18.405J/6.841J Advanced Complexity Theory March 22, 2001

Lecture 13

Lecturer: Dan Spielman *Scribe: Abhinav Kumar*

Grover's Algorithm

Search in $O(\sqrt{N})$ time. Let H be the Hadamard matrix

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

Also, let us consider the matrix corresponding to the gate NOT,

$$Q_{NOT_2} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

We shall use the matrices H and NOT to get a unitary transformation that flips the sign of one bit, namely $U = H \cdot NOT \cdot H$.

$$U = \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \cdot \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \cdot \begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

Using this machinery, we can construct a gate Q'_A for an oracle A, which takes $|x > to - |x >$ if $x \in A$, and leaves $|x >$ unchanged otherwise (note this is a unitary transformation, since it is unitary on the orthogonal basis vectors, and takes them to orthogonal vectors).

So if $A = 01$, $Q'_A|01 >= -|01 >$. Suppose we apply this transform to a uniform linear combination of states

$$|x_0 >= \frac{1}{2}(|00 > +|01 > +|10 > +|11 >)$$

We get out

$$\frac{1}{2}(|00 > -|01 > +|10 > +|11 >)$$

Now suppose to the result we apply a Hadamard transform to each bit, then apply the matrix

$$\text{R} = \begin{bmatrix}1 & & & \\ & -1 & & \\ & & -1 & \\ & & & -1\end{bmatrix} \text{(reflection about mean)}$$

to it, and again the Hadamard transform to it. We get out just $|01 >$!

The Hadamard transform acts as a Fourier transform. The general algorithm is based on these lines, the idea is to iterate, applying these two gates (the diffusion transform and Q'_A), when we have more than 2 inputs.

$$RQ'_ARQ'_A...|x_0 > (\frac{4}{\pi}\sqrt{2^n} \text{ times})$$

the dominant term will be the word we want to select. This takes time $O(\sqrt{N})$ since $N \approx 2^n$.