6.845 Problem Set 4: Quantum Lower Bounds and More

1. Let \( f \) be the \( \log_2 N \)-level AND/OR tree. Show that \( Q(f) = \Omega(\sqrt{N}) \). [Hint: Show that you can reduce a PARITY problem of size \( \sqrt{N} \) to \( f \).]

2. Suppose \( f : \{0,1\}^N \rightarrow \{0,1\} \) is a symmetric Boolean function: that is, it has the form \( f(x_1, \ldots, x_N) = f(k) \) where \( k = x_1 + \cdots + x_N \) is the Hamming weight of \( x \). Suppose also that \( f(k^*) \neq f(k^* + 1) \) for some Hamming weight \( k^* \). Using Ambainis’s quantum adversary theorem, show that \( Q(f) = \Omega\left(\sqrt{(N-k^*)(k^* + 1)}\right) \).

3. Consider the following graph connectivity problem: given an undirected graph \( G = (V, E) \) with \( |V| = N \), which is specified by an \( N \times N \) adjacency matrix, decide whether or not \( G \) is connected.
   
   (a) Show that any classical algorithm for this problem (even a randomized one) requires \( \Omega(N^2) \) queries to the adjacency matrix entries.
   
   (b) Give a quantum algorithm that solves the problem with bounded error using \( O(N^{3/2} \log N) \) queries. [Hint: Use Grover’s algorithm as a subroutine.]
   
   (c) Show that any quantum algorithm requires \( \Omega(N^{3/2}) \) queries. [For this problem, you can assume Ambainis’s quantum adversary theorem. Partial credit for proving a weaker lower bound of \( \Omega(N) \).]

4. A Boolean function \( f : \{0,1\}^N \rightarrow \{0,1\} \) is called monotone if \( f(x_1, \ldots, x_N) \leq f(y_1, \ldots, y_N) \) whenever \( x_i \leq y_i \) for all \( i \).
   
   (a) Show that if \( f \) is monotone, then \( C(f) = bs(f) \).
   
   (b) Conclude that \( D(f) = O(Q(f)^4) \) for all monotone \( f \).

5. Given a Boolean function \( f : \{0,1\}^N \rightarrow \{0,1\} \), let \( R_0(f) \) denote the zero-error randomized query complexity of \( f \): that is, the minimum expected number of queries made by any randomized algorithm that computes \( f(x) \) with probability 1 for every input \( x \) (maximized over \( x \)). Also, recall that \( R(f) \) denotes the bounded-error randomized query complexity of \( f \): that is, the minimum expected number of queries made by any randomized algorithm that computes \( f(x) \) with probability at least 2/3 for every input \( x \) (maximized over \( x \)). In this problem, you will prove the best-known analogues of the \( D(f) = O\left(Q(f)^6\right) \) theorem for \( D(f) \) versus \( R_0(f) \) and \( D(f) \) versus \( R(f) \).
   
   (a) Show that \( R_0(f) \geq C(f) \) for all Boolean functions \( f \). Combining with the \( D(f) \leq C(f)^2 \) theorem, conclude that \( D(f) \leq R_0(f)^2 \).
   
   (b) Show that \( D(f) \leq C(f) \cdot bs(f) \) for all Boolean functions \( f \). [Hint: Consider the algorithm from class used to show \( D(f) \leq C(f)^2 \). Show that this algorithm terminates not merely after \( C(f) \) iterations, but after \( bs(f) \) iterations.]
(c) Show that \( R(f) = \Omega (bs(f)) \) for all Boolean functions \( f \). Combining with part b., conclude that \( D(f) = O \left( R(f)^2 \right) \) for all \( f \).

6. The swap test is an amazing procedure that takes as input two quantum states \( |\psi\rangle \) and \( |\varphi\rangle \), and determines whether they are close or far. To apply it, we first place a control qubit in the state \( \frac{|0\rangle + |1\rangle}{\sqrt{2}} \). Next, conditioned on the control qubit being \( |1\rangle \), we swap \( |\psi\rangle \) and \( |\varphi\rangle \). This produces the state

\[
\frac{|0\rangle |\psi\rangle |\varphi\rangle + |1\rangle |\varphi\rangle |\psi\rangle}{\sqrt{2}}
\]

Finally, we apply a Hadamard gate to the control qubit, measure the control qubit in the standard basis, and accept if and only if we get the outcome \( |0\rangle \).

(a) Show that swap test accepts with probability equal to \( \frac{1 + |\langle \psi | \varphi \rangle|^2}{2} \) —so in particular, if \( |\psi\rangle = |\varphi\rangle \) then the test accepts with probability 1, while if \( |\psi\rangle \) and \( |\varphi\rangle \) are orthogonal then the test accepts with probability 1/2. [Hint: You may find the identities \( \|a\rangle + |b\rangle\|^2 = \langle a | + \langle b |) (|a\rangle + |b\rangle) = \langle a |a\rangle + \langle b |b\rangle + \langle a |b\rangle + \langle b |a\rangle \) and \( \langle a | \otimes |b\rangle \) \langle c | \otimes |d\rangle = \langle a |c\rangle \langle b |d\rangle \) to be helpful.]

(b) Prove that there is no analogue of the swap test with classical probability distributions in place of quantum states.

7. In this problem, we’ll consider a system of \( k \) identical fermions in \( n \geq k \) modes. Suppose the initial state of this system is \( |1, \ldots, k\rangle \): that is, the first \( k \) modes are occupied by a single fermion each, while the remaining \( n-k \) modes are unoccupied. Also, suppose we apply an \( n \times n \) unitary transformation \( U = (u_{i,j}) \) to the modes. Then you saw from Alex’s lecture that the new state of the \( k \) fermions will be

\[
\sum_{1 \leq i_1 \leq \cdots \leq i_k \leq n} \det \left( \begin{array}{ccc} u_{1,i_1} & \cdots & u_{1,i_k} \\ \vdots & \ddots & \vdots \\ u_{k,i_1} & \cdots & u_{k,i_k} \end{array} \right) |i_1, \ldots, i_k\rangle.
\]

Using the above formula, explain why we will never see two or more of the \( k \) fermions “colliding” (i.e., occupying the same mode). (Physicists know this fact as the Pauli exclusion principle.)

8. In quantum communication complexity, suppose we require Alice and Bob to send pure states rather than mixed states at every time step. Show that this increases the communication complexity by at most a factor of 2.

9. Recall that the equality function, \( EQ(x, y) \) for Boolean strings \( x, y \in \{0, 1\}^N \), evaluates to 1 if \( x = y \) and to 0 otherwise. Show that \( Q(EQ) \), the bounded-error quantum communication complexity of the equality function, is \( \Theta (\log N) \). [Hint: For the lower bound, use a counting argument.]