Quantum Computing, Final exam

December 14, 2000
13:30–16:30

Those who want their grade for the mid-term exam to determine half of their total grade, should answer questions 4–9. All others are to make questions 1–7. You are allowed to answer in English or Dutch.

1. Consider the 2-qubit operation $(H \otimes H)\mathrm{CNOT}(H \otimes H)$.
   (a) Give the 4×4 unitary matrix corresponding to this operation.
   (b) Draw the simplest circuit for this operation.
2. Use Shor's algorithm to find the period of the function $f(a) = 7^a \bmod 10$ (using a Fourier transform over $q = 128$ elements). Write down all intermediate superpositions of the algorithm.
3. Suppose we have a database with N slots, containing t ones and $N - t$ zeroes.
   (a) Show that we can use Grover's algorithm to find the positions of all t ones, using an expected number of $O(t\sqrt{N})$ queries to the database.
   (b) Show that this can be improved to an expected number of $O(\sqrt{tN})$ queries.
4. The majority-function $MAJ : \{0,1\}^N \to \{0,1\}$ is defined as $MAJ(X) = 1$ if the number of ones in X is strictly greater than $N/2$, and $MAJ(X) = 0$ otherwise.
   (a) Prove that $deg(MAJ) \geq N/2$.
   (b) What does this imply for the query complexity $Q_E(MAJ)$ of exact quantum algorithms that compute majority?
5. Suppose Alice and Bob have the following 2-qubit state:
$$\frac{1}{\sqrt{2}}|0\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + \frac{1}{\sqrt{2}}|1\rangle \otimes (\alpha|1\rangle - \beta|0\rangle).$$
   Alice has the first qubit, Bob has the second (α and β are real numbers with $\alpha^2 + \beta^2 = 1$).
   (a) Compute the density matrix of the 2-qubit system.
   (b) Compute the reduced density matrix of Bob's 1-qubit system.
   (c) What are the probabilities of seeing $|0\rangle$ and $|1\rangle$ when Bob measures his state in the computational basis?

6. Consider *one-round* quantum communication complexity. Alice gets input $x \in \{0,1\}^n$, Bob gets input $y \in \{0,1\}^n$, and they want to compute some Boolean function $f(x,y)$ of their inputs. Assume that all rows of the communication matrix are different, i.e. for all x and x' there is a y such that $f(x,y) \neq f(x',y)$. They are allowed only one round of communication: Alice sends a quantum message to Bob and Bob must then be able to give the right answer with probability 1. Prove that Alice needs to send n qubits to Bob for this.
Hint: Use the fact that 2 non-orthogonal states cannot be distinguished perfectly (Nielsen & Chuang, p.87), and that a set of 2^n vectors that are pairwise orthogonal must have dimension 2^n.

7. Shor's 9-qubit code allows to *correct* a bit flip and/or a phase flip on one of its 9 qubits. Below we give a 4-qubit code which allows to *detect* a bit flip and/or a phase flip. By this we mean that after the detection procedure we either have the original uncorrupted state back, or we know that an error occurred (though we do not know which one). The logical 0 and 1 are encoded as:

$$|0\rangle_L = \tfrac{1}{2}(|00\rangle + |11\rangle) \otimes (|00\rangle + |11\rangle)$$
$$|1\rangle_L = \tfrac{1}{2}(|00\rangle - |11\rangle) \otimes (|00\rangle - |11\rangle)$$

   (a) Show which measurements we can do to detect a bit flip error.
   (b) Show which measurements we can do to detect a phase flip error.
   (c) Does that mean that we can now detect any 1-qubit error? Explain your answer.

8. Consider the *sorting* problem: there are N numbers $a_1, \ldots, a_N$ and we want to sort these. We can only access the numbers by making *comparisons*. A comparison is similar to a block-box query: it takes 2 indices i, j as input and outputs whether $a_i < a_j$ or not. The output of a sorting algorithm should be the list of N indices, sorted in increasing order. It is known that for classical computers, $N\log(N) + O(N)$ comparisons are necessary and sufficient for sorting. Prove that a quantum algorithm needs at least $\Omega(N)$ comparisons for sorting.
Hint: show how you can use sorting to solve the majority-problem and then use the lower bound for majority from Question 4 to get a lower bound on sorting.

9. Teleportation transfers an arbitrary unknown qubit from Alice to Bob, using 1 EPR-pair and 2 classical bits of communication from Alice to Bob. Prove that these 2 bits of communication are necessary (i.e. you cannot teleport an arbitrary unknown qubit using 1 EPR-pair and only 1 classical bit of communication.)
Hint: Use the fact that 1 classical bit of communication can only send 1 bit of information, no matter how much entanglement Alice and Bob share. Combine this fact with superdense coding.