Problem Set #2

CO 639: Quantum Error Correction
Instructor: Daniel Gottesman

Due Tues., Feb. 10

Problem 1. Standard Form for Stabilizers

In this problem, we will use the representation of Pauli operators as $2n$-dimensional binary vectors. In this representation, a stabilizer with r generators is a $r \times 2n$ matrix.

a) Using Gaussian reduction (row additions, plus rearrangements of columns simultaneously on both the left and right halves of the matrix), show that the stabilizer can always be put into the following form:

$$\left(\begin{array}{cc|cc} I & A & B & C \\ 0 & 0 & D & E \end{array} \right) \tag{1}$$

b) Show that the submatrix E in eq. 1 has maximum rank, and that further Gaussian reduction can take it to the form $(I|E')$ and C to the form $(0|C')$.

c) From the standard form, explain how to immediately find a Pauli operator with a given error syndrome. (Note, though, that this is not necessarily the smallest Pauli operator with that syndrome.)

Problem 2. Error Syndromes and Cosets

Recall that $N(S) = \{P | [P, M] = 0 \,\forall M \in S\}$, that S is a normal subgroup of $N(S)$, and that the elements of $N(S)/S$ (i.e., cosets of S in $N(S)$) correspond to logical $\overline{X}$ and $\overline{Z}$ operators.

a) Show that two Pauli errors E and F have the same error syndrome for a stabilizer code S iff they are in the same coset of $N(S)$.

b) Suppose that for each coset of $N(S)$ we pick some particular coset representative E and perform E whenever syndrome measurement indicates that coset. Suppose, however, a different error F had actually occurred. Relate the overall action on the codespace to an element of $N(S)/S$.

c) For the 5-qubit code, we choose the coset representatives to be the single-qubit errors (and the identity for the 0 syndrome), as there is exactly one in each coset. Use the result of part b to find the actions resulting from the errors $X_1 Z_3$ and $Y_2 X_4 Z_5$.

Problem 3. Logical $\overline{X}$ and $\overline{Z}$

a) For the [[6, 4, 2]] code with generators $X \otimes X \otimes X \otimes X \otimes X \otimes X$ and $Z \otimes Z \otimes Z \otimes Z \otimes Z \otimes Z$, find possible values of the encoded X and Z operators $\overline{X_i}$ and $\overline{Z_i}$ ($i = 1, \ldots, 4$).

b) Show that for a CSS code, we can always choose the $\overline{X}$ operators to be tensor products of all Xs and the $\overline{Z}$ operators to be tensor products of all Zs.

Problem 4. Creating CSS Codes: Reed-Muller codes

a) The (classical) 1st order Reed-Muller codes $\mathcal{R}(1, m)$ are linear codes on $n = 2^m$ bits, and have generator matrices whose rows are the all-1s vector and the vectors v_i ($i = 1, \ldots, m$), where the jth coordinate of v_i is equal to the ith bit of j, when j is expanded in binary (and assuming j runs from 0 to $n - 1$). For instance, for $n = 4$, $v_1 = (0011)$ and $v_2 = (0101)$. $\mathcal{R}(1, m)$ has $k = m + 1$ encoded bits. What is its distance?

b) The rth order Reed-Muller code $\mathcal{R}(r, m)$ has as rows of its generator matrix all products of up to r of the vectors v_i, where product means the bitwise product (1 iff all vectors in the product are 1 at a given coordinate), so for instance, $\mathcal{R}(2, m)$ has the additional generator $v_1 v_2 = (0001)$. (The all-1s generator is also included as, in some sense, the product of 0 of the v_i's.) How many bits does $\mathcal{R}(r, m)$ encode? What is the distance of $\mathcal{R}(r, m)$?

c) Show that the dual of $\mathcal{R}(r, m)$ is $\mathcal{R}(m - r - 1, m)$ ($r \leq m - 1$).

d) When can you make a CSS code out of two copies of $\mathcal{R}(r, m)$ (one each for the X part and the Z part), and what are its parameters $[[n, k, d]]$?

Problem 5. Stabilizer Codes via GF(4) Codes

The Hamming codes over GF(4) are given by writing down parity check matrices with r rows whose columns are not scalar multiples of each other (i.e., not the same and not multiples of ω or ω^2).

a) Write down the 21-register GF(4) Hamming code. Show that it satisfies the symplectic duality condition.

b) Write down the stabilizer for a 21-qubit perfect code.

c) Show that the GF(4) Hamming codes exist when $n = (4^r - 1)/3$, and that they satisfy the symplectic duality condition and therefore define stabilizer codes. Show that the distance of these quantum codes is 3 and conclude that perfect quantum codes exist for all of these values of n ($r \geq 2$).