Quantum Computing Exercises, October 20, 2000

A short summary of Monday's lecture: we can use degrees of polynomials to obtain strong lower bounds on the number of queries that quantum algorithms need. These lower bounds are significant, since virtually all existing quantum algorithm work in this query-setting (Deutsch-Jozsa, Bernstein-Vazirani, Simon, Grover, even Shor's period-finding). An N-variate multilinear polynomial p is something of the form $p(X) = \sum_S a_S \prod_{i\in S} x_i$, where $X = (x_1, \ldots, x_N) \in \{0,1\}^N$, the set S runs over all sets of variables, and the coefficients a_S are complex numbers. The term $a_S \prod_{i\in S} x_i$ is called a *monomial*. The *degree* of the monomial is the size of S. The degree of p is the largest degree among its monomials. Let $f : \{0,1\}^N \to \{0,1\}$ be a total Boolean function. There is a unique multilinear polynomial p which *represents* f (i.e. $f(X) = p(X)$ for all $X \in \{0,1\}^N$) and there are many p which *approximate* f ($|f(X) - p(X)| \leq 1/3$ for all $X \in \{0,1\}^N$). We use $deg(f)$ for the degree of the representing polynomial for f, and $\widetilde{deg}(f)$ for the minimal degree among all approximating polynomials for f. For example $p(x_1, x_2) = x_1 + x_2 - 2x_1x_2$ represents f = PARITY on 2 variables, so $deg(f) = 2$. The following lemma was proven in class:

Lemma 1 *Consider a T-query quantum algorithm. The amplitudes $\alpha_k(X)$ in its final superposition*

$$\sum_k \alpha_k(X)|k\rangle,$$

can be written as N-variate multilinear polynomials of degree $\leq T$. Therefore the acceptance probability

$$p(X) = \sum_{k \text{ ends with } 1} |\alpha_k(X)|^2$$

is an N-variate multilinear polynomial of degree $\leq 2T$.

Let $D(f), Q_E(f), Q_2(f)$ be the number of queries needed to compute f for classical deterministic, exact quantum, and bounded-error quantum algorithms, respectively. Note that the acceptance probability of a T-query exact quantum algorithm for f equals f on all inputs X. Since this probability is a multivariate polynomial $p(X)$ of degree $\leq 2T$, we have $Q_E(f) \geq deg(f)/2$. Similarly, the acceptance probability of a T-query *bounded-error* algorithm for f is an *approximating* polynomial for f of degree $\leq 2T$, hence $Q_2(f) \geq \widetilde{deg}(f)/2$. With a lot more work, we can also show $D(f) \leq O(\widetilde{deg}(f)^6)$, which implies $D(f) \leq O(Q_2(f)^6)$. This means that for all *total* functions, a bounded-error quantum algorithm can be at most polynomially more efficient (in terms of number of queries) than a deterministic classical algorithm. Notice that this is not the case for *promise* functions like the problems of Deutsch-Jozsa, Simon, or Shor, where quantum algorithms can be exponentially more efficient than classical algorithms.

Exercises:

1. Give the representing polynomial for OR on 2 variables.
2. Give two different degree-1 approximating polynomials for OR on 2 variables.
3. Show that AND and OR have the same degrees (exact as well as approximate) for every N.
4. Construct the symmetrized version $p^{sym}(x_1, x_2, x_3)$ of the following approximating polynomial for OR:
$$p(x_1, x_2, x_3) = x_1 + x_2 + \frac{4}{3}x_3 - \frac{2}{3}x_1x_2 - x_2x_3 - x_1x_3.$$
Construct a single-variate polynomial q such that $q(|X|) = p^{sym}(X)$.
5. Prove that $Q_E(AND) = N$.
Hint: prove that there is a basis state $|k\rangle$ (where k ends with a 1) in the final superposition whose amplitude $\alpha_k(X)$ is non-zero iff $X = (1, \ldots, 1)$. Such a polynomial must have degree N.