Synthesis of Logical Clifford Operators via Symplectic Geometry

Narayanan Rengaswamy*, Robert Calderbank*, Swanand Kadhe†, and Henry D. Pfister*
*Department of Electrical and Computer Engineering, Duke University, Durham, North Carolina 27708, USA
Email: {narayanan.rengaswamy, robert.calderbank, henry.pfister}@duke.edu
†Department of Electrical Engineering and Computer Science, University of California, Berkeley, California 94720, USA
Email: swanand.kadhe@berkeley.edu

***Abstract*—Quantum error-correcting codes can be used to protect qubits involved in quantum computation. This requires that logical operators acting on protected qubits be translated to physical operators (circuits) acting on physical quantum states. We propose a mathematical framework for synthesizing physical circuits that implement logical Clifford operators for stabilizer codes. Circuit synthesis is enabled by representing the desired physical Clifford operator in $\mathbb{C}^{N\times N}$ as a $2m \times 2m$ binary symplectic matrix, where $N = 2^m$. We show that for an $[\![m, m-k]\!]$ stabilizer code every logical Clifford operator has $2^{k(k+1)/2}$ symplectic solutions, and we enumerate them efficiently using symplectic transvections. The desired circuits are then obtained by writing each of the solutions as a product of elementary symplectic matrices. For a given operator, our assembly of all of its physical realizations enables optimization over them with respect to a suitable metric. Our method of circuit synthesis can be applied to any stabilizer code, and this paper provides a proof of concept synthesis of universal Clifford gates for the well-known $[\![6, 4, 2]\!]$ code. Programs implementing our algorithms can be found at https://github.com/nrenga/symplectic-arxiv18a.**

***Index Terms*—Heisenberg-Weyl group, symplectic geometry, Clifford group, stabilizer codes, logical operators, automorphisms**

I. Introduction

The first quantum error-correcting code (QECC) was discovered by Shor [1], and CSS codes were introduced by Calderbank and Shor [2], and Steane [3]. The general class of stabilizer codes was introduced by Calderbank, Rains, Shor and Sloane [4], and by Gottesman [5]. A QECC protects $m-k$ logical qubits by embedding them into a physical system comprising m physical qubits. QECCs can be used for the realization of fault-tolerant quantum computation [6]. For this purpose, any desired operation on the $m-k$ logical (protected) qubits must be implemented as a physical operation on the m physical qubits, while preserving the code space.

For stabilizer codes, physical realizations of Clifford operators on logical qubits can be represented by $2m \times 2m$ binary symplectic matrices, reducing the complexity *dramatically* from 2^m complex variables to $2m$ binary variables (see [7], [8] and Section II). We exploit this fact to propose an algorithm that efficiently assembles *all* symplectic matrices representing physical transformations (circuits) that realize a given logical operator on the protected qubits. This makes it possible to optimize the choice of circuit with respect to a suitable metric, that might be a function of the quantum hardware. During the process of computation on the logical qubits, such efficient assembly of choices for an operation could be useful since each of them might interact differently with the current state and control parameters of the system. This paper provides a proof of concept demonstration using the well-known $[\![6, 4, 2]\!]$ QECC [9], [10], where our metric is to reduce the circuit depth for each operator (see [11] for a detailed discussion).

II. Physical and Logical Operators

This section summarizes the mathematical framework for quantum error correction introduced in [2], [4], [5] and described in detail in [9]. The quantum states of a single qubit system are expressed as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathbb{C}^2$, where $|0\rangle \triangleq \begin{bmatrix}1\\0\end{bmatrix}$ and $|1\rangle \triangleq \begin{bmatrix}0\\1\end{bmatrix}$ are called the *computational basis* states, and $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta|^2 = 1$ as per the *Born rule* [12, Chap. 3]. Any single qubit error can be expanded in terms of flip, phase and flip-phase errors (on a state $|\psi\rangle$) described by the Pauli matrices

$$X \triangleq \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\ Z \triangleq \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \text{ and } Y \triangleq \iota XZ = \begin{bmatrix}0 & -\iota\\ \iota & 0\end{bmatrix}$$

respectively [6, Chap. 10], where $\iota \triangleq \sqrt{-1}$. The states of an m-qubit system are described by (linear combinations of) Kronecker products of single-qubit states, and the corresponding (Pauli) errors are expressed as Kronecker products

$$\pm\, E_1 \otimes E_2 \otimes \cdots \otimes E_m,\ \pm\iota\ E_1 \otimes E_2 \otimes \cdots \otimes E_m,$$

where $E_i \in \{I_2, X, Z, Y\}$ is the error on the i-th qubit and I_2 is the 2×2 identity matrix. These matrices form the Heisenberg-Weyl group HW_N of order $4N^2$ (also called the Pauli group), where $N = 2^m$. Note that the elements of HW_N are interpreted as both m-qubit operators and errors.

Given row vectors $a, b \in \mathbb{F}_2^m$ we define the m-qubit operator

$$D(a, b) \triangleq X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_m} Z^{b_m}, \tag{1}$$

so that the group HW_N consists of operators $\pm D(a, b)$ and $\pm\iota D(a, b)$. Multiplication in HW_N satisfies

$$D(a, b)D(a', b') = (-1)^{a'b^T + b'a^T} D(a', b')D(a, b). \tag{2}$$

The standard *symplectic inner product* in $\mathbb{F}_2^{2m}$ is defined as

$$\langle [a, b], [a', b'] \rangle_{\mathrm{s}} \triangleq a'b^T + b'a^T = [a, b]\ \Omega\ [a', b']^T, \tag{3}$$

where the symplectic form in $\mathbb{F}_2^{2m}$ is $\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$ (see [4], [11]). Therefore, two operators $D(a,b)$ and $D(a',b')$ commute if and only if $\langle [a,b],[a',b'] \rangle_s = 0$. The isomorphism $\gamma\colon HW_N/\langle \pm\iota I_N \rangle \rightarrow \mathbb{F}_2^{2m}$ allows us to represent (up to multiplication by scalars) elements of HW_N as binary vectors (i.e., $\gamma(D(a,b)) \triangleq [a,b]$).

The Clifford group Cliff_N consists of all unitary matrices $g \in \mathbb{C}^{N\times N}$ for which $gD(a,b)g^\dagger \in HW_N$, where $g^\dagger$ is the Hermitian transpose of g [8]. It is the *normalizer* of HW_N in the unitary group. We regard operators in Cliff_N as *physical* operators acting on quantum states in $\mathbb{C}^N$, to be implemented by quantum circuits. By definition, an operator $g \in \mathrm{Cliff}_N$ induces an automorphism of HW_N by conjugation. Note that the inner automorphisms induced by matrices in HW_N preserve every conjugacy class $\pm D(a,b)$, because (2) implies that elements in HW_N either commute or anti-commute. For $E(a,b) \triangleq \iota^{ab^T} D(a,b)$, automorphism induced by g satisfies

$$gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right) \ , \text{ where } \ F_g = \begin{bmatrix} A_g & B_g \\ C_g & D_g \end{bmatrix} \quad (4)$$

is a symplectic matrix. So it preserves symplectic inner products, i.e., $\langle [a,b]F_g, [a',b']F_g \rangle_s = \langle [a,b],[a',b'] \rangle_s$ (see [8], [13]). This means that $F_g \Omega F_g^T = \Omega$ or equivalently

$$A_g B_g^T = B_g A_g^T, \ C_g D_g^T = D_g C_g^T, \ A_g D_g^T + B_g C_g^T = I_m. \quad (5)$$

The fact that F_g is symplectic expresses the property that the automorphism induced by g must respect commutativity in HW_N. Let $\mathrm{Sp}(2m,\mathbb{F}_2)$ denote the group of symplectic $2m \times 2m$ matrices over $\mathbb{F}_2$. Then the map $\phi\colon \mathrm{Cliff}_N \rightarrow \mathrm{Sp}(2m,\mathbb{F}_2)$ defined by $\phi(g) \triangleq F_g$ is a homomorphism with kernel HW_N, and every Clifford operator maps down to a matrix F_g. Hence HW_N is a normal subgroup of Cliff_N and $\mathrm{Cliff}_N/HW_N \cong \mathrm{Sp}(2m,\mathbb{F}_2)$.

A *stabilizer* is a subgroup S of HW_N generated by commuting Hermitian matrices [5], [6]. For $a,b \in \mathbb{F}_2^m$, note that $\pm E(a,b) = \pm\iota^{ab^T} D(a,b)$ is Hermitian, $E(a,b)^2 = I_N$, and the operators $\frac{I_N \pm E(a,b)}{2}$ project onto the ± 1 eigenspaces of $E(a,b)$, respectively. A stabilizer S has the additional property that if it contains an operator g, then it does not contain $-g$. Consider a stabilizer S generated by Hermitian matrices $E(a_i,b_i)$, where $[a_i,b_i], i = 1,2,\ldots,k$ are linearly independent vectors in $\mathbb{F}_2^{2m}$. The *stabilizer code* corresponding to S is the subspace $V(S)$ fixed pointwise by S, i.e.,

$$V(S) = \{|\psi\rangle \in \mathbb{C}^N \ : \ g\,|\psi\rangle = |\psi\rangle \ \ \forall\ g \in S\}. \quad (6)$$

Observe that the operator $\frac{I_N + E(a_1,b_1)}{2} \times \cdots \times \frac{I_N + E(a_k,b_k)}{2}$ projects onto $V(S)$, and that $\dim\ V(S) = 2^{m-k} \triangleq M$. Such a code encodes $m-k$ *logical* qubits into m *physical* qubits. Hence an $[\![m, m-k]\!]$ QECC is an embedding of a 2^{m-k}-dimensional Hilbert space into a 2^m-dimensional Hilbert space. Note that all quantum codes are not necessarily stabilizer codes (see [4]). Logical qubits are commonly referred to as *protected* qubits or *encoded* qubits.

TABLE I
A UNIVERSAL SET OF LOGICAL OPERATORS AND CORRESPONDING PHYSICAL OPERATORS. The number of 1s in Q and R directly relates to number of gates. The N coordinates are indexed by binary vectors $v \in \mathbb{F}_2^m$, and e_v denotes the standard basis vector in $\mathbb{C}^N$ with an entry 1 in position v and all other entries 0. Here H_{2^k} denotes the Walsh-Hadamard matrix of size 2^k, $U_k = \mathrm{diag}\,(I_k, O_{m-k})$ and $L_{m-k} = \mathrm{diag}\,(O_k, I_{m-k})$.

Logical Operator F_g	Physical Operator $\bar{g}$
$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$	$H_N = H_2^{\otimes m}$
$A_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix}$	$a_Q : e_v \mapsto e_{vQ}$
$T_R = \begin{bmatrix} I_m & R \\ 0 & I_m \end{bmatrix}$ (R symmetric)	$t_R = \mathrm{diag}\left(\iota^{vRv^T}\right)$
$G_k = \begin{bmatrix} L_{m-k} & U_k \\ U_k & L_{m-k} \end{bmatrix}$	$g_k = H_{2^k} \otimes I_{2^{m-k}}$

Unitary operators $g^L \in \mathbb{U}_M$, where $M = 2^{m-k}$, acting on the logical qubits are called *logical* operators. QECCs encode a *logical* state in $\mathbb{C}^M$ into a *physical* state in $\mathbb{C}^N$. The process of *synthesizing* a logical operator g^L for a QECC refers to finding a *physical* operator $\bar{g} \in \mathbb{U}_N$ that preserves the code space (i.e., normalizes S) and realizes the action of g^L on the protected qubits. Two well-known methods to synthesize logical Pauli operators were described in [5] and [14]. For stabilizer codes, these imply that for all $h^L \in HW_M$ the associated physical operator $\bar{h} \in HW_N$ as well. Hence for all $g^L \in \mathrm{Cliff}_M$ we also have $\bar{g} \in \mathrm{Cliff}_N$. The physical operators $\bar{h}$ have a representation in $\mathbb{F}_2^{2m}$ via the map γ. Using the map ϕ, we regard a logical Clifford operator $g^L \in \mathrm{Cliff}_M$ as a symplectic matrix $F_g \in \mathrm{Sp}(2(m-k),\mathbb{F}_2)$. For stabilizer codes, in order to translate g^L into a physical operator $\bar{g}$, there are multiple ways to embed F_g into $F_{\bar{g}} \in \mathrm{Sp}(2m,\mathbb{F}_2)$ such that the corresponding $\bar{g}$ operates on states in $\mathbb{C}^N$ and acts as desired on the states of the QECC. For each $g^L \in \mathrm{Cliff}_M$ our algorithm allows one to identify *all* such embeddings. The idea is as follows.

We observe that the logical Clifford operators $g^L \in \mathrm{Cliff}_M$ are uniquely defined by their conjugation relations with the logical Paulis h^L (also see [6], [8], [9]). Therefore these relations can be directly translated to their physical equivalents $\bar{g}$ and $\bar{h}$, i.e., $g^L h^L (g^L)^\dagger = (h')^L \in HW_M \Rightarrow \bar{g}\bar{h}\bar{g}^\dagger = \bar{h}' \in HW_N$ as well. Using the relation in (4), these conditions are translated into linear constraints on $F_{\bar{g}}$. Then, linear constraints that require $F_{\bar{g}}$ to normalize S are added. The set of all $F_{\bar{g}} \in \mathrm{Sp}(2m,\mathbb{F}_2)$ that satisfy these constraints identify all embeddings of F_g into $\mathrm{Sp}(2m,\mathbb{F}_2)$. After we obtain $F_{\bar{g}}$, we synthesize a corresponding physical operator $\bar{g}$ by factoring $F_{\bar{g}}$ into elementary symplectic matrices from Table I. Note that there are multiple circuits $\bar{g}$ for a given $F_{\bar{g}}$. In the next section, we carry out the process of finding universal Clifford gates for the well-known $[\![6,4,2]\!]$ CSS code [9], [10], and then discuss the general case.

III. Logical Operator Synthesis: The $[\![6,4,2]\!]$ Code

The $[6,5,2]$ single-parity check code $\mathcal{C}$ is generated by

$$G_{\mathcal{C}} = \begin{bmatrix} H_{\mathcal{C}} \\ G_{\mathcal{C}/\mathcal{C}^\perp} \end{bmatrix} \; ; \; G_{\mathcal{C}/\mathcal{C}^\perp} \triangleq \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \quad (7)$$

where the parity-check matrix is $H_{\mathcal{C}} = [1\ 1\ 1\ 1\ 1\ 1]$. The rows $\underline{h}_i$, for $i = 1,2,3,4$, of $G_{\mathcal{C}/\mathcal{C}^\perp}$ generate all coset representatives for $\mathcal{C}^\perp$ in $\mathcal{C}$. The CSS construction [2], [3], [6] provides a $[\![6,4,2]\!]$ stabilizer code $\mathcal{Q}$ spanned by the states

$$\frac{1}{\sqrt{2}} \left| (000000) + \sum_{i=1}^{4} x_i \underline{h}_i \right\rangle + \frac{1}{\sqrt{2}} \left| (111111) + \sum_{i=1}^{4} x_i \underline{h}_i \right\rangle, \quad (8)$$

where $x_i \in \mathbb{F}_2,\ i = 1,2,3,4$. Let X_t and Z_t denote the X and Z operators, respectively, acting on the t-th physical qubit. Then the physical operators

$$\boldsymbol{g}^X = X_1X_2X_3X_4X_5X_6,\ \boldsymbol{g}^Z = Z_1Z_2Z_3Z_4Z_5Z_6 \quad (9)$$

generate the stabilizer group S that determines $\mathcal{Q}$.

A. Logical Operators for Protected Qubits

We construct logical Clifford operators by synthesizing physical operators $\bar{g}$ on the physical qubits. Since the operator $\bar{g}$ preserves $\mathcal{Q}$, conjugation by $\bar{g}$ must preserve the stabilizer S and its normalizer $S^\perp$ in HW_N, i.e., the dual of S with respect to the symplectic inner product [4]. We note that $\bar{g}$ need not commute with every element of the stabilizer S.

1) Logical Paulis: Let $|\underline{x}\rangle_L$ be the logical state defined by $\underline{x} = [x_1, x_2, x_3, x_4] \in \mathbb{F}_2^4$ in (8). Then the generating set $\{X_i^L, Z_i^L \in HW_{2^4}, i = 1,2,3,4\}$ for the logical Pauli operators are defined by the actions

$$X_i^L |\underline{x}\rangle_L = |\underline{x}'\rangle_L, \text{ where } x'_j = \begin{cases} x_i \oplus 1, & \text{if } j = i \\ x_j, & \text{if } j \neq i \end{cases}$$
$$\text{and} \quad Z_i^L |\underline{x}\rangle_L = (-1)^{x_i} |\underline{x}\rangle_L. \quad (10)$$

We denote the physical operators corresponding to X_i^L and Z_i^L as $\bar{X}_i$ and $\bar{Z}_i$, respectively. Set $G^X_{\mathcal{C}/\mathcal{C}^\perp} \triangleq G_{\mathcal{C}/\mathcal{C}^\perp}$ and set

$$G^Z_{\mathcal{C}/\mathcal{C}^\perp} \triangleq \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}. \quad (11)$$

We use the rows of these two matrices to define logical Pauli operators $\bar{X}_i, \bar{Z}_i, i = 1,2,3,4$ as follows (see [11, Section V]).

$$\begin{array}{l|l} \bar{X}_1 = X_1X_2 & \bar{Z}_1 = Z_2Z_6 \\ \bar{X}_2 = X_1X_3 & \bar{Z}_2 = Z_3Z_6 \\ \bar{X}_3 = X_1X_4 & \bar{Z}_3 = Z_4Z_6 \\ \bar{X}_4 = X_1X_5 & \bar{Z}_4 = Z_5Z_6 \end{array}. \quad (12)$$

These operators commute with every element of the stabilizer S and satisfy, as required,

$$\bar{X}_i\bar{Z}_j = \begin{cases} -\bar{Z}_j\bar{X}_i & \text{if } i = j, \\ \bar{Z}_j\bar{X}_i & \text{if } i \neq j \end{cases}. \quad (13)$$

In general, to define valid logical Pauli operators, it can be observed that the matrices $G^X_{\mathcal{C}/\mathcal{C}^\perp}, G^Z_{\mathcal{C}/\mathcal{C}^\perp}$ must satisfy $G^X_{\mathcal{C}/\mathcal{C}^\perp}\left(G^Z_{\mathcal{C}/\mathcal{C}^\perp}\right)^T = I_{m-k}$ and $G^Z_{\mathcal{C}} = \begin{bmatrix} H_{\mathcal{C}} \\ G^Z_{\mathcal{C}/\mathcal{C}^\perp} \end{bmatrix}$ must form another generator matrix for the (classical) code $\mathcal{C}$. It can be verified that the above matrices satisfy these conditions.

2) Logical Phase Gate: The phase gate $\bar{g} = \bar{P}_1$ on the first logical qubit (i.e., the physical implementation) is defined by

$$\bar{P}_1\bar{X}_j\bar{P}_1^\dagger = \begin{cases} \bar{Y}_j & \text{if } j = 1, \\ \bar{X}_j & \text{if } j \neq 1, \end{cases}, \quad \bar{P}_1\bar{Z}_j\bar{P}_1^\dagger = \bar{Z}_j \ \forall\ j = 1,2,3,4. \quad (14)$$

One can express $\bar{P}_1$ in terms of the physical Paulis X_t, Z_t as follows. The condition $\bar{P}_1\bar{X}_1\bar{P}_1^\dagger = \bar{Y}_1$ implies $\bar{P}_1$ must transform $\bar{X}_1 = X_1X_2$ into $\bar{Y}_1 \triangleq \iota\bar{X}_1\bar{Z}_1 = \iota X_1X_2Z_2Z_6 = X_1(\iota X_2Z_2)Z_6 = X_1Y_2Z_6$. Similarly, the other conditions imply that all other $\bar{X}_j$s and all $\bar{Z}_j$s must remain unchanged.

Direct inspection of these conditions yields the circuit given below. First we find an operator which transforms X_2 to Y_2 and leaves other Paulis unchanged; this is P_2, the phase gate on the second physical qubit. Then we find an operator that transforms Y_2 into Y_2Z_6, which is CZ_{26} as $X_2\mathrm{CZ}_{26}X_2^\dagger = X_2Z_6$ and $Z_i\mathrm{CZ}_{26}Z_i^\dagger = Z_i, i = 1,2,\ldots,6$. Here CZ_{26} is the controlled-Z gate on physical qubits 2 and 6. But this also transforms X_6 into Z_2X_6 and hence the circuit $\mathrm{CZ}_{26}P_2$ does not fix the stabilizer $\boldsymbol{g}^X$. Hence we include P_6 so that the full circuit $P_6\mathrm{CZ}_{26}P_2$ fixes $\boldsymbol{g}^X, \boldsymbol{g}^Z$ and also realizes $\bar{P}_1$.

We now describe how this same circuit can be synthesized via symplectic geometry. Let $F = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ be the symplectic matrix corresponding to $\bar{P}_1$. The conditions imposed in (14) on logical qubit operators $\bar{X}_j, j = 1,2,3,4$ give, as per (4),

$$[110000, 000000]F = [110000, 010001]\ (X_1X_2 \mapsto X_1Y_2Z_6)$$
$$\Rightarrow (\underline{e}_1 + \underline{e}_2)A = \underline{e}_1 + \underline{e}_2,\ (\underline{e}_1 + \underline{e}_2)B = \underline{e}_2 + \underline{e}_6,$$
$$\text{and } (\underline{e}_1 + \underline{e}_i)A = \underline{e}_1 + \underline{e}_i,\ (\underline{e}_1 + \underline{e}_i)B = \underline{0},\ i = 3,4,5.$$

Similarly, the conditions imposed on $\bar{Z}_j, j = 1,2,3,4$ give

$$(\underline{e}_i + \underline{e}_6)C = 0,\ (\underline{e}_i + \underline{e}_6)D = \underline{e}_i + \underline{e}_6,\ i = 2,3,4,5.$$

Although it is sufficient for $\bar{P}_1$ to just normalize S, we can always require that the physical operator commute with every element of S, i.e., *centralize* S (see [11, Theorem 28]).

$$(\underline{e}_1 + \ldots + \underline{e}_6)A = \underline{e}_1 + \ldots + \underline{e}_6 = (\underline{e}_1 + \ldots + \underline{e}_6)D,$$
$$(\underline{e}_1 + \ldots + \underline{e}_6)B = \underline{0} = (\underline{e}_1 + \ldots + \underline{e}_6)C.$$

We observe that one solution is $F = T_B$ (see Table I), where

$$B \triangleq B_P = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow F = \begin{bmatrix} I_6 & B \\ 0 & I_6 \end{bmatrix}.$$

The resulting physical operator $\bar{P}_1 = \mathrm{diag}\left(\iota^{vB_P v^T}\right)$ satisfies $\bar{P}_1 = P_6 \mathrm{CZ}_{26} P_2$ and hence coincides with the above circuit. Henceforth, we refer to $\bar{g}$ itself as the logical operator.

3) Logical Controlled-Z (CZ): The logical operator $\overline{\mathrm{CZ}}_{12}$ is defined by its action on the logical Paulis as

$$\overline{\mathrm{CZ}}_{12} \bar{X}_j \overline{\mathrm{CZ}}_{12}^\dagger = \begin{cases} \bar{X}_1 \bar{Z}_2 & \text{if } j = 1, \\ \bar{Z}_1 \bar{X}_2 & \text{if } j = 2, \\ \bar{X}_j & \text{if } j \neq 1, 2 \end{cases},$$
$$\overline{\mathrm{CZ}}_{12} \bar{Z}_j \overline{\mathrm{CZ}}_{12}^\dagger = \bar{Z}_j \ \forall\ j = 1, 2, 3, 4. \tag{15}$$

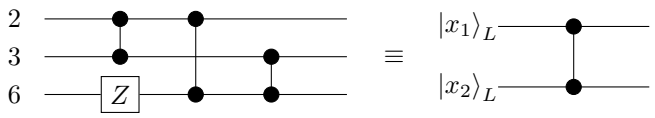
We first express the logical operator $\overline{\mathrm{CZ}}_{12}$, on the first two logical qubits, in terms of the physical Pauli operators X_t, Z_t.

$$\begin{array}{l|l} \bar{X}_1 = X_1 X_2 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1 X_2 Z_3 Z_6 & \bar{Z}_1 = Z_2 Z_6 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} Z_2 Z_6 \\ \bar{X}_2 = X_1 X_3 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1 X_3 Z_2 Z_6 & \bar{Z}_2 = Z_3 Z_6 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} Z_3 Z_6 \end{array}.$$

$\bar{X}_3, \bar{X}_4, \bar{Z}_3, \bar{Z}_4$ are left unchanged by $\overline{\mathrm{CZ}}_{12}$. As with the phase gate, we translate these conditions into linear equations involving the constituents of the corresponding symplectic transformation F. We again obtain $F = T_B$, where

$$B \triangleq B_{\mathrm{CZ}} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

The physical operator $\overline{\mathrm{CZ}}_{12} = \mathrm{diag}\left(\iota^{vB_{\mathrm{CZ}} v^T}\right)$ commutes with the stabilizer $\boldsymbol{g}^Z$ but not with $\boldsymbol{g}^X$; it takes $X^{\otimes 6}$ to $-X^{\otimes 6}$. This is remedied through post multiplication by Z_6, resulting in the circuit obtained by Chao and Reichardt [10]:



4) Logical Controlled-NOT (CNOT): The logical operator $\overline{\mathrm{CNOT}}_{2\to 1}$, where logical qubit 2 controls 1, is defined by

$$\overline{\mathrm{CNOT}}_{2\to 1} \bar{X}_j \overline{\mathrm{CNOT}}_{2\to 1}^\dagger = \begin{cases} \bar{X}_1 \bar{X}_2 & \text{if } j = 2, \\ \bar{X}_j & \text{if } j \neq 2 \end{cases},$$
$$\overline{\mathrm{CNOT}}_{2\to 1} \bar{Z}_j \overline{\mathrm{CNOT}}_{2\to 1}^\dagger = \begin{cases} \bar{Z}_1 \bar{Z}_2 & \text{if } j = 1, \\ \bar{Z}_j & \text{if } j \neq 1. \end{cases} \tag{16}$$

We approach synthesis via symplectic geometry, and express the operator $\overline{\mathrm{CNOT}}_{2\to 1}$ in terms of the physical operators X_t, Z_t as shown below.

$$\begin{array}{l|l} \bar{X}_1 = X_1 X_2 \overset{2\to 1}{\longmapsto} X_1 X_2 & \bar{Z}_1 = Z_2 Z_6 \overset{2\to 1}{\longmapsto} Z_2 Z_3 \\ \bar{X}_2 = X_1 X_3 \overset{2\to 1}{\longmapsto} X_2 X_3 & \bar{Z}_2 = Z_3 Z_6 \overset{2\to 1}{\longmapsto} Z_3 Z_6 \end{array}.$$

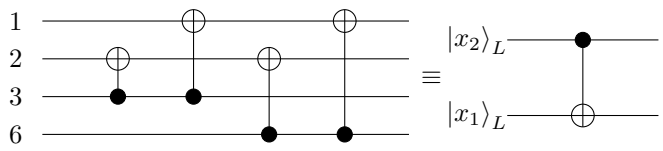
$\bar{X}_3, \bar{X}_4, \bar{Z}_3, \bar{Z}_4$ are again left unchanged by $\overline{\mathrm{CNOT}}_{2\to 1}$. As before, we translate these conditions into linear equations involving the constituents of the corresponding symplectic transformation F. We identify the solution $F = \begin{bmatrix} A & 0 \\ 0 & A^{-T} \end{bmatrix}$, where

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},\ A^{-T} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The action of $\overline{\mathrm{CNOT}}_{2\to 1}$ on logical qubits is related to the action on physical qubits through the generator matrix $G_{\mathcal{C}/\mathcal{C}^\perp}$. The map $\underline{v} \mapsto \underline{v}A$ fixes the code $\mathcal{C}$ (i.e., $e_v = |\underline{v}\rangle \mapsto e_{vA} = |\underline{v}A\rangle$ fixes $\mathcal{Q}$ and hence its stabilizers $\boldsymbol{g}^X$ and $\boldsymbol{g}^Z$) and induces a linear transformation on the coset space $\mathcal{C}/\mathcal{C}^\perp$ (which defines the CSS state). The action K on logical qubits (bits) is related to the action A on physical qubits (bits) by $K \cdot G^X_{C/C^\perp} = G^X_{C/C^\perp} \cdot A$ and we obtain

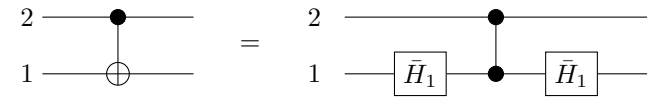
$$K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

as desired. The circuit shown on the left below implements the operator $e_v \mapsto e_{vA}$ on physical qubits, where e_v is a standard basis vector in $\mathbb{C}^N$ as defined in Table I. The circuit on the right implements $e_x \mapsto e_{xK}$, where $x \in \mathbb{F}_2^4$, i.e. $\overline{\mathrm{CNOT}}_{2\to 1}$.



We note that [15] discusses codes and operators where A is a permutation matrix corresponding to an automorphism of $\mathcal{C}$.

Remark: To implement $\overline{\mathrm{CNOT}}_{2\to 1}$ we can also use the identity



where $\bar{H}_1$ is the targeted Hadamard operator (synthesized below). However, this construction might require more gates.

5) Logical Targeted Hadamard: The Hadamard gate $\bar{H}_1$ on the first logical qubit is defined by the actions

$$\bar{H}_1 \bar{X}_j \bar{H}_1^\dagger = \begin{cases} \bar{Z}_j & \text{if } j = 1, \\ \bar{X}_j & \text{if } j \neq 1, \end{cases},\ \bar{H}_1 \bar{Z}_j \bar{H}_1^\dagger = \begin{cases} \bar{X}_j & \text{if } j = 1, \\ \bar{Z}_j & \text{if } j \neq 1, \end{cases}. \tag{17}$$

As before, we translate these conditions into linear equations involving the constituents of the corresponding symplectic transformation F. We identify one possible solution as

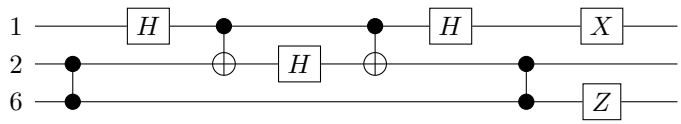
$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},\ B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$C = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}, \; D = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{18}$$

The unitary operation corresponding to this solution commutes with each stabilizer element. Another solution for $\bar{H}_1$ which fixes $Z^{\otimes 6}$ but takes $X^{\otimes 6} \leftrightarrow (111111, 000000)$ to $Y^{\otimes 6} \leftrightarrow (111111, 111111)$ is given by just changing B above to

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{19}$$

However, for both these solutions the resulting symplectic transformation does not correspond to any of the elementary forms in Table I. Hence the unitary needs to be determined by expressing F as a sequence of elementary transformations and then multiplying the corresponding unitaries. An algorithm for this is given in [13] (see [11, Theorem 23]). For the solution (18), we verified our matrix with the circuit in [10]:



B. Proposed Algorithm and Discussion

The synthesis of logical Paulis by Gottesman [5] and by Wilde [14] exploits symplectic geometry over the binary field. Building on their work we have demonstrated, using the $[\![6, 4, 2]\!]$ code as an example, that symplectic geometry provides a systematic framework for synthesizing physical implementations of any logical operator in the logical Clifford group Cliff_M. The algorithm comprises the following steps:

1) Determine the target logical operator $\bar{g}$ by specifying its conjugation relations with the logical Pauli operators [8].
2) Transform the above relations into linear equations on the target symplectic transformation F. Add conditions for normalizing the stabilizer S.
3) Derive a feasible solution for F (satisfies $F\Omega F^T = \Omega$).
4) Factor F into a product of elementary symplectic transformations listed in Table I, possibly using the algorithm given in [13] (see [11, Algorithm 3]), and compute $\bar{g}$.
5) Check for conjugation of $\bar{g}$ with the stabilizer generators and for the conditions derived in step 1. If some signs are incorrect, post-multiply by an element from HW_N as necessary to satisfy these conditions (use [6, Proposition 10.4]). Note that every Pauli operator in HW_N induces the symplectic transformation I_{2m}, so post-multiplication does not change the target matrix.
6) Express the operator $\bar{g}$ as a sequence of physical Clifford gates to obtain the desired circuit for $\bar{g}$.

In step 3 one can obtain all valid solutions F as follows: Combine all linear conditions on F obtained in step 2 to obtain a system of equations $UF = V$. Then vectorize both sides to get $(I_{2m} \otimes U)\,\mathrm{vec}(F) = \mathrm{vec}(V)$. Perform Gaussian elimination on the augmented matrix $[(I_{2m} \otimes U)\,,\ \mathrm{vec}(V)]$. If ℓ is the number of non-pivot variables in the row-reduced echelon form, then there are 2^ℓ solutions to the linear system. All such solutions that satisfy $F\Omega F^T = \Omega$ are feasible symplectic solutions for $\bar{g}$. In [11] we give a more elegant and efficient algorithm for this task using symplectic transvections. We explicitly show that for an $[\![m, m-k]\!]$ stabilizer code every logical Clifford operator has $2^{k(k+1)/2}$ symplectic solutions.

IV. Conclusion

In this work we have used symplectic geometry to propose a systematic framework for synthesizing logical Clifford operators for any stabilizer code. Our algorithm provides as a solution all feasible symplectic matrices, which are then transformed into circuits by decomposing them into elementary forms. This decomposition is not unique, and in future work we will optimize for circuit complexity and fault-tolerance.

Acknowledgment

The authors would like to thank Jungsang Kim and Jianfeng Lu for helpful discussions. S. Kadhe would like to thank Alex Sprintson for his continued support.

References

[1] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. R2493–R2496, 1995.
[2] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, Aug 1996.
[3] A. M. Steane, "Simple quantum error-correcting codes," *Phys. Rev. A*, vol. 54, no. 6, pp. 4741–4751, 1996.
[4] A. Calderbank, E. Rains, P. Shor, and N. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1369–1387, Jul 1998.
[5] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, 1997.
[6] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge university press, 2010.
[7] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum Error Correction and Orthogonal Geometry," *Phys. Rev. Lett.*, vol. 78, no. 3, pp. 405–408, 1997.
[8] D. Gottesman, "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation," *arXiv preprint arXiv:0904.2557*, 2009.
[9] D. Gottesman, "A Theory of Fault-Tolerant Quantum Computation," *arXiv preprint arXiv:quant-ph/9702029*, 1997.
[10] R. Chao and B. W. Reichardt, "Fault-tolerant quantum computation with few qubits," *arXiv preprint arXiv:1705.05365*, 2017.
[11] N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Synthesis of Logical Clifford Operators via Symplectic Geometry," *arXiv preprint arXiv:1803.06987*, 2018.
[12] M. M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2013.
[13] T. Can, "An algorithm to generate a unitary transformation from logarithmically many random bits." Research Independent Study, Preprint, 2017.
[14] M. M. Wilde, "Logical operators of quantum codes," *Phys. Rev. A*, vol. 79, no. 6, p. 062322, 2009.
[15] M. Grassl and M. Roetteler, "Leveraging automorphisms of quantum codes for fault-tolerant quantum computation," in *Proc. IEEE Int. Symp. Inform. Theory*, pp. 534–538, Jul 2013.