6.896 Quantum Complexity Theory October 2, 2008

Lecture 9

Lecturer: Scott Aaronson

In this class we discuss Grover's search algorithm as well as the BBBV proof that it is optimal.

1 Grover's Algorithm

1.1 Setup

Given N items $\{x_1, x_2, ..., x_N\}$ we wish to find an index i such that $x_i = 1$. We are able to query the values x_i in quantum superposition (as usual). Grover's algorithm solves this problem using $O(\sqrt{N})$ quantum queries.

1.2 The Algorithm

Grover's algorithm can be described by the following circuit. In figure 1 the query operator is the

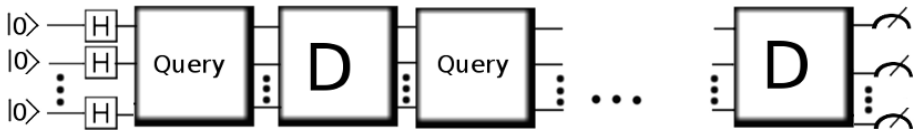
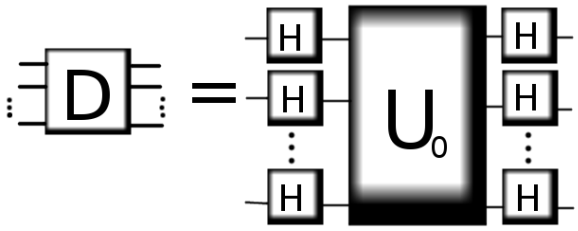


Figure 1: Circuit for Grover Search

standard phase query which transforms $\sum_i \alpha_i |i> \rightarrow \sum_i \alpha_i (-1)^{x_i} |i>$. The operator labeled D is called the Grover Diffusion Operator, which is given by the circuit in figure 2. We could also write



$$U_0 = 2|0\rangle\langle 0| - 1$$

Figure 2: Grover Diffusion Operator

the Grover Diffusion operator as a N by N matrix in the computational basis as follows:

$$\begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \frac{2}{N} & \dots & \frac{2}{N} \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N}-1 \end{pmatrix}$$

Note that this is a unitary transformation. Let's consider the action of this operator on a general quantum state $\sum_{i=1}^{N} \alpha_i |i>$. From figure 2, the operator has the effect of first switching from the computational basis to the Fourier basis (effected by the Hadamard transforms), applying a phase of (-1) to the zero Fourier mode , and then switching back to the computational basis. This operator has the net effect of inverting the amplitudes of the quantum state about their mean value,as illustrated in the following picture. Grover's algorithm , which is sometimes called

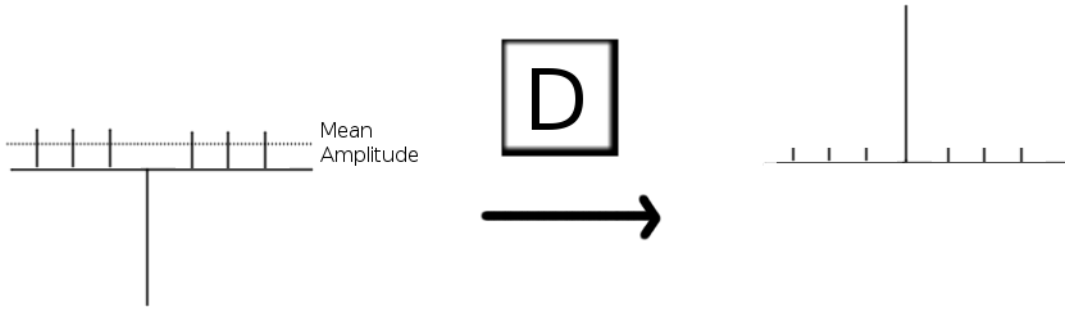


Figure 3: The Grover Diffusion Operator

'amplitude amplification' simply consists of alternating the query and diffusion operators. For the first few steps of the algorithm the amplitude of the solution is increased by approximately $\frac{2}{\sqrt{N}}$ (this is not the case when the amplitude of the solution is large, i.e when we are nearing the end of the algorithm. A more detailed analysis follows.). The reason we can get the answer with constant probability in $O(\sqrt{N})$ steps is because in quantum mechanics we're dealing with the L_2 norm as opposed to the L_1 norm for classical probability. Now let's analyse the algorithm in more detail. Write a_t for the amplitude of the marked item after time t (i.e after t iterations of Query+Diffusion).

We have $a_0 = \frac{1}{\sqrt{N}}$. The state vector after time t can be written as:

$$\begin{pmatrix} \sqrt{\frac{1-(a_t)^2}{N-1}} \\ \sqrt{\frac{1-(a_t)^2}{N-1}} \\ . \\ . \\ . \\ a_t \\ . \\ . \\ . \\ \sqrt{\frac{1-(a_t)^2}{N-1}} \end{pmatrix}$$

We can then apply the query operator followed by inversion about average to obtain an expression for a_{t+1} in terms of a_t:

$$a_{t+1} = \left(1 - \frac{2}{N}\right) a_t + \frac{2}{N}\sqrt{\left(1 - a_t^2\right)(N-1)} \tag{1}$$

We see from the above that when $a_t << 1$, "$\frac{da}{dt}$" $= a_{t+1} - a_t \approx 2\frac{\left(1-a_t^2\right)\sqrt{N-1}}{N}$. If you solve this equation exactly for a_t, given $a_0 = \frac{1}{\sqrt{N}}$, you will obtain that indeed the number of iterations required to get the solution with constant probability is $O(\sqrt{N})$. It is also the case that if you do too many iterations, the amplitude a_t will decrease again. The exact expression(see [1]) is $a_t = sin\left(\frac{(2t+1)\theta}{2}\right)$ where $sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{1}{N}}$.

There is also a geometric interpretation of Grover's algorithm. The state of the system at all times during the algorithm is in the subspace of the Hilbert space spanned by the states $|x_i>$ and $\frac{1}{\sqrt{N-1}}\sum_{j\neq i}|j>$, where i is the index of the solution. Each time the Query/Diffusion operators are applied, the state vector is rotated by the angle θ in this subspace.

2 Optimality of Grover's Algorithm (Bennett-Bernstein-Brassard-Vazirani[2])

This is the "Hybrid" argument from [2]. Let's assume we have some quantum algorithm which consists of a sequence of unitaries and phase queries: $U_1, Q_1, U_2, Q_2, ...Q_T, U_T$. At first we imagine doing a trial run of the algorithm, where the oracle has $x_j = 0 \forall j \in \{1, ..., N\}$. Define

$$\alpha_{i,t} = \text{ Total amplitude with which the algorithm queries } x_i \text{ at step t.} \tag{2}$$

So if the state of the system at time t is $\sum_{i,z}\alpha_{i,z,t}|i,z>$ (z is an additional register) then $\alpha_{i,t} = \sqrt{\sum_z |\alpha_{i,z,t}|^2}$. Then define the query magnitude of i to be:

$$m_i = \sum_{t=1}^{T} |\alpha_{i,t}|^2 \tag{3}$$

$$= \text{"Query magnitude of i"} \tag{4}$$

We have that $\sum_{i=1}^{N} m_i = \sum_{i=1}^{N} \sum_{t=1}^{T} \sum_z |\alpha_{i,z,t}|^2 = \sum_{t=1}^{T} 1 = T$. This means that there must exist a $\tilde{i} \in \{1, ..., N\}$ such that $m_{\tilde{i}} \leq \frac{T}{N}$. So:

$$\sum_{t=1}^{T} |\alpha_{\tilde{i},t}|^2 \leq \frac{T}{N} \tag{5}$$

$$\Rightarrow \sum_{t=1}^{T} |\alpha_{\tilde{i},t}| \leq \sqrt{\sum_{t=1}^{T} |\alpha_{i,t}|^2} \sqrt{T} \quad \text{(Cauchy-Schwarz inequality)} \tag{6}$$

$$\leq \frac{T}{\sqrt{N}} \quad \text{(From 2 lines above)} \tag{7}$$

Now suppose that we modify the first oracle so that item $\tilde{i}$ is marked when it is first used in the algorithm (at t=1), but then use an oracle with no marked item for the rest of the queries throughout the algorithm. Then the state at time t=1 is modified by replacing $\alpha_{i,z,1} \rightarrow -\alpha_{i,z,1}$. We can think of this modified state as the old state (in the case the oracle had no marked item) plus an error term. The state after the rest of the algorithm after the first step still only differs by a small error term.

If we then change the oracles used so that $x_{\tilde{i}} = 1$ at $t = 1, 2$ but $x_i = 0$ for $t = 3, 4, ...T$, we also obtain another error term which adds to the one above. We can then continue this process until the oracle has $x_{\tilde{i}} = 1$ for all $t \in \{1, ..., T\}$. The total amount by which the amplitude in state $\tilde{i}$ of the final state of the algorithm can change during this process (changing from no marked item to one marked item for all t) is $\frac{cT}{\sqrt{N}}$ where c is a constant. So assuming that the probability of detecting a marked item is zero when there is no marked item, it cannot be greater than $\frac{cT^2}{N}$ when there is a marked item.

If $N = 2^n$ then any quantum algorithm requires $\Omega\left(2^{\frac{n}{2}}\right)$ queries to find the marked item with constant probability.

2.1 Oracle Separation $NP^A \not\subseteq BQP^A$

This result implies that there is an oracle A for which $NP^A \not\subseteq BQP^A$. The oracle A computes a boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$. Then any quantum algorithm requires $\Omega\left(2^{\frac{n}{2}}\right)$ queries to determine if there exists a value x for which $f(x) = 1$. Standard diagonalisation techniques can be used to make this rigorous.

3 Query Complexity

Definition 1 *Given a boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$, define the quantum query complexity Q(f) to be the minimum number of queries required by a quantum computer to compute f with error probability $\leq \frac{1}{3}$ on all inputs.*

What we know about query complexity so far:

$$Q(OR_n) = O(\sqrt{n}) \quad \text{[Grover]} \tag{8}$$
$$Q(OR_n) = \Omega(\sqrt{n}) \quad \text{[BBBV]} \tag{9}$$
$$Q(PARITY) \leq \frac{n}{2} \quad \text{[Deutsch-Josza]} \tag{10}$$
$$Q(PARITY) = \Omega(\sqrt{n}) \quad \text{[BBBV]} \tag{11}$$
$$\tag{12}$$

In fact, $Q(PARITY) \geq \frac{n}{2}$, which we will see next time using the polynomial method.

References

[1] *Quantum computation and quantum information*. Cambridge University Press, New York, NY, USA, 2000.

[2] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing, 1997.

6.845 Quantum Complexity Theory
Fall 2010