Lecture 2: QW search and collision finding

Tuesday, 4 January 2022 07:33

Motivation: COLLISION FINDING.

- array $x_1, x_2, \dots, x_N \in \mathbb{Z}$
- "collision" = pair $i \neq j$ s.t. $x_i = x_j$
- ? # queries to array to find collision

* classically: $\Omega(N)$ queries.
* quantum: $o(N)$ queries!

→ $\tilde{O}(N^{3/4})$ with Grover search

→ $\tilde{O}(N^{2/3})$ with quantum walks (essentially optimal)

GROVER SEARCH:

- set V of n elements
- subset $M \subseteq V$ of m "marked" elements
- algorithm:
  1. Set up $|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{x \in V} |x\rangle$

1. Set up $|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{x \in V} |x\rangle$

2. Do $O(\sqrt{n/m})$ times:

   (a) Reflect around marked elements:

   $$2\Pi_M - \mathbb{1} = 2 \sum_{x \in M} |x\rangle\langle x| - \mathbb{1}$$

   (b) Reflect around $|\pi\rangle$:

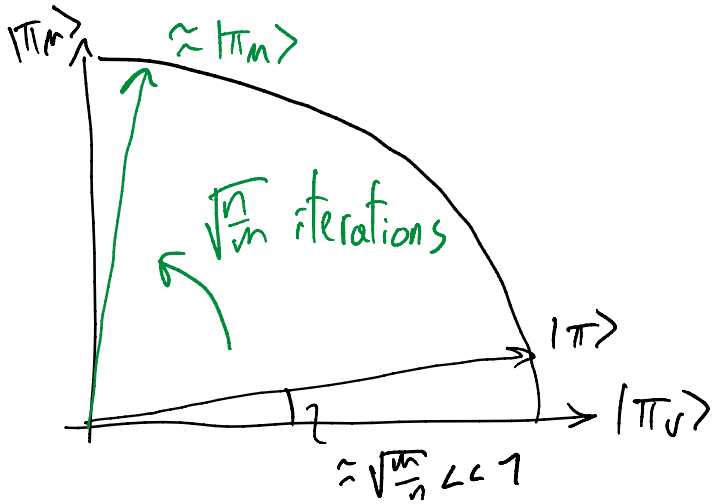
   $$2|\pi\rangle\langle\pi| - \mathbb{1}$$

3. Measure the state.

Recall:

step 2. = rotation in subspace spanned by

$$|\pi_M\rangle = \frac{1}{\sqrt{m}} \sum_{x \in M} |x\rangle, \quad |\pi_V\rangle = \frac{1}{\sqrt{n-m}} \sum_{x \notin M} |x\rangle.$$



7. "cost" (= query complexity) of Grover search

* SETUP COST S
  = cost of preparing $|\pi\rangle$
  = map $|0\rangle \mapsto U_\pi|0\rangle = |\pi\rangle$

* REFLECTION COST R
  = cost of reflecting around $|\pi\rangle$

  ! $R \leq 2S$: $2|\pi\rangle\langle\pi| - \mathbb{1}$

  $= U_\pi^\dagger (2|0\rangle\langle 0| - \mathbb{1}) U_\pi$

* CHECKING COST C
  = check if element x is marked
  = map $|x\rangle|0\rangle \mapsto U_c|x\rangle|0\rangle = \begin{cases} |x\rangle|1\rangle & \text{if } x \in M \\ |x\rangle|0\rangle & \text{if } x \notin M \end{cases}$

→ reflect around Π_M:

$|\psi\rangle = \sum \alpha_x |x\rangle|0\rangle$

$\xrightarrow{U_c} \sum_{x\in M} \alpha_x |x\rangle|1\rangle + \sum_{x\notin M} \alpha_x |x\rangle|0\rangle$

$\mathbb{1}\otimes|1\rangle\langle 1| \longmapsto \sum_{x\in M} \alpha_x |x\rangle|1\rangle - \sum_{x\notin M} \alpha_x |x\rangle|0\rangle$

$$\mathbb{1}\otimes|1\rangle\langle 1| \quad \mapsto \sum_{x\in M}\alpha_x|x\rangle|1\rangle - \sum_{x\notin M}\alpha_x|x\rangle|0\rangle$$

$$-\mathbb{1}\otimes|0\rangle\langle 0| \quad \overset{U_c^+}{\mapsto} \left(\sum_{x\in M}\alpha_x|x\rangle - \sum_{x\notin M}\alpha_x|x\rangle\right)|0\rangle = (2\Pi_M - \mathbb{1})|\psi\rangle$$

↳ TOTAL COST $= S + \sqrt{\frac{n}{m}}(R+C)$

$$\lesssim \sqrt{\frac{n}{m}}(S+C).$$

GROVER SEARCH FOR COLLISION FINDING

NAIVE: search over all $\binom{N}{2}$ pairs of indices

→ cost $\approx N$ ↯

BDHHMSW '01: search over larger subsets!

* elements: "words" $y = (Y, x_Y)$

↳ list of integers $\{x_j, j\in Y\}$

$Y\subseteq[N]$, $|Y|=k$

↳ $n = \binom{N}{k}$ elements

$$|\Pi\rangle = \frac{1}{\sqrt{n}} \sum_{Y\subseteq[N]:} |y = (Y, x_Y)\rangle$$

$$|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{\substack{y \subseteq [N]: \\ |y| = k}} |y = (y, x_y)\rangle$$

* marked elements: $q = (y, x_y)$ s.t. y contains (at least) one index of a collision

Exercise:

(i) Show that $\frac{m}{n} \geq \frac{k}{N}$ if $\exists$ collision.

(ii) Show that checking cost C is $O(\sqrt{N})$ using Grover search.

↳ Solution: (i) say collision $(i,j) \subseteq [N]$.

marked sets $m \geq \binom{N-1}{k-1} = \frac{(N-1)!}{(k-1)!(N-k)!}$

so $\frac{m}{n} \geq \frac{\binom{N-1}{k-1}}{\binom{N}{k}} = \frac{(N-1)!}{(k-1)!(N-k)!} \cdot \frac{k!(N-k)!}{N!} = \frac{k}{N}$

(ii) find $j \in [N]$ s.t. $\exists i \in y$ with $x_i = x_j$

↳ COST $\sqrt{N}$.

Bound SETUP COST S

= cost of constructing $|\pi\rangle = \frac{1}{\sqrt{n}} \sum_y |y = (y, x_y)\rangle$

$$|0\rangle \longmapsto \frac{1}{\sqrt{n}} \sum_{|y|=k} |y, 0\rangle \quad \text{(no queries)}$$

$$\longmapsto \frac{1}{\sqrt{n}} \sum_{|y|=k} |y, x_y\rangle \quad (k \text{ queries})$$

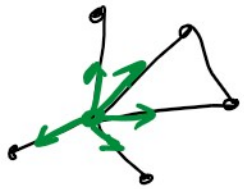
$\rightarrow \sqrt{n} \sum_{|y|=k} |y, xy\rangle$ (k queries)

TOTAL COST:

$$\sqrt{\frac{n}{m}}\,(S+C) \leq \sqrt{\frac{N}{k}}\,(k+\sqrt{N})$$

$$\approx N^{3/4} \quad \text{if } k=\sqrt{N}$$

QUANTUM WALK SEARCH



Recall: - d-regular graph $G=(V,E)$

- star states $|\psi_x\rangle = \frac{1}{\sqrt{d}} \sum_{y\sim x} |x,y\rangle$

- QW operator $W = S \cdot C$

$S|x,y\rangle = |y,x\rangle$ $\quad C = 2\sum_x |\psi_x\rangle\langle\psi_x| - \mathbb{1}$

SPECTRUM:

- stationary state $|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{x\in V} |\psi_x\rangle$

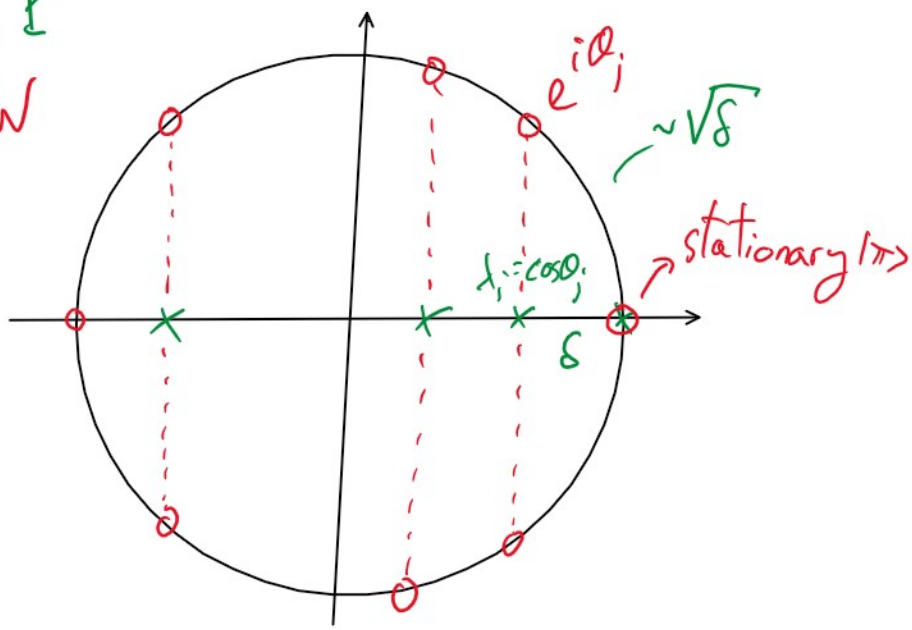
s.t. $W|\pi\rangle = |\pi\rangle$

- nontrivial eigenvalues ($\neq \pm 1$):

SZEGEDY'S SPECTRAL LEMMA

× eigenvalues P

o eigenvalues W



I.e., for every eigenpair of P

$$\left(\lambda_j = \cos\theta_j,\ |v_j\rangle = \sum v_j(x)|x\rangle\right),$$

W has eigenpairs

$$\left(e^{i\theta_j},\ |\phi_j^+\rangle\right),\ \left(e^{-i\theta_j},\ |\phi_j^-\rangle\right)$$

s.t. $$\sum v_j(x)|\psi_x\rangle = \frac{|\phi_j^+\rangle + |\phi_j^-\rangle}{\sqrt{2}}.$$

OBSERVATION 1:

OBSERVATION 1:

any state $\sum \alpha_x |\psi_x\rangle$ in star subspace

is in $\text{span}\{|\pi\rangle, |\phi_1^+\rangle, |\phi_1^-\rangle, \ldots, |\phi_{n-1}^+\rangle, |\phi_{n-1}^-\rangle\}$.

→ we characterized "relevant subspace"

OBSERVATION 2:

"phase gap" $\Delta = \min\{\theta_j \mid \theta_j > 0\}$

$= \arccos(\lambda_2)$

$\geq \arccos(1-\delta)$ ← RW sp-gap

Exercise: prove that $\Delta \in \Omega(\sqrt{\delta})$.

(hint: use that $\cos(x) \geq 1 - \frac{x^2}{2}$)

↳ solution: $x \geq \sqrt{2(1-\cos(x))}$

$\Rightarrow \arccos(y) \geq \sqrt{2(1-y)}$

$\Rightarrow \arccos(1-\delta) \geq \sqrt{2\delta}$.

→ quadratically larger gap!

QUANTUM WALK SEARCH

QUANTUM WALK SEARCH

we bounded $R \leq 2S$ → prepare $|\pi\rangle$

reflect around $|\pi\rangle$

! Sometimes $R \ll S$

= exploited in QW search

* QW search: (Grover but $|x\rangle \mapsto |\psi_x\rangle$)

1. Set up $|\pi\rangle = \frac{1}{\sqrt{n}} \sum_{x \in V} |\psi_x\rangle$ → S

2. Do $O(\sqrt{\frac{n}{m}})$ times

   (a) reflect around marked elements:

   $$2\Pi_M - \mathbb{1} = 2 \sum_{x \in M} |\psi_x\rangle\langle\psi_x| - \mathbb{1} \rightarrow C$$

   (b) reflect around $|\pi\rangle$ → R

3. Measure first register.

$= S + \sqrt{\frac{n}{m}}(R+C)$

Again, dynamics in

$$\text{Span}\left\{ |\pi_V\rangle = \frac{1}{\sqrt{n-m}} \sum_{x \notin M} |\psi_x\rangle,\ |\pi_M\rangle = \frac{1}{\sqrt{m}} \sum_{x \in M} |\psi_x\rangle \right\}.$$

$\subseteq$ star subspace !

$$\text{Span}\left\{|\pi_V\rangle = \frac{1}{\sqrt{n-m}} \sum_{x \notin m} |f_x\rangle,\ |\pi_m\rangle = \frac{1}{\sqrt{m}} \sum_{x \in m} |f_x\rangle\right\}.$$

$\subseteq$ star subspace !

* QW reflection :

consider $|f\rangle = \alpha|\pi\rangle + \beta|\pi^\perp\rangle$

$= \alpha|\pi\rangle + \sum \beta_j |\phi_j\rangle$ (since $|f\rangle$ in star subspace)

↳ WANT to map to

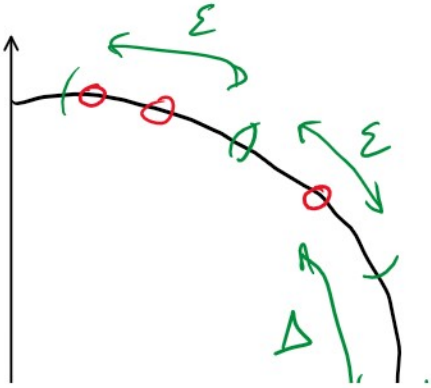
$(2|\pi\rangle\langle\pi| - \mathbb{1})|f\rangle = \alpha|\pi\rangle - \beta|\pi^\perp\rangle$

→ PHASE ESTIMATION:

$$U_P\left(\alpha|\pi\rangle|0\rangle + \sum \beta_j |\phi_j\rangle|0\rangle\right)$$

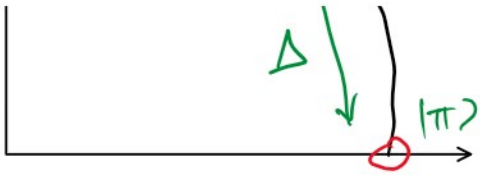
$$= \alpha|\pi\rangle|0\rangle + \sum \beta_j |\phi_j\rangle|\tilde{\theta}_j\rangle$$

↳ estimate s.t. $|\theta_j - \tilde{\theta}_j| \leq \varepsilon$



$\varepsilon < \Delta$

$\Rightarrow \tilde{\theta}_j > 0$



$\Rightarrow \tilde{\theta}_j > 0$

cost $= \tilde{O}(1/\varepsilon)$ calls to QW operator W

$\in \tilde{O}(1/\Delta) \in \tilde{O}(1/\sqrt{\delta})$ ↓ "update cost" U

ALGORITHM:

$|\psi\rangle|0\rangle = \alpha|\pi\rangle|0\rangle + \beta|\pi^\perp\rangle|0\rangle$

$= \alpha|\pi\rangle|0\rangle + \sum \beta_j |\phi_j\rangle|0\rangle$

$\xrightarrow{U_E} \alpha|\pi\rangle|0\rangle + \sum \beta_j |\phi_j\rangle|\tilde{\theta}_j\rangle$ → $1/\sqrt{\delta}\, U$

$\mathbb{1}\otimes|0\rangle\langle 0|$

$-\mathbb{1}\otimes(\mathbb{1}-|0\rangle\langle 0|)$ $\longrightarrow \alpha|\pi\rangle|0\rangle - \sum \beta_j |\phi_j\rangle|\tilde{\theta}_j\rangle$

$\xrightarrow{U_E^+} \alpha|\pi\rangle|0\rangle - \sum \beta_j |\phi_j\rangle|0\rangle$

$= (2|\pi\rangle\langle\pi| - \mathbb{1})|\psi\rangle|0\rangle.$ → $1/\sqrt{\delta}\, U$

→ $R \leq \frac{1}{\sqrt{\delta}} U$

* QW search algorithm:

cost $S + \sqrt{\frac{n}{m}}(R + C)$

cost $\delta + \sqrt{m}\,(\delta^{-1}C)$

$\lesssim \delta + \sqrt{\frac{n}{m}}\left(\frac{1}{\sqrt{\delta}}U + C\right).$

$\#\,\text{QW steps} \simeq \frac{1}{\sqrt{\delta}}\sqrt{\frac{n}{m}}$

→ compare with RW search:

$\#$ (expected) RW steps, starting from π

$= HT(M) \in O\left(\frac{1}{\delta}\frac{1}{\pi(M)}\right) = O\left(\frac{1}{\delta}\frac{n}{m}\right).$

quadratic speedup using QW!

QW algorithm for collision finding

input $x_1, x_2, \dots, x_N$. Collision: i, j s.t. $x_i = x_j$?

→ **QW search:**

- elements $y = (Y, x_Y)$, $Y \subseteq [N]$, $|Y| = k$

  $x_Y = \{x_i\}_{i \in Y}$

- y "marked" if Y contains collision

- y marked if Y contains collision
$(\exists i,j \in Y \text{ s.t. } x_i = x_j)$

EXERCISE: Show that $\frac{m}{n} \in \Omega(k^2/N^2)$.
↳ $n = \binom{N}{k}$, $m \geq \binom{N-2}{k-2}$

- graph G:
vertex set: $V = \{ y = (Y, x_Y) \}$
edge set: $y = (Y, x_Y) \sim y' = (Y', x_{Y'})$
iff $|Y \cap Y'| = k-1$.

= "Johnson graph" $J(N,k)$,

Fact: $J(N,k)$ is $k(n-k)$-regular and has spectral gap $\delta \in \Omega(1/k)$ when $k \ll n$.

- star states:

- slar slates:

$$|\psi_y\rangle = \frac{1}{\sqrt{k(n-k)}} \sum_{y' \sim y} |y, y'\rangle$$

- stationary state: $\frac{1}{\sqrt{n}} \sum_y |\psi_y\rangle$

→ **COST:** $S + \sqrt{\frac{n}{m}}\left(\frac{1}{\sqrt{\delta}} U + C\right)$

$$= S + \frac{N}{k}\left(\sqrt{k}\, U + C\right).$$

Bounding costs:

* checking cost $C = 0$
* setup cost S = cost of creating $|\pi\rangle$

k queries → 1. prepare $\frac{1}{\sqrt{n}} \sum_y |y\rangle|0\rangle$

2. implement mapping $U_f\left(\frac{1}{\sqrt{n}} \sum_y |y\rangle|0\rangle\right) = |\pi\rangle$

(a) $|y\rangle|0\rangle \mapsto \frac{1}{\sqrt{k(n-k)}} \sum |y\rangle|(y,0)\rangle$

(a) $|\psi\rangle|0\rangle \mapsto \frac{1}{\sqrt{k(n-k)}} \sum_{y' \sim y} |y'\rangle |(y;0)\rangle$

1 query ↳ since $|x_{y'} \oplus x_y| = 1$

$\mapsto \frac{1}{\sqrt{k(n-k)}} \sum_{y' \sim y} |y'\rangle |(y; x_{y'} \oplus x_y)\rangle$

$\rightarrow$ $S \simeq k$

* update cost U

= cost of implementing

$W = S \cdot C$

$= S \cdot \left(2 \sum_y |\psi_y\rangle\langle\psi_y| - \mathbb{1}\right)$

$= S \cdot U_\psi \left(2 \sum_y |y\rangle\langle y| \otimes |0\rangle\langle 0| - \mathbb{1}\right) U_\psi^\dagger$

U_ψ: 1 query

$2 \sum_y |y\rangle\langle y| \otimes |0\rangle\langle 0| - \mathbb{1} = \mathbb{1} \otimes |0\rangle\langle 0| - \mathbb{1} = \Pi_0$

→ no queries

↳ $U \simeq 1$

TOTAL COST: $S + \frac{N}{k}\left(\sqrt{k}\, U + C'\right)$

total cost: $\frac{1}{k}(\text{VK} \cdot \text{C})$

$\approx k + \frac{N}{\sqrt{k}} = N^{2/3}$ if $k = N^{2/3}$.

[Aaronson - Shi '04]: $\Omega(N^{2/3})$.