CS 410/510 Introduction to Quantum Computing

Homework 4

Portland State U, Spring 2017 — *May 16, 2017*
Lecturer: Fang Song — *Due: May 30, 2017*

Instructions. Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea. For this problem set, a random subset of problems will be graded. Problems marked with "**[G]**" are required for graduate students. Undergraduate students will get bonus points for solving them. Bonus problems in this homework have extended due date till June 10.

You may collaborate with others on this problem set. However, you must ***write up your own solutions*** and ***list your collaborators*** for each problem.

1. (15 points) (OR gate as a quantum operation) Recall the binary OR operation, denoted as $\vee$, defined as $a \vee b = 0$ if $a = b = 0$ and $a \vee b = 1$ otherwise. Here we consider operations that map the two-qubit state $|a, b\rangle$ to the one-qubit state $|a \vee b\rangle$, for all $a, b \in \{0, 1\}$. Of course, no unitary operation can perform this mapping, since the input and output dimension do not match; however, general quantum operations can compute this mapping.
   (a) Give a sequence of 2×4 matrices $A_1, \ldots, A_k$ with $\sum_{j=1}^{k} A_j^\dagger A_j = I$ that compute the OR operation in the sense that, for all $a, b \in \{0, 1\}$, when $\rho = |a, b\rangle\langle a, b|$, $\sum_{j=1}^{k} A_j \rho A_j \dagger = |a \vee b\rangle\langle a \vee b|$.
   (b) The operation from part (a) maps all basis states to pure states. Does it map all pure input states to pure output states? Either prove it, or provide a counterexample.

2. (Entropy) Let $H(\cdot)$ denote the Shannon entropy and $S(\cdot)$ be the von Neumann entropy. $S(A : B)$ denotes quantum mutual information.
   (a) (Exercise) Let X be a random variable taking values in $\{0, \ldots, 2^{m^2}\}$ with probability distribution $p_x = \begin{cases} 1 - 1/m & \text{if } x = 0 \\ \frac{1}{m 2^{m^2}} & \text{otherwise} \end{cases}$. Calculate $H(X)$? Conclude that $H(X) \to \infty$ as $m \to \infty$, but one sample of X is almost certainly 0.
   (b) (5 points) Let $\rho = p|0\rangle\langle 0| + (1 - p)|+\rangle\langle +|$. Compute $S(\rho)$. How does it compare to the entropy of a biased coin X where HEADS appears with probability p?
   (c) (10 points) Suppose that p_x are probabilities, $|x\rangle$ are orthogonal states for a system A, and ρ_x is any set of density matrices for another system B.

i) Show that $S\left(\sum_x p_x|x\rangle\langle x| \otimes \rho_x\right) = H(p_x) + \sum_x p_x S(\rho_x)$.

ii) Consider ensemble of density matrices $\mathcal{E} := \{p_x, \rho_x\}$. Show that the following two definitions of Holevo's information quantity χ are equivalent.

$$\chi(\mathcal{E}) := S(A:B), \text{ with } \rho_{AB} = \sum_x p_x|x\rangle\langle x| \otimes \rho_x\,;$$

$$\& \quad \chi(\mathcal{E}) := S(\sum_x p_x\rho_x) - \sum_x p_x S(\rho_x)\,.$$

Update: $S(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$ is the quantum mutual information between system A and B.

3. (Quantum error-correcting)

(a) (15 points) Let E be an arbitrary 1-qubit unitary, and I, X, Y, Z are the four 2×2 Pauli matrices.

i) Show that it can be written as $E = \alpha_0 I + \alpha_1 X + \alpha_2 Y + \alpha_3 Z$, for some complex coefficients α_i with $\sum_{i=0}^{3} |\alpha_i|^2 = 1$. (Hint: compute the trace $Tr(E^\dagger E)$ in two ways, and use the fact that $Tr(AB) = 0$ if A and B are distinct Pauli matricies, and $Tr(AB) = Tr(I) = 2$ if A and B are the same Pauli.)

ii) Write the 1-qubit Hadamard transform H as a linear combination of the four Pauli matrices.

iii) Suppose an H-error happens on the first qubit of $\alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$ using the 9-qubit code. Give the various steps in the error-correction procedure that corrects this error.
Note: $|\bar{b}\rangle$ represents a logical qubit, which is the encoded state of $|b\rangle$ under the considered code.

(b) (10 points) Show that there cannot be a quantum code that encodes one logical qubit by $2k$ physical qubits while being able to correct errors on up to k of the qubits. (Hint: No-cloning theorem)

4. (Learning parities) Let $s \in \{0,1\}^n$ be a secret n-bit string. Suppose $f : \{0,1\}^n \to \{0,1\}$ computes the dot product $f(x) = s \cdot x = \sum_{i=1}^{n} s_i x_i \pmod 2$ (i.e., the parity of the bits in s chosen by the non-zero positions of x). In this problem, we will (mainly) consider the query complexity of learning s.

(a) (8 points) How many queries are needed to classically learn s with zero-error (i.e., always outputting the correct answer)? Give an algorithm for this problem, and show that it is optimal.

(b) (7 points) Explain why even if we allow the classical algorithm to fail with some fixed probability (e.g., probability $1/3$), it requires the same asymptotic query complexity as the zero-error case.

(c) (10 points) How many queries are needed by a *quantum* algorithm to learn s with zero-error? Give an algorithm for this problem, and show that it is optimal.

As usual, we assume a quantum oracle O_f: $|x\rangle|y\rangle \mapsto |x\rangle|x \cdot s \pmod 2\rangle$ is given. (Hint: Deutsch-Josza)

(d) (Bonus 10pts) Now consider a *noisy* version $\tilde{f}$ of f: $\tilde{f}(x) = x \cdot s + e_x \pmod 2$ where $e_x \in \{0,1\}$ is a random bit independently drawn for each x, and $b_x = 1$ with probability η. Given oracle access to $\tilde{f}$, how many queries are needed by a quantum algorithm for finding s with probability at least $\Omega((1-2\eta)^2)$?

(e) (Bonus 15pts) Suppose that we no longer have oracle access to f. Instead we are given a sequence of classical samples $(x_i, y_i), i = 1, \ldots, m$, where $x_i \leftarrow \{0,1\}^n$ chosen uniformly at random and $y_i = s \cdot x_i + e_{x_i} \pmod 2$ with independent $e_{x_i} \leftarrow \mathrm{COIN}_\eta$. Let m be a polynomial in n. Give a (quantum or classical) algorithm that runs in time polynomial in n for finding s for constant η (e.g., $\eta = 1/4$).

5. (Testing entanglement) Suppose that Alice and Bob share a two-qubit state, and they want to test if it is the EPR pair $|\phi^+\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with local measurements and classical communication. Consider the following procedure: they randomly select a measurement basis: with probability $1/2$, they both measure in the standard basis $\{|0\rangle, |1\rangle\}$; and, with probability $1/2$, they both measure in the Hadamard (diagonal) basis $\{|+\rangle, |-\rangle\}$. Then they perform the measurement and they accept if and only if their outcomes are the same.

(a) (5 points) Show that the state ϕ^+ is always accepted by this test with zero-error.

(b) (8 points) Show that, for an arbitrary 2-qubit state $|\mu\rangle$, the probability that it passes the test is at most

$$\frac{1 + |\langle \mu | \phi^+ \rangle|^2}{2}.$$

(Hint: decomposing $|\mu\rangle$ under the four Bell states.)

(c) (7 points) Now consider another (malicious) party Eve, who may have intervened with the state that Alice shares with Bob. Let ρ_{ABE} be their joint state. Now assume that Alice and Bob are certain that they two perfectly share $|\phi^+\rangle$, show that Alice and Eve's state cannot be in $|\phi^+\rangle$ as well.

Note: we can actually show that ρ_{ABE} must be of form $|\phi^+\rangle\langle\phi^+|_{AB} \otimes \rho_E$ (i.e., Eve's state is uncorrelated with that of Alice and Bob). This is an example of *monogamy of entanglement*: the more system A is entangled with B, the less A is entangled with another system C.

6. (Bonus: Quantum rewinding.) Let Q be a unitary quantum circuit that takes an m-qubit input state $|\psi\rangle$ and ancilla $|0^k\rangle$, and let the output state be

$$Q|\psi\rangle|0^k\rangle = \sqrt{p(\psi)}|0\rangle|\phi_0(\psi)\rangle + \sqrt{1-p(\psi)}|\phi_1(\psi)\rangle.$$

Namely if we measure the first of the $m+k$ output qubits, we see 0 (1 respectively) with probability $p(\psi)$ ($1-p(\psi)$ resp.) and the state collapses to $|0\rangle|\phi_0(\psi)\rangle$ ($|1\rangle|\phi_1(\psi)\rangle$

resp.) Suppose that we would like to produce $|\phi_0(\psi)\rangle$ from input state $|\psi\rangle$. If we have multiple copies of $|\psi\rangle$, we may repeat running Q and hope to measure 0 in one of the instances. This problem explores when we can do so with just a single copy of (unknown) $|\psi\rangle$. In general, measuring one qubit may already collapse the state, and it is not clear if it is possible to get $|\phi_0(\psi)\rangle$ if the measurement outcome was 1.

(a) (Do not need to turn it in) Consider a special case that $p(\psi) = p$ is constant over all choices of the $|\psi\rangle$ with $p \in (0,1)$). Show that for every $\varepsilon > 0$ there is a general quantum circuit R, with $\text{size}(R) = O(\log(1/\varepsilon) \cdot \text{size}(Q))$ such that the output $\rho(\psi)$ of R satisfies

$$\langle \phi_0(\psi)|\rho(\psi)|\phi_0(\psi)\rangle \geq 1 - \varepsilon\,.$$

(Hint: techniques in Grover's algorithm.) Note: we may weaken the condition slightly to *almost constant* probabilities of measuring 0 and 1 and show a similar "quantum rewinding" procedure. Read more on `https://cs.uwaterloo.ca/~watrous/Papers/ZeroKnowledgeAgainstQuantum.pdf`.

(b) (Bonus 10pts) Under the same condition above, show how to recover $|\psi\rangle$ exactly from $|\phi_1(\psi)\rangle$. (Therefore you may repeat running Q from start again and again utill you get $|\phi_0(\psi)\rangle$)

(c) (Bonus 15pts) Can you identify other conditions where quantum rewinding is possible?