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

Examiners: Michele Mosca and Ashwin Nayak
Spring term, May 26, 2015
1 pm to 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 novelty as well as in difficulty. They are ordered according to topic. You may find it useful to pick out your favourite three or four questions in the first pass.

If you attempt more than five questions, please indicate which five you wish to have graded.

Question 1. Measurements.

For any operator $X \in \mathrm{L}(\mathcal{H})$, define $\|X\|_{\mathrm{tr}}$ as the sum of the singular values of X.

Part 1.1 Prove that $\|M\|_{\mathrm{tr}} = \max_A |\mathrm{Tr}(AM)|$, where $A \in \mathrm{L}(\mathcal{H})$ ranges over all operators on $\mathrm{L}(\mathcal{H})$ with spectral norm $\|A\| \leq 1$.

Part 1.2 Let $\rho, \sigma \in \mathrm{L}(\mathcal{H})$ be quantum states. Show that there is a measurement such that the ℓ_1 distance between the probability distributions obtained by measuring these states according to the measurement is $\|\rho - \sigma\|_{\mathrm{tr}}$.

Question 2. Algorithms for hidden shifts.

Consider a function f that maps $(b, x) \mapsto f(b, x)$, $b \in \{0, 1\}$, $x \in \{0, 1, 2, \ldots, M-1\}$ for some large integer M, with the property that the values of $f(0, x)$ are all distinct, and $f(1, y) = f(0, x)$ iff $y = x + s \mod M$.

Suppose you are a given a black box for mapping $|b, x\rangle|0\rangle \mapsto |b, x\rangle|f(b, x)\rangle$.

Part 2.1 Show how to create a state of the form

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\frac{ks}{M}}\frac{1}{\sqrt{2}}|1\rangle\right)|k\rangle$$

for a uniform random integer $k \in \{0, 1, \ldots, M-1\}$.

Part 2.2 Suppose we were lucky enough to sample n such states, with values for k equal to $1, 2, \ldots, 2^j, 2^{j+1}$, $\ldots, 2^{n-1}$. Explain how you could obtain an approximation of s/M that with high probability has error at most $1/2^n$.

Part 2.3 In reality, it is extremely unlikely to sample any specific value of k, and it will be helpful to have a procedure that takes states

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\frac{k_1 s}{M}}\frac{1}{\sqrt{2}}|1\rangle\right)|k_1\rangle$$

and

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\frac{k_2 s}{M}}\frac{1}{\sqrt{2}}|1\rangle\right)|k_2\rangle$$

and with probability $\frac{1}{2}$ outputs

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\frac{(k_1-k_2)s}{M}}\frac{1}{\sqrt{2}}|1\rangle\right)|1\rangle$$

and with probability $\frac{1}{2}$ outputs

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \mathrm{e}^{2\pi\mathrm{i}\frac{(k_1+k_2)s}{M}}\frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle.$$

Describe such a procedure.

Question 3. Black Box Complexity.

Let the PARITY function denote the map from $\{0,1\}^N \mapsto \{0,1\}$ that maps $X_1X_2\ldots X_N$ to $X_1 \oplus X_2 \oplus \ldots \oplus X_N$. Assume N is even.

Part 3.1 Find a multi-linear real polynomial $p(X_1, X_2, \ldots, X_N)$ that represents PARITY (i.e., we have $p(X_1, X_2, \ldots, X_N) = \mathrm{PARITY}(X_1, X_2, \ldots, X_N)$ on all $X_1, X_2, \ldots, X_N \in \{0,1\}$).

Part 3.2 What is the degree of p?

Part 3.3 What query lower bound does this imply for any exact quantum algorithm (i.e. an algorithm that outputs the correct answer with certainty) that makes queries to an oracle that maps $|j\rangle|b\rangle \mapsto |j\rangle|b \oplus X_j\rangle$ for $b \in \{0,1\}$ and $j \in \{0, 1, \ldots, N-1\}$?

Part 3.4 Describe a quantum algorithm that meets that lower bound.

Question 4. BQP $\subseteq$ P$^{\#\mathrm{P}}$**.**

#P is the complexity class of non-negative integer valued functions 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 BQP $\subseteq$ P$^{\#\mathrm{P}}$, i.e., a language in BQP may be recognized by a polynomial-time algorithm that has access to a #P oracle.

You may follow the steps below, or give an alternative proof. For the steps below, descriptions will suffice; no formal proofs are required.

Part 4.1 Explain why we may assume that all the gates in a quantum circuit are *real* unitary (i.e., orthogonal linear transformations).

Part 4.2 Explain why we may assume that there is exactly *one* accepting computational basis state in a BQP computation.

Part 4.3 Show that if we approximate the transition amplitudes in the gates in the circuit with rationals of the form $a/2^T$, where T is is a suitable polynomial in the size of the circuit, the resulting approximation of the acceptance probability is within o(1) of the original value.

Part 4.4 Note that with the above modifications, the acceptance probability of a BQP computation may be approximated by a rational of the form $(a-b)^2/2^{2T}$, $a, b \in \mathbb{Z}$. Using these simplifications, show that $\mathrm{BQP} \subseteq \mathrm{P}^{\#\mathrm{P}}$.

Question 5. Quantum cryptography.

Suppose Alice has the means to prepare any one of the four states $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ and send it into a channel controlled by Eve. Eve can send any state she wishes (including the state Alice sent into the quantum channel) to Bob.

Bob can choose to measure in either the computational basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\}$.

Part 5.1 Explain how the standard BB84 quantum key distribution (QKD) protocol would lead to a secret key shared by Alice and Bob, assuming the adversary does not interfere with the communication between Alice and Bob, and no experimental errors occur. (i.e. explain how it works when nothing goes wrong).

Part 5.2 Suppose Bob notices a 25% error rate in the qubits he measures. Suppose he and Alice attempt to establish a secret key in any case. Explain how Eve might know 100% of the key established by Alice and Bob.

Part 5.3 Suppose that in the position degree of freedom, there are two distinguishable position states, $|x\rangle$ and $|y\rangle$, and that Alice's faulty apparatus in fact sends

$$|0\rangle|x\rangle, |1\rangle|y\rangle, \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|y\rangle, \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)|x\rangle \ .$$

Explain how Eve can determine 100% of the key without detection (assuming they follow the usual protocol).

Question 6. Fault tolerant computation.

Let $\mathrm{I}, \mathrm{X}, \mathrm{Y}, \mathrm{Z}$ denote the 1-qubit Pauli operators. Let $C \subset \mathrm{Z}_2^{2n-1}$ be a $[2n-1, n, d]$ classical linear binary error correcting code. (C encodes n bits into $(2n-1)$ bits and has distance d.) Denote the generator matrix for C and $C^\perp$ by G and $G^\perp$ respectively; the row-space of the generator matrix equals the code.

Part 6.1 We would like to construct a quantum CSS code Q based on C by taking both the X- and Z-generators of the stabilizer S of Q to be the rows of $G^\perp$. What are the conditions on C and $C^\perp$ for this construction to be valid? What are the parameters k and d_q for the resulting $[[2n-1, k, d_q]]$ quantum code Q?

Part 6.2 For the above quantum code, explain why the logical operators $\bar{\mathrm{X}}$ and $\bar{\mathrm{Z}}$ on an encoded qubit can be chosen to be $\mathrm{X}^{\otimes 2n-1}, \mathrm{Z}^{\otimes 2n-1}$.

Part 6.3 Recall that a fault tolerant operation acting on several code blocks takes one error in any input code block to at most one error in each output code block. Recall also that the Clifford group is generated by the CNOT, the Hadamard gate and the Phase gate $P = \mathrm{diag}(1, i) = \sqrt{\mathrm{Z}}$. Suppose $C^\perp$ is doubly even (i.e., each element has hamming weight divisible by 4).

Describe how you may implement any Clifford group generator fault tolerantly on encoded qubits.
Hint: The Clifford group is the normalizer of the Pauli group, thus the action of each Clifford element on the quantum code can be determined by its action on the Pauli group.

Question 7. Communication complexity of Inner Product.
The inner product function $\mathrm{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as

$$\mathrm{IP}_n(x,y) \quad = \quad \sum_{i=1}^{n} x_i \cdot y_i \quad (\mathrm{mod}\ 2).$$

Suppose there is a one-message quantum protocol for computing the inner product of two arbitrary n-bit inputs x, y given to Alice and Bob, respectively. Further, suppose that in this protocol Alice sends a pure state $|\phi_x\rangle$ over m qubits (the lone message) to Bob, who can then compute the inner product exactly, i.e., with probability 1.

Part 7.1 Show how Bob can modify his computation so that he can learn Alice's input x from $|\phi_x\rangle$.

Part 7.2 State and justify a non-trivial lower bound for the length m of the message $|\phi_x\rangle$.