Ph/CS 219b Winter 2020 **Problem Set 1**
Prof. Fernando Brandão
fbrandao@caltech.edu

Due: 5:00pm, 01/28/2020

---

1 CSS Codes [10 Points]

In class, we saw how to construct that $[7, 4, 3]$ Hamming code and its $[7, 3, 4]$ dual code. From this pair of classical linear codes, we constructed a $[[7, 1, 3]]$ Calderbank-Shor-Steane (CSS) quantum code.

(a) Using a similar method as in the construction of the [7,4,3] code, construct a $[15, 11, 3]$ classical linear code, and find its dual code. From this pair of classical codes, show that a $[[15, 7, 3]]$ CSS quantum code can be constructed. (HINT: In class, it was important that all columns of the parity check matrix of the [7,4,3] code were distinct.)

(b) Generalizing this construction further, construct a $[[n, k, 3]]$ CSS code, where $n = 2^m - 1$, $k = n - 2m$, and $m \geq 3$ is an integer.

2 More CSS Codes [10 points]

In class, we saw that for some stabilizer group $\mathcal{S}$, we can construct the normalizer $\mathcal{N}(\mathcal{S})$, and because $\mathcal{S}$ is normal in $\mathcal{N}(\mathcal{S})$ we can construct the quotient group $\mathcal{N}(\mathcal{S})/\mathcal{S}$ which represents equivalence classes of transformations which map the codespace to itself.

To make it easier to work with, we can further simplify our normalizer by quotienting by $-I$ to get rid of any meaningless signs. We denote this reduced normalizer as $\hat{\mathcal{N}}(\mathcal{S}) = \mathcal{N}(\mathcal{S})/\{-I\}$. This simply identifies any Pauli $N \in \mathcal{N}(\mathcal{S})$ with its negative $-N$. This way, we can see that the reduced logical group $\hat{\mathcal{N}}(\mathcal{S})/\mathcal{S}$ can simply be generated by a logical X operator and a logical Z operator on any qubit: $\hat{\mathcal{N}}(\mathcal{S})/\mathcal{S} = \langle \overline{X}_i, \overline{Z}_i \rangle_{i=1}^k$. This is the most compact description we can give for the set of logical transformations of the encoded qubits in the codespace.

(a) Find a pair $\left(\overline{X}, \overline{Z}\right)$ of generators for $\hat{\mathcal{N}}(\mathcal{S})/\mathcal{S}$ for the 9-qubit Shor code.

(b) Consider the binary matrix

$$\delta = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}. \tag{1}$$

Let us associate to each row j an X-type stabilizer

$$M_j = \prod_{l=1}^{5} X_l^{\delta_{j,l}} \tag{2}$$

and to each column a Z-type stabilizer

$$N_j = \prod_{l=1}^{5} Z_l^{\delta_{j,l}}. \tag{3}$$

Use that $\delta^2 = 0 \bmod 2$ to argue that $\{M_j, N_j\}_j$ defines a stabilizer code $\mathcal{Q}$.

For the rest of this problem, it will be useful to have read sections 7.9.3 and 7.9.4 of Preskill's notes if you attempt this before that section is covered in class (with particular attention paid to 7.9.4d).

(c) Find parity-check matrices H_1 and H_2 such that $\mathcal{Q}$ is $CSS(H_1, H_2)$. Find associated generator matrices G_1 and G_2. Use this to find a set of generators for $\hat{\mathcal{N}}(\mathcal{S})/\mathcal{S}$ (grouped into pairs $\{(\overline{X}_i, \overline{Z}_i)\}$).

(d) What is the distance of this code?

(e) Give an algorithm which, starting from the parity check matrices H_1 and H_2 of a general CSS code, computes a set of generators for $\hat{\mathcal{N}}(\mathcal{S})/\mathcal{S}$ (grouped into pairs $\{(\overline{X}_i, \overline{Z}_i)\}$). Show, in particular, that we can always choose each $\overline{X}_i$ as an X-type operator (made up of only X or I on physical qubits), and each $\overline{Z}_i$ as a Z-type operator (made up of only Z or I on physical qubits).

3 Permutation-Invariant Codes [10 Points]

Recall that the group S_n of permutations acts unitarily on the space of n-qubits by permuting them. That is, for $\pi \in S_n$ we can define the unitary U_π by

$$U_\pi \left(|\phi_1\rangle \otimes ... \otimes |\phi_n\rangle \right) = |\phi_{\pi^{-1}(1)}\rangle \otimes ... \otimes |\phi_{\pi^{-1}(n)}\rangle \tag{4}$$

for all product states $|\phi_1\rangle \otimes ... \otimes |\phi_n\rangle$ (and linearly extended to all of $(\mathbb{C}^2)^{\otimes n}$). Let $(ij) \in S_n$ denote the transposition of $i \neq j$ and define the subspace

$$\mathcal{Q} = \{|\Psi\rangle \in ((\mathbb{C}^2)^{\otimes n}) | U_{(ij)} |\Psi\rangle = |\Psi\rangle \,,\ \forall i \neq j\}. \tag{5}$$

(a) Give a basis of $\mathcal{Q}$. What is the projector P onto $\mathcal{Q}$? Express it as a linear combination of the operators U_π, $\pi \in S_n$.

(b) Show that the set of errors

$$\mathcal{E} = \left\{ \sum_{\pi \in S_n} a_\pi U_\pi | (a_\pi) \in \mathbb{C} \right\} \tag{6}$$

is correctable. Is the code degenerate? Find an operator basis $\{F_j\}_j$ of $\mathcal{E}$ which diagonalizes the matrix C_{ab}.

(c) Show that a single bit flip, e.g. $E = X_1$, is undetectable.

(d) Show that $E = X^{\otimes n}$ is an undetectable error. More generally, argue that for any $U \in SU(2^n)$, $U \neq I$, the error $E = U^{\otimes n}$ satisfies

- (i) $E\mathcal{Q} = \mathcal{Q}$ (Hint: use the fact that $[U^{\otimes n}, U_\pi] = 0$ for all $U \in SU(2)$ and $\pi \in S_n$ according to a result called Schur-Weyl duality).
- (ii) E is an undetectable error.

4 Generating the Clifford Group [10 Points]

Recall that in class, we gave the following definition of the Pauli group on n qubits:

$$G_n = \{I, X, Y, Z\} \times \{\pm 1\}, \tag{7}$$

where, $Y = ZX$ was chosen to be real and anti-hermitian so that we didn't have to worry about complex phases.

The 'full' definition of the n-qubit *Pauli group* is defined as

$$\mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n} \times \{\pm 1, \pm i\} \tag{8}$$

where, here, $Y = iXZ$ is its 'usual' complex hermitian operator self. So, each element of $\mathcal{P}_n$ is (with an overall phase $\pm 1, \pm i$) a tensor product of Pauli matrices and identity matrices acting on the n qubits. The n-qubit Clifford group $\mathcal{C}_n$ is the *normalizer* of the Pauli group – a unitary operator U acting on n qubits is contained in $\mathcal{C}_n$ if and only if

$$UMU^\dagger \in \mathcal{P}_n, \ \forall \ M \in \mathcal{P}_n \tag{9}$$

That is, U acting by conjugation takes a tensor product of Pauli matrices to a tensor product of Pauli matrices. Actually, an element of the Clifford group is defined as this action by conjugation, so that the overall phase of U is not relevant.

In this exercise, you will show that the Clifford group can be generated by three quantum gates: the single-qubit gates H and S, and the two-qubit gate CNOT $= \Lambda(X)$. Here H denotes the Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{10}$$

(a rotation by π about the axis $\hat{x} + \hat{z}$), and S denotes the phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \tag{11}$$

(a rotation by $\pi/2$ about the $\hat{z}$ axis).

It follows that quantum circuits constructed from these gates can be efficiently simulated by a classical computer, because the action of $\mathcal{C}_n$ on $\mathcal{P}_n$ can be succinctly described and easily updated after each gate.

(a) Compute how H, S, and $\Lambda(X)$ act on Pauli operators by conjugation, and verify that H and S are in $\mathcal{C}_1$ and that $\Lambda(X)$ is in $\mathcal{C}_2$.

(b) Show that H and S generate $\mathcal{C}_1$. (Hint: Note that the elements of the one-qubit Clifford group are the permutations of X, Y, Z, with minus signs appropriately chosen so that the product $XYZ = iI$ remains invariant).

(c) Let $\Lambda(X)$ denote the two-qubit gate that applies σ to the target qubit if the control qubit is $|1\rangle$, and acts trivially if the control qubit is $|0\rangle$. Let σ_j denote σ acting on qubit j. Show that $\Lambda(Z)$ and $\Lambda(Y)$ can be constructed from $\Lambda(X)$, H and S. Show that

$$\Lambda(\sigma) Z_1 \Lambda(\sigma) = Z_1, \quad \Lambda(\sigma) X_1 \Lambda(\sigma) = X_1 \sigma_2, \tag{12}$$

where qubit 1 is the control of the $\Lambda(\sigma)$ and qubit 2 is its target. Here $\Lambda(\sigma)$ is one of X, Y, Z, so that in particular $\sigma^2 = I$.

We will prove that H, S, and $\Lambda(X)$ generate $\mathcal{C}_n$ by induction. We have already shown (b). Now assume, as an inductive hypothesis, that H, S, and $\Lambda(X)$ generate $\mathcal{C}_n$. We need to show that they generate $\mathcal{C}_{n+1}$.

(d) Suppose that U is an element of $\mathcal{C}_{n+1}$. Show that there is a W generated by H, S, and $\Lambda(X)$ such that the action of WU by conjugation is

$$WU: \quad X_1 \to X_1 M \tag{13}$$
$$Z_1 \to Z_1 N, \tag{14}$$

where each of M, N is a tensor product of Pauli matrices acting on qubits 2 through $n+1$.

(e) Now consider

$$V \equiv \Lambda(M) H_1 \Lambda(N) H_1 W U, \tag{15}$$

where $\Lambda(M)$ denotes the transformation controlled by the first qubit that applied M to the other n qubits, and similarly for $\Lambda(N)$. Note that $\Lambda(M)$ and $\Lambda(N)$ can be constructed from H, S, and $\Lambda(X)$. It follows from (c) that the action of $\Lambda(M)$ by conjguation is

$$\Lambda(M): X_1 \quad \to \quad X_1 M \tag{16}$$
$$Z_1 \quad \to \quad Z_1. \tag{17}$$

Show that the action of V by conjugation is

$$V: \quad X_1 \to X_1 \tag{18}$$
$$Z_1 \to Z_1. \tag{19}$$

(f) Show that V is in $\mathcal{C}_n$, and therefore can be constructed from H, S, and $\Lambda(X)$. Show that U can also be constructed from H, S, and $\Lambda(X)$. This completes the inductive step, and the proof.
