PhD Comprehensive examination in Quantum Computation

Department of C&O
University of Waterloo

Examiners: Debbie Leung and Ashwin Nayak
Spring term, June 7, 2006

Instructions

Answer any **five** out of the following six questions. Each question carries 10 marks.

Question 1. 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] 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 2. Lower bounds via polynomials.

Let $X = X_1 X_2 \ldots X_N$ 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 that acts on $n + 1 + d$ qubits, all initialized to $|0\rangle$, that uses O_X a total of T times (i.e., makes T queries).

1. [4 marks] Prove that the amplitude of any basis state in the final state of the qubits is a multi-linear polynomial of degree at most T in the variables $X_1, X_2, \ldots, X_N$.
2. [1 mark] 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 $X_1, X_2, \ldots, X_N$.
3. [1 mark] Let F be a function mapping $\{0, 1\}^N$ to $\{0, 1\}$. What lower bound do parts (1) and (2) of this question imply for the query complexity of computing $F(X_1, X_2, \ldots, X_N)$ **exactly** (i.e., with probability 1)?
4. The OR function, is defined as

   $$\mathrm{OR}(X_1, X_2, \ldots, X_N) \quad = \quad X_1 \vee X_2 \vee \cdots \vee X_N;$$

   it is equal to 1 iff at least one of its N boolean inputs is 1.

   [2 marks] Find a multilinear polynomial that represents the OR function, i.e., equals the OR function on all points in $\{0, 1\}^N$.

5. [2 marks] Prove a linear lower bound for the query complexity of computing $\mathrm{OR}(X_1, X_2, \ldots, X_N)$ with probability 1.

Question 3. BB84 and provably insecure error rates

Suppose Alice and Bob can communicate over a quantum channel. The quantum channel is noiseless in the absence of eavesdropping, a condition that cannot be guaranteed. They can also communicate over a classical channel which may be tapped, but not disturbed.

1. [3 marks] Describe the standard BB84 scheme (sans error-correction and privacy amplification). Clearly explain the test for eavesdropping.
2. [5 marks] Define an observable "error rate" e for your test for eavesdropping. State a numerical value e_{thres} such that if $e \geq e_{\text{thres}}$ then Alice and Bob cannot establish any secure key. Explain why.
3. [2 marks] The key rate is the number of bits of raw key generated per qubit sent. Suppose that Alice and Bob both use the computational basis with probability $1 - \epsilon$, in order to achieve a key rate close to 1. Could ϵ be chosen to be 10^{-3} while still guaranteeing qualitatively the same security as in the BB84 scheme? How small may ϵ be for a non-trivial level of security?

Question 4. Communication complexity.

1. Suppose Alice is given a bit-string $x \in \{0,1\}^n$, unknown to Bob. Consider a one-message quantum protocol in which Alice encodes x into a (possibly mixed) quantum state ρ_x over m qubits, and sends this to Bob. Suppose that Bob can measure the received state ρ_x and determine x with probability 1.
   [5 marks] Prove from first principles that $m \geq n$, i.e., Alice necessarily sends at least n qubits to Bob.
2. The set intersection function $\mathrm{SI}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as

$$\mathrm{SI}_n(x, y) \quad = \quad \bigvee_{i=1}^{n} (x_i \wedge y_i).$$

   Suppose there is a one-message quantum protocol for computing the set intersection of two arbitrary n-bit inputs x, y given to Alice and Bob, respectively. Further, suppose that in this protocol Alice sends a quantum state ρ_x over m qubits (the lone message) to Bob, who can then compute the function exactly, i.e., with probability 1.
   [5 marks] Explain how Bob can modify his computation so that he can learn Alice's input x from ρ_x. What non-trivial lower bound for m does this imply?

Question 5. CSS codes and Fault Tolerant Clifford group operations

Let I, X, Y, Z denote the 1-qubit Pauli operators. Let $C \subset Z_2^{2n-1}$ 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.

1. [3 marks] 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?
2. [1 marks] For the above quantum code, explain why the logical operators $\bar{X}$ and $\bar{Z}$ on an encoded qubit can be chosen to be $X^{\otimes 2n-1}, Z^{\otimes 2n-1}$.
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 $P = \mathrm{diag}(1, i) = \sqrt{Z}$. Suppose $C^{\perp}$ is doubly even (i.e. each element has hamming weight divisible by 4).

   [6 marks] 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 6. Quantum circuits and universality.

Let I, X, Y, Z denote the 1-qubit Pauli operators. Let S_1 denote the set of all 1-qubit gates.

1. [3 marks] Explain why S_1, together with $e^{-i\frac{\pi}{4}Z\otimes Z}$ (on any chosen pair of qubits) is universal. (You can quote known universal sets of gates from the text book.)
2. [3 marks] By using the Taylor series expansion of $e^{-iZ\otimes Zt}$, and the fact $XX = I$ and the anticommutivity of X and Z, show that $\forall t$, $(I \otimes X)\, e^{-iZ\otimes Zt}\, (I \otimes X) = e^{+iZ\otimes Zt}$.
3. [4 marks + 2 extra points] For 3 qubits, let $G = Z \otimes Z \otimes I + I \otimes Z \otimes Z + Z \otimes I \otimes Z$. Given the set of gates $S = \{e^{-iGt}\}_t \cup S_1$ show how to apply CZ for any selected pair of qubits. (Thus the set of gates S is universal.)