# Lower Bound for Unstructured Search

Note Title 5/4/2012

Have access to $f$ through an oracle $O_f$ for $f$.

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

We don't know $x$ but the algorithm must work with high probability for every $x$.

An algorithm can be described as a series of applications to $O_x$ interleaved with unitaries (computation).

The main technical tool used in the proofs of both lemmas is the Cauchy-Schwartz inequality:

For any two vectors $|v\rangle$ + $|w\rangle$ (arbitrary length)

$$\underbrace{\langle v|v\rangle \langle w|w\rangle}_{\substack{\text{length}^2 \text{ of the projection} \\ \text{if } |v\rangle + |w\rangle \text{ are pointing in} \\ \text{the same direction.}}} \geq \underbrace{|\langle v|w\rangle|^2}_{\substack{\text{square of the length of the projection} \\ \text{of } |v\rangle \text{ onto } |w\rangle.}}$$

For $\begin{matrix} v_1, \ldots, v_N \\ w_1, \ldots, w_N \end{matrix} \in \mathbb{C}$ $\qquad \left| \sum_x v_x \bar{w}_x \right|^2 \geq \sum_x |v_x|^2 \sum_y |w_y|^2$

If $a_x$ and $b_x$ are real

$$\left(\sum_{x=1}^{N} a_x\right)^{1/2} \left(\sum_{x=1}^{N} b_y\right)^{1/2} \geq \sum_x a_x b_x$$

if the $b_y = 1$ we get: $\qquad N \sum_{x=1}^{N} a_x \geq \left(\sum_x a_x\right)^2$

The algorithm can be seen as a sequence of calls to the oracle $O_f$ interleaved with computation (unitaries). Suppose there are $T$ calls to the oracle.

Let $\alpha_{x,t}$ be the amplitude with which $x$ is queried in the $t^{th}$ oracle call. In other words just be for the $t^{th}$ oracle call, the input register is in state $\sum_x \alpha_{x,t}|x\rangle$.

for the case that $f(x)=0$ $\forall x$.

Note that $\sum_x |\alpha_{x,t}|^2 = 1$, so $\sum_{t=1}^{T}\sum_x |\alpha_{x,t}|^2 = T$

and switching the order of summation $\sum_x \underbrace{\sum_{t=1}^{T} |\alpha_{x,t}|^2} = T$

We want to pick the $x$ which is queried the least which is the $x$ that minimizes this sum

Suppose the sum is minimized for $z$: $\sum_{t=1}^{T} |\alpha_{z,t}|^2 \le T/N$

(the minimum is at most the average $x$)

using Cauchy-Schwartz $T\sum_{t=1}^{T}|\alpha_{z,t}|^2 \ge \left(\sum_t |\alpha_{z,t}|\right)^2$

and $\sum_t |\alpha_{z,t}| \le T/\sqrt{N}$

Now we define two functions: $f(x)=0$ $\forall x$.

$g(x)=0$ $\forall x\neq z$ $g(z)=1$

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

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

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

$$|\phi_f\rangle = U_T O_f U_{T-1} O_f \cdots \underset{\text{oracle call}}{O_f} \underset{\text{computation}}{U_0} |\phi_{start}\rangle$$

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

We will define a series of intermediate states
$|\psi_t\rangle$ will be defined above with the first k oracle calls
to $O_f$ and the last $T-t$ calls to $O_g$:

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

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

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

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

Using this, we will have

$$\| |\phi_f\rangle - |\phi_g\rangle \| \leq \sum_{t=1}^{T} \| |\psi_t\rangle - |\psi_{t-1}\rangle \| \leq \sqrt{2} \sum_{t=1}^{T} |\alpha_{z,t}|$$

$$\leq \frac{\sqrt{2}\,T}{\sqrt{N}}$$

Note that if $\| |\phi_f\rangle - |\phi_g\rangle \|$ are close
there is no measurement that will
distinguish between the two cases with
high probability. We will formalize this, but first we prove (*).

Proof of

$\| |\psi_t\rangle - |\psi_{t-1}\rangle \| \le \sqrt{2}\, |\alpha_{z,t}|$ : $|\psi_t\rangle$ + $|\psi_{t-1}\rangle$ differ at only one place:

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

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

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

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

$$\| |\psi_t\rangle - |\psi_{t-1}\rangle \| = \| (O_f - O_g)\, |\phi\rangle \|$$
$$\left[ (\alpha_{z0,t} - \alpha_{z1,t})^2 + (\alpha_{z1,t} - \alpha_{z0,t})^2 \right]^{1/2}$$
$$= \sqrt{2}\, | \alpha_{z0,t} - \alpha_{z1,t} | \le \sqrt{2} \left[ |\alpha_{z0,t}| + |\alpha_{z1,t}| \right]$$
$$= \sqrt{2}\, |\alpha_{z,t}|$$

//

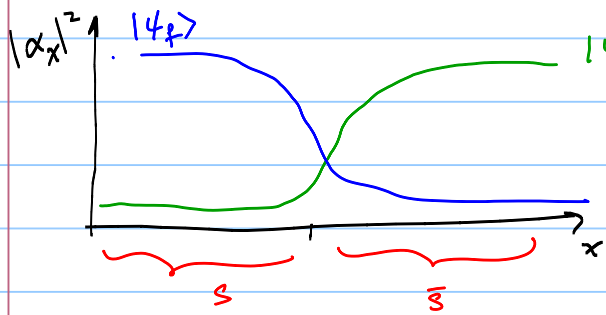
We have established that $\| |\phi_g\rangle - |\phi_f\rangle \| \le \frac{2T}{\sqrt{N}}$.

Presumably, if these two states are close, we will not be able to distinguish between them with a single measurement.

The algorithm will perform a measurement and based on the outcome will output "f" or "g".
We can assume the measurement is in the standard basis (otherwise we can insert a unitary op which changes the basis).

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

Intuitively, for there to be small error we need:




But this would imply that $\| |\psi_f\rangle - |\psi_g\rangle \|$ is large.

Error is $\displaystyle\sum_{y\in S} |\alpha_{y,g}|^2 \le 1/3.$

$$\sum_{y\in \bar{S}} |\alpha_{y,f}|^2 \le 1/3. \quad \Longrightarrow \quad \sum_{y\in S} |\alpha_{y,f}|^2 \ge 2/3$$

$$1/3 \le \sum_{y\in S} \underbrace{|\alpha_{y,g}|^2}_{|\alpha_{y,f} + (\alpha_{y,g}-\alpha_{y,f})|^2} - |\alpha_{y,f}|^2 \le \sum_{y\in S} 2|\alpha_{y,f}|\,|\alpha_{y,f}-\alpha_{y,g}| + (\alpha_{y,f}-\alpha_{y,g})^2$$

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

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

$$\le 2\| |\psi_f\rangle - |\psi_g\rangle \| + \| |\psi_f\rangle - |\psi_g\rangle \|^2 \le 2\frac{T}{\sqrt{N}} + \frac{T^2}{N}.$$

$\Rightarrow$ $T$ is $\Omega(\sqrt{N})$