Monday, November 19, 2018 10:01 AM

Unstructured Search

We have access to a function $f : \{0,1\}^n \to \{0,1\}$ through an oracle O_f :

$$O_f : \underbrace{|x\rangle}_{n \text{ qubits}} \underbrace{|y\rangle}_{1 \text{ qubit.}} \longrightarrow |x\rangle |y \oplus f(x)\rangle$$

We want to determine if $\exists$ a s.t. $f(a) = 1$.

Let $M = \left| \{ x \mid f(x) = 1 \} \right|$ $M \geq 1$?

Last time we showed that if we are guaranteed that if $M=0$ or $M=1$ then there is a quantum circuit that can distinguish between those two cases using $O(\sqrt{N})$ queries to f.

We still need to give an algorithm that can handle general M. (coming later.)

In this lecture we will show that even if you are told that $M=0$ or $M=1$, a quantum circuit will require $\Omega(\sqrt{N})$ queries.

Remember that $N = 2^n$ n = # input variables to f.
So this is an exponential lower bound.

Unstructured Search Lower Bound - page 2

Monday, November 19, 2018 10:01 AM

The main technical tool used in the proof is the Cauchy-Schwartz inequality:

For any two complex vectors of the same length: $|v\rangle$ and $|w\rangle$:

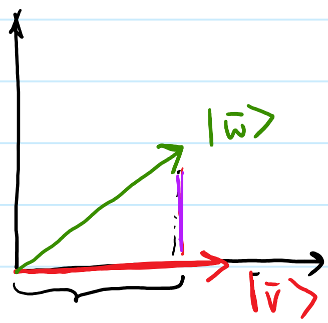
$$\langle v|v\rangle \langle w|w\rangle \geq |\langle v|w\rangle|^2$$

Normalize $|v\rangle$ and $|w\rangle$:

$$|\bar{v}\rangle = \frac{|v\rangle}{(\langle v|v\rangle)^{1/2}} \qquad |\bar{w}\rangle = \frac{|w\rangle}{(\langle w|w\rangle)^{1/2}}$$

Note $\langle \bar{v}|\bar{v}\rangle = \langle \bar{w}|\bar{w}\rangle = 1$.

Look at $|\langle \bar{v}|\bar{w}\rangle|$:



The length of the projection of $|\bar{w}\rangle$ onto $|\bar{v}\rangle$ is ≤ 1.

$$|\langle \bar{v}|\bar{w}\rangle| \leq 1$$

$$\left| \frac{\langle v|w\rangle}{\langle v|v\rangle^{1/2}\langle w|w\rangle^{1/2}} \right| \leq 1$$

$$\Rightarrow \frac{|\langle v|w\rangle|^2}{\langle v|v\rangle \langle w|w\rangle} \leq 1$$

$$|\langle v|w\rangle|^2 \leq \langle v|v\rangle \langle w|w\rangle$$

Unstructured Search Lower Bound - page 3

Monday, November 19, 2018 10:01 AM

Cauchy-Schwartz

For any two complex vectors of the same length: $|v\rangle$ and $|w\rangle$:

$$\langle v|v\rangle \langle w|w\rangle \geq |\langle v|w\rangle|^2$$

We will use this in a particular way.

Suppose: $|v\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{pmatrix}$ $|w\rangle = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$

$$\sum_{j=1}^{N} |\alpha_j|^2 \cdot \underbrace{\sum_{j=1}^{N} |\beta_j|^2}_{1} \geq \left| \sum_{j=1}^{N} \alpha_j^* \underset{1}{\beta_j} \right|^2.$$

Plug in $\beta_1 = \beta_2 \cdots = \beta_N = 1$. $\alpha_j \leftarrow |\alpha_j|$

$$N \cdot \sum_{j=1}^{N} |\alpha_j|^2 \geq \left(\sum_{j=1}^{N} |\alpha_j| \right)^2.$$

For any complex vector $(\alpha_1, \ldots, \alpha_N)$

$N \leftarrow T$

$\alpha_j = |\alpha_{z,t}|$

$$N \cdot \sum_{j=1}^{N} |\alpha_j|^2 \geq \left(\sum_{j=1}^{N} |\alpha_j| \right)^2.$$

Monday, November 19, 2018 10:01 AM

Any algorithm can be seen as a sequence of calls to O_f interleaved with computation (unitaries)

Suppose there are T calls to the oracle.

Let $\alpha_{x,t}$ be the amplitude of $|x\rangle$ just before the t^{th} call to O_f.

That is, just before the t^{th} call to O_f the input register is in state: $\sum_x \alpha_{x,t}|x\rangle$

Since $\sum_x |\alpha_{x,t}|^2 = 1$ then $\sum_{t=1}^{T} \underbrace{\sum_x |\alpha_{x,t}|^2}_{=1} = T$

Switching Summations gives: $\sum_{x} \sum_{t=1}^{T} |\alpha_{x,t}|^2 = T$

N

Select the x that minimizes this sum. Suppose it is minimized at z.

$$\sum_{t=1}^{T} |\alpha_{z,t}|^2 \leq \frac{T}{N}$$

The minimum is at most the average.

By Cauchy-Schwarz: $\left(\sum_{t=1}^{T} |\alpha_{z,t}|\right)^2 \leq T \cdot \sum_{t=1}^{T} |\alpha_{z,t}|^2$

$$\left(\sum_{t=1}^{T} |\alpha_{z,t}|\right)^2 \leq T^2/N \Rightarrow \sum_{t=1}^{T} |\alpha_{z,t}| \leq T/\sqrt{N}.$$

Unstructured Search Lower Bound - page 5

Monday, November 19, 2018 10:01 AM

Now define two functions : $\Rightarrow f(x) = 0 \quad \forall x$

$\Rightarrow g(x) = 0 \quad \forall x \neq z, \; g(z) = 1.$

The algorithm must be able to distinguish between these two functions with reasonably high probability.

$\Rightarrow$ Let $|\phi_f\rangle$ be the final state of the algorithm with oracle O_f

$\Rightarrow$ Let $|\phi_g\rangle$ be the final state of the algorithm with oracle O_g

$$|\phi_f\rangle = U_T \, O_f \, U_{T-1} \, O_f \cdots \cdots O_f \, U_0 |\phi_{start}\rangle$$

$$|\phi_g\rangle = U_T \, O_g \, U_{T-1} \, O_g \cdots \cdots O_g \, U_0 |\phi_{start}\rangle$$

oracle call. computation

We will define a series of intermediate states. $|\psi_t\rangle$ will be the state that results if

- first t calls to O_f.
- last $T-t$ calls to O_g.

$$|\psi_t\rangle = \underbrace{U_T \, O_g \, U_{T-1} O_g \cdots U_{t+1} \, O_g}_{T-t,} \; \underbrace{U_t \, O_f \, U_{t-1} \cdots O_f \, U_0}_{t} |\phi_{start}\rangle$$

$$|\psi_0\rangle = |\phi_g\rangle \qquad\qquad |\psi_T\rangle = |\phi_f\rangle$$

$(|\psi_T\rangle - \cancel{|\psi_{T-1}\rangle}) + \cdots + (|\psi_3\rangle - \cancel{|\psi_2\rangle}) + (\cancel{|\psi_2\rangle} - \cancel{|\psi_1\rangle}) + (\cancel{|\psi_1\rangle} - |\psi_0\rangle)$

Monday, November 19, 2018 10:01 AM

$$|\psi_t\rangle = \underbrace{U_T O_g U_{T-1} O_g \cdots U_{t+1} O_g}_{T-t} \underbrace{U_t O_f U_{t-1} \cdots O_f U_0}_{t} |\phi_{start}\rangle$$

$$|\psi_0\rangle = |\phi_g\rangle \qquad |\psi_T\rangle = |\phi_f\rangle$$

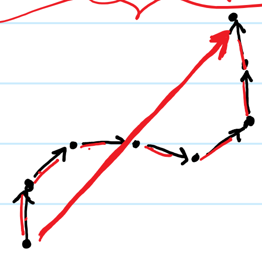
$$|\phi_f\rangle - |\phi_g\rangle = |\psi_T\rangle - |\psi_0\rangle = \sum_{t=1}^{T} |\psi_t\rangle - |\psi_{t-1}\rangle$$

(*) We will show that $\| |\psi_t\rangle - |\psi_{t-1}\rangle \| \leq 2 |\alpha_{z,t}|$

Using this we have:

$$\| |\phi_f\rangle - |\phi_g\rangle \| = \left\| \sum_{t=1}^{T} |\psi_t\rangle - |\psi_{t-1}\rangle \right\| \leq \sum_{t=1}^{T} \| |\psi_t\rangle - |\psi_{t-1}\rangle \|$$

$$\leq 2 \sum_{t=1}^{T} |\alpha_{z,t}| \leq \frac{2 \cdot T}{\sqrt{N}}.$$



Note that if $|\phi_f\rangle$ is close to $|\phi_g\rangle$ there is no measurement that will distinguish between the two cases with high probability.

We will formalize this, but first we'll prove (*).

Monday, November 19, 2018 10:01 AM

Claim

$$\| |\psi_t\rangle - |\psi_{t-1}\rangle \| \leq 2 |\alpha_{z,t}|$$

Proof $|\psi_t\rangle$ and $|\psi_{t-1}\rangle$ differ in only one place:

$$|\psi_t\rangle = \underbrace{U_T O_g U_{T-1} O_g \cdots U_t}_{U} O_f \underbrace{U_{t-1} O_f U_{t-2} O_f \cdots O_f U_0 |\phi_{start}\rangle}_{|\phi\rangle}$$

$$|\psi_{t-1}\rangle = U_T O_g U_{T-1} O_g \cdots U_t O_g U_{t-1} O_f U_{t-2} O_f \cdots O_f U_0 |\phi_{start}\rangle$$

$$|\psi_t\rangle = U \, O_f |\phi\rangle$$
$$|\psi_{t-1}\rangle = U \, O_g |\phi\rangle$$

Note that O_f + O_g are the same except on two basis vectors: $|z\rangle|0\rangle$ & $|z\rangle|1\rangle$

$f(z)=0$ $\quad O_f \; |z\rangle|0\rangle \to |z\rangle|0\rangle \qquad O_f \; |z\rangle|1\rangle \to |z\rangle|1\rangle$

$g(z)=1$ $\quad O_g \; |z\rangle|0\rangle \to |z\rangle|1\rangle \qquad O_g \; |z\rangle|1\rangle \to |z\rangle|0\rangle$

Amplitude of $|z\rangle|0\rangle$ in $|\phi\rangle$ is $\alpha_{z0,t}$

Amplitude of $|z\rangle|1\rangle$ in $|\phi\rangle$ is $\alpha_{z1,t}$

$$|\alpha_{z,t}|^2 = |\alpha_{z0,t}|^2 + |\alpha_{z1,t}|^2$$

$$O_f|\phi\rangle - O_g|\phi\rangle = \alpha_{z0,t}|z\rangle|0\rangle + \alpha_{z1,t}|z\rangle|1\rangle - \alpha_{z1,t}|z\rangle|0\rangle - \alpha_{z0,t}|z\rangle|1\rangle$$

Unstructured Search Lower Bound - page 8

Tuesday, November 20, 2018 8:46 AM

$|\psi_t\rangle = U\, O_f|\phi\rangle$

$|\psi_{t-1}\rangle = U\, O_g|\phi\rangle$.

$$O_f|\phi\rangle - O_g|\phi\rangle = \alpha_{z0,t}|z\rangle|0\rangle + \alpha_{z1,t}|z\rangle|1\rangle - \alpha_{z1,t}|z\rangle|0\rangle - \alpha_{z0,t}|z\rangle|1\rangle$$

$$\| |\psi_t\rangle - |\psi_{t-1}\rangle \| = \| O_f|\phi\rangle - O_g|\phi\rangle \|$$

$$= \left[|\alpha_{z0,t} - \alpha_{z1,t}|^2 + |\alpha_{z1,t} - \alpha_{z0,t}|^2 \right]^{1/2}$$

$(a+b)^2 \le 2(a^2+b^2)$

$$= \left[2\, |\alpha_{z0,t} - \alpha_{z1,t}|^2 \right]^{1/2} = \sqrt{2}\, |\alpha_{z0,t} - \alpha_{z1,t}|$$

$$\le \sqrt{2}\left(|\alpha_{z0,t}| + |\alpha_{z1,t}| \right) = \sqrt{2}\left[\left(|\alpha_{z0,t}| + |\alpha_{z1,t}| \right)^2 \right]^{1/2}$$

$|\alpha_{z,t}|^2 = |\alpha_{z0,t}|^2 + |\alpha_{z1,t}|^2$

$$\le \sqrt{2}\left[2\left(|\alpha_{z0,t}|^2 + |\alpha_{z1,t}|^2 \right) \right]^{1/2}$$

$$= \sqrt{2}\,\sqrt{2}\left(|\alpha_{z0,t}|^2 + |\alpha_{z1,t}|^2 \right)^{1/2} = 2\,|\alpha_{z,t}|.$$

We have established that $\| |\phi_g\rangle - |\phi_f\rangle \| \le \frac{2T}{\sqrt{N}}$.

Presumably if the two states are close, we can not distinguish between them with a single measurement with high probability.

The algorithm will perform some measurement and based on the outcome will output "f" or "g".

Unstructured Search Lower Bound - page 9

Tuesday, November 20, 2018 8:54 AM

We can assume this last measurement is in the standard basis (otherwise we can insert a unitary operation which changes the basis.

1- qubit example.

Same outcomes.

* Measure in $|\phi\rangle$ $|\phi^\perp\rangle$ basis.
* Apply unitary $|\phi\rangle \to |0\rangle$, $|\phi^\perp\rangle \to |1\rangle$. Then measure in 0/1 basis.

Let S be the set of outcomes for which the answer is "f".

Let $\bar{S}$ be the set of outcomes for which the answer is "g".

For small error we would need:

Unstructured Search Lower Bound - page 10

Tuesday, November 20, 2018 9:01 AM

Suppose the error is $\leq 1/3$.

$$\sum_{y \in S} |\alpha_{y,g}|^2 \leq \frac{1}{3}.$$

$$1 = \sum_y |\alpha_{y,f}|^2 = \| |\phi_f\rangle \|^2$$

$$\sum_{y \in \bar{S}} |\alpha_{y,f}|^2 \leq \frac{1}{3} \Rightarrow \sum_{y \in S} |\alpha_{y,f}|^2 \geq 2/3$$

Then we know: $\sum_{y \in S} \underbrace{|\alpha_{y,f}|^2}_{\geq 2/3} - \underbrace{|\alpha_{y,g}|^2}_{\leq 1/3} \geq \frac{1}{3}$

Will show:

$$\frac{1}{3} \leq \sum_{y \in S} |\alpha_{y,f}|^2 - |\alpha_{y,g}|^2 \leq 2 \| |\phi_f\rangle - |\phi_g\rangle \| + \| |\phi_f\rangle - |\phi_g\rangle \|^2$$

From before: $\| |\phi_f\rangle - |\phi_g\rangle \| \leq \frac{2T}{\sqrt{N}}$.

$$\frac{1}{3} \leq \frac{4T}{\sqrt{N}} + \frac{4T^2}{N}.$$

$T = \Omega(\sqrt{N})$

Unstructured Search Lower Bound - page 11

Tuesday, November 20, 2018 9:39 AM

Need to show:

$$\sum_{y\in S} |\alpha_{y,g}|^2 - |\alpha_{y,f}|^2 \le 2\,\|\,|\phi_f\rangle - |\phi_g\rangle\| + \|\,|\phi_f\rangle - |\phi_g\rangle\|^2$$

$$\sum_{y\in S} \underbrace{|\alpha_{y,g}|^2}_{|(\alpha_{y,f}) + (\alpha_{y,g} - \alpha_{y,f})|^2 \le} - \cancel{|\alpha_{y,f}|^2}$$

$|a+b|^2 \le |a|^2 + 2|a||b| + |b|^2$

$$\cancel{|\alpha_{y,f}|^2} + 2\,|\alpha_{y,f}|\,|\alpha_{y,g} - \alpha_{y,f}| + |\alpha_{y,g} - \alpha_{y,f}|^2$$

$$\le 2\left[\left(\sum_{y\in S} \underbrace{|\alpha_{y,f}|}_{a_i}\,\underbrace{|\alpha_{y,g} - \alpha_{y,f}|}_{b_i}\right)^2\right]^{1/2} + \underbrace{\sum_{y\in S} |\alpha_{y,g} - \alpha_{y,f}|^2}_{\le \|\,|\phi_g\rangle - |\phi_f\rangle\|^2}$$

$$\le 2\left[\underbrace{\sum_{y\in S} |\alpha_{y,f}|^2}_{\le 1}\ \sum_{y\in S} |\alpha_{y,f} - \alpha_{y,g}|^2\right]^{1/2}$$

$$\left(\sum_i a_i b_i\right)^2 \le \sum_i (a_i)^2 \sum_i (b_i)^2$$

$$\le 2\left[\underbrace{\sum_{y\in S} |\alpha_{y,f} - \alpha_{y,g}|^2}_{}\right]^{1/2} + \|\,|\phi_g\rangle - |\phi_f\rangle\|^2$$

$$\underbrace{\|\,|\phi_g\rangle - |\phi_f\rangle\|}_{}$$