Solution Set #5

Quantum Error Correction
Instructor: Daniel Gottesman

Problem #1. Qudit Stabilizer Codes

a) Inspired by the distance 2 qubit codes, we pick one stabilizer generator to be X^{a_i} on each qudit, and one to be Z^{b_i} on each qudit. We need $a_i, b_i \neq 0 \; \forall i$ so that the code has distance 2, and we need $\sum a_i b_i = 0 \pmod p$ so that the two generators commute.

If we choose $a_i = b_i = 1$ for $i = 1, \ldots, n-1$ and $a_n = 1$, $b_n = -(n-1) \pmod p$, we satisfy these conditions when $n \neq 1 \pmod p$. For the remaining case, we can again let $a_i = 1$ for all i, but let $b_i = 1$ for $i \leq n-2$, $b_{n-1} = 2$, $b_n = -1$. Since $p > 2$, this code satisfies the conditions for $n = 1 \pmod p$.

b) Let us use the points $\alpha_i = \{1, 2, 3, 4, 5\}$. The code C_1 in the standard basis consists of all polynomials of degree 2 or less. We can therefore take its generator matrix to be given by the monomials 1, x, and x^2:

$$G_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 2 & 4 \end{pmatrix}. \tag{1}$$

(Recall we are working modulo 7.) In order to find the dual matrix, it is helpful to put G_1 in what is known as "systematic form" by using row operations to put it in the form $(I|G)$. By subtracting row 1 from rows 2 and 3, then subtracting row 2 from 1 once and 3 times from row 3, then subtracting row 3 from row 1 3 times and from row 2 once, and finally dividing row 3 by 2, we get

$$G_1' = \begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 4 & 6 \\ 0 & 0 & 1 & 3 & 6 \end{pmatrix} \tag{2}$$

as an alternate generator matrix for C_1. Then we can read off two generating rows of the dual by putting $1, 0$ and $0, 1$ in the last two places:

$$H_1 = \begin{pmatrix} 6 & 3 & 4 & 1 & 0 \\ 4 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{3}$$

This gives us the two Z generators of the stabilizer. For the X generators, we know that $C_2^\perp$ is a subcode of C_1, and using the particular definition of a polynomial code from class, $C_2^\perp$ is the subcode with constant term 0 (since encoded qudits correspond to other values of the constant term, which are cosets of $C_2^\perp$). Thus,

$$H_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 2 & 4 \end{pmatrix}. \tag{4}$$

Therefore the stabilizer is

$$\begin{matrix} Z^6 & Z^3 & Z^4 & Z & I \\ Z^4 & Z & Z & I & Z \\ X & X^2 & X^3 & X^4 & X^5 \\ X & X^4 & X^2 & X^2 & X^4 \end{matrix} \tag{5}$$

Problem #2. Transversal Operations

a) We can choose the following coset representatives for the four logical operations:

$$\overline{X}_1 = X \otimes X \otimes I \otimes I \tag{6}$$
$$\overline{X}_2 = X \otimes I \otimes X \otimes I \tag{7}$$
$$\overline{Z}_1 = Z \otimes I \otimes Z \otimes I \tag{8}$$
$$\overline{Z}_2 = Z \otimes Z \otimes I \otimes I. \tag{9}$$

(Recall all logical Pauli operations must commute with the stabilizer, and the logical Pauli operations must have the correct commutation relations between pairs.)

b) $H^{\otimes 4}$ clearly preserves the stabilizer, as the two generators $X \otimes X \otimes X \otimes X$ and $Z \otimes Z \otimes Z \otimes Z$ are swapped. It also swaps logical Pauli operations $\overline{X}_1 \leftrightarrow \overline{Z}_2$ and $\overline{X}_2 \leftrightarrow \overline{Z}_1$. Thus it does logical Hadamard on both encoded qubits, plus it swaps the qubits.

$R^{\otimes 4}$ maps $Z \otimes Z \otimes Z \otimes Z$ to itself and $X \otimes X \otimes X \otimes X$ to $Y \otimes Y \otimes Y \otimes Y$ (the product of the two generators), so it is a valid encoded operation. It maps $\overline{Z}_1$ and $\overline{Z}_2$ to themselves and maps

$$\overline{X}_1 \mapsto Y \otimes Y \otimes I \otimes I = -\overline{X}_1\overline{Z}_2 \tag{10}$$
$$\overline{X}_2 \mapsto Y \otimes I \otimes Y \otimes I = -\overline{X}_2\overline{Z}_1. \tag{11}$$

Without the minus signs, we would recognize this as the controlled-Z operation between the two logical qubits ($|i\rangle|j\rangle \mapsto (-1)^{ij}|i\rangle|j\rangle$). With the minus signs, it becomes $Z_1 Z_2$ followed by controlled-Z, or an overall operation

$$|i\rangle|j\rangle \mapsto (-1)^{ij+i+j}|i\rangle|j\rangle. \tag{12}$$

The CNOT between two blocks is a valid transversal operation, as this is a CSS code, and performs logical CNOTs between the corresponding encoded qubits of each code. (That is, logical CNOT from the first encoded qubit of block 1 to the first encoded qubit of block 2, and similarly for the second encoded qubit.)

c) From problem 1a we have the stabilizer

$$\begin{array}{ccccc} Z^6 & Z^3 & Z^4 & Z & I \\ Z^4 & Z & Z & I & Z \\ X & X^2 & X^3 & X^4 & X^5 \\ X & X^4 & X^2 & X^2 & X^4 \end{array} \tag{13}$$

The logical X can be chosen from the discarded row of G_1: $\overline{X} = X \otimes X \otimes X \otimes X \otimes X$. The logical Z we must deduce by choosing a third row for H_1 that is orthogonal to H_2. We put H_2 in systematic form:

$$H_2' = \begin{pmatrix} 1 & 0 & 4 & 6 & 6 \\ 0 & 1 & 3 & 6 & 3 \end{pmatrix}, \tag{14}$$

and choose as $\overline{Z} = Z^3 \otimes Z^4 \otimes Z \otimes I \otimes I$.

The encoded SUM gate is automatic, as this is a CSS code: we simply perform a transversal SUM gate. (Actually, the logical scalar multiplication gates S_c are too, but we do not need them as part of our generating set.)

To find the remaining two logical gates (Fourier transform F and quadratic phase R), it will be convenient to change to an alternate pair of X generators of the stabilizer that are of the same form as the two Z generators — that is, with one I on the fourth or fifth position. This is because transversal gates will never change an I to something else, and we can use the fixed positions of the Is to narrow down our search. For instance, we can make the fifth qudit I by taking the first X generator squared times the second one: $X^3 \otimes X \otimes X \otimes X^3 \otimes I$. We can make the fourth qudit I by taking the first X generator times the second to the power -2: $X^6 \otimes X \otimes X^6 \otimes I \otimes X^4$. It is easy to see that the other X elements of these two forms are simply powers of these two elements. Thus we have the stabilizer generated by

$$\begin{array}{ccccc} Z^6 & Z^3 & Z^4 & Z & I \\ Z^4 & Z & Z & I & Z \\ X^3 & X & X & X^3 & I \\ X^6 & X & X^6 & I & X^4 \end{array} \tag{15}$$

For the logical Fourier transform F, we must map Xs to Zs in the logical operations. We can always find a Clifford group element that maps $X^a \mapsto Z^b$ for any two a and b, and can further choose that $Z \mapsto X^c$, but we cannot choose c, as it is determined by the commutation relation: $X^a Z = \omega^{-a} Z X^a$ and $Z^b X^c = \omega^{bc} X^c Z^b$, which tells us $c = -a/b$. (We can implement this Clifford group operation by Fourier transform followed by scalar multiplication by a/b.)

We then perform $X^3 \mapsto Z^6$ on the first qudit, $X \mapsto Z^3$ on the second qudit, $X \mapsto Z^4$ on the third qudit, and $X^3 \mapsto Z$ on the fourth qudit, and some other operation $X^4 \mapsto Z^r$ on the fifth qudit, with r yet to be specified. This maps the first X generator to the first Z generator. When we do this, the second X generator becomes $Z^5 \otimes Z^3 \otimes Z^3 \otimes I \otimes Z^r$, which we can recognize as the second Z generator cubed, with $r = 3$.

At the same time, we are transforming the Zs:

$$Z_1 \mapsto X_1^3 \tag{16}$$
$$Z_2 \mapsto X_2^2 \tag{17}$$
$$Z_3 \mapsto X_3^5 \tag{18}$$
$$Z_4 \mapsto X_4^4 \tag{19}$$
$$Z_5 \mapsto X_5. \tag{20}$$

The first Z generator then becomes $X^4 \otimes X^6 \otimes X^6 \otimes X^4 \otimes I$, which we can recognize as the first X generator to the sixth power. The second Z generator becomes $X^5 \otimes X^2 \otimes X^5 \otimes I \otimes X$, which is the second X generator squared. Thus, this gate gives us a valid encoded operation.

We can discover what it is by looking at the logical X and Z: $\overline{X} \mapsto \overline{X}' = Z^2 \otimes Z^3 \otimes Z^4 \otimes Z^5 \otimes Z^6$. We wish to write $\overline{X}'$ as some power of the original $\overline{Z}$ times an element of the stabilizer. Since a power of $\overline{Z}$ will still be I on the fourth and fifth qudits, we know that the relevant element of the stabilizer is the fifth power of the first Z generator times the sixth power of the second Z generator: $Z^5 \otimes I \otimes Z^5 \otimes Z^5 \otimes Z^6$. That is, $\overline{X}' = Z^4 \otimes Z^3 \otimes Z^6 \otimes I \otimes I = \overline{Z}^{-1}$.

Thus, the logical operation we are performing must be F^{-1}, so $\overline{Z} \mapsto \overline{X}$. We can check this without too much difficulty: $\overline{Z} \mapsto \overline{Z}' = X^2 \otimes X \otimes X^5 \otimes I \otimes I$. We can identify this as $\overline{X}$ times the square of the first X generator (in systematic form) times the fifth power of the second X generator.

For the logical R gate (quadratic phase gate), we will do some power of R on each qudit, since that maps $X \mapsto XZ^a$. Indeed, if we use the same powers as for the Fourier transform,

$$X_1 \mapsto X_1 Z_1^2 \tag{21}$$
$$X_2 \mapsto X_2 Z_2^3 \tag{22}$$
$$X_3 \mapsto X_3 Z_3^4 \tag{23}$$
$$X_4 \mapsto X_4 Z_4^5 \tag{24}$$
$$X_5 \mapsto X_5 Z_5^6, \tag{25}$$

We already know that the first X generator will be mapped to itself times the first Z generator, and the second X generator will be mapped to itself times the cube of the second Z generator. Therefore this is a valid transversal gate. We can identify it immediately as R^{-1}, since

$$\overline{X} \mapsto XZ^2 \otimes XZ^3 \otimes XZ^4 \otimes XZ^5 \otimes XZ^6 = \overline{XZ}^{-1}. \tag{26}$$

(The Z generators and $\overline{Z}$ get trivially mapped to themselves.)

This gives us SUM, F^{-1}, and R^{-1}, which is clearly also a generating set of the qudit Clifford group (e.g., $F = (F^{-1})^3$ and $R = (R^{-1})^6$). Therefore all Clifford group operations can be performed transversally on this code.