PhD Comprehensive examination in Quantum Computation
Department of C&O
University of Waterloo

Examiners: Andris Ambainis and Ashwin Nayak
Spring term, July 3, 2007

Instructions

Answer any **five** out of the following six questions. Each question carries 10 marks. Partial anwsers get appropriate credit. You may be able to answer parts of a question assuming the earlier parts, or independent of them.

Question 1. Quantum circuits and universality.

1. [2 marks] Explain what it means for a set of unitary operators over two qubits (i.e., in $\mathrm{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$) to be universal.
2. [5 marks] A *two-level* unitary operator on n qubits is a unitary operator whose restriction to the space spanned by all but two classical basis states is the identity. Show how we can implement any given two-level unitary operator by a quantum circuit consisting of CNOT and single qubit gates, possibly using up to $\mathrm{O}(n)$ ancillary qubits.

   (You may assume that every single qubit unitary operator can be decomposed as $A\mathrm{X}B\mathrm{X}C$, up to an overall phase, where A, B, C are single qubit unitary operators such that $ABC = \mathrm{I}$, and X is the NOT operator.)
3. [3 marks] Explain how any unitary matrix in $\mathrm{L}(\mathbb{C}^3)$ can be decomposed into a product of two-level unitary matrices.

Question 2. Quantum lower bounds.

Consider a quantum query algorithm that has access to a black box that performs the transformation $|i, j, z\rangle \rightarrow |i, j \oplus x_i, z\rangle$, for $i \in \{1, \ldots, N\}$, $j \in \{0, 1\}$, and z arbitrary. Besides queries to the black box, the algorithm is allowed to perform arbitrary unitary transformations that do not depend on $x_1, \ldots, x_N$.

1. [3 marks] Prove that after the algorithm has performed t queries its state can be written as $|\psi\rangle = \sum_{i,j,z} \alpha_{i,j,z}(x_1, \ldots, x_N)|i, j, z\rangle$, with $\alpha_{i,j,z}(x_1, \ldots, x_N)$ being polynomials in $x_1, \ldots, x_N$ of degree at most t.
2. [5 marks] Show that any *exact* quantum algorithm that computes $\mathrm{OR}(x_1, \ldots, x_N)$ (i.e., a quantum algorithm for which the answer obtained by measuring its final state is always equal to $\mathrm{OR}(x_1, \ldots, x_N)$) uses at least N queries. (*Note:* do not confuse N with $\Omega(N)$.)
3. [2 marks] Consider a following generalization of the query model to functions with multivalued variables $x_1, \ldots, x_N \in \{1, \ldots, M\}$. We represent the basis states as $|i, j, k\rangle$ with $i \in \{1, \ldots, N\}$, $j \in \{1, \ldots, M\}$ and k being arbitrary. In one query, the black box performs the transformation $|i, j, k\rangle \rightarrow |i, (j + x_i) \bmod M, k\rangle$. Prove that, after t queries, the algorithm's state can be written as $|\psi\rangle = \sum_{i,j,k} \alpha_{i,j,k}(y_{11}, \ldots, y_{NM})|i, j, k\rangle$, with $\alpha_{i,j,k}(y_{11}, \ldots, y_{NM})$ being polynomials of degree at most t in variables y_{ij} defined by $y_{ij} = 1$ if $f(i) = j$ and $y_{ij} = 0$ otherwise.

Question 3. Quantum error correction.

A CSS code is a quantum code defined using two classical linear codes $C_2 \subseteq C_1$. Suppose that C_1 and C_2 are classical $[n, k_1]$ and $[n, k_2]$ codes and C_1 and $(C_2)^\perp$ both correct t errors. We can then define a quantum code as follows. Let

$$|x + C_2\rangle = \frac{1}{2^{k_2/2}} \sum_{y \in C_2} |x + y\rangle.$$

We define a CSS code as the subspace spanned by $|x + C_2\rangle$ for all $x \in C_1$.

1. [6 marks] Show that this code can correct up to t bit flip (i.e., X) and t phase flip (i.e., Z) errors.
2. [4 marks] Restrict to the case when $k_1 = k_2 + 1$. Let $|\tilde{0}\rangle = |x + C_2\rangle$ for some $x \in C_2$ and $|\tilde{1}\rangle = |x' + C_2\rangle$ for some $x' \notin C_2$. Consider a $2n$ qubit system, with the first n qubits carrying a superposition of $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$ and the second n qubits carrying another superposition of $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$. We perform a CNOT gate on the first and the $(n+1)^{\text{st}}$ qubit, a CNOT gate on the 2^{nd} and the $(n+2)^{\text{nd}}$ qubit and so on. Prove that this results in a logical CNOT operation, i.e., a CNOT being performed on the encoded subspace spanned by $|\tilde{i}\rangle \otimes |\tilde{j}\rangle$, $i, j \in \{0, 1\}$.

Question 4. Communication complexity.

1. [5 marks] Consider the "tribes function" T_n over n^2 Boolean variables, defined as

   $$T_n(z) \quad = \quad \wedge_{i=1}^{n} \left[\vee_{j=1}^{n} z_{ij} \right],$$

   where $z \in \{0,1\}^{n^2}$.

   Suppose Alice is given a bit-string $x \in \{0,1\}^{n^2}$, and Bob is given another bit-string $y \in \{0,1\}^{n^2}$. Describe a bounded-error quantum communication protocol, with non-trivial communication cost (i.e., cost $o(n^2)$), for computing $T_n(x \wedge y)$, where $x \wedge y$ is the string z of bit-wise AND of the two strings: $z_{ij} = x_{ij} \wedge y_{ij}$. What is the complexity of your protocol?
2. [5 marks] The Equality function $\text{EQ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as

   $$\text{EQ}_n(x, y) \quad = \quad \wedge_{i=1}^{n} (x_i = y_i).$$

   Suppose there is a one-message quantum protocol, with error at most ϵ for determining the equality of two arbitrary n-bit inputs x, y given to Alice and Bob, respectively. If the message has m qubits, show that there exist $2m$-qubit pure states $|\psi_x\rangle$ such that $|\langle \psi_x | \psi_y \rangle| \leq 2\sqrt{\epsilon}$ for all $y \neq x$.

Question 5. Impossibility results in quantum cryptography.

1. [3 marks] A startup company QWave is selling a system for quantum bit commitment. The system works as follows:

(a) To commit a bit a, Alice generates a uniformly random bit $x \in \{0,1\}$, prepares the state

$$|\psi_{ax}\rangle = \begin{cases} |0\rangle & a = x = 0 \\ |1\rangle & a = 0, x = 1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle & a = 1, x = 0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle & a = x = 1 \end{cases}$$

and sends it to Bob. Bob stores the state for future verification.

(b) To reveal, Alice reveals both a and x. Bob verifies that Alice has not cheated by measuring the stored state in a basis consisting of $|\psi_{ax}\rangle$ and the orthogonal state. He accepts if the result is $|\psi_{ax}\rangle$.

Describe an attack that makes this system insecure.

2. [7 marks] Oblivious transfer is a cryptographic primitive with two parties, *sender* and *receiver*. The sender has with two bits x_0 and x_1 and the receiver has a bit i. The goal is that the receiver learns x_i but *not* x_{1-i}, and the sender gets no information about the value of i. A quantum protocol is *perfectly sender secure* if, for any strategy of the sender, the sender has no information about i at the end of the protocol. Prove that in any perfectly sender-secure protocol, there is a strategy for the receiver that allows receiver to learn the values of both x_0 and x_1.

Question 6. Discrete Logarithms.

Consider the multiplicative group $\mathbb{Z}_p^*$, where p is a prime. Let the element g be a generator of the group. In the Discrete Logarithm problem, the input is an element $x = g^k \in \mathbb{Z}_p^*$ (where k is unknown) and the task is to determine $k \pmod{p-1}$.

1. [2 marks] Consider the following superposition over group elements:

$$|\psi_j\rangle \quad = \quad \frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} \omega^{ij} |g^i\rangle, \qquad (1)$$

where ω is a primitive $(p-1)$-th root of unity. Show that this is an eigenvector of the unitary operator defined by

$$U_a : |y\rangle \mapsto |ay\rangle,$$

where $a \in \mathbb{Z}_p^*$. Find the corresponding eigenvalue.

2. [4 marks] Suppose you are given the group element $x = g^k$ (k unknown), $j \in \mathbb{Z}_{p-1}^*$, and the superposition $|\psi_j\rangle$ in Eq. (1) as input. Using part (1) above, show how you can efficiently construct the superposition

$$\frac{1}{\sqrt{p-1}} \sum_{i=0}^{p-2} \omega^{-ik} |i\rangle.$$

3. [2 marks] Assuming that you can perform the quantum Fourier transform over $\mathbb{Z}_{p-1}$ efficiently, describe how you may construct the state $|\psi_j\rangle$ (in Eq. (1)) above efficiently, for *some* $j \in \mathbb{Z}_{p-1}^*$.

4. [2 marks] Describe an efficient quantum algorithm based on the above to compute Discrete Logarithms. State its time and space complexity in terms of the the complexity of the quantum Fourier transform over $\mathbb{Z}_{p-1}$.