CSCE 440/640 Quantum Algorithms

Homework 5

Texas A&M U, Spring 2019 — *April 10, 2019*

Lecturer: Fang Song — *Due: April 29, 2019, before class*

Instructions. Only PDF format is accepted (type it or scan clearly). 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. 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.

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. (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)

2. (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 $\eta < 1/2$ (i.e., a biased coin and we denote it COIN_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 assuming constant η (e.g., $\eta = 1/4$).

3. (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 $|\phi^+\rangle$ 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.

4. (Distinguishing states)

   (a) (10 points) Explain how a device which, upon input of one of two non-orthogonal quantum states $|\psi\rangle$ or $|\phi\rangle$ correctly identified the state, could be used to build a device which cloned the states $|\psi\rangle$ and $|\phi\rangle$. Conversely, explain how a device for cloning could be used to distinguish non-orthogonal quantum states.

   (b) (5 points) Suppose Bob is given $|\psi_0\rangle = |0\rangle$ or $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Help Bob design a POVM which distinguishes the states some of the time, but never makes an error of mis-identification.

   (c) (5 points) **[G]** Suppose Bob is given a quantum state chosen from a set of linearly independent states $\{|\psi_0\rangle, \dots |\psi_{m-1}\rangle\}$. Construct a POVM $\{E_0, E_2, \dots, E_m\}$ such that if outcome E_i occurs, $0 \le i \le m-1$, then Bob knows with certainty that he was given the state $|\psi_i\rangle$. (The POVM must be such that $\langle\psi_i|E_i|\psi_i\rangle > 0$ for each i.)