Problem set #3
Due Monday, March 14, 2005

1. Concatenated codes. (10 points) Let C_1 and C_2 be quantum codes of type $[[n_1, 1, d_1]]$ and $[[n_2, 1, d_2]]$, respectively, and let $V_1 : \mathbb{C}^2 \to (\mathbb{C}^2)^{\otimes n_1}$ and $V_2 : \mathbb{C}^2 \to (\mathbb{C}^2)^{\otimes n_2}$ be the corresponding encodings. The encoding for a concatenated code is defined by first using V_1, and then applying V_2 to each of the resulting qubits:

$$V = V_2^{\otimes n_1} V_1 : \mathbb{C}^2 \to (\mathbb{C}^2)^{\otimes n_1 n_2}. \tag{1}$$

Let us denote the concatenated code $C = \operatorname{Im} V$ by $C_1 \triangleleft C_2$. (Note that this definition depends on the choice of V_2.) Concatenated classical codes are defined analogously.

a) Show that the distance of C is at least $d_1 d_2$.

b) The example of Shor's code shows that in general $C_1 \triangleleft C_2 \neq C_2 \triangleleft C_1$, even for CSS codes. However, if C_1 and C_2 are *classical* linear codes and the encoding V_2 is linear, then $C_1 \triangleleft C_2 = C_2 \triangleleft C_1$. Prove this statement.

2. Distillation of Shor's ancillas. (20 points) In the first scheme of fault-tolerant quantum computation [Peter Shor, `quant-ph/9605011`] the following state was used:

$$|\Psi_{000}\rangle = 2^{-3/2} \sum_{z_1, z_2, z_3} (-1)^{z_1 z_2 z_3} |z_1, z_2, z_3\rangle.$$

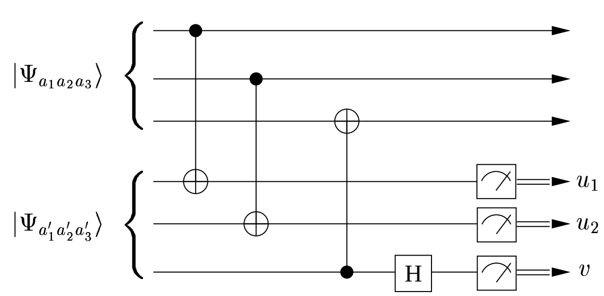
More generally, let

$$|\Psi_{a_1 a_2 a_3}\rangle \;=\; 2^{-3/2} \sum_{z_1, z_2, z_3} (-1)^{z_1 z_2 z_3 + a_1 z_1 + a_2 z_2 + a_3 z_3} |z_1, z_2, z_3\rangle. \tag{2}$$

We will discuss a distillation procedure that increases the fraction of $|\Psi_{000}\rangle$ in a random mixture of such states. The procedure will only use symplectic unitaries with classical control, Pauli measurements, and classical computation.

a) Find three commuting symplectic operators A_1, A_2, A_3 such that $|\Psi_{a_1 a_2 a_3}\rangle$ is an eigenvector of A_j with eigenvalue $(-1)^{a_j}$ (for $j = 1, 2, 3$).

b) Suppose we are given the state $|\Psi_{a_1 a_2 a_3}\rangle \otimes |\Psi_{a'_1 a'_2 a'_3}\rangle$, where the values of $a_1, a_2, a_3, a'_1, a'_2, a'_3$ are unknown. Let us perform the following circuit:



(3)

Show that if the measured values are $u_1 = u_2 = v = 0$, then $a_3 = a_3'$ and the resulting quantum state is $|\Psi_{a_1+a_1', a_2+a_2', a_3}\rangle$.

c) Modify the circuit so that it works for arbitrary u_1, u_2. **Hint:** We need to apply some symplectic operator after the measurement of u_1, u_2 but before we measure v. We still post-select states satisfying $v = 0$, which should be equivalent to the condition $a_3 = a_3'$.

d) Suppose we have many imperfect copies of the state $|\Psi_{000}\rangle$, and we want to distill fewer copies with higher fidelity. To be specific, each copy is characterized by the mixed state

$$\rho = \sum_{a_1,a_2,a_3} w(a_1,a_2,a_3)|\Psi_{a_1a_2a_3}\rangle\langle\Psi_{a_1a_2a_3}|, \qquad w(a_1,a_2,a_3) = \prod_{j=1}^{3}(1-p_j)^{1-a_j}p_j^{a_j}, \quad (4)$$

where $p_1 = p_2 = p_3 = p$. The above procedure allows us to decrease p_3 at cost of increasing p_1 and p_2 (and sacrificing half of the copies). We can then repeat the procedure for a different order of qubits. Find the threshold value of p below which the distillation succeeds.

e) If p is a constant below the threshold, we can transform n poor copies into one copy that has fidelity $1 - \epsilon$, where

$$\ln(1/\epsilon) \sim n^{\alpha}. \quad (5)$$

Find the exponent α.