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

Examiners: Ashwin Nayak and Jon Yard
Spring term, June 18, 2018
1–4 pm

Instructions

Answer any **five** out of the following seven questions. Each question carries 10 marks. Partial answers get appropriate credit.

You may be able to answer parts of a question independently of the previous parts, or by assuming them.

The questions vary in how long they may take to answer, in novelty as well as difficulty. They are ordered according to topic. You may find it useful to pick out your favorite three or four questions as a first pass.

Please clearly label which parts of your writing constitute the answer to each question. Rough work that you do not consider to be part of your answer can be put in clearly labelled boxes (rather than being crossed out or erased). At the end of the exam, if you have attempted more than five questions, please indicate on the first page of the answer booklet which five should be graded. However, you should turn in all your work.

Question 1. Measurements.

Let $\mathrm{L}(\mathcal{H})$ denote the space of linear operators on the finite dimensional Hilbert space $\mathcal{H}$. The trace norm of an operator $M \in \mathrm{L}(\mathcal{H})$ is defined as $\|M\|_{\mathrm{tr}} = \mathrm{Tr}(\sqrt{M^\dagger M})$.

1. [5 marks] Prove that $\|M\|_{\mathrm{tr}} = \max_U |\mathrm{Tr}(UM)|$, where $U \in \mathrm{L}(\mathcal{H})$ ranges over all unitary operators on $\mathcal{H}$.
2. [5 marks] Let $\rho, \sigma \in \mathrm{L}(\mathcal{H})$ be quantum states and let $A_1, \ldots, A_m \in L(\mathcal{H})$ be a POVM. Show that the ℓ_1 distance between the corresponding probability distributions $P_i = \mathrm{Tr}\rho A_i$ and $Q_i = \mathrm{Tr}\sigma A_i$ is bounded by $\|\rho - \sigma\|_{\mathrm{tr}}$.

Question 2. Phase estimation.

Suppose there is a family of quantum circuits $C(j, U)$, that implement the controlled-U^j operation, where U is a unitary operation on m qubits. Let $|\phi\rangle$ be an eigenvector of U with eigenvalue $\exp(2\pi i\theta)$, $\theta \in [0, 1)$.

1. [3 marks] You are given a single copy of the state $|\phi\rangle$ as input. Describe an efficient quantum algorithm that computes an n-bit approximation to θ, with probability at least $3/4$, using the circuits $C(\cdot, \cdot)$ as subroutines.
2. [2 marks] What is the complexity of your algorithm in terms of the number of single and two-qubit gates, and the number of calls to $C(\cdot, \cdot)$?
3. [5 marks] Prove the correctness of your algorithm.

Question 3. Lower bound for quantum search.

For a function $f : \{1, 2, \ldots, n\} \to \{0, 1\}$, the search problem consists of determining if there is an index $i \in \{1, 2, \ldots, n\}$ such that $f(i) = 1$. Prove that every quantum algorithm with oracle (or black-box) access to the function f that solves the search problem with bounded error makes $\Omega(\sqrt{n}\,)$ queries to the oracle. What is the implication of this lower bound for quantum algorithms for NP-complete problems?

Question 4. 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 5. Quantum adder Consider a binary adder $A_n|x\rangle = |x + 1 \bmod 2^n\rangle$, where $|x\rangle = |x_1\rangle \cdots |x_n\rangle$ and $x_1 x_2 \cdots x_n$ is the representation of the integer $x \in \{0, \ldots, 2^n - 1\}$ in binary. In what follows, you will implement A_n using single-qubit unitaries and (possibly multiply) controlled single-qubit unitaries.

1. [1 mark] Give a quantum circuit for A_2 over the above gate set.
2. [2 marks] Give a quantum circuit for A_3 over the above gate set.
3. [3 marks] Give a recursive description of a quantum circuit for A_n.
4. [4 marks] For which n is A_n in the n-qubit Clifford group? Justify your answer.

Question 6. Quantum communication

1. [5 marks] State, in terms of resource conversion, what teleportation and superdense coding achieve.
2. [5 marks] Suppose Alice and Bob try to perform quantum teleportation using a noisy entangled state, obtained by passing Bob's qubit through a depolarizing channel $\mathcal{N}_p(\rho) = (1 - p)\rho + pI/2$. If Alice tries to teleport a state $|\psi\rangle$, the state of the qubit held by Bob at the end of the protocol will be described by a density matrix ρ that depends on $|\psi\rangle$. Give an expression for this density matrix and also for the fidelity $F(|\psi\rangle, \rho) = \langle\psi|\, \rho |\psi\rangle$.

Question 7. Impossibility of quantum bit commitment Consider a bipartite quantum state $|\psi\rangle = \sum_{j,k=1}^{d} \alpha_{jk}|j\rangle|k\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$, where $\{|j\rangle\}$ is an orthonormal basis.

1. [2 marks] Show that $|\psi\rangle = \sum_{j=1}^{d} \beta_j |\eta_j\rangle|\mu_j\rangle$ for $\beta_j \geq 0$ and orthonormal bases $\{|\eta_j\rangle\}, \{|\mu_j\rangle\}$ for $\mathbb{C}^d$.
2. [2 marks] Show that if $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ satisfy $\mathrm{Tr}_1 |\psi_1\rangle \langle\psi_1| = \mathrm{Tr}_1 |\psi_2\rangle \langle\psi_2|$, then $|\psi_2\rangle = (U \otimes I)|\psi_1\rangle$ for some $U \in \mathrm{U}(d)$.
3. [4 marks] In a bit commitment protocol, Alice holds an input bit a that is unknown to Bob. The protocol consists of two phases: the commit phase and the reveal phase, each possibly consisting of multiple rounds of communication. After the commit phase, Bob holds a quantum state that may depend on Alice's bit a. In the reveal phase, Alice sends Bob a bit b, and engages in a protocol to convince him that $a = b$. The protocol is said to be *concealing* if Bob has no information about a before the reveal phase, and *binding* if Alice cannot convince Bob to accept $b \neq a$ at the end of the reveal phase. Prove that bit commitment cannot be both perfectly concealing and perfectly binding.
4. [2 marks] What happens if bit commitment is nearly, but not perfectly, concealing?