PhD Comprehensive examination in Quantum Computation

Department of C&O
University of Waterloo

Examiners: Michele Mosca and Ashwin Nayak
Spring term, June 7, 2005

Instructions

Answer any **five** out of the following seven questions. They are each worth 10 marks.

Questions

1. **Quantum cryptography: Impossibility of Bit Commitment**

   Bit-commitment is a cryptographic protocol between two parties Alice, and Bob. The input to the protocol is a bit $a \in \{0,1\}$ which is held by Alice, and is not known to Bob. The protocol consists of two phases: the *commitment* phase, and the *reveal* phase, each possibly consisting of multiple rounds. At the end of the commitment phase, Bob has a state that depends upon a. In the reveal phase, Alice sends Bob a bit b, and engages in a protocol to convince him that she had earlier committed to the bit b.

   In ideal bit commitment, we require that the protocol satisfy two properties:

   - (**sealing**) Bob should not be able to get any information about the bit a during the commitment phase.
   - (**binding**) During the reveal phase, Alice should not be able to convince Bob (with non-zero probability) that she committed to a value b different from a, the one she had initially.

   (a) Formalize the sealing and the binding requirements in terms of quantum protocols.

   (b) Prove that we cannot achieve the two requirements above simultaneously, even for quantum protocols.

   In other words, show that ideal quantum bit commitment is impossible.

2. **Universality: one qubit gates**

   Let R_θ denote rotation of a single qubit by angle θ, and P_α denote the phase shift gate:

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \qquad P_\alpha = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

   (a) Show that (up to global phase) any one-qubit (unitary) gate can be decomposed into the form $P_\beta R_\theta P_\alpha$ for some real values α, β, θ.

   (b) Give a finite set of one-qubit gates that generate a dense subset of $SU(2)$ and prove that it does so.

3. **Lower bounds: Polynomial method**

Let $X = X_1X_2 \ldots X_N$ denote an N-bit binary string, $N = 2^n$. Consider a quantum oracle O_X that maps

$$|j\rangle|b\rangle \rightarrow |j\rangle|b \oplus X_j\rangle$$

where $j \in \{1, 2, \ldots, N\}$ and $b \in \{0, 1\}$.

Consider a quantum circuit on $n + 1 + d$ qubits, all initialized to $|0\rangle$, that uses O_X a total of T times.

(a) Prove that the final amplitude of any basis state is a multi-linear polynomial of degree at most T in the variables $X_1, X_2, \ldots, X_N$.

(b) Prove that the probability of measuring the first qubit and obtaining a 1 is a real multilinear polynomial of degree at most $2T$ in the variables $X_1, X_2, \ldots, X_N$.

(c) Find a multilinear polynomial that represents the PARITY function, where

$$\text{PARITY}(X_1, X_2, \ldots, X_N) \quad = \quad X_1 \oplus X_2 \oplus \cdots \oplus X_N.$$

(Hint: Note that $(-1)^{X_j} = 1 - 2X_j$ for $X_j \in \{0, 1\}$, so it suffices to find an expression in terms of $(-1)^{X_j}$.)

(d) Let F be a function mapping $\{0, 1\}^N$ to $\{0, 1\}$. What lower bound do parts (a) and (b) of this question imply for the query complexity of computing $F(X_1, X_2, \ldots, X_N)$?

(e) Prove a tight lower bound for the query complexity of $PARITY(X_1, X_2, \ldots, X_N)$. Prove the tightness by finding an algorithm that achieves the lower bound.

4. **Quantum complexity theory:** $\text{BQP} \subseteq \text{P}^{\#\text{P}}$

#P is the complexity class of non-negative integer valued function on $\{0, 1\}^*$ corresponding to languages in the class NP. A function $f : \{0, 1\}^* \mapsto \mathbb{Z}$ is said to be in #P if there is a polynomial time non-deterministic Turing machine M such that for every x, $f(x)$ equals the number of accepting paths in the computation of M on input x.

The goal of this question will be to show that $\text{BQP} \subseteq \text{P}^{\#\text{P}}$. You may follow the steps below, or give an alternative proof. For the steps below, descriptions will suffice; no formal proofs are required.

(a) Explain why we may assume that all the gates in a quantum circuit are *real* unitary (i.e., orthogonal linear transformations).

(b) Explain why we may assume that there is exactly *one* accepting computational basis state in a BQP computation.

(c) Show that we may approximate the transition amplitudes in all the gates by fractions of the form $a/2^T$, where T is polynomial in the size of the circuit, such that the acceptance probability of the resulting circuit changes by $o(1)$.

(d) Note that with the above modifications, the acceptance probability of a BQP computation may be approximated as $(a - b)^2/2^{2T}$. Using these simplifications, show that $\text{BQP} \subseteq \text{P}^{\#\text{P}}$.

5. **Quantum error correction : Sufficient conditions**

An *error* in a single qubit is an unknown completely positive trace preserving map on that qubit. (This is equivalent to a unitary operator on that qubit together with some number of fresh qubits initialised to $|0\rangle$.)

(a) Prove that for single qubit quantum error correction to be possible, it suffices to be able to detect and correct a unitary set of errors such as $\{I, \sigma_x, \sigma_y, \sigma_z\}$. Generalize this property to multiple-qubits errors.

(b) Describe sufficient conditions for a discrete set of single qubit errors (such as the Pauli errors given in part (a)) acting on a subspace $\mathcal{C}$ of $\mathbb{C}^{2^n}$ to be correctible.

(c) In CSS coding, a further property of Pauli errors is used: the duality of bit and phase errors. What is this duality? How is this duality reflected in the CSS construction? (You need only describe the properties of CSS coding that result from the said duality. A definition of CSS codes is not required.)

6. **Quantum searching and communication complexity**

With the same notation as in Question 3 above, assume that exactly one of the N bits X_i is 1.

(a) Describe an $O(\sqrt{N})$ query quantum algorithm for the search problem. I.e., given the oracle O_X, your algorithm should invoke the oracle at most $O(\sqrt{N})$ times, and should locate, with probability at least $2/3$, an $i \in \{1, 2, \ldots, N\}$ such that $X_i = 1$.

(b) Analyze the algorithm you described in part (a).

(c) Suppose that two parties, Alice and Bob, are given an N-bit string each (U, V, respectively). Describe a quantum communication protocol between them, with sublinear communication, for computing the Set Disjointness function: $\mathrm{DISJ}(U, V) = \bigvee_{i=1}^{N}(U_i \wedge V_i)$. What is the communication complexity of your protocol?

7. **Quantum algorithms : Eigenvalue Estimation and Order Finding**

Let N be a large integer, and let $a \in \{2, 3, \ldots, N-2\}$ be relatively prime to N. Consider the unitary operator U_a that maps $|x\rangle$ to $|ax\rangle$, where ax is defined as multiplication modulo N.

(a) Decompose $|1\rangle$ as a superposition of eigenvectors of U_a. Describe explicitly the eigenvectors used.

(b) Suppose you are given one eigenvector $|\Psi\rangle$ of U_a. Give an algorithm to approximate its eigenvalue with n bits of precision with high probability. I.e., your algorithm should output a value that will, with high probability, be within $\frac{1}{2^n}$ of the corresponding eigenvalue.

(c) Explain how to efficiently (probabilistically) find the order of a modulo N. (You may cite results about continued fractions without giving details of the continued fractions algorithm).