Lecture 16

24 MAR 2014

Amplitude amplification is a generic way to get speedups for any classical probabilistic algorithm.

Given is a Boolean function $f: \{0,1\}^n \to \{0,1\}$

Suppose we have a classical or quantum algorithm that finds a solution (x such that $f(x)=1$) w/ probability p when acting on the initial state $|0\ldots0\rangle$

(again we can use the techniques of reversible computation to have a quantum circuit.)

Classically we would have to execute the algorithm roughly $1/p$ times before finding a solution.

quantumly, we only need $O\left(\frac{1}{\sqrt{p}}\right)$ repetitions.

When we apply the algorithm A to an initial state $|00\ldots0\rangle$, we end up w/

$$|\psi\rangle = \sum_x \alpha_x |x\rangle |junk(x)\rangle$$

& split this into

$$= \sum_{x \in X_{good}} \alpha_x |x\rangle |junk(x)\rangle + \sum_{x \in X_{bad}} \alpha_x |x\rangle |junk(x)\rangle$$

& $p = p_{good} \equiv \sum_{x \in X_{good}} |\alpha_x|^2$ (success prob.)

$$p_{bad} = 1 - p_{good}$$

If $p_{good} = 1$, there is no need for AA, & if $p_{bad} = 0$, AA will not help at all.

We can then write

$$|\psi_{good}\rangle = \sum_{x \in X_{good}} \frac{\alpha_x}{\sqrt{p_{good}}} |x\rangle |junk(x)\rangle$$

$$|\psi_{bad}\rangle = \sum_{x \in X_{bad}} \frac{\alpha_x}{\sqrt{p_{bad}}} |x\rangle |junk(x)\rangle$$

& $|\psi\rangle = \sqrt{p_{good}}\, |\psi_{good}\rangle + \sqrt{p_{bad}}\, |\psi_{bad}\rangle$

or $|\psi\rangle = \sin\theta\, |\psi_{good}\rangle + \cos\theta\, |\psi_{bad}\rangle$

w/ θ such that $\sin^2\theta = p_{good}$

Can now define the Grover iterate to be

$$A\, U_0^{\perp}\, A^{\dagger}\, U_f$$

where $U_f = |x\rangle \rightarrow (-1)^{f(x)} |x\rangle$

& $U_{0^\perp} = \begin{cases} |x\rangle \rightarrow -|x\rangle & \text{if } x \neq 0 \\ |0\rangle \rightarrow |0\rangle & \text{otherwise} \end{cases}$

4

So $AU_0^{\perp}A^{+} = \begin{cases} |\psi\rangle \to |\psi\rangle \\ |\phi\rangle \to -|\phi\rangle \text{ for all } |\phi\rangle \perp |\psi\rangle \end{cases}$

By same reasoning as last time, k applications of $AU_0^{\perp}A^{+}U_f$ to $|\psi\rangle$ lead to

$$\sin((2k+1)\theta)\,|\psi_{good}\rangle + \cos((2k+1)\theta)\,|\psi_{bad}\rangle$$

so we need to pick k such that $(2k+1)\theta \approx \pi/2$

if ~~[illegible]~~ p_{good} is small then $\sin\theta \approx \theta$ & $\theta = \sqrt{p_{good}}$

so that the number of iterations is $O(1/\sqrt{p_{good}})$

if A is a simple algorithm that simply uniformly samples the input, then $p_{good} = M/N$ where M is # of soln's

If we don't know p_{good}, then we don't know how many times we should repeat the algorithm. As a special case, if we don't know the # of solutions, then we don't know how many times to repeat Grover search.

<u>Amplitude estimation</u> is an algorithm which estimates the amplitude w/ which an algorithm A maps $|00\ldots0\rangle$ to the subspace of solutions to $f(x)=1$

The input is 1) A w/ the property that

$$A|00\ldots0\rangle = \sin\theta\,|\psi_{good}\rangle + \cos\theta\,|\psi_{bad}\rangle$$

2) operator U_f taking

$$|\psi_{good}\rangle \to -|\psi_{good}\rangle \;\&$$
$$|\psi_{bad}\rangle \to |\psi_{bad}\rangle$$

problem is to estimate $\sin\theta$

We can see that quantum counting is a special case of this

w/ $|\psi_{good}\rangle = \sum_{j\in X_{good}} \frac{1}{\sqrt{M}} |j\rangle$

$$|\psi_{bad}\rangle = \sum_{j\in X_{bad}} \frac{1}{\sqrt{N-M}} |j\rangle$$

&

$$A|00\cdots 0\rangle = \sqrt{\frac{M}{N}}\, |\psi_{good}\rangle + \sqrt{\frac{N-M}{N}}\, |\psi_{bad}\rangle$$

So, here, $\sin^2\theta = \frac{M}{N}$

Back to amplitude estimation,

Focus on the case in which

$0 < \sin\theta < 1$

Recall that amplitude amplification

$A U_0^{\perp} A^{\dagger} U_f$ is a rotation of the subspace spanned by $\{|\psi_{bad}\rangle, |\psi_{good}\rangle\}$ by an angle 2θ

so it's described by a rotation matrix

$$\begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}$$

Can show that two independent eigenvectors of this matrix are

$$\psi_+ = \begin{pmatrix} i/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}, \quad \psi_- = \begin{pmatrix} -i/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$$

w/ eigenvalues $e^{i2\theta}$ & $e^{-i2\theta}$

So we can write

$$|\psi_+\rangle = \frac{i}{\sqrt{2}}|\psi_{bad}\rangle + \frac{1}{\sqrt{2}}|\psi_{good}\rangle$$

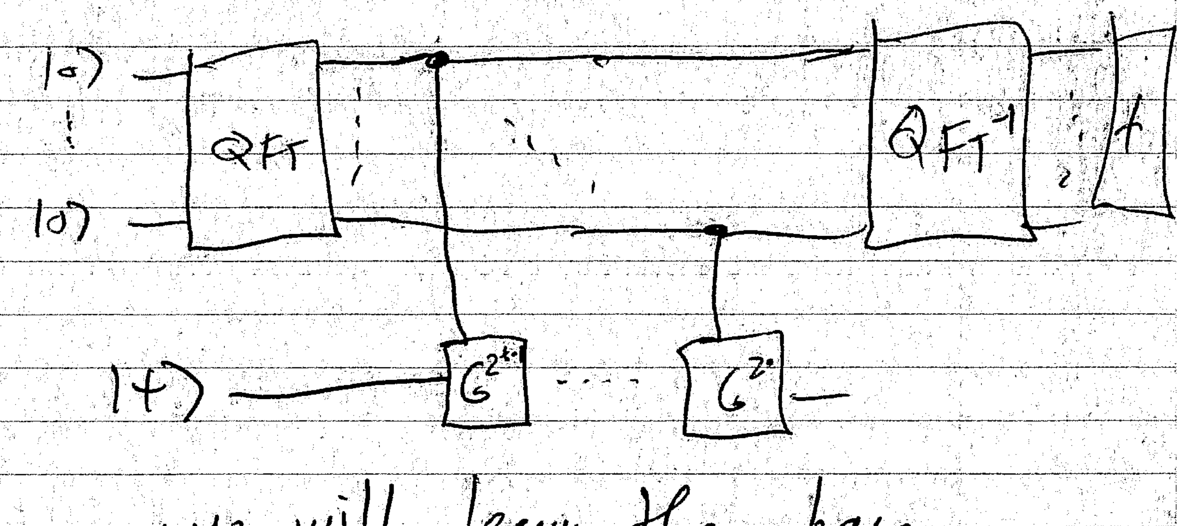
$$|\psi_-\rangle = \frac{-i}{\sqrt{2}}|\psi_{bad}\rangle + \frac{1}{\sqrt{2}}|\psi_{good}\rangle$$

We can write the initial state of ~~the~~ amplitude estimation as

$$A|00\cdots 0\rangle = \sin\theta\,|\psi_{good}\rangle + \cos\theta\,|\psi_{bad}\rangle$$

$$= \frac{e^{i\theta}}{\sqrt{2}}|\psi_+\rangle - \frac{e^{-i\theta}}{\sqrt{2}}|\psi_-\rangle$$

So if we employ the quantum phase estimation algorithm as



we will learn the phase

2θ up to some accuracy.

There are of course accuracy issues, but we merely state the ~~the~~ overall running time is still $O(1/$