Lecture 13

In which we prove a lower bound for quantum search algorithms via the polynomial method.

We want to show that a quantum algorithm that, given a function $f : \{0,1\}^n \to \{0,1\}$, finds a solution x such that $f(x) = 1$ if one exists, must have running time at least $\Omega(\sqrt{2^n})$, provided that access to the function $f()$ is only given to the algorithm via a unitary transformation U_f over $n+1$ qubits such that $U_f|x,b\rangle = |x\rangle|b \oplus f(x)\rangle$. In the last lecture we considered the case in which f is "given" via a unitary transformation U_f such that $U_f|x\rangle = (-1)^{f(x)}|x\rangle$. The result that we prove today is only stronger, because from a unitary transformation U_f like the one we consider today we can derive a unitary transformation like the one considered in the last lecture as

$$U_f \cdot \left(I_n \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right) U_f$$

Theorem 1 (Main) *Let A be a quantum algorithm that given in input $|0 \cdots 0\rangle$, performs unitary operations independent of f and applies U_f to its first $n+1$ qubits a total of at most T times, and, at the end, outputs 1 with probability $\geq 90\%$ if there is an x such that $f(x) = 1$ and outputs 0 with probability $\geq 90\%$ if for all x we have $f(x) = 0$.*

Then $T \geq \Omega(\sqrt{2^n})$.

Again, this is somewhat stronger than we proved in the last lecture, in which we required the algorithm to output an x such that $f(x) = 1$ with probability $\geq 90\%$if such an x exists. Indeed, such an algorithm can be easily converted to an algorithm that satisfies the assumptions of the theorem.

The main theorem is proved in the following way.

Lemma 2 *Suppose that we have a quantum algorithm as in the assumption of the Main Theorem.*

Then there is an N-variate real polynomial $p(x_1, \ldots, x_N)$, $N = 2^n$, of degree $2T$ such that $0 \leq p(0, \cdots, 0) \leq .1$ and for all $(b_1, \ldots, b_N) \in \{0,1\}^N - \{(0, \cdots, 0\}$ we have $.9 \leq p(b_1, \ldots, b_N) \leq 1$.

Lemma 3 *Let $p(x_1, \ldots, x_N)$ be a real polynomial such that $0 \leq p(0, \cdots, 0) \leq .1$ and for all $(b_1, \ldots, b_N) \in \{0,1\}^N - \{(0, \cdots, 0\}$ we have $.9 \leq p(b_1, \ldots, b_N) \leq 1$.*
Then the degree of p is $\geq \Omega(\sqrt{N})$.

1 Proof of Lemma 2

We first prove the following fact.

Lemma 4 *If a quantum algorithm starts in the state $|0 \cdots 0\rangle$ and alternates applications of unitary transformations independent of f and applications of U_f, then, after t applications of f, each amplitude of the state of the algorithm is a polynomial of degree t in the values $f(x)$.*

This is proved by induction on t. When $t = 0$, the amplitudes are constant independent of f, that is, polynomials of degree 0 in the values of $f()$. For the inductive step, if $|a\rangle$ is a quantum state

$$|a\rangle = \sum_{x,b,w} a_{x,b,w} |x, b, w\rangle$$

and each amplitude $a_{x,b,w}$ is a polynomial of degree t in the values of $f()$, then the amplitude of x, b, w in $U_f|a\rangle$ is

$$(1 - f(x)) \cdot a_{x,b,w} + f(x) \cdot a_{x,1-b,w}$$

which is a polynomial of degree $t + 1$ in the values of f.

Now, let S be the set of final accepting states of the algorithm, and let a_z be the amplitude of each possible final state z. Then each a_z is a polynomial of degree at most T in the values $f(x)$, and the probability that the algorithm accepts is

$$p(f(x_1), \ldots, (x_{2^n})) = \left| \sum_{z \in S} a_z \right|^2$$

where $p()$ is a polynomial of degree at most $2T$, and $x_1, \ldots, x_{2^n}$ is an enumeration of the elements of $\{0,1\}^n$. Note that, for every real-valued input, p has a real value, so p is a polynomial with real coefficients, and that p satisfies all the properties of the conclusion of Lemma 2.

2 Proof of Lemma 3

First we prove the following fact.

Lemma 5 *Let p be a polynomial of degree d as in the assumptions of Lemma 3. Then there is a univariate polynomial q of degree at most d such that $0 \leq q(0) \leq .1$ and for each $i \in \{1, \ldots, N\}$ we have $.9 \leq q(i) \leq 1$.*

PROOF: First of all, we can assume without loss of generality that p is a multilinear polynomial, that is, every variable appears with degree at most one in each monomial. This is because the properties that we assume about p are about inputs in $\{0,1\}^n$, and if we replace every occurrence of x_i^k with $k \geq 2$ by x_i, we do not change the value of p on such inputs. Define now the *symmetrization* of p as

$$\overline{p}(x_1, \ldots, x_N) = \frac{1}{N!} \sum_{\pi} p(x_{\pi(1)}, \ldots, x_{\pi(N)})$$

This is still a multilinear polynomial of degree at most d, and we have that $0 \leq \overline{p}(0, \ldots, 0) \leq .1$ and for all $(b_1, \ldots, b_N) \in \{0,1\}^N - \{(0, \ldots, 0)\}$, $.9 \leq \overline{p}(b_1, \ldots, b_N) \leq 1$. Furthermore, $\overline{p}$ is a constant plues a linear combination of symmetric polynomials of degree at most d, where the symmetric polynomial of degree $k \geq 1$ is

$$s_k(x_1, \ldots, x_N) := \sum_{S \subseteq \{1, \ldots, N\}, |S|=k} \prod_{i \in S} x_i$$

the sum of all degree k multilinear monomial. (Notice that each monomial of degree k of p becomes a multiple of s_k in $\overline{p}$.)

The next observation is that

Claim 6 *For each $k \geq 1$, there is a univariate polynomial q_k of degree k such that for all boolean inputs $(b_1, \ldots, b_N) \in \{0,1\}^n$ we have $s_k(b_1, \ldots, b_N) = q_k(b_1 + \cdots b_n)$.*

This can be proved by induction on k: the base case $k = 1$ is trivial. Assuming we have the statement up to $k - 1$, consider the expansion of $(x_1 + \cdots + x_n)^k$ and then repeatedly apply the equation $x^2 = x$ to the expansion: we get a polynomial that is equal to s_k plus a linear combination of the symmetric polynomials $s_1, \ldots, s_{k-1}$. Each of the latter polynomials can be written (for inputs in $\{0,1\}^n$) as a polynomial of degree $\leq k - 1$ in $(\sum_i x_i)$, and so overall we have written s_k as a polynomial of degree $\leq k$ in $(\sum_i x_i)$.

This means that we can find a univariate polynomial q of degree d such that for every $(b_1, \ldots, b_N) \in \{0,1\}^N$ we have

$$q\left(\sum_i b_i\right) = \overline{p}(b_1, \ldots, b_N)$$

and q satisfies the conclusions of the lemma. $\square$

We then derive Lemma 3 by applying the following fact to the univariate polynomial q of the previous lemma.

Lemma 7 *Let q be a univariate real polynomial of degree d such that for every integer $i \in \{0, \ldots, N\}$ we have $b_1 \leq q(i) \leq b_2$, and let $c := \sup_{x \in [0,N]} |q'(x)|$, where q' is the derivative of q. Then*

$$d \geq \sqrt{\frac{Nc}{b_2 - b_1 + c}}$$

Because the polynomial q of Lemma 5 is such that $0 \leq q(i) \leq 1$ for all $i \in \{0, \ldots, N\}$, and since $q(0) \leq .1$ and $q(1) \geq .9$ it must be that $q'(x) \geq .8$ for some $x \in [0, 1]$, and so $d \geq \Omega(\sqrt{N})$.

It remains to prove Lemma 7

3 Proof of Lemma 7

We use the following result of Markov, that we state without proof.

Theorem 8 *Let q be a univariate polynomial of degree d such that $\forall x \in [a_1, a_2]$ we have $b_1 \leq q(x) \leq b_2$. Then, for all $x \in [a_1, a_2]$,*

$$|q'(x)| \leq d^2 \cdot \frac{b_2 - b_1}{a_2 - a_1}$$

Now let us consider a univariate polynomial q as in the assumptions of Lemma 7. Then for each $x \in [0, N]$ we have

$$b_1 - \frac{c}{2} \leq q(x) \leq b_2 + \frac{c}{2}$$

Because the value of q at a point z in the interval $[i, i + 1/2]$ for $i = 0, \ldots, N - 1$ is

$$q(z) = q(i) + \int_i^x q'(x)dx \geq q(i) - c \cdot (x - i) \geq b_1 - \frac{c}{2}$$

$$q(z) = q(i) + \int_i^x q'(x)dx \leq q(i) + c \cdot (x - i) \leq b_2 + \frac{c}{2}$$

and applying Markov's theorem we have

$$c \leq d^2 \cdot \frac{b_2 - b_1 + c}{N}$$