

CSS Construction - An Operator Perspective

Narayanan Rengaswamy
Department of ECE, Duke University, USA

Oct. 9, 2017

The purpose of this article is to understand the construction of a Calderbank-Shor-Steane (CSS) quantum code \mathcal{Q} [1] from classical codes \mathcal{C}_1 and \mathcal{C}_2 , satisfying $\mathcal{C}_2 \subseteq \mathcal{C}_1$, by giving explicit forms for the stabilizers and logical operators of \mathcal{Q} in terms of the rows of the generator and parity-check matrices of \mathcal{C}_1 and \mathcal{C}_2 . We will denote a vector u as \underline{u} and use the notation $[k] \triangleq \{1, 2, \dots, k\}$. Let us begin by reviewing stabilizer codes.

1 Stabilizer Codes: A Quick Review

Define the single qubit operators

$$I \triangleq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y \triangleq iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

where $i \triangleq \sqrt{-1}$. X and Z satisfy $X|x\rangle = |x \oplus 1\rangle$, $Z|x\rangle = (-1)^x|x\rangle$ for $x \in \{0, 1\}$. Each of them is unitary and Hermitian, so we have $P^2 = I$ for $P \in \{I, X, Y, Z\}$. These are called the *Pauli* operators on a single qubit and form the group

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}.$$

The Pauli group on n qubits is defined as

$$G_n \triangleq \{A_1 \otimes A_2 \otimes \dots \otimes A_n : A_i \in G_1, i \in [n]\},$$

where \otimes denotes the Kronecker product on matrices. Suppose S is a subgroup of G_n and let V_S be the subspace of n -qubit states that are fixed by the elements of S , i.e. $\mathbf{g}|\psi\rangle = |\psi\rangle \forall \psi \in V_S, \mathbf{g} \in S$. Then V_S is said to be *stabilized* by S and S is called the *stabilizer* of the subspace V_S . If $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \in G_n$ are independent and generate the group S then they are called *generators* for S , denoted as

$$S = \langle \mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_k \rangle.$$

It can be shown that V_S is a non-trivial subspace if the elements of S commute and $-I_n \notin S$, where I_n is the $n \times n$ identity matrix. The subspace V_S of quantum states stabilized by S is said to be the *stabilizer code* described uniquely by S . Given k generators, the space V_S has dimension 2^{n-k} .

Since a stabilizer code is used to encode logical states, we need to be able to transform a universal set of logical qubit operations into an equivalent set of operations in the code domain, which is often called the *physical* domain. In other words, for every logical operator we have we need to find a physical operator that executes that operation in the code domain. Hence, for practical purposes, an appropriate subgroup S of G_n along with the definition of such physical operators completes the description of a stabilizer code, although the code itself is defined simply by S .

2 CSS Code from Self-Orthogonal Codes

First let us consider CSS codes constructed from classical codes \mathcal{C}_1 and \mathcal{C}_2 that satisfy $\mathcal{C}_2 = \mathcal{C}_1^\perp$, so that \mathcal{C}_2 is a self-orthogonal code.

2.1 Binary Self-Orthogonal Codes

Let $\mathcal{C}^\perp \subset \mathbb{F}_2^n$ be an $[n, k]$ classical binary self-orthogonal code with generator and parity-check matrices $G_{\mathcal{C}^\perp}$ and $H_{\mathcal{C}^\perp}$ respectively. Then it is contained its dual \mathcal{C} which is an $[n, n - k]$ classical binary code with generator and parity-check matrices $G_{\mathcal{C}} = H_{\mathcal{C}^\perp}$ and $H_{\mathcal{C}} = G_{\mathcal{C}^\perp}$ respectively. Since $\mathcal{C}^\perp \subseteq \mathcal{C}$ we immediately have $k \leq \frac{n}{2}$, so that \mathcal{C} has rate at least $1/2$. As \mathcal{C} is a subgroup of \mathbb{F}_2^n and \mathcal{C}^\perp is a subgroup of \mathcal{C} , the quotient group $\mathcal{C}/\mathcal{C}^\perp$ is the set of all *distinct* cosets of \mathcal{C}^\perp in \mathcal{C} ,

$$\mathcal{C}/\mathcal{C}^\perp = \left\{ \{\underline{u} + \mathcal{C}^\perp\} : \underline{u} \in \{0\} \cup (\mathcal{C} \setminus \mathcal{C}^\perp) \right\}.$$

From each coset $\{\underline{u} + \mathcal{C}^\perp\}$ select a vector \underline{v} as the *representative* of that coset. Then the group $\mathcal{C}/\mathcal{C}^\perp$ is isomorphic to the group of all such representatives \underline{v} and we will denote this group as $\mathcal{C}/\mathcal{C}^\perp$ as well. Since this group is also a subspace of \mathbb{F}_2^n over the field \mathbb{F}_2 , we can find a basis for it. Let $G_{\mathcal{C}/\mathcal{C}^\perp}$ be the matrix whose rows form a basis for the group $\mathcal{C}/\mathcal{C}^\perp$. Then, since \mathcal{C} is a self-orthogonal code we can split the rows of its generator matrix to obtain the form

$$G_{\mathcal{C}} = \begin{bmatrix} H_{\mathcal{C}} \\ G_{\mathcal{C}/\mathcal{C}^\perp} \end{bmatrix}_{(n-k) \times n} = \begin{bmatrix} G_{\mathcal{C}^\perp} \\ G_{\mathcal{C}/\mathcal{C}^\perp} \end{bmatrix}_{(n-k) \times n}, \quad (1)$$

where $H_{\mathcal{C}} = G_{\mathcal{C}^\perp}$ is a $k \times n$ matrix and $G_{\mathcal{C}/\mathcal{C}^\perp}$ is a $(n - 2k) \times n$ matrix. Note that there is no unique choice for $G_{\mathcal{C}/\mathcal{C}^\perp}$ as there could be multiple bases for a vector space. Denote the rows of $H_{\mathcal{C}}$ as \underline{g}_i for $i = 1, 2, \dots, k$ and the rows of $G_{\mathcal{C}/\mathcal{C}^\perp}$ as \underline{h}_i for $i = 1, 2, \dots, n - 2k$. Then for some $\underline{x} \in \{0, 1\}^{n-2k}$ a coset representative \underline{v} can be expressed as

$$\underline{v} = \sum_{i=1}^{n-2k} x_i \underline{h}_i. \quad (2)$$

Example

Let \mathcal{C} be the $[6, 5, 2]$ single-parity check code with $n = 6, k = 1$ and minimum distance $d = 2$. The dual code \mathcal{C}^\perp is the $[6, 1, 6]$ repetition code of length $n = 6$ which contains only two codewords: $\mathcal{C}^\perp = \{000000, 111111\}$. So $G_{\mathcal{C}^\perp} = H_{\mathcal{C}} = [1 \ 1 \ 1 \ 1 \ 1 \ 1]$. This implies \mathcal{C} contains all length 6 binary vectors that contain an even number of 1s. One possible generator matrix for \mathcal{C} is

$$G_{\mathcal{C}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \underline{g}_1 \\ \underline{h}_1 \\ \underline{h}_2 \\ \underline{h}_3 \\ \underline{h}_4 \end{bmatrix} ; \quad G_{\mathcal{C}/\mathcal{C}^\perp} \triangleq \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$$

So the group $\mathcal{C}/\mathcal{C}^\perp$ of 16 coset representatives is generated by binary linear combinations of the rows of $G_{\mathcal{C}/\mathcal{C}^\perp}$.

2.2 Construction of the CSS Code

Given an $[n, n - k]$ classical binary code \mathcal{C} that contains its dual \mathcal{C}^\perp , the CSS quantum code \mathcal{Q} is constructed as follows. Let $\underline{v} \in \mathbb{F}_2^n$ be a length- n binary vector. Then the quantum state corresponding to this vector is defined as

$$|\psi_v\rangle \equiv \left| \underline{v} + \mathcal{C}^\perp \right\rangle \triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c} + \underline{v}\rangle, \quad (3)$$

where $\underline{c} + \underline{v} = \underline{c} \oplus \underline{v}$ is component-wise binary addition of vectors. Note that the vectors $\underline{c} + \underline{v}$ for all $\underline{c} \in \mathcal{C}^\perp$ generate the coset $\underline{v} + \mathcal{C}^\perp$ and hence the notation for the quantum state.

The CSS code \mathcal{Q} is defined as the collection of all such *distinct* quantum states generated by the coset representatives $\underline{v} \in \mathcal{C}/\mathcal{C}^\perp$. As $|\mathcal{C}| = 2^{n-k}$ and $|\mathcal{C}^\perp| = 2^k$, by Lagrange's theorem we have $|\mathcal{C}/\mathcal{C}^\perp| = 2^{n-2k}$ and so the (binary) dimension of $\mathcal{C}/\mathcal{C}^\perp$ is $n - 2k$. Since each bit of \underline{v} corresponds to a qubit of $|\psi_v\rangle$, which has dimension 2, the dimension of the quantum code \mathcal{Q} is 2^{n-2k} . Formally we write \mathcal{Q} is an $[[n, n - 2k]]$ CSS quantum code.

Now recall from (2) that a coset representative can be expressed as $\underline{v} = \underline{x} \cdot G_{\mathcal{C}/\mathcal{C}^\perp}$. So if we have a $(n - 2k)$ -qubit state $|\underline{x}\rangle_L$, called the *logical* state, then the CSS code will encode this into the quantum state

$$|\psi_x\rangle \equiv \left| \underline{x} \cdot G_{\mathcal{C}/\mathcal{C}^\perp} + \mathcal{C}^\perp \right\rangle \triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \left| \underline{c} + \underline{x} \cdot G_{\mathcal{C}/\mathcal{C}^\perp} \right\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \left| \underline{c} + \sum_{i=1}^{n-2k} x_i \underline{h}_i \right\rangle, \quad (4)$$

where \underline{h}_i form the rows of $G_{\mathcal{C}/\mathcal{C}^\perp}$. The logical state $|\underline{x}\rangle_L$ is also called the *encoded* state and its $(n - 2k)$ component qubits are called *encoded* qubits.

Example

Consider again our example of the $[6, 5]$ single-parity check code with $n = 6, k = 1$. The CSS construction gives us a $[[6, 4]]$ quantum code \mathcal{Q} with the states defined as

$$|\psi_x\rangle = \frac{1}{\sqrt{2}} \left| (000000) + \sum_{i=1}^4 x_i \underline{h}_i \right\rangle + \frac{1}{\sqrt{2}} \left| (111111) + \sum_{i=1}^4 x_i \underline{h}_i \right\rangle ; \quad \underline{x} \in \{0, 1\}^4.$$

2.3 Stabilizer for the CSS Code

Consider an $[[n, n - 2k]]$ CSS code \mathcal{Q} defined using an $[n, n - k]$ classical binary code \mathcal{C} that contains its dual \mathcal{C}^\perp . We will now demonstrate that it is indeed a stabilizer code and give the set of generators for its stabilizer. Particularly, if we can find commuting operators $\mathbf{g}_1, \mathbf{g}_2, \dots, \mathbf{g}_{2k}$ such that they do not generate $-I_n$ and satisfy $\mathbf{g}_i |\psi_v\rangle = |\psi_v\rangle \quad \forall |\psi_v\rangle \in \mathcal{Q}, i = 1, 2, \dots, 2k$ then we have defined the stabilizer of \mathcal{Q} .

Consider the generator matrix representation for \mathcal{C} given in (1). Again, denote the rows of $H_{\mathcal{C}}$ as $\underline{g}_1, \underline{g}_2, \dots, \underline{g}_k$. Then for $i \in [k]$ we have $\underline{g}_i \cdot \underline{v} = 0$ for all $\underline{v} \in \mathcal{C}$ and particularly for all $\underline{v} \in \mathcal{C}/\mathcal{C}^\perp$, which are the vectors that define the states in \mathcal{Q} . Denote the elements of the vector \underline{g}_i as g_{it} so that $\underline{g}_i = [g_{i1}, g_{i2}, \dots, g_{in}]$. Now define the $2k$ operators

$$\mathbf{g}_i^X \triangleq \bigotimes_{t=1}^n X_t^{g_{it}} \quad ; \quad \mathbf{g}_i^Z \triangleq \bigotimes_{t=1}^n Z_t^{g_{it}} \quad ; \quad i = 1, 2, \dots, k \quad (5)$$

where $X_t = X$ and $Z_t = Z$ denote the X and Z operators, respectively, on the t -th physical qubit.

Theorem 1. *The set of $2k$ n -qubit operators $\mathbf{g}_i^X, \mathbf{g}_i^Z$ defined in (5) commute with each other and do not generate $-I_n$.*

Proof. Since the X operator trivially commutes with itself and similarly the Z operator commutes with itself, it is clear that $\mathbf{g}_i^X \mathbf{g}_j^X = \mathbf{g}_j^X \mathbf{g}_i^X$ and $\mathbf{g}_i^Z \mathbf{g}_j^Z = \mathbf{g}_j^Z \mathbf{g}_i^Z$ for all $i, j \in [k]$. This is written in commutation notation as

$$[\mathbf{g}_i^X, \mathbf{g}_j^X] = \mathbf{0} \quad , \quad [\mathbf{g}_i^Z, \mathbf{g}_j^Z] = \mathbf{0},$$

where $\mathbf{0}$ is the zero operator, i.e. a matrix with all entries set to 0.

However, the X operator anti-commutes with the Z operator so that $XZ = -ZX$. So to check if \mathbf{g}_i^X and \mathbf{g}_j^Z commute or anti-commute we only have to count the number of indices t with $g_{it} = 1$ and $g_{jt} = 1$. Now observe that since \mathcal{C}^\perp is a self-orthogonal code and $\underline{g}_i \in \mathcal{C}^\perp$, we have $\underline{g}_i \cdot \underline{g}_j = 0 \forall i, j \in [k]$. This implies $b_{ij} \triangleq |\{t \in [n] : g_{it} = 1, g_{jt} = 1\}|$ is even. Hence we see that for all $i, j \in [k]$ we have

$$\mathbf{g}_i^X \mathbf{g}_j^Z = (-1)^{b_{ij}} \mathbf{g}_j^Z \mathbf{g}_i^X = \mathbf{g}_j^Z \mathbf{g}_i^X \Rightarrow [\mathbf{g}_i^X, \mathbf{g}_j^Z] = \mathbf{0}.$$

Thus we see that the above defined set of $2k$ operators commute with each other and clearly do not generate $-I_n$. \square

So these operators generate a valid stabilizer S for some subspace V_S of n qubits. We are left only to verify that $V_S = \mathcal{Q}$.

Theorem 2. *The set of $2k$ n -qubit operators $\mathbf{g}_i^X, \mathbf{g}_i^Z$ defined in (5) generate the stabilizer for the CSS code \mathcal{Q} .*

Proof. First we observe that since X is a bit-flip operator satisfying $X|0\rangle = |0+1\rangle = |1\rangle$, $X|1\rangle = |1+1\rangle = |0\rangle$, the operator \mathbf{g}_i^X satisfies

$$\mathbf{g}_i^X |\underline{u}\rangle = |\underline{u} + \underline{g}_i\rangle$$

for any vector $\underline{u} \in \{0, 1\}^n$, where $\underline{g}_i \in \mathcal{C}^\perp$ is the row of H_C used to define \mathbf{g}_i^X in (5). Since $\underline{c} + \underline{g}_i \in \mathcal{C}^\perp$ for all $\underline{c} \in \mathcal{C}^\perp$ we have

$$\mathbf{g}_i^X |\psi_v\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \mathbf{g}_i^X |\underline{c} + \underline{v}\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |(\underline{c} + \underline{g}_i) + \underline{v}\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c} + \underline{v}\rangle = |\psi_v\rangle.$$

Similarly, since Z is a phase-flip operator satisfying $X|0\rangle = |0\rangle$, $X|1\rangle = -|1\rangle$, the operator \mathbf{g}_i^Z satisfies

$$\mathbf{g}_i^Z |\underline{u}\rangle = (-1)^{\underline{g}_i \cdot \underline{u}} |\underline{u}\rangle$$

for any vector $\underline{u} \in \{0, 1\}^n$. In each term of the superposition in the CSS state $|\psi_v\rangle$, we observe that $\underline{c} + \underline{v} \in \mathcal{C}$. As \underline{g}_i is a row of the parity-check matrix of \mathcal{C} it automatically satisfies $\underline{g}_i \cdot (\underline{c} + \underline{v}) = 0$. Therefore we have

$$\mathbf{g}_i^Z |\psi_v\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \mathbf{g}_i^Z |\underline{c} + \underline{v}\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} (-1)^{\underline{g}_i \cdot (\underline{c} + \underline{v})} |\underline{c} + \underline{v}\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c} + \underline{v}\rangle = |\psi_v\rangle.$$

Thus we have shown that all the $2k$ operators $\mathbf{g}_i^X, \mathbf{g}_i^Z$ defined in (5) stabilize the states $|\psi_v\rangle \in \mathcal{Q}$. Also, the dimension of the space V_S stabilized by the group generated by $\{\mathbf{g}_i^X, \mathbf{g}_i^Z ; i \in [k]\}$ is 2^{n-2k} , which is exactly the dimension of \mathcal{Q} too. Therefore $V_S = \mathcal{Q}$. \square

Example

For our running example of the $[[6, 4]]$ CSS code, we have $k = 1$ and $\underline{g}_1 = [1 \ 1 \ 1 \ 1 \ 1 \ 1]$. This gives the stabilizers

$$\mathbf{g}_1^X \triangleq X_1 X_2 X_3 X_4 X_5 X_6 = X^{\otimes 6} \quad , \quad \mathbf{g}_1^Z \triangleq Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 = Z^{\otimes 6}.$$

Clearly we have

$$\mathbf{g}_1^X \mathbf{g}_1^Z = X^{\otimes 6} Z^{\otimes 6} = (XZ)^{\otimes 6} = (-1)^6 (ZX)^{\otimes 6} = Z^{\otimes 6} X^{\otimes 6} = \mathbf{g}_1^Z \mathbf{g}_1^X.$$

2.4 Logical Operators for the CSS Code

We will begin by defining the logical Pauli operators for each of the $(n - 2k)$ logical qubits in the CSS code \mathcal{Q} . Let us now reiterate the representation of the generator matrix for the code \mathcal{C} from (1):

$$G_{\mathcal{C}} = \begin{bmatrix} H_{\mathcal{C}} \\ G_{\mathcal{C}/\mathcal{C}^\perp} \end{bmatrix}_{(n-k) \times n} = \begin{bmatrix} G_{\mathcal{C}^\perp} \\ G_{\mathcal{C}/\mathcal{C}^\perp} \end{bmatrix}_{(n-k) \times n},$$

where $H_{\mathcal{C}} = G_{\mathcal{C}^\perp}$ is a $k \times n$ matrix and $G_{\mathcal{C}/\mathcal{C}^\perp}$ is a $(n - 2k) \times n$ matrix. The $(n - 2k)$ logical Pauli operators $\bar{X}_i, \bar{Z}_i, i \in [n - 2k]$ are defined from the rows of the generator matrix for $\mathcal{C}/\mathcal{C}^\perp$ represented above as $G_{\mathcal{C}/\mathcal{C}^\perp}$. However, the logical operators need to satisfy the (anti-)commutation conditions

$$\bar{X}_i \bar{Z}_j = \begin{cases} -\bar{Z}_j \bar{X}_i & \text{if } i = j, \\ \bar{Z}_j \bar{X}_i & \text{if } i \neq j. \end{cases} \quad (6)$$

So for a general CSS code we might need two generator matrices for $\mathcal{C}/\mathcal{C}^\perp$ which we represent as $G_{\mathcal{C}/\mathcal{C}^\perp}^X, G_{\mathcal{C}/\mathcal{C}^\perp}^Z$ because they will be used to define the logical X and logical Z operators respectively. Denote the rows of $G_{\mathcal{C}/\mathcal{C}^\perp}^X$ as $\underline{h}_1, \dots, \underline{h}_{n-2k}$ and the rows of $G_{\mathcal{C}/\mathcal{C}^\perp}^Z$ as $\underline{h}'_1, \dots, \underline{h}'_{n-2k}$. The entries of \underline{h}_i are denoted as h_{i1}, \dots, h_{in} and similarly the entries of \underline{h}'_i are denoted as h'_{i1}, \dots, h'_{in} . Then the logical Pauli operators are defined as

$$\bar{X}_i \triangleq \bigotimes_{t=1}^n X_t^{h_{it}} \quad , \quad \bar{Z}_i \triangleq \bigotimes_{t=1}^n Z_t^{h'_{it}} \quad , \quad \bar{Y}_i \triangleq (\sqrt{-1}) \bar{X}_i \bar{Z}_i. \quad (7)$$

for $i = 1, 2, \dots, n - 2k$.

Lemma 3. *The logical Pauli operators defined in (7) satisfy the commutation relations given in (6) if and only if $G_{\mathcal{C}/\mathcal{C}^\perp}^X \left(G_{\mathcal{C}/\mathcal{C}^\perp}^Z\right)^T = I_{n-2k}$, where I_{n-2k} is the $(n-2k) \times (n-2k)$ identity matrix.*

Proof. Assume $G_{\mathcal{C}/\mathcal{C}^\perp}^X \left(G_{\mathcal{C}/\mathcal{C}^\perp}^Z\right)^T = I_{n-2k}$. This implies $\underline{h}_i \cdot \underline{h}'_j = 1$ if $i = j$ and $\underline{h}_i \cdot \underline{h}'_j = 0$ if $i \neq j$. Then using the property $(A \otimes B)(C \otimes D) = AC \otimes BD$ of Kronecker products we have

$$\bar{X}_i \bar{Z}_j = \bigotimes_{t=1}^n X_t^{h_{it}} Z_t^{h'_{it}} = \bigotimes_{t=1}^n (-1)^{h_{it} h'_{it}} Z_t^{h'_{it}} X_t^{h_{it}} = (-1)^{\underline{h}_i \cdot \underline{h}'_j} \bigotimes_{t=1}^n Z_t^{h'_{it}} X_t^{h_{it}} = \begin{cases} -\bar{Z}_j \bar{X}_i & \text{if } i = j, \\ \bar{Z}_j \bar{X}_i & \text{if } i \neq j. \end{cases}$$

Conversely, it is easy to see that the last equality above requires $G_{\mathcal{C}/\mathcal{C}^\perp}^X \left(G_{\mathcal{C}/\mathcal{C}^\perp}^Z\right)^T = I_{n-2k}$. \square

We have the following theorem to verify that these operators indeed execute logical bit-flip and phase-flip operations by operating on the physical qubits.

Theorem 4. *Let $|\underline{x}\rangle_L$ be the logical state defined by $\underline{x} \in \{0, 1\}^{n-2k}$ and let $|\underline{x}'\rangle_L$ be the logical state such that $x'_i = x_i \oplus 1$ for some $i \in [n-2k]$ and $x'_j = x_j \forall j \in [n-2k]$ s.t. $j \neq i$. Then the logical Pauli operators defined in (7) satisfy*

$$\bar{X}_i |\psi_x\rangle = |\psi_{x'}\rangle \quad , \quad \bar{Z}_i |\psi_x\rangle = (-1)^{x_i} |\psi_x\rangle ,$$

where $|\psi_x\rangle$ is the CSS state defined in (4).

Proof. As observed in the proof of Theorem 2, we have $\bar{X}_i |\underline{u}\rangle = |\underline{u} + \underline{h}_i\rangle$ for any vector $\underline{u} \in \{0, 1\}^n$. Recall that the CSS state for $|\underline{x}\rangle_L$ is defined as

$$|\psi_x\rangle \triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c} + \underline{x}\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \left| \underline{c} + \sum_{j=1}^{n-2k} x_j \underline{h}_j \right\rangle .$$

Therefore we have

$$\bar{X}_i |\psi_x\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \bar{X}_i \left| \underline{c} + \sum_{j=1}^{n-2k} x_j \underline{h}_j \right\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \left| \underline{c} + \sum_{j=1, j \neq i}^{n-2k} x_j \underline{h}_j + (x_i \oplus 1) \underline{h}_i \right\rangle = |\psi_{x'}\rangle .$$

Similarly we have $\bar{Z}_i |\underline{u}\rangle = (-1)^{\underline{h}'_i \cdot \underline{u}} |\underline{u}\rangle$. For convenience we rewrite the CSS state $|\psi_x\rangle$ as

$$|\psi_x\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \left| \underline{c} + \sum_{j=1}^{n-2k} x_j \underline{h}_j \right\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} |\underline{c}\rangle = \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c}\rangle .$$

Using the commutation relations above we have $\bar{Z}_i \bar{X}_i = -\bar{X}_i \bar{Z}_i$ and $\bar{Z}_i \bar{X}_j = \bar{X}_j \bar{Z}_i$ for $j \neq i$. Also, since $\underline{h}'_i \in \mathcal{C}$ it satisfies $\underline{h}'_i \cdot \underline{c} = 0$ for all $\underline{c} \in \mathcal{C}^\perp$. This implies

$$\bar{Z}_i |\psi_x\rangle = \bar{Z}_i \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c}\rangle$$

$$\begin{aligned}
&= (-1)^{x_i} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \bar{Z}_i |\underline{c}\rangle \\
&= (-1)^{x_i} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} (-1)^{\underline{h}'_i \cdot \underline{c}} |\underline{c}\rangle \\
&= (-1)^{x_i} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c}\rangle \\
&= (-1)^{x_i} |\psi_x\rangle. \quad \square
\end{aligned}$$

Finally we need to verify that these logical operators commute with the elements of the stabilizer of the code. But this is directly true because $\underline{g}_i \cdot \underline{h}_j = 0$ and $\underline{g}_i \cdot \underline{h}'_j = 0 \forall i \in [k], j \in [n - 2k]$ since $\underline{g}_i \in \mathcal{C}^\perp$ and $\underline{h}_j, \underline{h}'_j \in \mathcal{C}$.

The other logical operators that comprise a universal set of gates need to be defined based on the specific CSS code and there is no general construction like we had for the logical Paulis above.

Example

For our $[[6, 4]]$ quantum code \mathcal{Q} we have the following two possible generator matrices for $\mathcal{C}/\mathcal{C}^\perp$:

$$G_{\mathcal{C}/\mathcal{C}^\perp}^X \triangleq \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad G_{\mathcal{C}/\mathcal{C}^\perp}^Z \triangleq \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Note that $G_{\mathcal{C}/\mathcal{C}^\perp}^Z$ is a generator matrix for an equivalent code of $\mathcal{C}/\mathcal{C}^\perp$ which is the code obtained by simply relabeling indices as 6, 5, ..., 1. But we will ignore this qualification and consider it to be a generator matrix for $\mathcal{C}/\mathcal{C}^\perp$ itself. It is easily verified that $G_{\mathcal{C}/\mathcal{C}^\perp}^X \left(G_{\mathcal{C}/\mathcal{C}^\perp}^Z\right)^T = I_4$. Furthermore, these give the logical operators

$$\begin{array}{l|l}
\bar{X}_1 = X_1 X_2 & \bar{Z}_1 = Z_2 Z_6 \\
\bar{X}_2 = X_1 X_3 & \bar{Z}_2 = Z_3 Z_6 \\
\bar{X}_3 = X_1 X_4 & \bar{Z}_3 = Z_4 Z_6 \\
\bar{X}_4 = X_1 X_5 & \bar{Z}_4 = Z_5 Z_6
\end{array}.$$

These clearly satisfy the commutation conditions

$$\bar{X}_i \bar{Z}_j = \begin{cases} -\bar{Z}_j \bar{X}_i & \text{if } i = j, \\ \bar{Z}_j \bar{X}_i & \text{if } i \neq j. \end{cases}$$

Recall that the stabilizer generators for this code are

$$\mathbf{g}_1^X \triangleq X_1 X_2 X_3 X_4 X_5 X_6 = X^{\otimes 6}, \quad \mathbf{g}_1^Z \triangleq Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 = Z^{\otimes 6}.$$

It is easily verified that for $i = 1, 2, 3, 4$ we have

$$[\bar{X}_i, \mathbf{g}_1^X] = \mathbf{0}, \quad [\bar{X}_i, \mathbf{g}_1^Z] = \mathbf{0}, \quad [\bar{Z}_i, \mathbf{g}_1^X] = \mathbf{0}, \quad [\bar{Z}_i, \mathbf{g}_1^Z] = \mathbf{0}.$$

For this code, the logical transversal Hadamard operator $\bar{H}^{\otimes 4}$, applied to all logical qubits simultaneously, is also easy to construct. This operator must satisfy the conditions $\bar{H}_i \bar{X}_i \bar{H}_i = \bar{Z}_i$, $\bar{H}_i \bar{Z}_i \bar{H}_i = \bar{X}_i$. If we apply physical Hadamard operator H transversally, i.e. $H_1 H_2 \cdots H_6$, we get the mappings

$$X_1 X_{i+1} \mapsto Z_1 Z_{i+1} \quad , \quad Z_{i+1} Z_6 \mapsto X_{i+1} X_6.$$

To complete the logical transversal Hadamard we now have to just swap physical qubits 1 and 6. This will give the desired mappings

$$\begin{array}{l|l} \bar{X}'_1 = Z_2 Z_6 & \bar{Z}'_1 = X_1 X_2 \\ \bar{X}'_2 = Z_3 Z_6 & \bar{Z}'_2 = X_1 X_3 \\ \bar{X}'_3 = Z_4 Z_6 & \bar{Z}'_3 = X_1 X_4 \\ \bar{X}'_4 = Z_5 Z_6 & \bar{Z}'_4 = X_1 X_5 \end{array} .$$

The target Hadamards \bar{H}_i and other logical operators are trickier to construct. These are discussed in [2].

2.5 CSS State Preparation

We have seen in the discussion above that the X stabilizers generated by \mathbf{g}_i^X satisfy $\mathbf{g}_i^X |\underline{u}\rangle = |\underline{u} + \underline{g}_i\rangle$ for $i = 1, 2, \dots, k$. The set of all X stabilizers is given by

$$S^X = \{\mathbf{g}_c^X : \underline{c} \in \mathcal{C}^\perp\} \quad ; \quad \mathbf{g}_c^X \triangleq \bigotimes_{j=1}^n X_j^{c_j}, \quad \underline{c} = [c_1 \ c_2 \ \dots \ c_n].$$

Hence these vectors satisfy $\mathbf{g}_c^X |0\rangle^{\otimes n} = \mathbf{g}_c^X |00 \dots 0\rangle = |\underline{c}\rangle$. Therefore, given logical qubits $|\underline{x}\rangle_L$ with $\underline{x} \in \{0, 1\}^{n-2k}$ we can first prepare the physical state $|0\rangle^{\otimes n}$ and then arrive at the desired CSS state $|\psi_x\rangle$ as follows:

$$\begin{aligned} |\psi_x\rangle &\triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \left| \underline{c} + \sum_{j=1}^{n-2k} x_j \underline{h}_j \right\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{\underline{c} \in \mathcal{C}^\perp} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} |\underline{c}\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \sum_{\underline{c} \in \mathcal{C}^\perp} |\underline{c}\rangle \\ &= \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \sum_{\underline{c} \in \mathcal{C}^\perp} \mathbf{g}_c^X |0\rangle^{\otimes n} \\ &= \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \prod_{j=1}^{n-2k} \bar{X}_j^{x_j} \sum_{\mathbf{g} \in S^X} \mathbf{g} |0\rangle^{\otimes n}. \end{aligned}$$

Note that this perspective requires us to apply *all* stabilizers to the state $|0\rangle^{\otimes n}$ which can be impractical. However, this representation of the CSS state could be potentially useful for arguing

about the effects of operators applied externally to a CSS state. We saw one such use (only using till the third equality above) in the argument for \bar{Z}_i in Theorem 4. An application of this final expression can be found in an important claim proven in [2].

References

- [1] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996.
- [2] R. Chao and B. W. Reichardt, “Fault-tolerant quantum computation with few qubits,” *arXiv preprint arXiv:1705.05365*, 2017. [Online]. Available: <http://arxiv.org/pdf/1705.05365.pdf>.