MASSACHUSETTS INSTITUTE 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, 2008

Problem Set #1

(due in class, 14-Feb-06)

Lecture Topics (2/5, 2/7, 2/12): 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: (**Operator Sum Representation: Examples**) 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

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

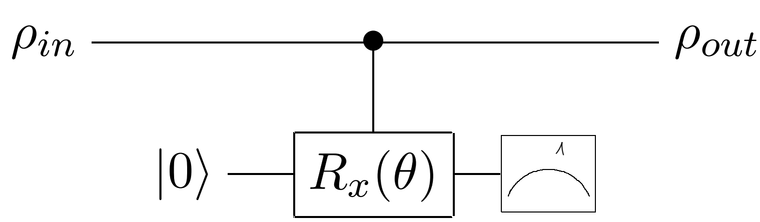
where the only condition on the operation elements E_k is that $\sum_k E_k^\dagger E_k = I$. This is known as the *operator sum representation* (OSR). Here, we explore some of the physics implied by this model, and study some important examples introduced in the lecture.

(a) You are given a black box which takes single qubit states ρ_{in} as input, and produces ρ_{out} as output. Suppose the box just replaces its input with $|0\rangle$, such that $\rho_{out} = |0\rangle\langle 0|$. Give a set of operation elements $\{E_k\}$ describing the black box, such that $\rho_{out} = \sum_k E_k \rho_{in} E_k^\dagger$.

(b) Suppose the black box replaces any input ρ_{in} with the completely randomized state $I/2$. Give $\{E_k\}$ describing the operation of this box. It is amazing that quantum codes can correct for this single qubit *erasure* error, which completely destroys the original qubit!

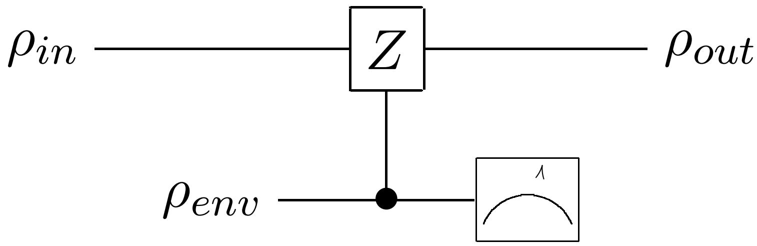
(c) From performing experiments, you determine that the black box performs $\mathcal{E}(\rho_{in}) = pI/2 + (1 - p)\rho_{in}$, where p is a probability. Give $\{E_k\}$ describing the operation of this box.

(d) You are given a schematic diagram for the quantum circuit inside the black box, which is



Each line represents a qubit; the top qubit is the qubit transferred into and out of the box, and the bottom qubit is the "environment" to which the box is connected. Give $\{E_k\}$ describing the operation of this box; write this in terms of λ, where $\cos(\theta/2) = e^{-\lambda}$.

(e) You are given another schematic diagram for the quantum circuit inside the black box, which is



The environment state $\rho_{env} = \alpha|0\rangle\langle 0| + (1-\alpha)|1\rangle\langle 1|$, where α is a probability. Give $\{E_k\}$ describing the operation of this box. How is this box related to that in part (d)? If they are related, give an expression relating α and λ.

P2: (**A 5-qubit quantum code**) We saw in class that a quantum code defined by projector $P = \sum_\ell |\psi_\ell\rangle\langle\psi_\ell|$, for codeword states $|\psi_\ell\rangle$, corrects errors E_k if and only if $PE_k^\dagger E_j P = d_k \delta_{jk} P$, for some constant d_k. Let the notation $U_1U_2U_3U_4U_5$ denote the tensor product $U_1 \otimes U_2 \otimes \cdots \otimes U_5$, as was used in class, where the U_j are Pauli matrices. Consider the matrix

$$\begin{aligned} P \;=\; & \frac{1}{16}\,[3IIIII \\ & + IZYYZ + ZYYZI + YYZIZ + YZIZY + ZIZYY \\ & + IXZZX + XZZXI + ZZXIX + ZXIXZ + XIXZZ \\ & + IYXXY + YXXYI + XXYIY + XYIYX + YIYXX \\ & + 2\,(ZXYYX + XYYXZ + YYXZX + YXZXY + XZXYY) \\ & -2ZZZZZ]\;. \end{aligned} \tag{2}$$

Note that while this looks complicated, many of the terms are actually cyclic shifts of others.

(a) Show that P is a projection operator onto a 6-dimensional subspace of the 5-qubit Hilbert space.

(b) Show that the space defined by P defines a quantum code which can correct for any single qubit erasure error.

(c) Explain why the distance of the code is $d = 2$, so that this is a $((5, 6, 2))$ quantum code.

P3: (**The CSS codes construction**) Classical linear codes can be translated directly into quantum codes. In this exercise, we explore an example using the CSS construction.

(a) A binary *linear code* C encoding k bits of information into an n bit code space is a k-dimensional subspace of the vector space of n-bit strings. The 2^k codewords in the code can be specified as the span of the columns of an n by k *generator matrix* G whose entries are zeros and ones. The codewords are given by Gx where x is a k-bit column vector representing the information string to be encoded. The arithmetic operations are modulo 2. Let the generator matrix

$$G = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \tag{3}$$

define the code $\mathcal{C}$. Write out $\mathcal{C}$ explicitly. Use the Gauss-Jordan procedure to column reduce G and arrive at the *standard (or systematic) form*

$$G = \begin{bmatrix} I \\ A \end{bmatrix} \tag{4}$$

where A is an $n-k$ by k matrix.

(b) Errors are detected by computing a collection of parity checks. The parity checks can be gathered into an $n-k$ by n *check matrix* H satisfying $Hx = 0$ for all codewords x. If $Hx' \neq 0$ for a vector x', then x' is not a codeword and an error has occurred. For a binary linear code in standard form $H = [IA]$. Verify that $Hx = 0$ for all the codewords of $\mathcal{C}$. Prove that $HG = 0$ for a binary linear code.

(c) The *minimum (Hamming) distance* over all pairs of codewords of $\mathcal{C}$,

$$d(\mathcal{C}) = \min_{x,y\in\mathcal{C},x\neq y} d(x,y), \tag{5}$$

where $d(x,y)$ is the number of bits where x and y differ, is the minimum number of bit flips that can lead to an undetectable error. A code can detect $d-1$ single qubit errors and correct $\lfloor (d-1)/2 \rfloor$ single qubit errors. What is $d(\mathcal{C})$ for this example? How many errors does this code correct?

(d) The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is the code with generator matrix $G^\perp = H^T$. Confirm that $C^\perp \subseteq C$ for this example. As a special case of the CSS construction, consider the quantum code that is the span of the states

$$|\psi(x)\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{y\in\mathcal{C}^\perp} |x+y\rangle \tag{6}$$

for $x \in \mathcal{C}$. Show that these states must be orthogonal if $x \neq y \bmod \mathcal{C}^\perp$. Write the set of unique states $|\psi(x)\rangle$ for this example. Confirm that single qubit Pauli errors map these states to orthogonal states. If k is the dimension of $\mathcal{C}$ and $k^\perp$ is the dimension of $\mathcal{C}^\perp$, what is $k - k^\perp$ for this example? How many qubits does this code encode?

(e) Let C_{jk} be the CNOT gate applied on qubits j and k, with j being the control qubit. Show that $C_{15}C_{26}C_{37}C_{48}|\psi(1100)\rangle \otimes |\psi(1010)\rangle = |\psi(1100)\rangle \otimes |\psi(0110)\rangle$. Explain the action of this gate on $|\psi(x)\rangle \otimes |\psi(y)\rangle$.