Lecture 17

26 MAR 2014

On the optimality of Grover's algorithm

We can prove that $\Omega(\sqrt{2^n})$ queries are needed for any quantum algorithm to solve the unstructured search problem

i.e., find x_0 such that $f(x_0) = 1$

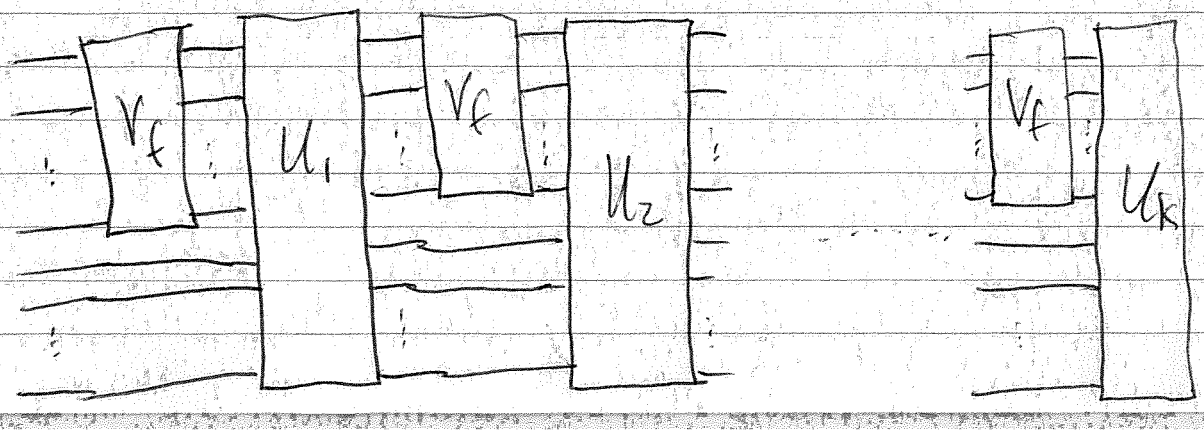
WLOG, let us assume that we are using the phase oracle

$$V_f |x\rangle = (-1)^{f(x)\oplus 1} |x\rangle$$

so that $V_f \equiv (I - |x_0\rangle\langle x_0|) - |x_0\rangle\langle x_0|$

$$= I - 2|x_0\rangle\langle x_0|$$

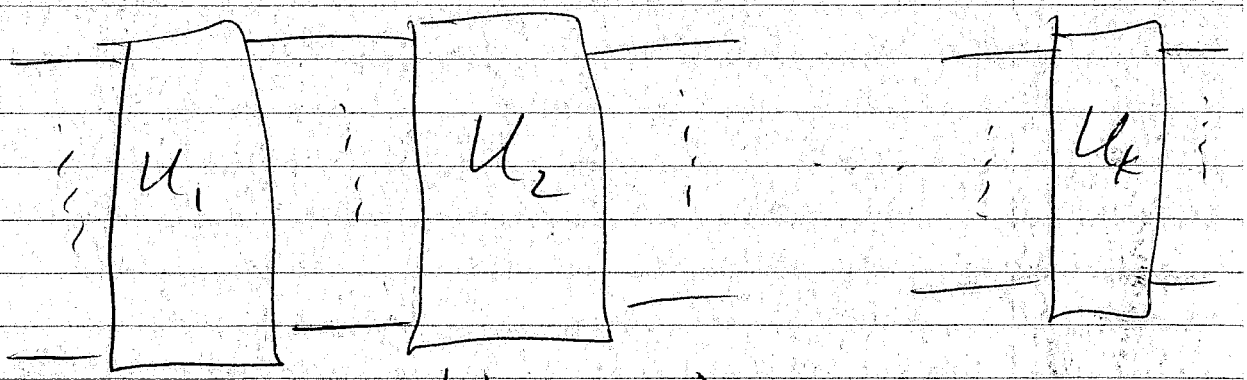
The most general quantum algorithm for this task has the form



Proof idea is this:

If we do not call the oracle at all, then we don't learn any information about f & so we are no better off than essentially a random guess. Thus, if we compare the states after each U_k w/ & w/out the oracle calls, these states should become more & more orthogonal as the algorithm proceeds.

So we compare to



Let $|\phi^k_{x_0}\rangle = \left(\prod_{i=1}^{k} U_i V_f\right)|\psi\rangle$

$|\phi^k\rangle = \left(\prod_{i=1}^{k} U_i\right)|\psi\rangle$

We could study an individual distance such as

$$\left\| |\phi^k_{x_0}\rangle - |\phi^k\rangle \right\|^2$$

but it turns out to be useful to symmetrize this expression by summing over all possible functions that have a single x_0 such that $f(x_0)=1$. So we instead analyze

$$r_k = \sum_{x_0 \in \{0,1\}^n} \left\| |\phi^k_{x_0}\rangle - |\phi^k\rangle \right\|^2.$$

The idea will be

1) place an upper bound on r_k:

$$r_k \leq 4k^2$$

2) Supposing that we wish to identify x_0 w/ probability $> 1/2$, then this will imply that

Part 1: bound $n_k \leq 4k^2$

$$\left\| |\phi_{x_0}^{k+1}\rangle - |\phi^{k+1}\rangle \right\|^2 = \left\| U_{k+1} V_f |\phi_{x_0}^{k}\rangle - U_{k+1} |\phi^k\rangle \right\|^2$$

$$= \left\| V_f |\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right\|^2$$

$$= \left\| V_f \left(|\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right) + (V_f - I)|\phi^k\rangle \right\|^2$$

$$= \left\| V_f \left(|\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right) - 2|x_0\rangle\langle x_0|\phi^k\rangle \right\|^2$$

$$= \left\| V_f \left(|\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right) + \left(-2\langle x_0|\phi^k\rangle \right)|x_0\rangle \right\|^2$$

$$\leq \left(\left\| V_f \left(|\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right) \right\| + 2\left|\langle x_0|\phi^k\rangle\right| \right)^2$$

$$= \left(\left\| |\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right\| + 2\left|\langle x_0|\phi^k\rangle\right| \right)^2$$

$$= \left\| |\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right\|^2 + 4 \left\| |\phi_{x_0}^{k}\rangle - |\phi^k\rangle \right\| \cdot \left|\langle x_0|\phi^k\rangle\right| + 4\left|\langle x_0|\phi^k\rangle\right|^2$$

Summing this over all x_0, we get that

$$r_{k+1} \leq r_k + 4 \sum_{x_0 \in \{0,1\}^n} \| |\phi_{x_0}^k\rangle - |\phi^k\rangle \| \cdot |\langle x_0|\phi^k\rangle| + 4$$

↑ b/c $4 \sum_{x_0} |\langle x_0|\phi^k\rangle|^2 = 4$

But now we use Cauchy-Schwarz to upper bound

$$\sum_{x_0 \in \{0,1\}^n} \| |\phi_{x_0}^k\rangle - |\phi^k\rangle \| \, |\langle x_0|\phi^k\rangle|$$

$$\leq \left(\sum_{x_0} \| |\phi_{x_0}^k\rangle - |\phi^k\rangle \|^2 \right)^{1/2} \left(\sum_{x_0} |\langle x_0|\phi_k\rangle|^2 \right)^{1/2}$$

$$= r_k^{1/2}$$

So,

$$r_{k+1} \leq r_k + 4 + 4\sqrt{r_k}$$

Now $r_1 = \sum_{x_0} \| |\phi_{x_0}^1\rangle - |\phi^1\rangle \|^2$

$$= \sum_{x_0} \| U_1 V_f |+\rangle - U_1 |+\rangle \|^2$$

$$= \sum_{x_0} \| (V_f - I) |+\rangle \|^2$$

$$= \sum_{x_0} \| -2 |x_0\rangle\langle x_0|+\rangle \|^2$$

$$= 4 \sum_{x_0} |\langle x_0|+\rangle|^2 = 4$$

So by the induction, we get $r_k \leq 4k^2$

$$r_{k+1} \leq 4k^2 + 4 + 4\sqrt{4k^2}$$

$$= 4(k^2 + 1 + 2k)$$

$$= 4(k+1)^2$$

So we conclude that $r_k \leq 4k^2$

Conclusion is that the oracle queries can only increase distinguishability by so much.

Part 2: $r_k \geq c \cdot 2^n$

Suppose We want the algorithm to be successful w/ prob. $\geq 1/2$

So this means that $|\langle x_0 | \phi_{x_0}^k \rangle|^2 \geq 1/2$ we should have

But this implies that

$$\| |\phi_{x_0}^k\rangle - e^{i\varphi} |x_0\rangle \|^2$$

$$= \left(\langle \phi_{x_0}^k| - e^{-i\varphi}\langle x_0|\right)\left(|\phi_{x_0}^k\rangle - e^{i\varphi}|x_0\rangle\right)$$

$$= 1 + 1 - e^{-i\varphi}\langle x_0|\phi_{x_0}^k\rangle - e^{i\varphi}\langle \phi_{x_0}^k | x_0\rangle$$

$$\leq 2 - \sqrt{2}$$

Now come back to r_k:

$$r_k = \sum'_{x_0 \in \{0,1\}^n} \left\| |\phi^k_{x_0}\rangle - |\phi^k\rangle \right\|^2$$

$$= \sum'_{x_0 \in \{0,1\}^n} \left\| |\phi^k_{x_0}\rangle - |x_0\rangle + |x_0\rangle - |\phi^k\rangle \right\|^2$$

$$\geq \sum'_{x_0 \in \{0,1\}^n} \left(\left\| |\phi^k_{x_0}\rangle - |x_0\rangle \right\| - \left\| |\phi^k\rangle - |x_0\rangle \right\| \right)^2$$

$$= \sum'_{x_0} \left\| |\phi^k_{x_0}\rangle - |x_0\rangle \right\|^2 - \sum'_{x_0} \left\| |\phi^k\rangle - |x_0\rangle \right\|^2$$

$$- 2 \sum'_{x_0} \left\| |\phi^k_{x_0}\rangle - |x_0\rangle \right\| \cdot \left\| |\phi^k\rangle - |x_0\rangle \right\|$$

Apply Cauchy-Schwarz to get

$$\sum'_{x_0} \left\| |\phi^k_{x_0}\rangle - |x_0\rangle \right\| \left(\cdot \left\| |\phi^k\rangle - |x_0\rangle \right\| \right)$$

$$\leq \left[\sum'_{x_0} \left\| |\phi^k_{x_0}\rangle - |x_0\rangle \right\| \cdot \sum'_{x_0} \left\| |\phi^k\rangle - |x_0\rangle \right\|^2 \right]^{1/2}$$

So conclude that

$$r_k \geq \left(- \left[\sum'_{x_0} \left\| |\phi^k_{x_0}\rangle - |x_0\rangle \right\|^2 \right]^{1/2} + \left[\sum'_{x_0} \left\| |\phi^k\rangle - |x_0\rangle \right\|^2 \right]^{1/2} \right)^2$$

From before, we require that

$$\left\| |\phi_{x_0}^k\rangle - |x_0\rangle \right\|^2 \leq 2 - \sqrt{2}$$

So this means that

$$\sum_{x_0} \left\| |\phi_{x_0}^k\rangle - |x_0\rangle \right\|^2 \leq 2^n \left(2 - \sqrt{2}\right)$$

&

$$r_k \geq \left(-\left[\left(2-\sqrt{2}\right) 2^n\right]^{1/2} + \left\{ \sum_{x_0} \left\| |\phi_k\rangle - |x_0\rangle \right\|^2 \right\}^{1/2} \right)^2$$

So we bound from below

$$\sum_{x_0} \left\| |\phi_k\rangle - |x_0\rangle \right\|^2 = \sum_{x_0} \left(\langle \phi_k| - \langle x_0| \right)\left(|\phi_k\rangle - |x_0\rangle \right)$$

$$= \sum_{x_0} \langle \phi_k|\phi_k\rangle + \langle x_0|x_0\rangle - \langle \phi_k|x_0\rangle - \langle x_0|\phi_k\rangle$$

$$\geq \sum_{x_0} \left(2 - 2\left|\langle \phi_k|x_0\rangle\right|\right)$$

But

$$\sum_{x_0} \left|\langle \phi_k|x_0\rangle\right| \leq \sqrt{\left(\sum_x 1\right)\left(\sum_x |\langle x|\phi_k\rangle|^2\right)}$$

$$= \sqrt{2^n}$$

So

$$\geq 2 \cdot 2^n - 2\sqrt{2^n} = 2\left(2^n - \sqrt{2^n}\right)$$

Plug in to find that

$$r_k \geq \left(-\left[(2-\sqrt{2})2^n\right]^{1/2} + \left[2\cdot(2^n-\sqrt{2^n})\right]^{1/2} \right)^2$$

$$= \left(\left[(2-\sqrt{2})2^n\right]^{1/2} - \left[2\cdot(2^n-\sqrt{2^n})\right]^{1/2} \right)^2$$

$$\geq \left(\left[(2-\sqrt{2})(2^n-\sqrt{2^n})\right]^{1/2} - \left[2\cdot(2^n-\sqrt{2^n})\right]^{1/2} \right)^2$$

$$= \left[(2-\sqrt{2})^{1/2} - \sqrt{2}\right]^2 \cdot 2^n - \sqrt{2^n}$$

$$\approx c\cdot 2^n \quad \text{for large } n$$

So combining

$$r_k \leq 4k^2$$

& $r_k \geq c\cdot 2^n$,

we see that $k \geq \Theta(\sqrt{2^n})$

to have a reasonable success probability.

Different topic: simulation of quantum systems (simple ideas)

In QM, time evolution of a q. state is governed by the Schrödinger equation:

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle$$

$H(t)$ is the Hamiltonian, generator of time translations

usually take $\hbar = 1$ for convenience

Also take $H(t)$ to be time independent for simplicity so that

$$H(t) = H$$

$\Rightarrow$ solution is $|\psi(t)\rangle = e^{-iHt}|\psi(0)\rangle$

Say that a Hamiltonian H acting on n qubits can be efficiently simulated if $\forall t, \varepsilon > 0$

$\exists$ a quantum circuit U consisting of $\text{poly}(n, t, 1/\varepsilon)$ gates such that $\|U - e^{-iHt}\| \leq \varepsilon$

we will not be able to simulate arbitrary Hamiltonians, but some of them we can.

Some trivial cases: if H acts on only a constant # of qubits then we just invoke Solovay-Kitaev to say there exists a quantum circuit of error at most ε using $\text{poly}\left(\log\left(\frac{1}{\varepsilon}\right)\right)$ 1- + 2-qubit gates

can also rotate the basis in which H is applied using any U w/ an efficient decomposition into basic gates. That is, if H has an efficient sim. & U has an eff. implementation, then $UHU^\dagger$ can be efficiently simulated. Follows from

$$Ue^{-iHt}U^\dagger = e^{-iUHU^\dagger t}$$

Suppose a Hamiltonian is diagonal in the computational basis $|a\rangle$ that any diagonal element can be computed efficiently

$$d(a) = \langle a|H|a\rangle$$

then we just do

$$|a,0\rangle \to |a,d(a)\rangle \quad \text{compute}$$

$$\to e^{-itd(a)} |a,d(a)\rangle \quad \text{add phase}$$

$$\to e^{-itd(a)} |a,0\rangle \quad \text{uncompute}$$

$$= e^{-iHt} |a,0\rangle$$

extend by linearity

Many physical Hamiltonians are expressed as a sum of terms

For example, particle in a potential

$$H = \frac{p^2}{2m} + V(x)$$

idea is to discretize the x coordinate

$V(x)$ is diagonal & natural discretizations of $p^2 = \frac{-d^2}{dx^2}$ are diagonal in the discrete Fourier basis.

so we can efficiently simulate both $V(x)$ & $p^2/2m$

Another example:

Ham. for spin system

$$H = \sum_i h_i X_i \sum_{i,j} J_{ij} Z_i Z_j$$

This is a sum of terms, each of which acts on no more than 2 qubits & thus are each easy to simulate

If H_1 & H_2 can be efficiently simulated, then so can

$$H_1 + H_2 .$$

How is this so?

If they commute, obvious

b/c $e^{-iH_1 t} e^{-iH_2 t} = e^{-i(H_1+H_2)t}$

But if they don't?

We have the Lie-Trotter product formula:

$$e^{-i(H_1+H_2)t} = \lim_{m\to\infty} \left(e^{-i\frac{H_1 t}{m}} e^{-i\frac{H_2 t}{m}} \right)^m$$

proof idea: can truncate the RHS to a finite # of terms & if we want to have

$$\left\| \left(e^{-i\frac{H_1 t}{m}} e^{-i\frac{H_2 t}{m}} \right)^m - e^{-i(H_1+H_2)t} \right\|$$

Taylor expand the exponential

we need $m = O((rt)^2/\varepsilon) \leq \varepsilon$

where $r = \max\{\|H_1\|, \|H_2\|\}$

can get improvements (smaller m) by considering

$$\left(e^{\frac{-iH_1 t}{2m}} e^{\frac{-iH_2 t}{m}} e^{\frac{-iH_1 t}{2m}} \right)^m$$

In general, we have

$$e^{-i(H_1 + \cdots + H_k)t} =$$

$$\lim_{m \to \infty} \left(e^{\frac{-iH_1 t}{m}} \cdots e^{\frac{-iH_k t}{m}} \right)^m$$