# Problem Set #3

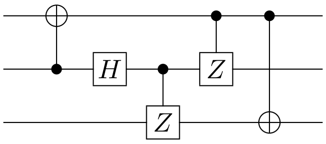
CO 639: Quantum Error Correction
Instructor: Daniel Gottesman

Due Tues., Feb. 24

Problem 1. Clifford Group Manipulations

a) Calculate the action of the two-qubit controlled-$Z$ gate and the controlled-$Y$ gate on the four generators of the two-qubit Pauli group ($X \otimes I$, $I \otimes X$, $Z \otimes I$, and $I \otimes Z$). Are either of these two gates in the Clifford group? The controlled-$U$ operation is a two-qubit gate that performs the unitary operation $U$ on the second qubit iff the first qubit is a $|1\rangle$. Note that the CNOT is a controlled-$X$ gate.

b) Compute the action of the following gate network on the six $\overline{X}$ and $\overline{Z}$ operators for three qubits.



c) Write down the unitary matrix corresponding to the gate network from part b).

d) Suppose the second and third qubits for the circuit from part b) are constrained to always start in an EPR pair (stabilizer generated by $X \otimes X$, $Z \otimes Z$). Can you simplify the action of the gate network on $\overline{X}$, $\overline{Z}$? (There is now only one of each.)

Problem 2. Generating the Clifford Group

In class, I claimed that the Clifford group is generated by the Hadamard transform $H$, the $\pi/4$ phase gate $P = \mathrm{diag}(1, i)$, and the CNOT gate acting on arbitrary pairs of qubits. In this problem you will prove this fact, and along the way give another proof that all linear operations which preserve the symplectic inner product correspond to Clifford group operations.

a) Suppose we have a general Clifford group operation $U$ mapping $X_i \mapsto \overline{X}_i$ and $Z_i \mapsto \overline{Z}_i$. Show that for any $n$-bit binary vectors $\vec{s}$ and $\vec{t}$, there exists a Clifford group operation mapping $X_i \mapsto (-1)^{s_i}\overline{X}_i$, $Z_i \mapsto (-1)^{t_i}\overline{Z}_i$. Based on this result, for the rest of the problem, we will ignore the signs of Pauli operators when determining whether a Clifford group operation exists and how to perform it.

b) For the one-qubit Pauli group, consider all 6 permutations of the 3 nonidentity Pauli operators, and show that all of them can be realized as products of $H$ (which maps $X \mapsto Z$ and $Z \mapsto X$) and $P$ (which maps $X \mapsto Y$ and $Z \mapsto Z$).

c) Use Clifford group arguments (i.e., following the transformations of Pauli operators) to show that the SWAP gate which interchanges two qubits can be realized as a sequence of 3 CNOT gates. Also, if you found that either or both of the two gates from problem 1a is or are in the Clifford group, show how to produce it or them from $H$, $P$, and CNOT.

d) Suppose $P$ and $Q$ are $n$-qubit Pauli operations and $\{P, Q\} = 0$. Show that there exists a series of SWAP gates and single-qubit Clifford group operations which maps $P \mapsto X \otimes P'$ and $Q \mapsto Z \otimes Q'$. Based on the previous two parts, we know this transformation can be done using just $H$, $P$, and CNOT.

e) Suppose we are given an arbitrary transformation $X_i \mapsto \overline{X}_i$ and $Z_i \mapsto \overline{Z}_i$ that satisfies the correct commutation relations. Based on the last part, we assume that $\overline{X}_1 = X \otimes P'$ and $\overline{Z}_1 = Z \otimes Q'$. Show that there exists a series of $H$, $P$, and CNOT operations that maps $X_1 \mapsto X \otimes P'$ and $Z_1 \mapsto Z \otimes Q'$. (We make no requirement at this stage on the transformation induced on the other $X_i$s or $Z_i$s.)

f) Call the Clifford group operation you produced in the previous part $U_1$. Then $U_1^\dagger$ maps $X \otimes P' \mapsto X_1$ and $Z \otimes Q' \mapsto Z_1$. Show that $U_1^\dagger$ maps $\overline{X}_i \mapsto I \otimes R_i$ and $\overline{Z}_i \mapsto I \otimes S_i$ $(i = 2, \ldots, n)$, and that $U_1$ therefore maps $I \otimes R_i \mapsto \overline{X}_i$ and $I \otimes S_i \mapsto \overline{Z}_i$. ($I$ being the identity on 1 qubit and $R_i$ and $S_i$ Pauli operators on $n-1$ qubits.)

g) Show that with $R_i$ and $S_i$ defined as per the last part, $[R_i, R_j] = [S_i, S_j] = [R_i, S_j] = 0$ when $i \neq j$, and $\{R_i, S_i\} = 0$. We can therefore consider the transformation on $n-1$ qubits mapping $X_i \mapsto R_{i+1}$, $Z_i \mapsto S_{i+1}$. Show that if there exists a Clifford group operation $V_2$ implementing this transformation, then $U_1(I \otimes V_2)$ performs the transformation $X_i \mapsto \overline{X}_i$ and $Z_i \mapsto \overline{Z}_i$ $(i = 1, \ldots, n)$.

h) Show by induction that $V_2$ can be realized as the product of $H$, $P$, and CNOT, and that therefore any Clifford group gate can be. What is the asymptotic number of gates used to realize an $n$-qubit Clifford group operation? (Ignore constants; only the $O(f(n))$ answer is required.)

i) Use the above construction to give an encoding circuit for the 5-qubit code. Note that you can consider this as a special case of the above construction by writing down a Clifford group operation that maps $Z_i$ $(i = 1, \ldots, 4)$ to the four generators of the stabilizer of the 5-qubit code. $X_5 \mapsto \overline{X}$ for the code, and $Z_5 \mapsto \overline{Z}$. The images of $X_i$ $(i = 1, \ldots, 4)$ are arbitrary, so long as they satisfy the appropriate commutation relations. This will produce a circuit that, when it acts on the input $|0000\rangle \otimes |\psi\rangle$ produces $|\overline{\psi}\rangle$, the encoded $|\psi\rangle$ state. Clearly this encoding circuit is not unique.

Problem 3. Using the Quantum MacWilliams Identity

Recall that, for a QECC with projector $\Pi$ on the coding subspace ($\operatorname{Tr} \Pi = 2^k$), we define

$$A_d = \frac{1}{2^{2k}} \sum_{E_d} \operatorname{Tr}(E_d \Pi) \operatorname{Tr}(E_d^\dagger \Pi) \tag{1}$$

$$B_d = \frac{1}{2^k} \sum_{E_d} \operatorname{Tr}(E_d \Pi E_d^\dagger \Pi), \tag{2}$$

where the sums are taken over Pauli operators $E_d$ of weight $d$. The quantum MacWilliams identity gives a relationship between $A(z) = \sum_d A_d z^d$ and $B(z) = \sum_d B_d z^d$.

a) Show that, for a general QECC, $B_d \geq A_d \geq 0$, and that $A_0 = B_0 = 1$. (Hint: Use the Cauchy-Schwarz inequality.)

b) Show that if a QECC has distance $d$, then $A_c = B_c$ for $c < d$. (We showed this in class only for stabilizer codes.)

c) The quantum Singleton bound allows a $[[3, 1, 2]]$ QECC. Write down the quantum MacWilliams identity for a QECC encoding 1 qubit in 3 qubits. Parts a and b put additional constraints on the $A_c$s and $B_c$s. Show that there is a single solution to all of these constraints, and find it. It turns out, however, that there is no $[[3, 1, 2]]$ QECC, and we shall see this in the next problem. (Note: I am being sloppy with notation here; really a $[[3, 1, 2]]$ code would have to be a stabilizer code. I instead want you in this part and the last part of the next problem to show that there is no distance 2 QECC encoding 1 qubit in 3 qubits. The correct notation for such a code would be $((3, 2, 2))$.).

Problem 4. The Quantum Shadow Enumerator

For a stabilizer code $S$, let $S_{\text{even}}$ be the set of $M \in S$ with even weight and let $S_{\text{odd}}$ be the set of $M \in S$ with odd weight. Then define the shadow $Sh(S)$ to be the set of Pauli operators $E$ such that $E$ commutes with all elements of $S_{\text{even}}$ and $E$ anticommutes with all elements of $S_{\text{odd}}$.

a) Let $Y^{\otimes n} = Y \otimes \cdots \otimes Y$ be the Pauli operator $Y$ acting on all $n$ qubits. We can define the shadow enumerator for a general QECC to be $Sh(z) = \sum_d Sh_d z^d$, with

$$Sh_d = \frac{1}{2^k} \sum_{E_d} \mathrm{Tr}(E_d \Pi E_d^\dagger Y^{\otimes n} \Pi^* Y^{\otimes n}), \tag{3}$$

where $\Pi^*$ is the complex conjugate of the projector $\Pi$. Show $Sh_d \geq 0$ for a general QECC. Show that for a stabilizer code, $Sh_d$ is the number of elements of weight $d$ in the shadow $Sh(S)$.

b) Note that of the one-qubit Pauli operators, only $Y$ has complex entries in its matrix, and that therefore a tensor product of Pauli operators is real iff it contains an even number of $Y$s. We say a stabilizer code is real iff all elements of the stabilizer are real (which implies that the projection on the code space is real too). Show that $S$ is real iff $Y^{\otimes n} \in Sh(S)$.

c) For a general QECC,

$$Sh(z) = \frac{1}{2^{n-k}} (1+3z)^n A\left(\frac{z-1}{1+3z}\right). \tag{4}$$

(We will not show this.) Note that this differs from the quantum MacWilliams identity only in the appearance of $z-1$ as the numerator of the argument of $A$ instead of $1-z$. Show that $Sh_n > 0$, and so the shadow of a stabilizer code always contains an element of maximum weight. (Hint: $\lim_{z\to\infty} Sh(z)/z^n = Sh_n$.)

d) Show that if a single-qubit Clifford gate $U$ acts on one qubit of a stabilizer code $S$ to give the code $U(S)$, then $U(Sh(S)) = Sh(U(S))$. Using this result and parts b and c, show that every stabilizer code is equivalent to a real code. What if $U$ is a multiple-qubit operation, such as CNOT?

e) Write down the consequences of eq. (4) for a $[[3,1]]$ QECC, and consider the constraints imposed by $Sh_d \geq 0$. Combine these constraints with the result of problem 3c and show that no $[[3,1,2]]$ QECC exists.