Quantum Computing Seminar

GMU Math & CS Depts., Spring 2024

Lectures 1 and 2

Casey Blacker

Shor's Algorithm

Peter Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer"

1. Outline
2. From orders to factors ~~Sec 5~~ §5
3. The quantum Fourier transform ~~Sec 4~~ §4
4. Finding the orders ~~Sec 5~~ §5

1. Outline

Fix $n \in \mathbb{N}$

Goal: factor n.

2 steps:

quantum 1. find the order r of a random $x \pmod n$
- use the quantum Fourier transform
- interpret by the "periodicity principle"

classical 2. use this to find a nontrivial factor of n.

2. From orders to factors

Fix $n \in \mathbb{N}$.

Def. The order of $x \pmod n$ is the least $r \geq 1$ s.t.

$$x^r \equiv 1 \pmod n.$$

Goal: factor n

Given: the ability to find $\text{ord}(x)$ for every $x \leq n$ w/ $\gcd(x,n) \stackrel{?}{=} 1$.

Steps:

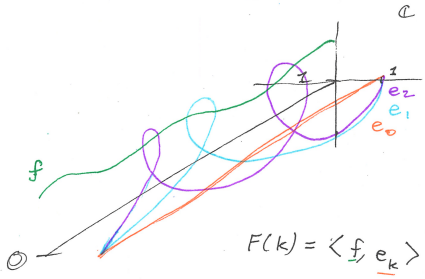
1. choose a random $x \leq n$ — $\gcd(x,n) > 1$ → done!
2. find its order r — r odd, $x^{r/2} \equiv \pm 1$

$$n \mid (x^r - 1) \implies n \mid \underbrace{(x^{r/2}+1)}_{a}\underbrace{(x^{r/2}-1)}_{b}$$

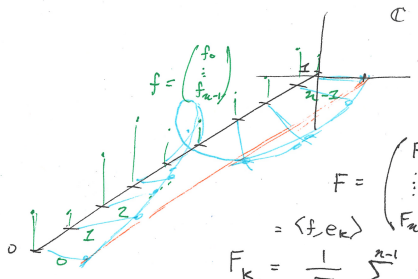
$n \nmid a, b$

3. compute $\boxed{\gcd(x^{r/2}-1, n)}$ > 1, $< n$

3. The quantum Fourier transform



$$F(k) = \langle f, e_k \rangle = \int_I f(x)\, \underbrace{e^{-2\pi i k x}}_{\overline{e_k}}\, dx$$



$$= \langle f, e_k \rangle$$

$$F_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} f_j\, e^{-2\pi i k \frac{j}{n}}$$

$$(F_k)_k = (\omega^{jk})_{k,j}\, (f_j)_j$$

$$\mathrm{DFT}: f \longmapsto F, \quad \begin{pmatrix} f_0 \\ \vdots \\ f_{n-1} \end{pmatrix} \longmapsto \begin{pmatrix} F_0 \\ \vdots \\ F_{n-1} \end{pmatrix}$$

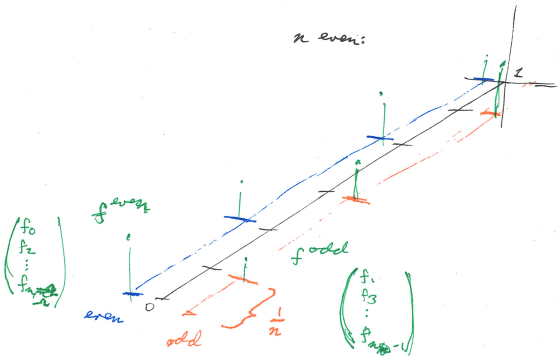
$$A_n \qquad \sum_{a=0}^{n-1} f_a |a\rangle \xrightarrow{\mathrm{QFT}} \sum_{c=0}^{n-1} F_c |c\rangle$$

$$|a\rangle \longmapsto \frac{1}{\sqrt{n}} \sum_{c=0}^{n-1} e^{2\pi i c \frac{a}{n}} |c\rangle$$

Fourier series ← approximates — $O(n^2)$ discrete FT

efficiently computes ↑

$O(n \log n)$ fast FT ← implements — quantum FT



$$F_k = \frac{1}{\sqrt{n}} \sum_{j\ \mathrm{even}} f_j\, e^{2\pi i k \frac{j}{n}} + \frac{1}{\sqrt{n}} \sum_{j\ \mathrm{odd}} f_j\, e^{2\pi i k \frac{j}{n}}$$

$j = 2l$ $\qquad$ $j = 2l+1$

$$= \underbrace{\frac{1}{\sqrt{n}} \sum_{l=0}^{n/2-1} f_{2l}\, e^{2\pi i k \frac{l}{n/2}}}_{F_k^{\mathrm{even}}} + \underbrace{\frac{1}{\sqrt{n}}\, e^{2\pi i k \frac{1}{n}} \sum_{l=0}^{n/2-1} f_{2l+1}\, e^{2\pi i k \frac{l}{n/2}}}_{e^{2\pi i k \frac{1}{n}} F_k^{\mathrm{odd}}}$$

$$= F_k^{\mathrm{even}} + e^{2\pi i \frac{k}{n}} F_k^{\mathrm{odd}}$$

* measuring $\sum_{c=0}^{n-1} F_c |c\rangle$ yields $|c\rangle$ with $\mathbb{P}(|c\rangle) = |F_c|^2$.

* We observe the index, $|c\rangle$.

* No direct access to the value F_c.

$$F \approx e_j \implies \mathbb{P}(|j\rangle) \approx 1$$

---

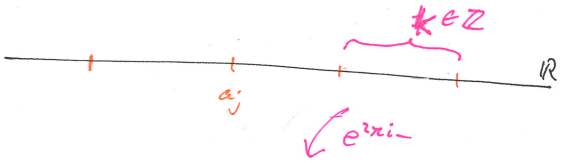
more generally,

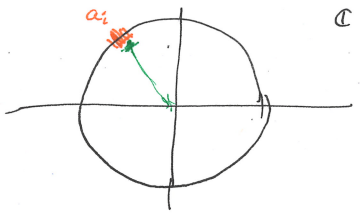
↳ nonstandard terminology

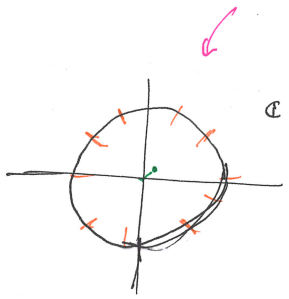
Periodicity principle

If $\{\alpha_j\}_{j\leq n}$ is approx. α-periodic, then

$$\left| \underbrace{\frac{1}{n} \sum_{j\leq n} e^{2\pi i \alpha_j}}_{\text{average}} \right|^2 \approx \begin{cases} 1 & \text{if } \alpha \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$$







4. Finding the order

Fix $n \in \mathbb{N}$, $x \leq n$ w/ $\gcd(x,n) = 1$, q s.t. w/ $n^2 \leq q \leq 2n^2$

Goal: Find the order r of $x \pmod n$

Steps:

1. Put the computer in state
$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |0\rangle$$

2. Compute $x^a \pmod n$ in the second register
$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a\rangle$$

3. Perform the QFT in the first register
$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e^{2\pi i ac/q} |c\rangle |x^a\rangle$$

4. Measure the state.

$$P(|c\rangle |x^k\rangle) = \left| \frac{1}{q} \sum_{a : x^a \equiv x^k} e^{2\pi i\, ac/q} \right|^2$$

$$= \left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} e^{2\pi i (br+k)c/q} \right|^2 \qquad a = br + k$$

$$= \left| \frac{1}{q} \sum_{b} e^{2\pi i\, brc/q} \right|^2, \qquad \{brc/q\}_b$$

periodicity principle $\Rightarrow$
$$\begin{cases} \text{large} & \text{if } rc/q \approx d \in \mathbb{Z} \\ \text{small} & \text{otherwise} \end{cases}$$

relatively high prob. that

$$\left|\frac{c}{q} - \frac{d}{r}\right| \leq \frac{1}{2q} \leq \frac{1}{n^2}$$

small, can be shown

$\Rightarrow$ at most one candidate in lowest terms $\frac{d_0}{r_0}$ $(r_0 < n)$

$$r_0 \mid r$$

Obtain more $r_1, r_2, \ldots r_k$ and take (best guess) $r = \text{lcm}(r_0, \ldots r_k)$.

The Hidden Subgroup Problem

1. Review
2. Problem statement
3. The abelian case
4. Graph isomorphism

---

1. Review

Shor's algorithm:

$n \in \mathbb{N}$, $x < n$, $\gcd(x,n)=1$, q power of 2 s.t. $n^2 < q \leq 2n^2$

Goal: Find the order of $x \pmod n$

Steps:

1. Prepare state

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |0\rangle$$

2. Compute $x^a \pmod n$ in 2nd register

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle |x^a\rangle$$

3. QFT in 1st register

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e^{2\pi i ac/q} |c\rangle |x^a\rangle$$

4. Measure

$$\mathbb{P}(|c\rangle |x^k\rangle) = \left| \frac{1}{q} \sum_{a : x^a = x^k} e^{2\pi i ac/q} \right|^2$$

$$= \left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r \rfloor} e^{2\pi i (br+k)c/q} \right|^2$$

$$= \left| \frac{1}{q} \sum_{b} e^{2\pi i brc/q} \right|^2$$

$$= \begin{cases} \text{larger} & \text{if } rc/q \approx d \in \mathbb{Z} \\ \text{smaller} & \text{otherwise} \end{cases}$$

simplify & abstract →

$q := n$

+ clean generalization
+ probabilities 0,1
− further from an actual implementation

Goal: Find a generator of the subgroup $\langle r \rangle \leq \mathbb{Z}_n$.

$\langle r \rangle = \ker\left(a \xmapsto{f} x^a\right)$

Steps:

1. Prepare state

$$\frac{1}{\sqrt{n}} \sum_{a \in \mathbb{Z}_n} |a\rangle |0\rangle$$

2. compute x^a in 2nd reg.

$$\frac{1}{\sqrt{n}} \sum_{a \in \mathbb{Z}_n} |a\rangle |x^a\rangle$$

3. DFT in 1st reg.

$$\frac{1}{n} \sum_{a \in \mathbb{Z}_n} \sum_{c \in \mathbb{Z}_n} e_c(a) |c\rangle |x^a\rangle$$

4. Measure.

$$\mathbb{P}(|c\rangle |x^k\rangle) = \left| \frac{1}{n} \sum_{a : x^a = x^k} e_c(a) \right|^2$$

$$= \left| \frac{1}{n} \sum_{a \in k + \langle r \rangle} e_c(a) \right|^2 \quad \text{(induces global phase factor)}, \quad \langle r \rangle \leq \mathbb{Z}_n$$

$$= \left| \frac{1}{n} \sum_{b \in \langle r \rangle} e_c(b) \right|^2 \quad \text{(no dependence on } k\text{)}$$

$= |\langle r \rangle| = \frac{n}{r}$ if $e_c = 1$ on $\langle r \rangle$; 0 otherwise

$$= \begin{cases} \frac{1}{r^2} & \text{if } e_c = 1 \text{ on } \langle r \rangle \\ 0 & \text{otherwise} \end{cases}$$

$$\Rightarrow \mathbb{P}(|c\rangle) = \begin{cases} \frac{1}{n^2} \cdot r = \frac{1}{r} & \text{if } e_c = 1 \text{ on } \langle r \rangle \quad (r \text{ cosets, each equally probable}) \\ 0 & \text{otherwise} \end{cases}$$

9

2. Problem statement

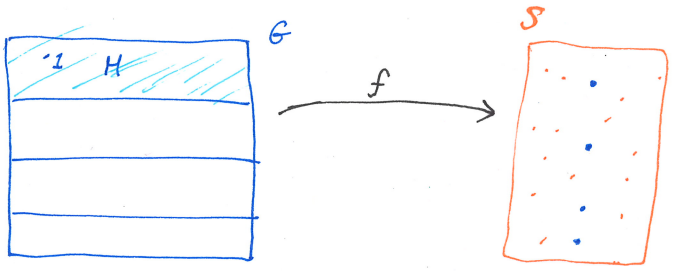
* G a group
* $H \leq G$ subgroup
* $f : G \longrightarrow S$ map of sets

def. (hidden subgroup). We say that $f : G \longrightarrow S$ *hides* $H \leq G$ if

i. f is constant on cosets G/H

ii. $\bar{f} : G/H \longrightarrow S$ is injective

i.e. f indexes the cosets of $H \leq G$.



def (HSP). Find H!

efficiently!

Leverage the ability to evaluate $f(g)$ to find a generating set for $H \leq G$.

ex. Shor's order-finding algorithm. $G = \mathbb{Z}_n$, $H = \langle r \rangle$, $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$, $a \longmapsto x^a$.

↑ the cyclic HSP

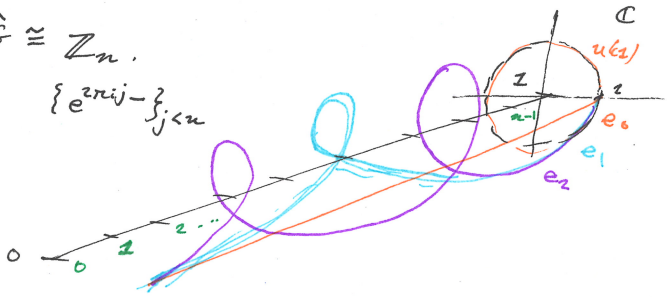
3. The abelian case

Suppose $f: G \to S$ hides $H \leq G$,
G finite abelian

def (character group)

$$\hat{G} := \{ \chi : G \to U(1) \subseteq \mathbb{C}^* \text{ homomorphism} \}$$

ex. $G = \mathbb{Z}_n$, $\hat{G} \cong \mathbb{Z}_n$.
$\{k\}_{k \in \mathbb{Z}_n}$ $\{e^{2\pi i j - }\}_{j < n}$



$e_\ell(k) = e^{2\pi i \ell k / n}$

Facts. i. $|\hat{G}| = |G|$

ii.

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{if } \chi \equiv 1 \in \mathbb{C}^* \\ 0 & \text{otherwise} \end{cases} \qquad (*)$$

prf ii.

$$\sum_{g \in G} \chi(g) \neq 0 \implies \forall h \in G: \underbrace{\sum_{g \in G} \chi(g)}_{\Sigma_g \chi(g)} = \sum_{g \in G} \chi(hg) = \chi(h) \underbrace{\sum_{g \in G} \chi(g)}_{\Sigma_g \chi(g)}$$

$$\implies \forall h \in G: \ \chi(h) = 1 .$$

def (Fourier transform)

$$|g\rangle \longmapsto \frac{1}{\sqrt{|G|}} \sum_{\chi \in \hat{G}} \chi(g) |\chi\rangle$$

idea: decompose a function $f: G \xrightarrow{11} \mathbb{C}$ as a linear combination of characters χ.

Goal: Find a generating set for $H \leq G$.

Steps:

1. Prepare
$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle$$

2. Compute f in 2nd reg.
$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle$$

3. Fourier transform in 1st reg.
$$\frac{1}{|G|} \sum_{g \in G} \sum_{\chi \in \hat{G}} \chi(g) |\chi\rangle |f(g)\rangle$$

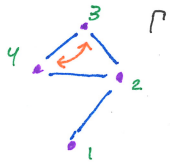
4. measure.
$$\mathbb{P}(|\chi\rangle |f(k)\rangle) = \left| \frac{1}{|G|} \sum_{g : f(g) = f(k)} \chi(g) \right|^2$$
$$= \left| \frac{1}{|G|} \sum_{g \in kH} \chi(g) \right|^2$$
$$= \left| \frac{1}{|G|} \sum_{h \in H} \chi(kh) \right|^2$$ (induces a global phase factor)
$$= |\chi(k)|^2 \cdot \left| \frac{1}{|G|} \sum_{h \in H} \chi(h) \right|^2$$ ($|\chi(k)|^2 = 1$; no dependence on k)
$$(*) \Rightarrow = \begin{cases} \frac{|H|^2}{|G|^2} & \text{if } \chi = 1 \text{ on } H \\ 0 & \text{otherwise} \end{cases}$$
$$\mathbb{P}(|\chi\rangle) = \begin{cases} [G:H] \cdot \frac{|H|^2}{|G|^2} = \frac{|H|}{|G|} & \text{if } \chi = 1 \text{ on } H \\ 0 & \text{otherwise} \end{cases}$$
($[G:H]$ = # of cosets, each equally probable)

4. Graph isomorphism

Graph automorphism:

Given: $\Gamma = (V, E)$ finite

Goal: Does Γ admit a nontrivial automorphism? (Y/N)



Γ

$V \cong [|V|] = [n]$

$\mathrm{Sym}\, V \cong S_n$

$\mathrm{Aut}\, \Gamma \leq S_n$ (preserves the relation E on V)

hidden by

$f : S_n \longrightarrow$ graphs on $[n]$

$\varphi \longmapsto \varphi \cdot \Gamma = (\varphi V, \varphi E)$

Given generators of $\mathrm{Aut}\, \Gamma$, check to see if any is nontrivial. If so, return Y. Otherwise, return N.

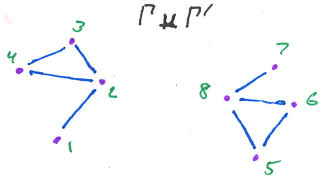
Graph isomorphism:

Given: $\Gamma = (V, E)$, $\Gamma' = (V', E')$ finite & connected

$V \cong V' \cong [n]$

Goal: Are Γ and Γ' isomorphic? (Y/N)

$\Gamma \sqcup \Gamma'$



no efficient quantum algorithm is known for the S_n hidden subgroup problem.

$\mathrm{Aut}\, \Gamma \sqcup \Gamma' \leq S_{2n}$

hidden by

$f : S_{2n} \longrightarrow$ graphs on $[2n]$

$\varphi \longmapsto \varphi(\Gamma \sqcup \Gamma')$

Given generators of $\mathrm{Aut}\,(\Gamma \sqcup \Gamma')$, check to see if any maps a vertex of Γ to Γ' (~~or vice versa~~). If so, ~~one~~ return Y. Otherwise, return N.