Synthesis of Logical Operators for Quantum Computers using Stabilizer Codes

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

Introduction

- Quantum computers solve some problems more efficiently than classical computers, e.g., Shor's algorithm for prime factorization is *exponentially* faster than classical ones [NC10].
- But the components of a quantum circuit, e.g., gates, measurements, wires, are faulty.
- An insightful idea is to *encode* the qubits using a **quantum error-correcting code (QECC)** and try to address faults via error-correction procedures [NC10].
- **Fault-tolerance**: 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.
- Goals of fault-tolerant quantum computation:
  - Find codes that efficiently encode information (logical qubits) into the code states (physical qubits).
  - The codes must also have sufficiently high error-correcting capacity.
  - 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.
  - Determine fault-tolerant implementations for a *universal* set of logical operators for the code. This guarantees reliable and *arbitrary* quantum computation.

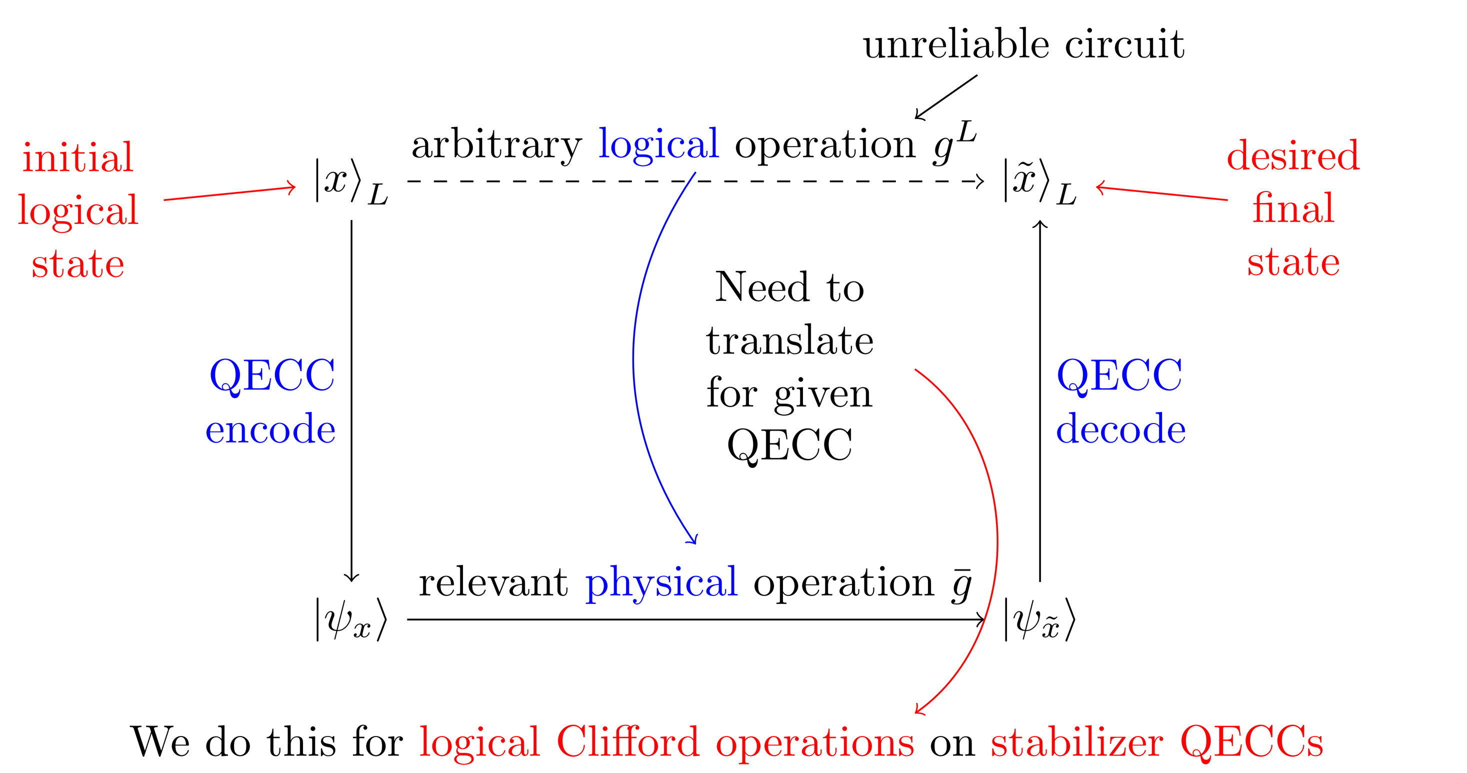


Figure 1: Problem: Quantum Operations on Encoded (Protected) Qubits

The Heisenberg-Weyl Group $HW_N (N = 2^m)$

- *Qubit*: Mathematically, a 2-dimensional Hilbert space over $\mathbb{C}$.
- *Pure state*: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$.
- Example (2 qubits): $|0\rangle \otimes |1\rangle = \begin{bmatrix}1\\0\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = |01\rangle$, a basis vector for $\mathbb{C}^4$.
- The single qubit *Pauli* operators are given by
$$I_2 \triangleq \begin{bmatrix}1&0\\0&1\end{bmatrix},\ X \triangleq \begin{bmatrix}0&1\\1&0\end{bmatrix},\ Z \triangleq \begin{bmatrix}1&0\\0&-1\end{bmatrix},\ Y \triangleq \imath \cdot XZ = \begin{bmatrix}0&-\imath\\ \imath&0\end{bmatrix};\ \imath \triangleq \sqrt{-1}.$$
- 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 Heisenberg-Weyl Group $HW_N (N = 2^m)$: Operators $\imath^\kappa D(a,b)$, where
$$D(a,b) \triangleq X^{a_1}Z^{b_1} \otimes X^{a_2}Z^{b_2} \otimes \cdots \otimes X^{a_m}Z^{b_m} \in \mathbb{U}_{2^m},$$
$a = (a_1, \ldots, a_m), b = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$, $\kappa \in \{0,1,2,3\}$ 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 vectors $[a,b], [a',b'] \in \mathbb{F}_2^{2m}$, define
$$\langle [a,b],[a',b'] \rangle_s \triangleq a'b^T + b'a^T = [a,b]\ \Omega\ [a',b']^T \pmod 2,$$
where $\Omega = \begin{bmatrix}0 & I_m\\ I_m & 0\end{bmatrix}$ is the symplectic form in $\mathbb{F}_2^{2m}$.
- $D(a,b)D(a',b') = (-1)^{\langle [a,b],[a',b'] \rangle_s} D(a',b')D(a,b) \Rightarrow$ 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

$\mathsf{Cliff}_N \triangleq \mathcal{N}_{\mathbb{U}_N}(HW_N)$: all $g \in \mathbb{U}_N$ s.t. $gHW_Ng^\dagger = HW_N$ (normalizer of HW_N in $\mathbb{U}_N$).
$$\mathsf{Cliff}_N = \langle HW_N, H, P, \mathsf{CNOT} \text{ or } \mathsf{CZ} \rangle.$$

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	$\mathsf{CNOT}_{1\to2} \triangleq \begin{bmatrix}I_2&0\\0&X\end{bmatrix}$	$\mathsf{CNOT}_{1\to2}(X \otimes I_2)\mathsf{CNOT}_{1\to2}^\dagger = X \otimes X = X_1X_2$
Controlled-Z	$\mathsf{CZ}_{12} \triangleq \begin{bmatrix}I_2&0\\0&Z\end{bmatrix}$	$\mathsf{CZ}_{12}(X \otimes I_2)\mathsf{CZ}_{12}^\dagger = X \otimes Z = X_1Z_2$

Symplectic Representation: Define $E(a,b) \triangleq \imath^{ab^T}D(a,b)$. If $g \in \mathsf{Cliff}_N$ then
$$gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right), \text{ where } F_g = \begin{bmatrix}A_g & B_g\\ C_g & D_g\end{bmatrix} \text{ is symplectic,}$$
i.e., $F_g \Omega F_g^T = \Omega$, and hence preserves inner products: $\langle [a,b],[a',b'] \rangle_s = \langle [a,b]F_g, [a',b']F_g \rangle_s$.

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

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

Stabilizer Codes and Logical Pauli Operators

- k-dimensional Stabilizer: commutative subgroup $S \subset HW_N$ generated by linearly independent Hermitian operators $E(a_j, b_j) \triangleq \imath^{a b^T} D(a_j, b_j)$, $j = 1, \ldots, k$.
- $[\![m, m-k, d]\!]$ Stabilizer Code: The 2^{m-k} dimensional subspace $V(S)$ jointly fixed by all elements of the stabilizer S, i.e., $V(S) \triangleq \left\{ |\psi\rangle \in \mathbb{C}^N \mid g|\psi\rangle = |\psi\rangle\ \forall\ g \in S \right\}$.
- The $[\![6,4,2]\!]$ Code: $S \triangleq \langle \boldsymbol{g}^X \triangleq X^{\otimes 6} = E(r,0),\ \boldsymbol{g}^Z \triangleq Z^{\otimes 6} = E(0,r) \rangle$, $r = [111111]$.
$\boldsymbol{g}^X = X_1X_2X_3X_4X_5X_6 = X^{\otimes 6}$, $\boldsymbol{g}^Z = Z_1Z_2Z_3Z_4Z_5Z_6 = Z^{\otimes 6}$.
- CSS Construction: Let $\mathcal{C}$ be the $[6,5,2]$ single-parity check code with $m = 6, k = 1$. The dual $\mathcal{C}^\perp \subset \mathcal{C}$ is the $[6,1,6]$ repetition code. Two possible generator matrices for $\mathcal{C}/\mathcal{C}^\perp$:
$$G^X_{\mathcal{C}/\mathcal{C}^\perp} = \begin{bmatrix}1&1&0&0&0&0\\1&0&1&0&0&0\\1&0&0&1&0&0\\1&0&0&0&1&0\end{bmatrix} =: \begin{bmatrix}h_1\\h_2\\h_3\\h_4\end{bmatrix} \quad \text{or} \quad G^Z_{\mathcal{C}/\mathcal{C}^\perp} = \begin{bmatrix}0&1&0&0&0&1\\0&0&1&0&0&1\\0&0&0&1&0&1\\0&0&0&0&1&1\end{bmatrix} =: \begin{bmatrix}h'_1\\h'_2\\h'_3\\h'_4\end{bmatrix}.$$
- So if we have an $(m-2k)$-qubit state $|x\rangle_L$ then the CSS code will encode this into
$$|\psi_x\rangle \equiv \left|v + \mathcal{C}^\perp\right\rangle \triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{c \in \mathcal{C}^\perp} \left|c + x \cdot G^X_{\mathcal{C}/\mathcal{C}^\perp}\right\rangle = \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{c \in \mathcal{C}^\perp} \left|c + \sum_{j=1}^{m-2k} x_j h_j\right\rangle.$$

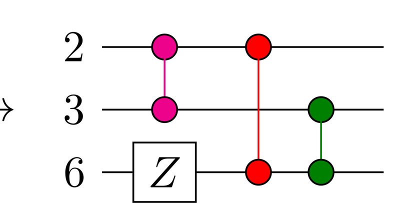
Synthesizing Logical Paulis: Find physical realizations $\bar{X}_j, \bar{Z}_j$ for X_j^L, Z_j^L resp. s.t.
- $\bar{X}_j, \bar{Z}_j \in \mathbb{U}_N$ act on $|\psi_x\rangle$ and realize action of X_j^L, Z_j^L (resp.) on $|x\rangle_L$.
- $\bar{X}_j, \bar{Z}_j$ satisfy the commutation relations: $\bar{X}_i\bar{Z}_j = \begin{cases} -\bar{Z}_j\bar{X}_i & \text{if } i = j,\\ \bar{Z}_j\bar{X}_i & \text{if } i \neq j\end{cases}$.
- $\bar{X}_j, \bar{Z}_j$ normalize the stabilizer S (preserve the code subspace) so that, for $g \in S\ \exists\ g' \in S$ s.t.
$$\bar{X}_j|\psi_x\rangle = \bar{X}_jg|\psi_x\rangle = (\bar{X}_jg\bar{X}_j^\dagger)\bar{X}_j|\psi_x\rangle = g'\bar{X}_j|\psi_x\rangle \text{ (similarly for } \bar{Z}_j).$$

- For the $[\![6,4,2]\!]$ CSS code the logical Pauli operators are given by
$$\begin{array}{l|l} \bar{X}_1 \triangleq D(h_1, 0) = X_1X_2 & \bar{Z}_1 \triangleq D(0, h'_1) = Z_2Z_6\\ \bar{X}_2 \triangleq D(h_2, 0) = X_1X_3 & \bar{Z}_2 \triangleq D(0, h'_2) = Z_3Z_6\\ \bar{X}_3 \triangleq D(h_3, 0) = X_1X_4 & \bar{Z}_3 \triangleq D(0, h'_3) = Z_4Z_6\\ \bar{X}_4 \triangleq D(h_4, 0) = X_1X_5 & \bar{Z}_4 \triangleq D(0, h'_4) = Z_5Z_6 \end{array}.$$

Synthesis of Logical Clifford Operators

- Conditions similar to that for logical Paulis, but commutation constraints $\bar{X}_i\bar{Z}_j$ replaced by conjugation constraints with logical Paulis, i.e., $\bar{g}$ must satisfy $\bar{g}\bar{X}_j\bar{g}^\dagger = \bar{h}$ if $g^L X_j^L (g^L)^\dagger = h^L \in HW_{2^{m-k}}$ and $\bar{g}\bar{Z}_j\bar{g}^\dagger = \bar{h}'$ if $g^L Z_j^L (g^L)^\dagger = (h')^L \in HW_{2^{m-k}}$.
- Synthesizing $g^L = \mathsf{CZ}_{12}^L$ for the $[\![6,4,2]\!]$ code: Find physical operator $\bar{g} = \overline{\mathsf{CZ}}_{12}$ such that
$$\overline{\mathsf{CZ}}_{12}\bar{X}_j\overline{\mathsf{CZ}}_{12}^\dagger \triangleq \begin{cases} \bar{X}_1\bar{Z}_2 & \text{if } j = 1,\\ \bar{Z}_1\bar{X}_2 & \text{if } j = 2,\\ \bar{X}_j & \text{if } j \neq 1,2 \end{cases},$$
$$\overline{\mathsf{CZ}}_{12}\bar{Z}_j\overline{\mathsf{CZ}}_{12}^\dagger \triangleq \bar{Z}_j\ \forall\ j = 1,2,3,4.$$
- Using the symplectic representation translate these into constraints on the desired symplectic matrix for $\overline{\mathsf{CZ}}_{12}$ as follows:
$$\bar{X}_1 = X_1X_2 \xmapsto{\overline{\mathsf{CZ}}_{12}} X_1X_2Z_3Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [110000, 000000]F_{\overline{\mathsf{CZ}}_{12}} = [110000, 001001]$$
$$\bar{X}_2 = X_1X_3 \xmapsto{\overline{\mathsf{CZ}}_{12}} X_1X_3Z_2Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [101000, 000000]F_{\overline{\mathsf{CZ}}_{12}} = [101000, 010001]$$
$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$$
$$\boldsymbol{g}^X = X^{\otimes 6} \xmapsto{\overline{\mathsf{CZ}}_{12}} X^{\otimes 6} = X_1X_2\cdots X_6 \overset{\gamma,\phi}{\Longleftrightarrow} [111111, 000000]F_{\overline{\mathsf{CZ}}_{12}} = [111111, 000000]$$
$$\boldsymbol{g}^Z = Z^{\otimes 6} \xmapsto{\overline{\mathsf{CZ}}_{12}} Z^{\otimes 6} = Z_1Z_2\cdots Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [000000, 111111]F_{\overline{\mathsf{CZ}}_{12}} = [000000, 111111].$$

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



$$\Downarrow$$
$$\overline{\mathrm{CZ}}_{12} = \mathrm{diag}\left(\imath^{vBv^T}\right)Z_6$$
$$= \mathrm{CZ}_{36}\mathrm{CZ}_{26}\mathrm{CZ}_{23}Z_6$$

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

- We solve such symplectic systems of linear equations using symplectic transvections.
- Definition: Given a row vector $h \in \mathbb{F}_2^{2m}$, the transvection $Z_h : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ is
$$Z_h(x) \triangleq x + \langle x, h \rangle_s h \iff F_h \triangleq I_{2m} + \Omega h^T h \in \mathsf{Sp}(2m, \mathbb{F}_2).$$

Summary of Our Results

- 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 $F \in \mathsf{Sp}(2m, \mathbb{F}_2)$. 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.
- For an $[\![m, m-k]\!]$ stabilizer code, the number of symplectic solutions for each logical Clifford operator is $2^{k(k+1)/2}$. We give a complete algorithm to determine all solutions and their circuits.
- 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.

References

1. N. Rengaswamy, R. Calderbank, S. Kadhe, and H. D. Pfister, "Synthesis of Logical Clifford Operators via Symplectic Geometry," *arXiv preprint arXiv:1803.06987*, 2018, [Online]. Available: http://arxiv.org/abs/1803.06987.
2. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge university press, 2010.
3. A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, pp. 1098–1105, 2 Aug. 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, no. 4, pp. 1369–1387, Jul. 1998.
5. 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.
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.