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

Examiners: Debbie Leung and Ashwin Nayak
Spring term, June 19, 2017
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. 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 any rotation of your choice by some angle that is an irrational multiple of π. You can use the property that the solution τ to the equation $\cos(\tau\pi) = \cos^2(\pi/8)$ is irrational.

(b) [5 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. Specify the rotation clearly, 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) [3 marks] Show how to use the H and the T gates to approximate any given rotation with error at most ϵ. Again, provide bounds on the number of uses of H and T. You can use (without proof) 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 algorithm for counting.

Suppose you are given a black-box function $f : X \to \{0, 1\}$, where X is a finite set, and you would like to estimate the value of $M = |\{x \in X : f(x) = 1\}|$.

(a) [4 marks] Define unitary operators

$$U = 1 - 2 \sum_{x:\, f(x)=1} |x\rangle\langle x| \qquad\qquad V = 1 - 2|X\rangle\langle X|$$

where $|X\rangle = \sum_{x \in X} |x\rangle / \sqrt{|X|}$. Compute the eigenvalues and eigenvectors of VU.

(b) [6 marks] Explain how phase estimation can be used to approximate M. Discuss the tradeoff between the quality of the approximation and the number of queries to f.

Question 3. Impossibility results in quantum cryptography.

(a) [3 marks] A startup company QWave is selling a system for quantum bit commitment. The system works as follows:

1. To commit a bit a, Alice generates a uniformly random bit $x \in \{0, 1\}$, prepares the state

$$|\psi_{ax}\rangle = \begin{cases} |0\rangle & a = x = 0 \\ |1\rangle & a = 0, x = 1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle & a = 1, x = 0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle & a = x = 1 \end{cases}$$

and sends it to Bob. Bob stores the state for future verification.

2. To reveal, Alice reveals both a and x. Bob verifies that Alice has not cheated by measuring the stored state in a basis consisting of $|\psi_{ax}\rangle$ and the orthogonal state. He accepts if the result is $|\psi_{ax}\rangle$.

Describe an attack that makes this system insecure.

(b) [7 marks] Oblivious transfer is a cryptographic primitive with two parties, *sender* and *receiver*. The sender has two bits x_0 and x_1 and the receiver has a bit i. The pair then communicate back and forth according to an arbitrary protocol, with the goal that the receiver learns x_i but *not* x_{1-i}, and the sender gets no information about the value of i. A quantum protocol is *perfectly sender secure* if, for any strategy of the sender (i.e. local operations different from the protocol), the sender has no information about i at the end of the protocol. Prove that in any perfectly sender-secure protocol in which the receiver learns the bit x_i with probability 1, there is a strategy for the receiver that allows receiver to learn the values of *both* x_0 and x_1 with probability 1.

Question 4. Polynomial method.

Let $[d]$ denote the set $\{0, 1, \ldots, d-1\}$. Suppose we are given a function $f : [n] \to [m]$ as a black-box that performs the transformation $|i, j, k\rangle \to |i, (j + f(i)) \bmod m, k\rangle$, where $i \in [n], j \in [m]$ and k is arbitrary.

(a) [5 marks] We may encode any function f as above by an nm-bit string x such that $x_{ij} = 1$ iff $f(i) = j$. Prove that the probability of acceptance of a t-query quantum algorithm with access to the black-box f is a multivariate polynomial of degree at most $2t$ in the variables (x_{ij}).

(b) [5 marks] Suppose f is a k-to-1 function, for some k that divides n: for each $j \in [m]$, we have $\left|f^{-1}(j)\right| \in \{0, k\}$. In other words, for each element in the image of f, there are precisely k pre-images.

Suppose we have a t-query quantum algorithm that computes some property of k. (An example of such a property is whether k is even or odd.) Prove that the acceptance probability of the algorithm, averaged over all k-to-1 functions, is a polynomial in k of degree at most $2t$.

Question 5. Theory of quantum error correction

(a) [7 marks] Consider a quantum error correcting code $\mathcal{C}$ which is a subspace of the ambient space $\mathcal{H}$. Let P be the projector onto $\mathcal{C}$, $\mathcal{E}(\rho) = \sum_i E_i \rho E_i^\dagger$ be a quantum operation taking states from $\mathcal{H}$ to some output space $\mathcal{K}$ which may or may not be the same as $\mathcal{H}$. Show that $\mathcal{E}$ is correctible (i.e., $\exists \mathcal{R}$ s.t. $\forall \rho \; \mathcal{R} \circ \mathcal{E}(\rho) = \rho$) if and only if

$$P E_i^\dagger E_j P = \alpha_{ij} P$$

where α_{ij} are entries of a positive semidefinite matrix α.

(b) [3 marks] Suppose C is a t-error correcting code with block length n. Using the notation in part (a), $\mathcal{H} = \mathcal{S}^{\otimes n}$ for some $\mathcal{S}$, and correctible quantum operations are those $\mathcal{E}$ with E_i's acting nontrivially on up to t systems. Show that erasures of up to $2t$ systems are correctible. (An erasure error on $\mathcal{S}$ replaces the state on $\mathcal{S}$ by an error symbol orthogonal to it.)

Question 6. Teleportation in the stabilizer formalism

(a) [2 marks] Alice is given an unknown qubit $|\psi\rangle$ in system C. Alice and Bob share $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ holding systems A and B respectively. Describe the steps and provide a short proof how $|\psi\rangle$ can be teleported from Alice to Bob in the usual pure state formalism.

(b) [2 marks] Treat the state on CAB before and after teleportation as two possible ways to encode the unknown qubit into two respective stabilizer codes $\mathcal{C}_1$ and $\mathcal{C}_2$. Write down the stabilizer generators and the logical X and Z operators for $\mathcal{C}_1$ (before teleportation). Justifications are not required.

(c) [6 marks] Show in detail how the stabilizer evolves in each step of teleportation, and derive the final stabilizer generators and the logical X and Z operators for $\mathcal{C}_2$ (after teleportation). You may use any result (without derivation) about the stabilizer formalism if it is directly from the syllabus; please state the result before use and an approximate location of the source.

Question 7. Two-way quantum communication using a swap gate

Consider the swap gate U acting on 2 qubits as $U|ij\rangle = |ji\rangle$. Consider the scenario when Alice holds the first input and output qubit and Bob holds the second input and output qubit. (You should think of the swap gate as a channel with two inputs and two outputs, and both of Alice and Bob are senders and receivers.) Suppose Alice and Bob can apply the swap gate n times for large n, and have unlimited local storage space and free local operations between each use of U. They want to maximize the number of classical bits sent to one another. We first consider the scenario when entanglement is free, and then a second scenario when no entanglement is free. In each scenario, we want to find out the maximum communication rate from Alice to

Bob, and then the trade-off as Bob also wants to maximize the communicate rate to Alice simultaneously. Throughout, you can assume that the three resources forward classical communication (from Alice to Bob), backward classical communication (from Bob to Alice) and entanglement are incomparable, in that having an unlimited supply of any two resources cannot increase the third resource.

(a) [2 marks] Suppose entanglement is free. Show that Alice cannot send more than $2n$ bits to Bob (even if Alice and Bob cooperate and maximize only forward communication).

(b) [1 mark] Suppose entanglement is free. Show that the above upper bound to the forward communication rate is achievable.

(c) [1 mark] Suppose entanglement is free. Show that Alice can send $2n$ bits to Bob and Bob can send $2n$ bits to Alice using n swap gates.

(d) [2 marks] Suppose there is no free entanglement. Show that Alice and Bob can create $2n$ EPR pairs using the swap gate n times but no more.

(e) [2 marks] Suppose there is no free entanglement. Explain how Alice can send "almost" $2n$ bits to Bob. (That is, show that the asymptotic rate is 2 bit per swap gate.)

(f) [2 marks] Suppose there is no free entanglement. What is the best total number of bits sent in the two directions combined?