

- Grover's algorithm is optimal for unordered search ($\S 23.1$)

Bennett - Bernstein - Brassard - Vazirani:

any quantum algorithm that receives input

function $f: \{0, 1, \dots, N-1\} \rightarrow \{0, 1\}$

and returns

$0 \leq x^* < N$ such that $f(x^*) = 1$

requires at least $\sim C\sqrt{N}$ queries ($\Omega(\sqrt{N})$)

How to model this

- quantum algorithm: chain of operators

$U_0, Q_0^f, U_1, Q_1^f, \dots$
 $\uparrow$ some unitary gate (without query) $\uparrow$ phase query with f $Q_1^f = Q_0^f, \dots : (-1)^{f(x)} |x\rangle$

- state after $Q_{t-1}^f : |\psi_t^f\rangle$

x : variable $0 \leq x < N$ (for querying)

m : ancillary variable ("workspace")

write $|\psi_t^f\rangle = \sum_{x,m} \alpha_{x,m,t}^f |x,m\rangle$

($|\psi_0\rangle$: some common initial vec.)

Suppose we need $T = TN$ steps

$$M_x^f = \sum_{0 \leq t \leq T} \underbrace{\sum_m |\alpha_{x,m,t}^f|^2}_{\text{write } M_{x,t}^f} \quad \text{query magnitude}$$

$$\text{Prop 1} \quad \frac{1}{N} \sum_x M_x^f = \frac{T}{N}$$

Proof each $|\psi_t^f\rangle$ is a state vector

$$\Rightarrow \sum_{x,m} |\alpha_{x,m,t}^f|^2 = 1 \Rightarrow \sum_{x,m,t} |\alpha_{x,m,t}^f|^2 = T \quad \square$$

Consider the function $f^0(x) = 0$ (all x)

Then $Q^{f^0} = I_N$, $|\psi_1^{f^0}\rangle = U_0 |\psi_0\rangle$, $|\psi_2^{f^0}\rangle = U_1 U_0 |\psi_0\rangle, \dots$

$$\text{Take } x^* \text{ s.t. } M_{x^*}^{f^0} \leq \frac{T}{N}$$

Prop 2 $\sum_{0 \leq t \leq T} \sqrt{M_{x^*}^{f^0, t}} \leq \frac{T}{\sqrt{N}}$

Proof Cauchy - Schwartz inequality implies

$$\sum_{0 \leq t \leq T} a_t \leq \sqrt{T} \sqrt{\sum_t a_t^2}, \text{ with equality iff } a_1 = a_2$$

Now, take $f: \{0, \dots, N-1\} \rightarrow \{0, 1\}$ defined by
 $f(x^*) = 1, \quad f(x) = 0 \quad (x \neq x^*)$

Then our quantum algorithm should give

$$|\psi_T^f\rangle = \sum_m \alpha_{x^*, m, T}^f |x^* m\rangle \quad (\text{measurement in the } x\text{-part should always give } x^*)$$

Idea for finding $T = \Omega(\sqrt{N})$:

- $|\psi_T^{f^0}\rangle$ and $|\psi_T^f\rangle$ are separated!
- changing one query from Q^{f^0} to Q^f cannot change the result by much

Prop 3 $\| |\psi_T^{f^0}\rangle - |\psi_T^f\rangle \| \geq \sqrt{1 - 2\sqrt{\frac{T}{N}}}$

Proof $\| |\psi_T^{f^0}\rangle - |\psi_T^f\rangle \|^2 \geq \sum_m |\alpha_{x^*, m, T}^f - \alpha_{x^*, m, T}^{f^0}|^2$
 $= \sum_m |\alpha_{x^*, m, T}^f|^2 - 2 \left(\sum_m \alpha_{x^*, m, T}^f \alpha_{x^*, m, T}^{f^0} \right)$
 $+ \sum_m |\alpha_{x^*, m, T}^{f^0}|^2$

$|\psi_T^f\rangle = \sum_m \alpha_{x^*, m, T}^f |x^* m\rangle \Rightarrow$ first sum is 1.

Cauchy - Schwartz $\Rightarrow$ second sum $\leq \sqrt{\sum_m |\alpha_{x^*, m, T}^{f^0}|^2}$
 $\leq \sqrt{M_{x^*}^{f^0}} \leq \sqrt{\frac{T}{N}} \quad \square$

Changing queries from Q^{f^0} to Q^f

Put $|\psi_T^{(1)}\rangle = Q^f |\psi_T^{f^0}\rangle$ (change the last query)

Prop 4 $\| |\psi_T^{(1)}\rangle - |\psi_T^{f^0}\rangle \| = 2\sqrt{M_{x^*}^{f^0}}$

Proof $|\psi_T^{(1)}\rangle = \sum_{x \neq x^*} \alpha_{x, m, T}^{f^0} |x m\rangle - \sum_m \alpha_{x^*, m, T}^{f^0} |x^* m\rangle$

cont.)

$$\leadsto \| |\psi_T^{(1)}\rangle - |\psi_T^{f^0}\rangle \|^2 = \sum_m |2 \alpha_{x^*, m, T}^{f^0}|^2 = 4 M_{x^*, T}^{f^0}$$

Next consider changing the last 2 queries

$$|\psi_{T-1}^{(2)}\rangle = Q^f |\psi_{T-1}^{f^0}\rangle, \quad |\psi_T^{(2)}\rangle = Q^f U_{T-1} |\psi_{T-1}^{(2)}\rangle$$

$$\begin{array}{c} |\psi_T^{f^0}\rangle \xrightarrow{Q^f} |\psi_T^{(1)}\rangle \xrightarrow{Q^f} |\psi_T^{(2)}\rangle \xrightarrow{Q^f} |\psi_T^f\rangle \\ \uparrow U_{T-1} \quad \uparrow Q^f \quad \uparrow U_{T-1} \\ |\psi_{T-1}^{f^0}\rangle \xrightarrow{Q^f} |\psi_{T-1}^{(2)}\rangle \xrightarrow{Q^f} |\psi_{T-1}^f\rangle \xrightarrow{Q^f} \dots \\ \uparrow U_0 \\ |\psi_0\rangle \end{array}$$

Prop 5. $\| |\psi_T^{(2)}\rangle - |\psi_T^{f^0}\rangle \| \leq 2 (\sqrt{M_{x^*, T-1}^{f^0}} + \sqrt{M_{x^*, T}^f})$

Proof. It's enough to estimate $\| |\psi_T^{(2)}\rangle - |\psi_T^{(1)}\rangle \|$

$$|\psi_T^{(1)}\rangle = Q^f U_{T-1} |\psi_{T-1}^{f^0}\rangle, \quad |\psi_T^{(2)}\rangle = Q^f U_{T-1} Q^f |\psi_{T-1}^{f^0}\rangle$$

$$\text{So } \| |\psi_T^{(2)}\rangle - |\psi_T^{(1)}\rangle \| = \| Q^f |\psi_{T-1}^{f^0}\rangle - |\psi_{T-1}^{f^0}\rangle \|$$

Then same argument as Prop 4 gives the claim. $\square$

Continuing this, we get $|\psi_T^{(T)}\rangle = |\psi_T^f\rangle$

$$\| |\psi_T^f\rangle - |\psi_T^{f^0}\rangle \| \leq 2 \left(\sum_{0 \leq t \leq T} \sqrt{M_{x^*, t}^{f^0}} \right) \stackrel{\text{Prop 2}}{\leq} \frac{2T}{\sqrt{N}}$$

If $T = T_N$ is $o(\sqrt{N})$ this would contradict Prop 3.

