PhD Comprehensive examination in Quantum Computation

Department of C&O
University of Waterloo

Examiners: Andrew Childs and Debbie Leung
Spring term, June 15, 2009
9 am to 12 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. 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. Universality of Hadamard and $\pi/8$ gates

The *Hadamard gate* is the one-qubit gate H acting as $|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, and the $\pi/8$ gate is the one-qubit gate T acting as $|0\rangle \mapsto |0\rangle$, $|1\rangle \mapsto e^{i\pi/4}|1\rangle$.

If we use the gate V to approximate the gate U, the error in the approximation is defined as $\max_{|\psi\rangle} \|(U - V)|\psi\rangle\|$ (where $\|\cdot\|$ denotes the Euclidean length, i.e., the 2-norm, of a vector).

Let $\hat{n} = (n_x, n_y, n_z)$ be a real unit vector. Let $R_{\hat{n}}(\theta) := \cos(\theta/2)I - i\sin(\theta/2)(n_x X + n_y Y + n_z Z)$, where I, X, Y, Z are qubit Pauli matrices. We call $R_{\hat{n}}(\theta)$ a rotation by angle θ about the axis $\hat{n}$.

(a) [2 marks] Show how to perform some rotation by an angle that is an irrational multiple of π. You can use the fact that the solution τ to the equation $\cos(\tau\pi) = \cos^2(\pi/8)$ is irrational.

(b) [6 marks] Use the H and T gates to approximate some rotation by a given angle α about any axis of your choice, with error at most ϵ. Describe the method, verify that the error is at most ϵ in the worst case, and derive the required number of uses of H and T in terms of ϵ.

(c) [2 marks] Show how to use the H and the T gates to approximate an arbitrary rotation with error at most ϵ. Again, provide bounds on the number of uses of H and T. You can use the fact that any rotation can be expressed as $R_{\hat{n}}(\theta_1)R_{\hat{m}}(\theta_2)R_{\hat{n}}(\theta_3)$ for some real $\theta_{1,2,3}$ if $\hat{m}$, $\hat{n}$ are not parallel.

Question 2. Quantum sampling

Suppose you are given a quantum black box specifying a probability distribution as follows: on input $j \in \{1, \ldots, n\}$, the black box computes $p_j \in [0, 1]$, where $\sum_{j=1}^n p_j = 1$. You would like to prepare the quantum state $|p\rangle := \sum_{j=1}^n \sqrt{p_j}|j\rangle$.

(a) [6 marks] Show that $|p\rangle$ can be prepared using $O(\sqrt{n})$ quantum queries. (Hint: You could begin by explaining how to prepare the state $\frac{1}{\sqrt{n}}\sum_{j=1}^{n}(\sqrt{p_j}|j\rangle \otimes |0\rangle + \sqrt{1-p_j}|j\rangle \otimes |1\rangle)$ using only two queries.)

(b) [4 marks] Explain why $\Omega(\sqrt{n})$ queries are necessary to prepare $|p\rangle$ in general. (You may refer to any well-known quantum lower bound in your explanation.)

Question 3. Counting stabilizer codes

(a) [3 marks] Suppose we have a stabilizer S on n qubits with r generators. Ignoring overall phase, how many Pauli operators are there that commute with every element in S but are not in S? (In other words, what is the size of $N(S)\backslash S$?)

(b) [2 marks] Suppose we want an *ordered* sequence $M_1, \cdots, M_r$ of *independent* commuting Pauli operators. How many ways are there to do this (again ignoring overall phase)?

(c) [2 marks] Suppose we have a stabilizer S on n qubits with r generators. How many ways are there to pick an ordered set of generators $M_1, \cdots, M_r$?

(d) [3 marks] Using parts (b) and (c), give a closed-form expression for the number of stabilizer codes on n qubits with r generators. (Hint: One mark of this part will be given for correct handling of the overall phases.)

Question 4. Impossibility of quantum bit commitment

Consider a bipartite quantum state $|\psi\rangle = \sum_{jk=1}^{n} \alpha_{jk}|j\rangle|k\rangle$ in $\mathbb{C}^n \otimes \mathbb{C}^n$, where $\{|x\rangle\}_{x=1,\ldots,n}$ is an orthonormal basis for $\mathbb{C}^n$.

(a) [2 marks] Show that $|\psi\rangle = \sum_{j}^{n} \beta_j|\eta_j\rangle|\mu_j\rangle$ for some nonnegative real numbers β_j and orthonormal bases $\{|\eta_x\rangle\}_{x=1,\ldots,n}$ and $\{|\mu_x\rangle\}_{x=1,\ldots,n}$ in $\mathbb{C}^n$.

(b) [2 marks] Show that if $|\psi_1\rangle$, $|\psi_2\rangle$ in $\mathbb{C}^n \otimes \mathbb{C}^n$ satisfy $\mathrm{Tr}_1|\psi_1\rangle\langle\psi_1| = \mathrm{Tr}_1|\psi_2\rangle\langle\psi_2|$, then $|\psi_1\rangle = U \otimes I|\psi_2\rangle$ for some unitary U.

(c) [5 marks] In a bit commitment protocol (BC), Alice holds an input bit a which 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. At the end of the commit phase, Bob has a state that may depend on a. In the reveal phase, Alice sends Bob a bit b, and engages in a protocol to convince him that $a = b$. BC 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 BC cannot be both perfectly concealing and perfectly binding.

(d) [1 mark] What happens if BC is nearly, but not perfectly, concealing?

Question 5. BPP vs. BQP

(a) [2 marks] Define the complexity classes BPP and BQP.

(b) [4 marks] Prove that BPP $\subseteq$ BQP.

(c) [4 marks] Give an oracle relative to which BPP $\neq$ BQP.

Question 6. From query complexity to communication complexity

(a) [7 marks] Suppose there is a t-query quantum algorithm for computing the function $f : \{0,1\}^n \to \{0,1\}$. Now suppose that Alice has an input $x \in \{0,1\}^n$ and Bob has an input $y \in \{0,1\}^n$. They wish to compute a function $g : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ obtained by first performing some binary operation $h : \{0,1\} \times \{0,1\} \to \{0,1\}$ to their inputs x and y bitwise, producing an n-bit string whose ith bit is $h(x_i, y_i)$, and then applying f to that string. Show that they can compute f by exchanging $O(t \log n)$ qubits.

(b) [3 marks] Suppose Alice and Bob each have a calendar with n possible time slots, and they would like to find a time slot when they are both free for a meeting. Using the result of part (a), give an upper bound on the number of qubits they must exchange.

Question 7. Communication through an erasure channel

Consider the *erasure channel* that transmits one qubit (spanned by $|0\rangle$, $|1\rangle$) from a sender, Alice, to a receiver, Bob. Bob receives the qubit state perfectly with probability $1 - e$, and receives an erasure symbol $|2\rangle$ orthogonal to $|0\rangle$ and $|1\rangle$ with probability $e < 0.5$.

Suppose Alice wants to send one qubit to Bob, and she has access to 5 uses of the erasure channel. They have the ability to perfectly apply arbitrary local operations. What is the maximum probability for successful transmission of the qubit in each of the following two scenarios?

(a) [5 marks] No additional resources are available.

(b) [5 marks] Before and after the 5 uses of the erasure channel, Alice can send an unlimited amount of classical data to Bob for free and vice versa.

In each case, describe in detail the method for achieving the maximum probability (proof of the correctness of the method is not needed) and explain briefly why the probability of success cannot be higher.