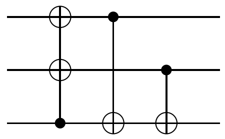
Solution Set #9

Quantum Error Correction
Instructor: Daniel Gottesman

Problem #1. Entanglement-Assisted Quantum Error Correction

a) For the 4-qubit error-detecting code, we use the $[[4, 2, 2]]$ code with stabilizer generated by $X \otimes X \otimes X \otimes X$ and $Z \otimes Z \otimes Z \otimes Z$. Initially, Alice and Bob share an EPR pair with stabilizer $I \otimes I \otimes X \otimes X$ and $I \otimes I \otimes Z \otimes Z$ (the first two qubits being Alice's input data qubits, and the fourth qubit being held by Bob).

Clearly, to do this encoding, Alice must choose a Clifford group operation that takes $I \otimes I \otimes X \mapsto X \otimes X \otimes X$ and $I \otimes I \otimes Z \mapsto Z \otimes Z \otimes Z$. Such a Clifford group operation certainly exists since the two initial operators and the two final operators both anticommute. For instance, we can use the following circuit:



If there is an error in the channel, it takes place on one of the first three qubits. Bob can detect it because the code is a distance 2 code. Indeed, he could have detected an error even if it was on the fourth qubit instead, so there is some extra power in this code which he is not using.

b) In general, we can choose products of the M_is so that the products commute and anticommute in pairs. That is, we can choose M'_i, $i = 1, \ldots, r$ such that $\{M_{2j-1}, M_{2j}\} = 0$ for $j \leq j_0$, and $[M_k, M_{k'}] = 0$ unless $k = 2j - 1$, $k' = 2j$, with $j \leq j_0$ (or vice-versa). If all the M_is commute to begin with, they are already in this form, with $j_0 = 0$. Otherwise, we put them in the requisite form by first identifying a pair M_{i_1} and M_{i_2} that anticommute and making them M'_1 and M'_2. If any other M_i anticommutes with M_{i_1}, multiply it by M_{i_2}, and if M_i anticommutes with M_{i_2}, multiply it by M_{i_1}. (If M_i anticommutes with both, we thus multiply it by both.) After these multiplications, the remaining modified M_is commute with both M'_1 and M'_2.

Then we pick another anticommuting pair and repeat the procedure until all remaining modified M_is commute with each other. The number of pairs we need to select this way gives us j_0, an invariant property of the original set $\{M_i\}$, essentially identifying the amount of anticommutativity in the group generated by the set. Also note that M'_is generate the same group as the original set $\{M_i\}$, and, in particular, it is possible to write each M_i as a product

$$M_i = \prod_k (M'_k)^{c_{ik}}, \tag{1}$$

with c_{ik} a binary $r \times r$ invertible matrix.

The set $\{M'_k\}$ by itself cannot generate a stabilizer unless $j_0 = 0$. We need to choose N'_is to cancel the anticommutativity. We thus set $n' = j_0$, and let $N'_{2j-1} = X_j$, $N'_{2j} = Z_j$ $(j \leq j_0)$, or $N'_k = I$ $(k > 2j_0)$. X_j and Z_j are the X and Z operators on the jth qubit out of the additional n' qubits. We then define a stabilizer S generated by $M'_i \otimes N'_i$. Since each $M_i = \prod (M'_k)^{c_{ik}}$, and c_{ik} is invertible, we can choose alternate generators for S in the form $M_i \otimes N_i$, with

$$N_i = \prod_k (N'_k)^{c_{ik}}. \tag{2}$$

No value of n' less than j_0 will work, since there will inevitably always then be two generators of the stabilizer that will anticommute. Consider the group generated by the M_is and consider its center Z (the subgroup of elements that commute with all the M_is). Clearly Z is the group generated by M'_k, for $k > 2j_0$, and is in invariant property of the set $\{M_i\}$, no matter how we choose anticommuting pairs in the procedure above. The size of Z tells us j_0: $2j_0 = r - \log_2 |Z|$.

c) We can choose a Clifford group operation that maps $X_j \mapsto M'_{2j-1}$, $Z_j \mapsto M'_{2j}$ $(j \leq j_0)$, and $Z_k \mapsto M'_{k+j_0}$ $(j_0 < k \leq r - j_0)$, since this transformation preserves commutation and anticommutation. Then we find that $n' = j_0$ EPR pairs plus $r - 2j_0$ ancilla qubits which start as $|0\rangle$ map to the stabilizer S. Therefore, we can set $n - k' - n' = r - 2j_0$, or $k' = (n - j_0) - (r - 2j_0) = n + j_0 - r$, and given any value of the k input data qubits, Bob's $n + n'$ qubits will end up in a codeword of S.

d) Suppose $E \notin N(S)$. Then we can certainly detect it. Since E acts on only the n qubits held initially by Alice, $E \notin N(S)$ iff $\{E, M_i\} = 0$ for some $i \in \{1, \ldots, r\}$; that is, E anticommutes with some operator from the original set.

Similarly, if $E \in N(S) \setminus S$, we cannot detect it. As above, $E \in N(S)$ iff it commutes with all M_is. But what does it mean for $E \in S$? It is not sufficient for $E \in S$ that E is in the group generated by the M_is: Imagine $E = M'_{2j-1}$ for $j \leq j_0$; then $E \notin S$, and indeed $\{E, M'_{2j}\} = 0$. We conclude that $E \in S$ iff E is in the group generated by the set $\{M'_k\}$ for $k > 2j_0$. (That is, the center Z mentioned at the end of the solution to part b above.)

Thus, E is detectable iff it either anticommutes with some M_i, or if it is in the group Z generated by the set $\{M'_k\}$ for $k > 2j_0$. (For this condition, it is actually sufficient, after all, to say that it is in the group generated by the M_is, since if it is in this group but outside S_A, it actually anticommutes with some M_i.) E is undetectable iff it commutes with all M_is but is not in S_A.

If Alice uses the protocol catalytically, she uses j_0 of the k' encoded qubits to create new EPR pairs to replace the ones used in the protocol. Since $k' = n + j_0 - r$, it follows that $k = n - r$.

Problem #2. Two-Way Entanglement Distillation

a) We start with two Bell states, eigenstates of $X \otimes X$ and $Z \otimes Z$ with syndromes (x, z) and (x', z'), respectively. Nontrivial z syndromes correspond to X errors, and nontrivial x syndromes correspond to Z errors, whereas a Y error leads to both syndromes being nontrivial.

The CNOTs change the stabilizer generators to

$$(-1)^x XX \otimes XX \tag{3}$$

$$(-1)^{x'} IX \otimes IX \tag{4}$$

$$(-1)^z ZI \otimes ZI \tag{5}$$

$$(-1)^{z'} ZZ \otimes ZZ \tag{6}$$

(with the left two qubits being held by Alice and the right two being held by Bob). We can replace the first and last generators by taking products of the first two and last two generators, so an equivalent presentation of the stabilizer is:

$$(-1)^{x\oplus x'} XI{\otimes}XI \tag{7}$$
$$(-1)^{x'} IX{\otimes}IX \tag{8}$$
$$(-1)^{z} ZI{\otimes}ZI \tag{9}$$
$$(-1)^{z\oplus z'} IZ{\otimes}IZ \tag{10}$$

This we identify as two Bell pairs, with syndromes $(x \oplus x', z)$ and $(x', z \oplus z')$. (In particular, the first pair, when we keep it, is a mixture of Bell states.)

When Alice and Bob measure Z for the second pair, they get the same result, and thus end up keeping the state, iff $z \oplus z' = 0$. The probability that z is 0 is $1 - p + p/3 = 1 - 2p/3$ (since a pure Z error causes 0 z syndrome), and similarly for z'. Alice and Bob keep the state when both are 0 or when both are 1. This happens with probability P_{keep}:

$$P_{\text{keep}} = (1 - 2p/3)^2 + (2p/3)^2 = 1 - \frac{4}{3}p + \frac{8}{9}p^2. \tag{11}$$

b) To calculate the conditional probability of X, Y, and Z errors, it is perhaps most straightforward to simply make a list of all possible errors with the resulting error on the first pair after the CNOTs (based on the first pair having syndrome $(x \oplus x', z)$).

Error	keep?	first pair	prob.
II	yes	I	$(1-p)^2$
IX	no	I	$p(1-p)/3$
IY	no	Z	$p(1-p)/3$
IZ	yes	Z	$p(1-p)/3$
XI	no	X	$p(1-p)/3$
XX	yes	X	$p^2/9$
XY	yes	Y	$p^2/9$
XZ	no	Y	$p^2/9$
YI	no	Y	$p(1-p)/3$
YX	yes	Y	$p^2/9$
YY	yes	X	$p^2/9$
YZ	no	X	$p^2/9$
ZI	yes	Z	$p(1-p)/3$
ZX	no	Z	$p^2/9$
ZY	no	I	$p^2/9$
ZZ	yes	I	$p^2/9$

We then calculate the conditional probabilities by adding up the absolute probabilities for the relevant yes cases and dividing by the probability of keeping the state:

$$P_I = \left[(1-p)^2 + p^2/9\right]/P_{\text{keep}} = \frac{1-2p+\frac{10}{9}p^2}{1-\frac{4}{3}p+\frac{8}{9}p^2} \tag{12}$$

$$P_X = \left(\frac{2}{9}p^2\right)/P_{\text{keep}} \tag{13}$$

$$P_Y = \left(\frac{2}{9}p^2\right)/P_{\text{keep}} \tag{14}$$

$$P_Z = \left[\frac{2}{3}p(1-p)\right]/P_{\text{keep}} \tag{15}$$

Clifford twirling mixes and redistributes the X, Y, and Z errors, but does nothing when there is no error, so the depolarizing channel error rate after twirling is

$$P_X + P_Y + P_Z = \left[\frac{\frac{2}{3}-\frac{2}{9}p}{1-\frac{4}{3}p+\frac{8}{9}p^2}\right]p. \tag{16}$$

We thus find the error rate decreases iff

$$\frac{2}{3} - \frac{2}{9}p < 1 - \frac{4}{3}p + \frac{8}{9}p^2, \tag{17}$$

that is, if

$$\frac{8}{3}p^2 - \frac{10}{3}p + 1 = (2p-1)(\frac{4}{3}p-1) > 0. \tag{18}$$

If $p < 1/2$, this is true, so the error rate decreases. (It is also true if $p > 3/4$, but then repeated iterations will drive $p \to 3/4$, which gives the completely mixed state.)

c) We can again consult the chart in part b, and we find that the I, X, Y, and Z outcomes, conditioned on throwing away the state, all have probability

$$\left[p(1-p)/3 + p^2/9\right]/(1-P_{\text{keep}}). \tag{19}$$

In other words, $P_I = P_X = P_Y = P_Z = 1/4$. The discarded states are completely randomized.