k$ gate appears $n-k$ times in QFT circuit.

Total error of replacing each $C\text{-}R_k$ gate with $\mathbb{1}$ for $k \ge K$:

$$\le \frac{2\pi}{2^K} \frac{(n-K)(n-K+1)}{2} \lessapprox \frac{n^2}{2^K}$$

If we tolerate ϵ error in our QFT unitary, we can ignore every $C\text{-}R_k$ gate for $K \ge \log\left(\frac{n^2}{\epsilon}\right)$.

We have reduced from $O(n^2)$ gates to $O(n \log \frac{n}{\epsilon})$ gates.

Time permitting, we will see how to generate any remaining gate approximately from a family of standard gates.

(Solovay-Kitaev theorem)

Next time:

- The classical setup / mathematics of Shor's factoring algorithm.

- Order finding and a quantum algorithm for it.