Quantum Error Correction: Problem Set #1

It for Qubit
Lecturer: Daniel Gottesman

Wed., July 20, 2016

Problem #1. The 9-Qubit Code

All parts of this problem refer to the 9-qubit code using the error correction method discussed in lecture. X_i, Y_i, or Z_i represents X, Y, or Z applied to the ith qubit.

a) Which of the following errors can be corrected by the 9-qubit code: X_1X_3, X_2X_7, X_5Z_6, Z_5Z_6, Y_2Z_8, $X_2 + X_1X_3$, $X_1 + X_2X_7$?

b) Suppose we perform the usual error correction procedure on the 9-qubit code after one of the errors from part a has occurred. This returns us to an encoded state, but it may not be the correct encoded state. For those errors that cannot be corrected, calculate the operation that is performed on the encoded state. That is, if we start with $\alpha|\overline{0}\rangle + \beta|\overline{1}\rangle$, what state do we end up with?

c) 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.)

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

Problem #2. 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 $\{1, \ldots, n\} \setminus B$ is an authorized set.

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. (It turns out that all of these values are actually achievable.)

e) Consider the following method of encoding 1 qutrit (a 3-dimensional Hilbert space) in 3 qutrits:

$$|0\rangle \mapsto |000\rangle + |111\rangle + |222\rangle \tag{1}$$
$$|1\rangle \mapsto |012\rangle + |120\rangle + |201\rangle \tag{2}$$
$$|2\rangle \mapsto |021\rangle + |210\rangle + |102\rangle. \tag{3}$$

Give one qutrit to each person. (If you prefer to formulate this in terms of qubits, imagine giving each person two qubits, with $|0\rangle \to |00\rangle$, $|1\rangle \to |01\rangle$, and $|2\rangle \to |10\rangle$.) Show that this gives a threshold quantum secret sharing scheme. What are k and n?

f) Prove that there cannot exist a threshold quantum secret sharing scheme (pure or not) with $k \leq n/2$.