Algebra and Computation Course Instructor: V. Arvind

Lecture 25: Needle in a Haystack: Grover Search

Lecturer: V. Arvind *Scribe: Ramprasad Saptharishi*

1 Overview

In this lecture, we shall look at another problem where quantum algorithms do better than classical algorithms. This, unlike the DJ problem, is deep and is truly one where the quantum model beats the classical model.

2 Grover's Search

The problem is the following. You are given a function $f : \{0,1\} \longrightarrow \{0,1\}$ as an oracle with the promise $f(x) = 1$ for precisely one x say x_0. The problem is to find the x_0. We want to do this with as few queries as possible.

This is equivalent to searching in an unordered list; the value x_0 is hidden in the list and you want to find it.

2.1 Lower bounds on classical models

It is clear that a deterministic algorithm will take $O(2^n)$ queries.

It is easy to show that even for randomized algorithms, it would need $O(2^n)$ queries to make the error probability bounded by a constant. We shall leave the proof to the interested reader.

2.2 The Quantum Model

Grover presented a quantum algorithms that makes $O\left(2^{n/2}poly(n)\right)$ queries and finds x_0 with error probability bounded by a constant.

3 The Algorithm

The basic idea is the following property:

Let M_1 and M_2 are two lines through the origin in the plane, and the angle separating them being α and let P is any point on the plane. If you reflect P about M_1 and then that reflection about M_2, the resultant point

is at an angle 2α from P in the direction M_1M_2.

Our setting is going to be like this. We will be working in $\mathbb{C}^{2^n}$ and there is one special coordinate axis labelled by x_0 that we want to find. Using the function provided as oracle, we can get the unitary transform of the rotation about x_0 eventhough we do not know what x_0 is. The idea is to take another vector whose angle with x_0 is known and use this rotation technique to get closer to x_0. Since we know the angles, we know precisely how many rotations need to be done and that will give us a vector with a very high probability amplitude on the x_0 coordinate at which point we can make a measurement.

3.1 The Reflection Maps

Consider the uniform superposition $|\psi\rangle = \frac{1}{N}\sum_x |x\rangle$. We know that it makes an angle of $\cos^{-1}(2^{-n/2})$ with each coordinate axis.

The unitary map given to us works as we have assumed always. And we have also seen that $|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$ goes to $(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$. By just dropping the second coordinate, we can think of this as a map

$$I_{x_0} : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

This is just the identity matrix with a -1 on the (x_0, x_0) entry. This can be compactly written as $I_{x_0} = I - 2|x_0\rangle\langle x_0|$. This is just reflection about the plan perpendicular to x_0.

Observation 1. *If U is any unitary operator, then $I_{U|0^n\rangle} = UI_{0^n}U^{-1}$.*

Proof. It follows from the observation that $I_x = I - 2|x\rangle\langle x|$. □

Observation 2. *For any states $|\phi\rangle$ and $|\psi\rangle$, I_ψ preserves the span of $|\phi\rangle, |\psi\rangle$.*

In particular, $I_{U|0^n\rangle}$ and I_{x_0} preserve the span S of x_0 and $U|0^n\rangle$.

Observation 3. *Let $|e_1\rangle = U|0^n\rangle$ and let e_2 be anything in S that is perpendicular to e_1. We can pull out the $e^{i\theta}$ factor out of e_i so that $\langle e_i, x_0\rangle$ is real. Hence we now have*

$$S = \{a|e_1\rangle + b|e_2\rangle \ : \ a, b \in \mathsf{R}\}$$

Observation 4. *Let $v \in S$ and let $v^\perp$ be another in S that is orthogonal to v in S. Then $I_v = -I_{v^\perp}$.*

Thus, we need not know what x_0 is but by just using I_{x_0} we can achieve the reflection about x_0. And let U be the hadamard transform and $U|0^n\rangle$ will now be the uniform superposition $|\psi\rangle$.

3.2 The Double Reflection

We know that $U0^n$ make an angle of $\cos^{-1}(2^{-n/2})$ with each coordinate axis, and this is almost a right angle. Thus instead of $U|0^n\rangle$, we shall look at the orthogonal vector $U|0^n\rangle^{\perp}$ in the span S and the reflection. The angle that x_0 makes with this $\sin^{-1}(2^{-n/2})$ which is very small. Now, the unitary transform that achieves the rotation about x_0 and then about $U|0^n\rangle^{\perp}$ is just $-UI_{0^n}UI_{x_0}$.

Now look at the uniform superposition $|\psi\rangle = \frac{1}{N}\sum_x |x\rangle$. This is in the plane and the double rotation will rotate it by an angle of $2\sin^{-1}(2^{-n/2})$. Thus with just $\frac{\pi}{4}\sqrt{2^n}$ such double rotations we would get very close to x_0.

At this point, we can safely make a measurement and obtain x_0 with high probability.

4 Implications on SAT

The problem can be transformed to a decision problem. We are given a function f as an oracle and we need to determine if f is 1 at atleast one x. This is certainly easier than determining the x_0 as we have seen.

A result of Valiant and Vazirani shows that any SAT instance ϕ can be reduced to another instance ϕ' in randomized polynomail time such that ϕ is satisfiable implies ϕ' has exactly one satisfiable instance, and ϕ is unsatisfiable implies ϕ' is also unsatisfiable.

Grover's algorithm shows that SAT can be solved in $O(\sqrt{2}^n)$ time using a quantum algorithm.

5 A glimpse into the finale

In the next class, we shall show that Grover's algorithm is infact tight, any quantum algorithm that has error probability bounded by a constant must take $O(2^{n/2})$ queries.

We shall prove this using two beautiful lower bound techniques in the oracle setting.