33-658, 758 Quantum Computation and Information Spring Semester, 2014
Assignment No. 10. NOT TO BE TURNED IN

ANNOUNCEMENT. There will be an hour exam on Tuesday afternoon, April 1, beginning at 3:00 pm (usual class hour). It is closed book, closed notes, no pocket calculators. Bring a pen or pencil. There will *not* be quantum information seminar that afternoon.

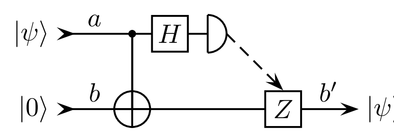
The exam will cover material up to and including the lecture on Thursday, March 20, and assignments 1 through 9, with emphasis on topics not covered in the first hour exam: dense coding, teleportation, computational complexity, quantum algorithms (Deutsch-Jozsa, Shor, Grover), quantum channels (Kraus operators). The following more recent topics will *not* be on the exam: POVMs, error correction, quantum codes.

READING:
GSGC = "Graph States and Graph Codes" on course web page
QCQI = Nielsen and Chuang, Quantum Computation and Quantum Information
QEC = "Quantum Error Correction" on course web page

Quantum error correction: QCQI Secs. 10.1, 10.2, 10.3; QEC; E. Knill, R. Laflamme, "Theory of quantum error-correcting codes," Phys. Rev. A 55 (1997) 900; arXiv:quant-ph/9604034
Graph States and Codes: GSGC

PRACTICE EXERCISES, some from previous hour exams, not be be turned in.

1. The circuit carries out one-bit teleportation from the input a to the output b', which is the b qubit at a later time.



a) Explain why the Z type of information (the difference between $|0\rangle$ and $|1\rangle$) at the input will arrive at the output even if the classical bit (dashed line) is omitted. Your explanation need not be long, but should show that you understand what the circuit is doing.

b) Show by using the unitary time development of $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, that the measurement outcome, equivalently the classical bit, contains no information about the input state $|\psi\rangle$.

c) What type of information about the input state $|\psi\rangle$ might be obtained if the measurement on qubit a were carried out in some basis other than the standard basis of $|0\rangle$ and $|1\rangle$? You need only consider X, Y and Z types. Can you relate this to the Exclusion theorem?

Exclusion theorem: Let a, b, and c be three systems and let $\mathcal{V} = \{|v_j\rangle\}$, $\mathcal{W} = \{|w_k\rangle\}$ be two mutually-unbiased orthonormal bases of $\mathcal{H}_a$, i.e., for all j and k $|\langle v_j|w_k\rangle| = 1/\sqrt{d_a}$, where d_a is the dimension of $\mathcal{H}_a$. Then if the $\mathcal{V}$ information about a is perfectly present in b, the $\mathcal{W}$ information about a is completely absent from c.

2. In Shor's factoring algorithm the first modular exponentiation step results in a state

$$|\Psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \otimes |f(x)\rangle,$$

where $f(x)$ is a periodic function with (smallest) period r, and $f(x) = f(x')$ if and only if $x' - x$ is a multiple of r. Next a quantum Fourier transform Q is applied to the argument (x) register and a measurement is carried out.

a) Use quantum principles to show that the probability of a measurement outcome $0 \le y \le M-1$ is given by

$$\Pr(y) = \sum_{x=0}^{r-1} |\langle y|Q|\psi_x\rangle|^2,$$

where

$$\sqrt{M}|\psi_x\rangle = |x\rangle + |x+r\rangle + \cdots |x + (q_x - 1)r\rangle.$$

Also, what determines the value of q_x in this formula?

b) In the special case where r divides M, i.e., $M = \nu r$ for some integer ν, what values of y have positive probabilities, and what are the probabilities of these different values? (Your probabilities should be properly normalized.)

c) There are periodic functions of (smallest) period r for which one can have $f(x) = f(x')$ in some cases even if $x' - x$ is not a multiple of r. For example $f(x) = \cos(2\pi x/N)$, where N is an integer, has period N, but $f(1) = f(-1)$. What goes wrong with the analysis in (a) for such a function or, equivalently, what would have to be modified? Why is it that for the $f(x)$ in Shor's algorithm we don't have to worry about this possibility?

3. Consider Grover's search algorithm for the case $N = 4$, and suppose there is a single marked item at $t = 1$. The oracle unitary is O: $O|x\rangle = |x\rangle$ for $x = 0, 1, \ldots N-1$, except $O|t\rangle = -|t\rangle$. The unitary which carries out reflection about the average or mean is denoted by $D = 2|\phi_o\rangle\langle\phi_o| - I$. Consistent with the notation in QCQI, let $G = DO$.

a) Find $O|\phi_0\rangle$, and $G|\phi_0\rangle = DO|\phi_0\rangle$, where $|\phi_0\rangle = (1/\sqrt{N})\sum|x\rangle$. How many iterations are required in this case in order to find the marked item?

b) Find two-qubit circuits which give the unitaries O and D, possibly up to a phase, constructed from CNOT and 1 qubit gates. [Hint: See QCQI, and note that a controlled-Z gate for two qubits, one that changes $|11\rangle$ to $-|11\rangle$, is the same as a controlled-not preceded and followed by a Hadamard acting on the target qubit.]

4. a) For the amplitude damping channel whose Kraus operators are given on p. 380 of QCQI, find the superoperator $\mathcal{S}$ as a map of Pauli matrices, i.e., find the S_{jk} matrix such that $\mathcal{S}(\sigma_k) = \sum_j S_{jk}\sigma_j$.

b) Describe the image of the Bloch sphere produced by this map in terms of shrinkage, rotation, and displacement.

c) What is the minimum fidelity of this channel as a function of the parameter γ?