Synthesis of Logical Clifford Operators via Symplectic Geometry

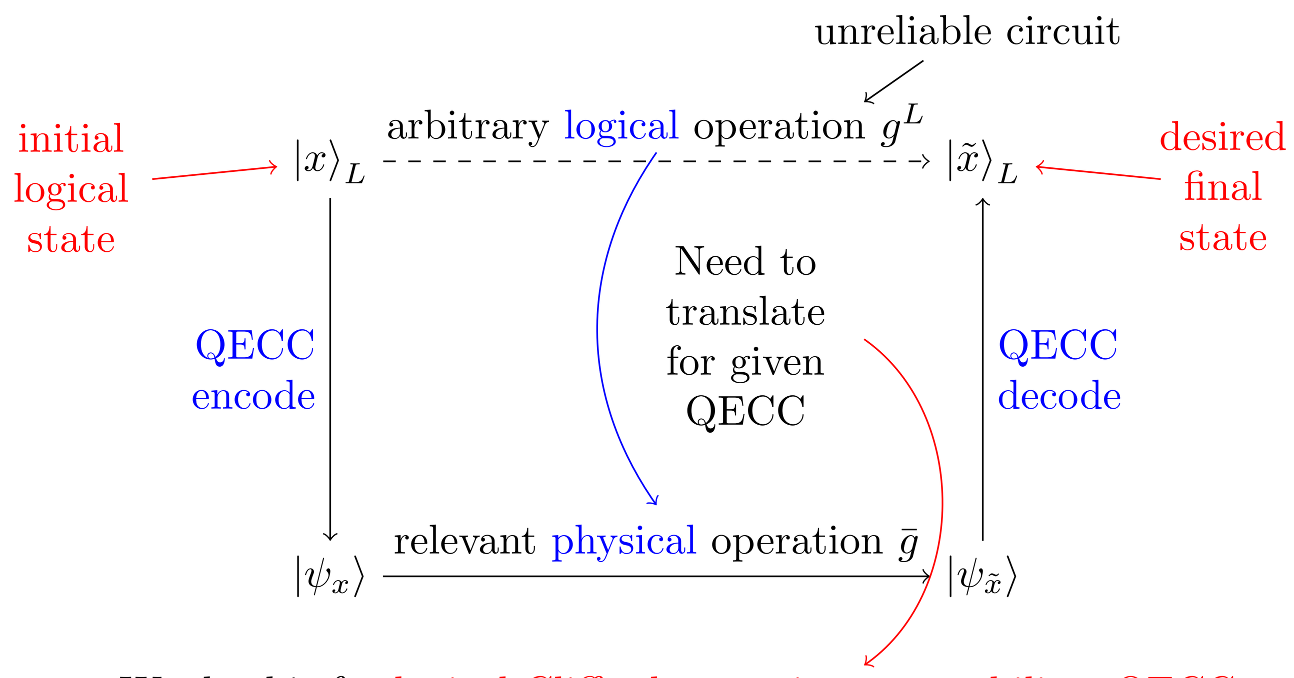
Narayanan Rengaswamy†, Robert Calderbank†, Swanand Kadhe*, and Henry D. Pfister†

†Information Initiative at Duke (iiD), Department of Electrical and Computer Engineering, Duke University, Durham, NC, USA

*Department of Electrical Engineering and Computer Science, University of California, Berkeley, CA, USA

Motivation and Contribution

- **Fault-tolerance**: Given a **quantum error-correcting code (QECC)**, if a quantum operation is performed on an encoded block of qubits, and a single component of the circuit fails, then the number of errors in the output state should be within the error-correcting capacity of the code.
- *Part of the goal:* For a chosen code, determine the circuits that realize non-trivial operations on the logical qubits. These physical circuits are called the logical operators for the code.
- Many works have concentrated on constructing codes with good properties and also on optimizing a given circuit for complexity or fault-tolerance, with respect to a chosen gate set.
- We provide a systematic and efficient algorithm for synthesizing logical Clifford operators on stabilizer codes. We also reveal the exact degeneracy in realizing these encoded operations. Our enumeration of all valid circuits can be useful in a compiler choosing codes even dynamically.



We do this for logical Clifford operations on stabilizer QECCs

Our algorithms, along with more utilities, are available open-source at:
`https://github.com/nrenga/symplectic-arxiv18a`

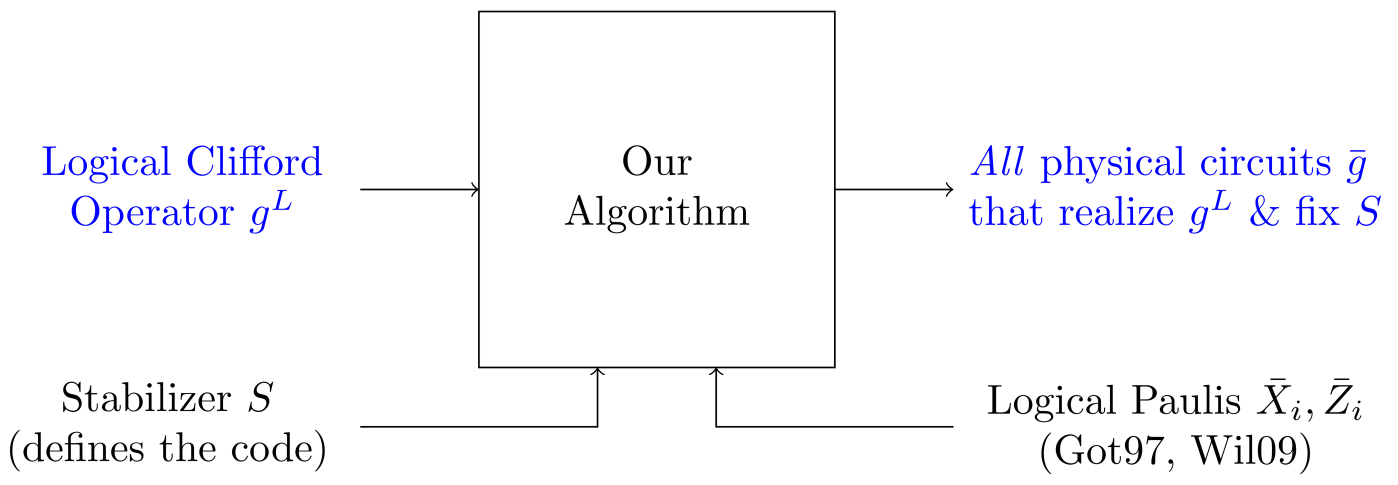


Figure 1: (top) Problem of Encoded Computation. (bottom) An abstract representation of our contribution.

Heisenberg-Weyl Group and Symplectic Vector Spaces

- The single qubit *Pauli* or *Heisenberg-Weyl* operators are given by

$$I_2 \triangleq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ Y \triangleq \imath \cdot XZ = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix}\ ;\ \imath \triangleq \sqrt{-1}. \qquad (1)$$

- Bit-flip ($X|v\rangle = |v \oplus 1\rangle$) and phase-flip ($Z|v\rangle = (-1)^v |v\rangle$) anti-commute: $XZ = -ZX$.

***m*-qubit Pauli (or) Heisenberg-Weyl Group** $HW_N (N = 2^m)$: Operators $\imath^\kappa D(a,b)$, where

$$D(a,b) \triangleq X^{a_1} Z^{b_1} \otimes X^{a_2} Z^{b_2} \otimes \cdots \otimes X^{a_m} Z^{b_m} \in \mathbb{U}_{2^m}, \qquad (2)$$

$a = (a_1, \ldots, a_m), b = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$, $\kappa \in \{0,1,2,3\}$ and $\mathbb{U}_N$ is the unitary group.

- Example: $D(a,b)|v\rangle = (-1)^{vb^T}|v+a\rangle \Rightarrow D(11010, 10110)|10101\rangle = |01111\rangle$.
$(XZ \otimes X \otimes Z \otimes XZ \otimes I_2)|10101\rangle = XZ|1\rangle \otimes X|0\rangle \otimes Z|1\rangle \otimes XZ|0\rangle \otimes I_2|1\rangle = |01111\rangle$.
- Symplectic Inner Product: For row vectors $[a,b], [a',b'] \in \mathbb{F}_2^{2m}$, define

$$\langle [a,b],[a',b'] \rangle_s \triangleq a'b^T + b'a^T = [a,b]\ \Omega\ [a',b']^T \pmod 2, \quad \text{where} \quad \Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}. \qquad (3)$$

- $D(a,b)D(a',b') = (-1)^{\langle [a,b],[a',b'] \rangle_s} D(a',b')D(a,b) \Rightarrow$ commute iff $\langle [a,b],[a',b'] \rangle_s = 0$.

Isomorphism γ: $HW_N / \langle \imath^\kappa I_N \rangle \to \mathbb{F}_2^{2m}$ defined as $\gamma(D(a,b)) \triangleq [a,b]$.

Clifford Group and Symplectic Matrices

$\text{Cliff}_N \triangleq \mathcal{N}_{\mathbb{U}_N}(HW_N)$: all $g \in \mathbb{U}_N$ s.t. $gHW_Ng^\dagger = HW_N$ (normalizer of HW_N in $\mathbb{U}_N$).

Gate	Unitary Matrix	Action on Paulis
Hadamard	$H \triangleq \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$HXH^\dagger = Z$ $HZH^\dagger = X$
Phase	$P \triangleq \begin{bmatrix} 1 & 0 \\ 0 & \imath \end{bmatrix}$	$PXP^\dagger = Y$ $PZP^\dagger = Z$
Controlled-NOT	$\text{CNOT}_{1\to 2} \triangleq \begin{bmatrix} I_2 & 0 \\ 0 & X \end{bmatrix}$	$\text{CNOT}_{1\to 2}(X \otimes I_2)\text{CNOT}_{1\to 2}^\dagger = X \otimes X = X_1X_2$
Controlled-Z	$\text{CZ}_{12} \triangleq \begin{bmatrix} I_2 & 0 \\ 0 & Z \end{bmatrix}$	$\text{CZ}_{12}(X \otimes I_2)\text{CZ}_{12}^\dagger = X \otimes Z = X_1Z_2$

Symplectic Representation: Define $E(a,b) \triangleq \imath^{ab^T} D(a,b)$. If $g \in \text{Cliff}_N$ then

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

i.e., $F_g \Omega F_g^T = \Omega$, and hence preserves inner products: $\langle [a,b],[a',b'] \rangle_s = \langle [a,b]F_g, [a',b']F_g \rangle_s$.

E.g., $g = \text{CZ}_{12}, F_g = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ & & 1 & 0 \\ & & 0 & 1 \end{bmatrix}$: $g(X \otimes I_2)g^\dagger = gE(10,00)g^\dagger = E\left([10,00]F_g\right) = E(10,01) = X_1Z_2$.

Homomorphism ϕ: $\text{Cliff}_N \to \text{Sp}(2m, \mathbb{F}_2)$ defined as $\phi(g) \triangleq F_g$, where $\text{Sp}(2m,\mathbb{F}_2)$ is the binary symplectic group. Note that for $g \in HW_N$ we have $F_g = I_{2m}$, i.e., HW_N is the kernel of the map ϕ.

Stabilizer Codes and Logical Pauli Operators

- k-dimensional Stabilizer: commutative subgroup $S \subset HW_N$ generated by linearly independent Hermitian operators
$E(a_j, b_j) \triangleq \imath^{ab^T} D(a_j, b_j),\ j = 1, \ldots, k$.
- $[\![m, m-k, d]\!]$ Stabilizer Code: The 2^{m-k} dimensional subspace $V(S)$ jointly fixed by all elements of the stabilizer S,
i.e., $V(S) \triangleq \left\{ |\psi\rangle \in \mathbb{C}^N : g|\psi\rangle = |\psi\rangle\ \forall\ g \in S \right\}$.
- The $[\![6,4,2]\!]$ CSS Code: $S \triangleq \langle \boldsymbol{g}^X \triangleq X^{\otimes 6} = E(111111, 000000),\ \boldsymbol{g}^Z \triangleq Z^{\otimes 6} = E(000000, 111111) \rangle$.
- CSS Construction: Let $\mathcal{C}$ be the $[6,5,2]$ single-parity check code ($m = 6$). The dual $\mathcal{C}^\perp \subset \mathcal{C}$ is the $[6,1,6]$ repetition code with generator $G_{\mathcal{C}^\perp} = H_{\mathcal{C}} = [1\ 1\ 1\ 1\ 1\ 1]$. Two possible generator matrices for the coset space $\mathcal{C}/\mathcal{C}^\perp$ are:

$$G^X_{\mathcal{C}/\mathcal{C}^\perp} = \begin{bmatrix} 1&1&0&0&0&0 \\ 1&0&1&0&0&0 \\ 1&0&0&1&0&0 \\ 1&0&0&0&1&0 \end{bmatrix} =: \begin{bmatrix} h_1 \\ h_2 \\ h_3 \\ h_4 \end{bmatrix} \quad \text{or} \quad G^Z_{\mathcal{C}/\mathcal{C}^\perp} = \begin{bmatrix} 0&1&0&0&0&1 \\ 0&0&1&0&0&1 \\ 0&0&0&1&0&1 \\ 0&0&0&0&1&1 \end{bmatrix} =: \begin{bmatrix} h'_1 \\ h'_2 \\ h'_3 \\ h'_4 \end{bmatrix}. \qquad (5)$$

- So if we have a 4-qubit *logical* state $|x\rangle_L$ then the CSS code will encode this into the *physical* state

$$|\psi_x\rangle \equiv \left| v + \mathcal{C}^\perp \right\rangle \triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{c \in \mathcal{C}^\perp} \left| c + x \cdot G^X_{\mathcal{C}/\mathcal{C}^\perp} \right\rangle = \frac{1}{\sqrt{2}} \sum_{c \in \mathcal{C}^\perp} \left| c + \sum_{j=1}^{4} x_j h_j \right\rangle. \qquad (6)$$

- For the $[\![6,4,2]\!]$ CSS code the logical Pauli operators are: $\bar{X}_j = D(h_j, 0) = X_1X_{j+1},\ \bar{Z}_j = D(0, h'_j) = Z_{j+1}Z_6$.

Synthesis of Logical Clifford Operators for Stabilizer Codes

- Conditions on $\bar{g}$: $\bar{g}\bar{X}_j\bar{g}^\dagger = \bar{h}$ if $g^LX_j^L(g^L)^\dagger = h^L \in HW_{2^{m-k}}$ and $\bar{g}\bar{Z}_j\bar{g}^\dagger = \bar{h}'$ if $g^LZ_j^L(g^L)^\dagger = (h')^L \in HW_{2^{m-k}}$.
- Synthesizing $g^L = \text{CZ}_{12}^L$ for the $[\![6,4,2]\!]$ CSS code: Find physical operator $\bar{g} = \overline{\text{CZ}}_{12}$ that normalizes S and satisfies

$$\overline{\text{CZ}}_{12}\bar{X}_j\overline{\text{CZ}}_{12}^\dagger \triangleq \begin{cases} \bar{X}_1\bar{Z}_2 & \text{if } j = 1, \\ \bar{Z}_1\bar{X}_2 & \text{if } j = 2, \\ \bar{X}_j & \text{if } j \neq 1,2 \end{cases},\quad \overline{\text{CZ}}_{12}\bar{Z}_j\overline{\text{CZ}}_{12}^\dagger \triangleq \bar{Z}_j\ \forall\ j = 1,2,3,4. \qquad (7)$$

- Using the **symplectic representation** translate these into constraints on the desired symplectic matrix for $\overline{\text{CZ}}_{12}$:

$$\overline{\text{CZ}}_{12}\bar{X}_1\overline{\text{CZ}}_{12}^\dagger = \bar{X}_1\bar{Z}_2 \Rightarrow\ \bar{X}_1 = X_1X_2 \xmapsto{\overline{\text{CZ}}_{12}} X_1X_2Z_3Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [110000, 000000]F_{\overline{\text{CZ}}_{12}} = [110000, 001001]$$

$$\overline{\text{CZ}}_{12}\bar{X}_2\overline{\text{CZ}}_{12}^\dagger = \bar{Z}_1\bar{X}_2 \Rightarrow\ \bar{X}_2 = X_1X_3 \xmapsto{\overline{\text{CZ}}_{12}} X_1X_3Z_2Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [101000, 000000]F_{\overline{\text{CZ}}_{12}} = [101000, 010001]$$

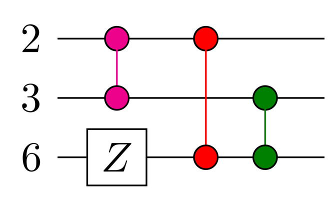
$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

$$\overline{\text{CZ}}_{12}\ \boldsymbol{g}^X\ \overline{\text{CZ}}_{12}^\dagger = \boldsymbol{g}^X \Rightarrow\ X^{\otimes 6} \xmapsto{\overline{\text{CZ}}_{12}} X^{\otimes 6} = X_1X_2\cdots X_6 \overset{\gamma,\phi}{\Longleftrightarrow} [111111, 000000]F_{\overline{\text{CZ}}_{12}} = [111111, 000000]$$

$$\overline{\text{CZ}}_{12}\ \boldsymbol{g}^Z\ \overline{\text{CZ}}_{12}^\dagger = \boldsymbol{g}^Z \Rightarrow\ Z^{\otimes 6} \xmapsto{\overline{\text{CZ}}_{12}} Z^{\otimes 6} = Z_1Z_2\cdots Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [000000, 111111]F_{\overline{\text{CZ}}_{12}} = [000000, 111111].$$

One possible solution

$$\Rightarrow F_{\overline{\text{CZ}}_{12}} = \begin{bmatrix} I_6 & B \\ 0 & I_6 \end{bmatrix}, B = \begin{bmatrix} 0&0&0&0&0&0 \\ 0&0&1&0&0&1 \\ 0&1&0&0&0&1 \\ 0&0&0&0&0&0 \\ 0&0&0&0&0&0 \\ 0&1&1&0&0&0 \end{bmatrix} \longleftrightarrow$$



$$\Downarrow$$

$$\overline{\text{CZ}}_{12} = \text{diag}\left(\imath^{vBv^T}\right) Z_6$$

$$= \text{CZ}_{36}\text{CZ}_{26}\text{CZ}_{23}Z_6$$

Not captured in $F_{\overline{\text{CZ}}_{12}}$ – added to fix signs

- We solve such symplectic systems of linear equations using binary symplectic transvections.
- Definition: Given a row vector $h \in \mathbb{F}_2^{2m}$, the corresponding symplectic transvection $Z_h : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ is defined as

$$Z_h(x) \triangleq x + \langle x, h \rangle_s h\ \Leftrightarrow\ F_h \triangleq I_{2m} + \Omega h^T h \in \text{Sp}(2m, \mathbb{F}_2). \qquad (8)$$

Our Generic Algorithm

1. Determine the target $\bar{g}$ by specifying its action on $\bar{X}_i, \bar{Z}_i$: $\bar{g}\bar{X}_i\bar{g}^\dagger = \bar{X}'_i, \bar{g}\bar{Z}_i\bar{g}^\dagger = \bar{Z}'_i$. Add conditions to normalize or centralize S.
2. Using the maps γ, ϕ, transform these relations into linear equations on $F_{\bar{g}} \in \text{Sp}(2m, \mathbb{F}_2)$, i.e., $\gamma(\bar{X}_i)F = \gamma(\bar{X}'_i), \gamma(\bar{Z}_i)F = \gamma(\bar{Z}'_i)$. Add the conditions for normalizing the stabilizer S, i.e., $\gamma(S)F = \gamma(S')$.
3. Find the feasible symplectic solution set $\mathcal{F}_{\bar{g}}$ using symplectic transvections and "nullspace-like" properties of symplectic matrices.
4. Factor *each* $F \in \mathcal{F}$ into a product of elementary symplectic transformations, possibly using the algorithm given in [Can17], and compute the physical Clifford operator $\bar{g}$.
5. Check for conjugation of $\bar{g}$ with $S, \bar{X}_i, \bar{Z}_i$. If some signs are incorrect, post-multiply by an element from HW_N as necessary to satisfy these conditions (apply [NC10, Prop. 10.4] to $S^\perp = \langle S, \bar{X}_i, \bar{Z}_i \rangle$). Note that every Pauli operator in HW_N induces the symplectic transformation I_{2m}, since HW_N is the kernel of the map ϕ, so post-multiplication does not change the target symplectic matrix F.
6. Express $\bar{g}$ as a sequence of Clifford gates, obtained from the factorization in step 4, which yields the desired physical circuit.

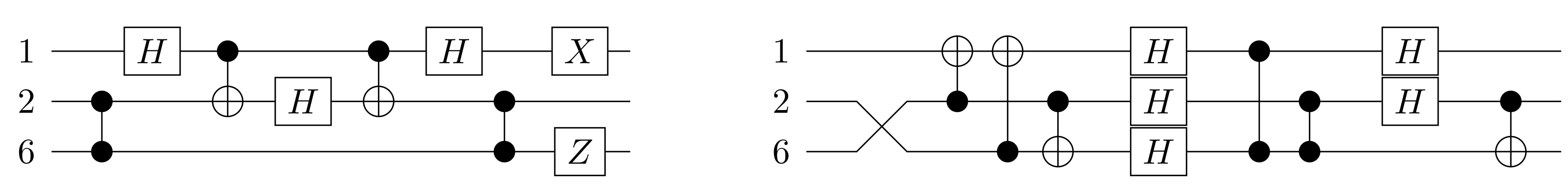


Figure 2: Logical Hadamard operator $\bar{H}_1$, synthesized by Chao and Reichardt [CR17] (left), and using our *generic* algorithm (right). This illustrates that, while our algorithm yields all symplectic solutions for the desired logical operator $\bar{g}$, the decomposition we use from [Can17] may not yield lowest circuit complexity or fault-tolerance. Hence, our circuits can potentially be further optimized for such purposes.

Summary of Our Technical Results

- For an $[\![m, m-k]\!]$ stabilizer code, the number of symplectic solutions for each logical Clifford operator is $2^{k(k+1)/2}$. Our generic algorithm above details the steps to determine all solutions and their circuits, using a particular decomposition of symplectic matrices.
- For an $[\![m, m-k]\!]$ stabilizer code with stabilizer S, each physical realization of a given logical Clifford operator that normalizes S can be converted into a circuit that centralizes S, i.e., commutes with every element of S, while realizing the same logical operation.
- Given a sequence of binary vectors $x_i, y_i,\ i = 1, \ldots, t \leq 2m$ s.t. $\langle x_i, x_j \rangle_s = \langle y_i, y_j \rangle_s$, there exists a symplectic matrix F, expressible as a product of at most $2t$ transvections, s.t. $x_iF = y_i$. We also given an explicit algorithm to compute such a matrix.
- Let $\{(u_a, v_a),\ a \in \{1, \ldots, m\}\}$ be a collection of pairs of binary vectors that form a symplectic basis for $\mathbb{F}_2^{2m}$, where $u_a, v_a \in \mathbb{F}_2^{2m}$. Consider a system of linear equations $u_iF = u'_i, v_jF = v'_j$, where $i \in \mathcal{I} \subseteq \{1, \ldots, m\}, j \in \mathcal{J} \subseteq \{1, \ldots, m\}$ and $F \in \text{Sp}(2m, \mathbb{F}_2)$. Let $\alpha \triangleq |\bar{\mathcal{I}}| + |\bar{\mathcal{J}}|$. Then there are $2^{\alpha(\alpha+1)/2}$ solutions F to the system. We also give an algorithm to efficiently enumerate them.

References

1. N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Synthesis of Logical Clifford Operators via Symplectic Geometry," *to appear in Proc. 2018 IEEE Int. Symp. Inform. Theory, arXiv preprint arXiv:1803.06987*, 2018, [Online]. Available: http://arxiv.org/abs/1803.06987.
2. D. Gottesman, "A Theory of Fault-Tolerant Quantum Computation," *arXiv preprint arXiv:quant-ph/9702029*, 1997, [Online]. Available: http://arxiv.org/pdf/quant-ph/9702029.pdf.
3. M. M. Wilde, "Logical operators of quantum codes," *Phys. Rev. A*, vol. 79, no. 6, p. 062 322, 2009. DOI: 10.1103/PhysRevA.79.062322.
4. T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, 2006. DOI: 10.1126/science.1131563. [Online]. Available: http://science.sciencemag.org/content/314/5798/436.
5. T. Can, "An algorithm to generate a unitary transformation from logarithmically many random bits," Research Independent Study, Preprint, 2017.
6. 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.