Problem Set #1

Quantum Error Correction
Instructor: Daniel Gottesman

Due Tues., Jan. 16, 2007

Problem #1. QECC Conditions and the 9-Qubit Code

a) For the 9-qubit code, calculate the matrix C_{ab} for the QECC conditions, $\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = C_{ab}\delta_{ij}$, where E_a and E_b run over the identity and the single-qubit Pauli matrices. (You may wish to lump together cases related by some straightforward symmetry.)

b) Diagonalize C_{ab} for the 9-qubit code, and give a basis of errors for which the matrix is diagonal.

Problem #2. Correcting Small Shifts

For this problem, consider the following operations X and Z acting on registers of size D:

$$X|j\rangle = |j+1 \bmod D\rangle, \tag{1}$$
$$Z|j\rangle = \omega^j|j\rangle, \quad \text{with } \omega = e^{2\pi i/D}. \tag{2}$$

a) Consider the following encoding in a register of size $D = 18$:

$$|\overline{0}\rangle = (|0\rangle + |6\rangle + |12\rangle)/\sqrt{3} \tag{3}$$
$$|\overline{1}\rangle = (|3\rangle + |9\rangle + |15\rangle)/\sqrt{3}. \tag{4}$$

Show that this encoding corrects all small shift errors, i.e., errors of the form X^aZ^b, with $a, b \in \{-1, 0, +1\}$.

b) Suppose that the codeword instead experiences the error X^2 (i.e., add 2 mod D), but we perform the error correction procedure designed for part a. What happens to the encoded qubit?

c) Find an operator of the form X^aZ^b which is not one of the nine from part a, but which leaves all codewords unchanged.

Problem #3. Quantum Secret Sharing

A quantum secret sharing scheme is an encoding of a quantum state which splits it among n people such that for any set of people, either that set of people can reconstruct the encoded quantum state, or that set of people by themselves have no information about the state. (Note that this must be true for encodings of all superpositions as well as the basis states.) More concretely, imagine that we encode a state in $N \geq n$ qubits and give qubits $a_{i-1}+1, \ldots, a_i$ to person i ($i = 1, \ldots, n$, $a_0 = 0$), so person i gets $a_i - a_{i-1}$ qubits. In general, we might allow the procedure to throw away qubits, but for this problem, consider the case with $a_n = N$; we call this a *pure state encoding.*

a) Some sets A of people should be able to reconstruct the encoded state; we call these *authorized sets.* Formulate this condition precisely in terms of correcting erasure errors.

b) Other sets B of people should have no information about the original encoded state; these are the *unauthorized sets*. Formulate this condition precisely in terms of the density matrix ρ_B jointly held by the people in set B.

c) Show that for a pure state quantum secret sharing scheme, a set B is an unauthorized set iff its complement $\{1, \dots, n\} \backslash B$ is an authorized set. (Hint: use an appropriate form of the QECC conditions)

d) In a *threshold scheme*, whether a set is authorized or unauthorized depends only on the number of people in the set: If there are $\geq k$ people in the set, it is authorized, and if there are $< k$ people, the set is unauthorized. For a pure state quantum secret sharing scheme, figure out the possible values for k and n based on part c.