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

Examiners: Debbie Leung and Michele Mosca
Spring term, June 18, 2012
11:30 am to 2:30 pm (MC 5158)

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. If desired, scratch 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 at the beginning of you exam which five should be graded. However, you should turn in all your work.

Question 1. Ulhmann's Theorem

Given positive semidefinite operators P and Q in $\mathrm{Pos}(\mathcal{X})$, where $\mathcal{X}$ is a complex Euclidean space, we define the fidelity between P and Q as

$$F(P,Q) = \|\sqrt{P}\sqrt{Q}\|_1$$

or equivalently

$$F(P,Q) = \mathrm{Tr}\sqrt{\sqrt{P}Q\sqrt{P}}.$$

Uhlmann's Theorem states that,

$$F(P,Q) = \max\{|\langle u|v\rangle| : |v\rangle \in \mathcal{X}\otimes\mathcal{Y},\, \mathrm{Tr}_{\mathcal{Y}}(|v\rangle\langle v|) = Q\}$$

where $\mathcal{Y}$ is a Euclidean space of dimension same as that of $\mathcal{X}$, and $|u\rangle$ is a unit vector that is a purification of P.

Prove Ulhmann's Theorem, focusing on the case when P and Q are trace 1.

We may use without proof that for all operators A and unitary U, $|\mathrm{Tr}(AU)| \leq \mathrm{Tr}|A|$ and equality is attained by choosing $U = V^\dagger$ where $A = |A|V$ is the polar decomposition of A.

Question 2. Tradeoff in quantum bit commitment

In a bit commitment protocol (BC), Alice has a bit that she wishes to commit to Bob, but she doesn't want Bob to know what it is until she chooses to reveal it.

More formally, the protocol consists of two phases, the commit phase and the reveal phase, each possibly consisting of multiple rounds of communication. At the end of the commit phase, Bob has a state ρ_a that may depend on Alice's initially committed bit a. In the reveal phase, Alice engages Bob in a protocol to convince him that she has committed to a bit b. Bob may accept or reject b (to be what Alice has committed to).

We consider the following class of quantum bit commitment protocols. Alice prepares a pure quantum state $|\psi_a\rangle$ in systems A and B and sends B to Bob to conclude the commit phase. In the open phase, she performs a quantum operation on A that takes it to A' and B' and sends B' to Bob, along with a bit b. Based on b, Bob measures BB' and decides if he accepts or rejects b.

Suppose we requires Bob to accept whenever a=b. We can quantify the security of BC with two parameters:

* BC is said to be ϵ concealing if $F(\rho_0, \rho_1) \geq 1 - \epsilon$,

* BC is said to be δ binding if the probability that Bob accepts b given $b \neq a$ is at most δ,

(a) Prove a tight tradeoff between ϵ and δ, which, in partciular, will imply that they cannot both be 0.

(b) Describe how the BC scheme above can be used to allow Alice and Bob to toss a fair coin c remotely. Suppose Alice wins if $c = 0$ and Bob wins otherwise. Upper bound the bias if Alice is dishonest and Bob is honest, and vice versa.

Question 3. Distance 2 quantum codes

Recall that an $[[n, k, d]]$ quantum error correcting code encodes k qubits in n qubits and has distance d.

(a) Write down the generators for a $[[4, 2, 2]]$ stabilizer code.

(b) Explain why your code is distance 2.

(c) Let $\mathcal{N}(\rho) = (1 - p)\rho + pI/2$ and each qubit in the code is acted on by $\mathcal{N}$. Explain how this code can be used to detect errors, and improve the error rate when no error is detected. Here, the $p \ll 1$ but it is unknown to the experimenter.

(d) Let n be an integer with $n \geq 4$. Does an $[[n, n-2, 2]]$ quantum error correcting code exist? (Hint: the answer can depend on n.) If so, write down the stabilizer (but you need not show correctness of the code). If not, give a brief explanation.

Question 4. Lower bounds on teleportation

(a) State, in terms of resource conversion, what teleportation and superdense coding achieve.

(b) Explain why entanglement cannot increase classical communication capacity of noiseless classical channels.

(c) Assuming the validity of Holevo's bound, show that 2 classical bits (even with unlimited amount of entanglement) is required to transmit one qubit.

Question 5. Algorithms and Complexity

1. Define the class QMA.
2. Give an example of a known QMA-complete problem. (You need to clearly state the problem, but you do not need to prove it is QMA-complete.)
3. Two graphs G_1 and G_2 on the vertices $1, 2, \cdots, n$ are isomorphic, denoted $G_1 \cong G_2$, if there exists a permutation σ of the vertices such that for any two distinct $v, w \in \{1, 2, \cdots, n\}$, the vertices v and w are adjacent in G_1 if and only if $\sigma(v)$ and $\sigma(w)$ are adjacent in G_2.

   Consider the graph isomorphism (GI) problem:

   Input: Description of two simple undirected n-vertex graphs, G_1 and G_2, on the vertices labelled by $1, 2, \cdots, n$

   Output: YES, if $G_1 \cong G_2$, NO otherwise.

   (a) Prove that GI $\in$ QMA.

   (b) (Trying to prove two graphs are not isomorphic)

   The Graph Non-Isomorphism problem has the same input as GI, but one must answer YES if $G_1 \ncong G_2$ and NO otherwise.

   Suppose for a given graph G on n vertices, you are able to construct (up to renormalization) the state

   $$|\psi_G\rangle = \sum_{\pi \in S_n} |\pi(G)\rangle$$

   where S_n denotes the group of permutations of the elements $1, 2, \cdots, n$ and $\pi(G)$ is the n-vertex graph with $\pi(v)$ adjacent to $\pi(w)$ if and only if v and w are adjacent in G (in other words, the graph obtained by relabelling each vertex v of G by $\pi(v)$).

   (i) Explain how given $|\psi_{G_1}\rangle$ and $|\psi_{G_2}\rangle$ one can decide whether $G_1 \ncong G_2$ with bounded probability of correctness.

   (ii) Explain (briefly) why the following incorrect proof that Graph Non-Isomorphism $\in$ QMA fails:

   The prover gives the verifier a quantum state $|\psi\rangle$ which allegedly equals $|\psi_{G_1}\rangle \otimes |\psi_{G_2}\rangle$. The verifier runs your protocol from part (i).

Question 6. Algorithms and Complexity

1. Define the Quantum Fourier Transform (QFT_{2^n}) on n qubits.
2. Draw a circuit for QFT_8 using the Hadamard gate H and controlled rotation gates.
3. Given a black-box that implements

   $$U_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix},$$

   show how to use the QFT (or its inverse) to approximate, with probability at least 1/2 , the value of ϕ with precision in $O(\frac{1}{2^n})$ with $O(2^n)$ uses of the black box U_ϕ.
4. Let $Q = -H^{\otimes n} U_{00\cdots 0} H^{\otimes n} U_f$ be the quantum search iterate, where $f : \{0,1\}^n \to \{0,1\}$, $U_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$, $U_{00\cdots 0} = I - 2|00\cdots 0\rangle\langle 00\cdots 0|$, and $H^{\otimes n}$ is the tensor product of n Hadamard gates.

Let $m = |f^{-1}(1)|$, the number of solutions to $f(x) = 1$. Assume $0 < m < 2^n$ (i.e. the number of solutions to $f(x) = 1$ is non-trivial).

Let $|\psi_0\rangle$ be a normalized uniform superposition of states $|x\rangle$ with $f(x) = 0$, and $|\psi_1\rangle$ be a normalized uniform superposition of states $|x\rangle$ with $f(x) = 1$.

(a) Let θ be the value satisfying $0 < \theta < \pi/2$ and $\sin^2(\theta) = m/2^n$.

Write down a closed-form expression (as a function of θ and k) for α and β in $Q^k H^{\otimes n}|00\cdots 0\rangle = \alpha|\psi_1\rangle + \beta|\psi_0\rangle$.

(b) What are the eigenvalues of Q?

(c) Draw and briefly explain a circuit for estimating an eigenvalue of Q (either one) on the subspace spanned by $|\psi_0\rangle$ and $|\psi_1\rangle$. (you do not need to draw the QFT circuit in detail)

Question 7. Black-Box Complexity

Let $OR(X_1, X_2, \cdots, X_N)$ be the function that equals 0 if $X_1 = X_2 = \cdots = X_N = 0$, and equals 1 otherwise.

1. Express OR as a polynomial in $X_1, X_2, \cdots, X_N$.
2. What is its degree?
3. Prove that a query algorithm that starts with a finite number of qubits initialized to $|0\rangle$, and performs a sequence of unitaries that includes T queries to the black-box $|j\rangle|b\rangle \mapsto |j\rangle|b \oplus X_j\rangle$, will produce a state whose amplitudes have degree at most T in the variables $X_1, X_2, \cdots, X_N$.
4. What non-trivial lower bound does this imply for the exact query complexity of OR?
5. What is the bounded-error query complexity of the OR function? (Just state the answer using big-O notation.)