1 Quantum Random Walks

- Exponential speedups on contrived problems → Childs et al.
- \sqrt{\text{speedups}} on some applicable problems → Ambainis’s algorithm for element distinctness

2 Grover’s Algorithm

- We have $N$ elements
  - One of the are ‘marked’ → Find it!
    * Classically : $O(N)$
    * Quantum Mechanically : $O(\sqrt{N})$

- Strategy
  - Use two operations
    * $G |i\rangle = - |i\rangle$ where $i$ is the marked one, $G |j\rangle = |j\rangle$ $\forall i \neq j$
    * $M : |\psi\rangle = \sum_{j=1}^{N} \frac{1}{\sqrt{N}} |j\rangle \rightarrow |\psi\rangle (M = 2 |\psi\rangle \langle \psi| - I)$
  - Start in $|\psi\rangle$
  - Perform $(MG)^t$ for $t = \frac{\pi}{4} \sqrt{N}$

- Why does it work?
  - The state stays in a subspace generated by $|\psi\rangle$, $|i\rangle$. 
3 Generalization

- Suppose you have a $\sqrt{N} \times \sqrt{N}$ grid.
- We will use following operations
  1. Move to adjacent vertex
  2. Ask “Is this vertex marked?”
- For $\sqrt{N} \times \sqrt{N}$ grid, there is $O(\sqrt{N} \log N)$ quantum algorithm.
- For $\dim \geq 3$ grids, $O(\sqrt{N})$ quantum algorithm exists.

4 Element Distinctness

- We have function $f[N] \rightarrow [M]$
  - $\exists i, j \text{ s.t. } f(i) = f(j), i \neq j$
  - Assume $i$ and $j$ are unique.
- Classically: Best way is to sort the elements, with time complexity $O(N \log N)$, $O(N)$ queries.
- Buhram $O(N^{3/4})$ queries
- Ambainis $O(N^{2/3})$ queries $\rightarrow$ Proven to be the lower bound (Shi)

4.1 Several Definitions and Generic Settings

1. Define graph
   - $S$ : Set of $r$ elements
   - $S'$ : Set of $r+1$ elements (if $S \subseteq S'$)
2. Mark a set if $f(i) = f(j)$, $i, j \in S$
3. Start in a superposition of all sets. Perform walk, search until you find a marked set.
   - Probability of a set being marked is $O(\frac{r^2}{N^2})$. 
Each takes time $r$ to check a set. \( \rightarrow \frac{N^2}{r^2} \log r \)

4. Keep $f(i) \forall i \in S$

- $A : |s \rangle |y \rangle \rightarrow |s \rangle \left( -1 + \frac{2}{N-r} |y \rangle + \frac{2}{N-r} \sum_{y'y \neq y} |y' \rangle \right)$
- $B : |s \rangle |y \rangle \rightarrow |s \rangle \left( -1 + \frac{2}{r+1} |y \rangle + \frac{2}{r+1} \sum_{y'y \neq y,S'=S-\{y\}\cup\{y'\}} |y' \rangle \right)$

### 4.2 Algorithm

1. Start in a superposition
   \[ \frac{1}{\sqrt{\binom{\binom{N}{2}}{r}}} \sum_{|S|=r,y \notin S} |S \rangle |y \rangle \]
   - Number of elements in $S : r = O(N^{2/3})$ (Why? \( \rightarrow \) Shown in the last part)

2. Query elements $f(i), i \in S \cup \{y\}$. Get $\sum |s \rangle |y \rangle \otimes_{i \in S} f(i) \times f(y)$

3. Repeat $\frac{N}{r}$ times
   - Apply phase $-1$ to marked states.
   - Apply $(AB)^t, t = O(\sqrt{r})$
   - Measure state. Find $f(i) = f(j)$ with probability $\epsilon > 0$.

### 4.3 Proof

The walk stays in a 5-dim subspace. Since

- \( \frac{1}{\binom{N-2}{r-2}} \sum |S, y \rangle : S \cup y \text{ contains no duplicated elements.} \)
- \( \frac{1}{\binom{N-2}{r-2}} \sum |S, y \rangle : S \text{ contains 1, } y \text{ not duplicated} \)
- \( \frac{1}{\binom{N-2}{r-2}} \sum |S, y \rangle : S \text{ contains 2, } y \text{ not duplicated} \)
- \( \frac{1}{\binom{N-2}{r-2}} \sum |S, y \rangle : S \text{ contains 0, } y \text{ duplicated} \)
- \( \frac{1}{\binom{N-2}{r-2}} \sum |S, y \rangle : S \text{ contains 1, } y \text{ duplicated} \)

**Lemma :** Suppose $U_1, U_2$ are unitaries on some $O(1)$-dimensional subspace, where $U_1$ is a reflection.

\[ U_1 |\varphi_{\text{good}}\rangle = - |\varphi_{\text{good}}\rangle \]
\[ U_1 |\varphi\rangle = |\varphi\rangle (\langle \psi |\varphi_{\text{good}}\rangle = 0) \]
$U_2$ is real and $U_2 |\varphi_{\text{start}} \rangle = |\varphi_{\text{start}} \rangle$. Other eigenvalues $e^{i\theta}$, $e^{-i\theta}$, where $\epsilon < \theta < 2\pi - \epsilon$. Let $\langle \varphi_{\text{good}} | \varphi_{\text{start}} \rangle = \alpha$. Then, $\exists t, t = O(\frac{1}{\alpha})$, so after $t$, iterations

$$| \langle \varphi_{\text{good}} | (U_1 U_2)^t | \varphi_{\text{start}} \rangle | \leq \delta$$

where $\delta > 0$ depends on $\epsilon$, not $\alpha$.

$BA$ has eigenvalue $O(\frac{1}{\sqrt{r}})$ and for $e^{i\theta}$, $\theta = O(\frac{1}{\sqrt{r}})$. Therefore, $(BA)^{\sqrt{r}}$ has eigenvalue $e^{i\theta}$, where $\theta > \epsilon > 0$.

Now we need to iterate $O(\frac{1}{\sqrt{\alpha}})$ times, where $\alpha = \langle \varphi_{\text{good}} | \varphi_{\text{start}} \rangle$.

- $\varphi_{\text{start}}$: Superposition of all $|S\rangle$
- $\varphi_{\text{good}}$: Superposition of all marked $|S\rangle$

Since $| \langle \varphi_{\text{start}} | \varphi_{\text{good}} \rangle |$ portions of marked $|S\rangle$s and $\alpha = \sqrt{r^2/N^2} = \frac{r}{N}$, total time is

$$O(r + \frac{N}{r} \sqrt{r}) = O(r + \frac{N}{\sqrt{r}})$$

which is minimized by taking $r = O(N^{2/3})$. → Running time becomes $O(N^{2/3})$. 