MASSACHUSETTS INSTITUE OF TECHNOLOGY

Department of Physics, EECS, and Department of Applied Math

MIT 6.443J / 8.371J / 18.409 / MAS.865

Quantum Information Science

February 7, 2006

Problem Set #1

(due in class, 16-Feb-06)

Lecture Topics (2/7, 2/9, 2/14): Quantum operations; quantum error correction critera; CSS codes

Recommended Reading: Nielsen and Chuang, Sections 4.2-4.4, 8.1-8.3, 10.1-10.4

Problems:

P1: (**Review**) Quantum gates and circuits are briefly reviewed in this problem.

(a) Compute the normalized eigenvectors of the Pauli matrices, X, Y, and Z, and plot these states as points on the Bloch sphere.

(b) The CNOT gate is a simple permutation whose action on an arbitrary two-qubit density matrix $\rho = \sum_{j,k\in\{00\cdots11\}} c_{jk}|j\rangle\langle k|$ is to rearrange the elements in the matrix. Write out this action explicitly on c_{jk}.

(c) Let $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Draw a quantum circuit using controlled-phase and Hadamard gates to produce $|\psi\rangle$ from the input $|00\rangle$.

(d) Give a quantum circuit to create the state $(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)/2\sqrt{2}$.

(e) Let U be a CNOT gate, and X_i and Z_i be the Pauli operators on qubit i. What are $UX_1U^\dagger$, $UX_2U^\dagger$, $UZ_1U^\dagger$, and $UZ_2U^\dagger$?

(f) The operator $R_y(\theta) = \exp(-iY\theta/2)$ rotates a qubit about the $\hat{y}$ axis on the Bloch sphere, and similarly $R_x(\theta) = \exp(-iX\theta/2)$ rotates about $\hat{x}$. Construct $R_z(\theta)$ for arbitrary θ, from a series of rotations about $\hat{x}$ and $\hat{y}$.

P2: (**Open Systems and the Operator Sum Representation**) In class, we learned that the interaction of any quantum system with an environment can be mathematically expressed by a *quantum operation*, $\mathcal{E}(\rho)$, defined as

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \,, \tag{1}$$

where the only condition on the operation elements E_k is that $\sum_k E_k^\dagger E_k = I$. This is known as the *operator sum representation* (OSR). Here, we explore some of the physics implied by this model, and study some important examples introduced in the lecture.

(a) If ρ has dimension d, then at most d^2 operation elements are required: $1 \le k \le d^2$. We can prove this fact by utilizing the *unitary degree of freedom* in the OSR. This is the fact that $\mathcal{E}$ and $\mathcal{F}$ are the same quantum operation if and only if their operation elements are related by $E_i = \sum_j u_{ij} F_j$, and u_{ij} is a unitary matrix.

Let $\{E_j\}$ be a set of operation elements for $\mathcal{E}$. Define a matrix $W_{jk} \equiv \mathrm{tr}(E_j^\dagger E_k)$. Show that the matrix W is Hermitian and of rank at most d^2, and thus there is unitary matrix u such that $uWu^\dagger$ is diagonal with at most d^2 non-zero entries. Use u to define a new set of at most d^2 non-zero operation elements $\{F_j\}$ for $\mathcal{E}$.

(b) Phase damping is an important decoherence mechanism, described by the operation elements

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix} \qquad E_1 = \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\lambda} \end{bmatrix}, \tag{2}$$

or, equivalently, by the operation elements

$$\tilde{E}_0 = \sqrt{\alpha} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \tilde{E}_1 = \sqrt{1-\alpha} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{3}$$

where $\alpha = (1 + \sqrt{1-\lambda})/2$. This fact was at the heart of Shor's invention of quantum error correction!

Explicitly show that $\sum_k E_k \rho E_k^\dagger = \sum_k \tilde{E}_k \rho \tilde{E}_k^\dagger$ for a general single-qubit ρ, and give the unitary transformation which relates E_k to $\tilde{E}_k$; that is, find u such that $\tilde{E}_k = \sum_j u_{kj} E_j$.

(c) Construct operation elements for a single qubit quantum operation $\mathcal{E}$ that upon input of any state ρ replaces it with the completely randomized state $I/2$. It is amazing that quantum codes can correct for this kind of error (if it acts on only one qubit), even if the noise completely destroys the qubit!

P3: (**Two-bit amplitude damping code**) Amplitude damping is an important process in real physical systems; it models spontaneous emission, inelastic scattering, thermalization of spins to the lattice, and many other microscopic processes where energy is exchanged between the system and environment. In this problem, we study a quantum code adapted for this error mechanism.

Recall that the ampltiude damping channel for a single qubit is described by $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$, where the operation elements are

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \qquad E_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix}. \tag{4}$$

Let $\gamma = 1 - e^{-t/T_1}$, where t is time and T_1 is the amplitude damping time constant.

(a) Let $|\psi_1\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $\rho_1 = \mathcal{E}(|\psi_1\rangle) = \sum_k E_k |\psi_1\rangle\langle\psi_1| E_k^\dagger$ be the density matrix obtained for the qubit after amplitude damping. Compute the fidelity of ρ_1 with respect to $|\psi_1\rangle$, $F_1(t) = F(|\psi_1\rangle, \rho_1) = \sqrt{\langle\psi_1|\rho_1|\psi_1\rangle}$ and plot as a function of t.

(b) Find the state $|\phi(t)\rangle$ which minimizes F_1 at each point in time, and plot this minimum value as a function of time.

(c) Let $|0_L\rangle = |01\rangle$ and $|1_L\rangle = |10\rangle$ be a quantum code encoding one logical qubit using two physical qubits. Define $|\psi\rangle = a|0_L\rangle + b|1_L\rangle$. Compute the output state

$$\rho' = \mathcal{E}(|\psi\rangle) = \sum_{j,k=\{0,1\}} (E_j \otimes E_k)\, |\psi\rangle\langle\psi|\, (E_j \otimes E_k)^\dagger \tag{5}$$

which results when each physical qubit is subject to amplitude damping.

(d) Compute the fidelity $F(|\psi\rangle, \rho') = \sqrt{\langle\psi|\rho'|\psi\rangle}$ of ρ' with respect to $|\psi\rangle$, and plot as a function of t for the worst case state.

(e) Suppose we project the output state into the space orthogonal to $|00\rangle$ (say by performing a measurement of $Z \otimes Z$ to measure the total excitation number), and keep only the cases when we do not obtain $|00\rangle$. What is the resulting state? What is its fidelity with respect to $|\psi\rangle$, as a function of t?

(f) (+5 points extra credit) How well does the Shor 9-qubit code correct against amplitude damping errors? Let the operation elements for this process be as above, applied to each physical qubit. Calculate the fidelity of the decoded state as a function of γ.

P4: (**CSS and the 7-qubit Steane code**) Certain classical linear codes can be translated directly into quantum codes, and in this exercise we explore an example which illustrates the procedure, and also introduces the basic ideas of classical linear codes.

(a) A *linear code* C encoding k bits of information into an n bit code space is a set of bit strings specified by an n by k *generator matrix* G whose entries are zeroes and ones. The 2^k codewords which comprise C are given by Gx, where x is a column vector specifying k bit values (note that arithmetic operaetions are all done modulo 2). For the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \tag{6}$$

give the sixteen seven-bit codewords.

(b) Errors are detected by computing various parity checks, which are forumlated in terms of an $n-k$ by n matrix H satisfying $Hx = 0$ for all codewords x. For the above code, we may choose

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \tag{7}$$

Verify that $Hx = 0$ for all the codewords you just found, and prove that $HG = 0$.

(c) An error can be modeled as addition (modulo 2) of a random bit string e to a codeword x, giving $y = x + e$. As long as y is not a codeword, the error can be detected by computing $Hy = e \neq 0$. Show that for this code, if only a single bit error occurs, then $Hy = e_j$ is just a binary representation for j, telling us which bit to flip to correct the error.

(d) The maximum number of bit flip errors that can be tolerated is given by the minimum Hamming distance between any two codewords,

$$d(C) = \min_{x,y \in C, x \neq y} d(x,y) \tag{8}$$

where $d(x,y)$ is the number of bits where x and y differ. What is $d(C)$ for the above code?

(e) Consider a code $C^\perp$ which has generator matrix $G' = H^T$ and parity check matrix $H' = G^T$. Show that $C^\perp$ is a $n=7$, $k=3$ code, and furthermore, $C^\perp \subseteq C$.

(f) Prove that if $x \in C^\perp$ then $\sum_{y \in C} (-1)^{x \cdot y} = |C|$, while if $x \notin C^\perp$ then $\sum_{y \in C} (-1)^{x \cdot y} = 0$.

(g) Define the quantum state

$$|\psi(x)\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{y \in C^\perp} |x+y\rangle \tag{9}$$

for $x \in C$. Explicitly give $|\psi(0000000)\rangle$ and $|\psi(1111111)\rangle$.

(h) Let e_1 and e_2 be vectors of n bits which indicate where errors occur; for nonzero bits of e_1 bit flips occur, and for nonzero bits of e_2 phase flip errors occur. Assume that the $d(e_1, 0) \leq 1$ and $d(e_2, 0) \leq 1$. Show that if $|\psi(x)\rangle$ is the initial state, then after such errors the resulting state is

$$|\psi_{\text{b+perr}}\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{y \in C^\perp} (-1)^{(x+y)\cdot e_2} |x+y+e_1\rangle \,. \tag{10}$$

(i) Recall that H is the parity check matrix for C. Explain how to compute the transformation $|x\rangle|0\rangle \to |x\rangle|Hx\rangle$ using a circuit composed entirely of controlled-NOTs. Show that you can thus obtain e_1 by applying this circuit to $|\psi_{\text{b+perr}}\rangle$. Since e_1 has at most one error, we can thus obtain

$$|\psi_{\text{perr}}\rangle = \frac{1}{\sqrt{|C^\perp|}} \sum_{y \in C^\perp} (-1)^{(x+y)\cdot e_2} |x+y\rangle \,. \tag{11}$$

(j) Give the state obtained by applying Hadamard gates to each and every qubit of $|\psi_{\text{perr}}\rangle$, and show that by applying the appropriate parity check matrix (which one?), and using your result from part (f), you can obtain e_2, and thus reconstruct the original state $|\psi(x)\rangle$. In this manner, it becomes apparent that C is used to correct for bit flip errors, and $C^\perp$ for phase flip errors. Since those errors form a basis for an arbitrary error, the quantum code we have constructed can correct for an arbitrary single qubit error.