Synthesis of Logical Operators for Quantum Computers using Stabilizer Codes

Narayanan Rengaswamy
Ph.D. Student, Information Initiative at Duke (iiD)
Duke University, USA

Seminar, Department of Electrical Engineering
Indian Institute of Technology, Madras, India

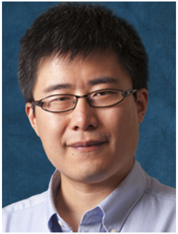
arXiv:1803.06987

April 26, 2018

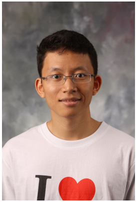
Joint Work

Robert Calderbank

Henry Pfister



Jianfeng Lu



Trung Can

Swanand Kadhe

Jungsang Kim

Problem: Operations on Encoded Qubits

unreliable circuit

initial logical state

$$\begin{tikzcd}[column sep=huge, row sep=huge] |x\rangle_L \arrow[r, "\text{arbitrary logical operation}"] \arrow[d, "\text{QECC encode}"'] & |\tilde{x}\rangle_L \\ |\psi_x\rangle \arrow[r, "\text{relevant physical operation}"] & |\psi_{\tilde{x}}\rangle \arrow[u, "\text{QECC decode}"'] \end{tikzcd}$$

desired final state

QECC: Quantum Error-Correcting Codes

Problem: Operations on Encoded Qubits

unreliable circuit

$$\begin{tikzcd} \text{initial logical state} \arrow[r] & |x\rangle_L \arrow[r, "\text{arbitrary logical operation}"] \arrow[d, "\text{QECC encode}"'] & |\tilde{x}\rangle_L & \text{desired final state} \arrow[l] \\ & |\psi_x\rangle \arrow[r, "\text{relevant physical operation}"] & |\psi_{\tilde{x}}\rangle \arrow[u, "\text{QECC decode}"'] & \end{tikzcd}$$

Need to translate for given QECC

We do this for logical Clifford operations on stabilizer QECCs

QECC: Quantum Error-Correcting Codes

In this talk...

- Synthesis of logical Pauli operators for CSS codes
  - Two popular algorithms in the literature: [Got97b; Wil09].
  - We provide a closely-related but classical coding-theoretic perspective.
- Synthesis of logical Clifford operators for stabilizer codes
  - Methods seem to exist only for particular QECCs and operations, e.g., [Got97a; Fow+12; GR13; CR17].
  - We propose a systematic framework using symplectic geometry.
  - We efficiently enumerate all symplectic matrices representing a given operator.
  - We highlight some technical results from our paper.

Overview

Kronecker Products of Matrices

Given a $p \times q$ matrix $A = [a_{ij}]$ and a $r \times s$ matrix $B = [b_{kl}]$, the Kronecker product $A \otimes B$ is defined by

$$A \otimes B \triangleq \begin{bmatrix} a_{11}B & \cdots & a_{1q}B \\ \vdots & & \vdots \\ a_{p1}B & \cdots & a_{pq}B \end{bmatrix}_{pr \times qs} .$$

Lemma

Given matrices A, B, A', B', we have

$$(A \otimes B)(A' \otimes B') = (AA') \otimes (BB'),$$

and in general $(A_1 \otimes \cdots \otimes A_m)(B_1 \otimes \cdots \otimes B_m) = (A_1 B_1) \otimes \cdots \otimes (A_m B_m)$.

Pure States

Qubit: Mathematically, it is 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 ($m = 2$ qubits) :
$$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle ,$$
$$|1\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle .$$

Note that $\mathbb{C}^N = \mathbb{C}^{2^m} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ (m times). $N = 2^m$.

Heisenberg-Weyl Group HW_N

The Heisenberg-Weyl (or Pauli) group for a single qubit:

$$HW_2 \triangleq \iota^{\kappa}\{I_2, X, Z, Y\},\ \iota \triangleq \sqrt{-1},\ \kappa \in \{0,1,2,3\}.$$

$$\text{Bit-Flip}: \quad X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \Rightarrow X\left|v\right\rangle = \left|v \oplus 1\right\rangle,\ v \in \{0,1\}.$$

$$\text{Phase-Flip}: \quad Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow Z\left|v\right\rangle = (-1)^v\left|v\right\rangle.$$

$$\text{Bit-Phase Flip}: \quad Y \triangleq \begin{bmatrix} 0 & -\iota \\ \iota & 0 \end{bmatrix} = \iota XZ.\ XZ = -ZX.$$

$\{I_2, X, Z, Y\}$ forms an orthonormal basis for the real vector space of Hermitian operators on $\mathbb{C}^2$, under the trace inner product.

For m Qubits: $HW_N \triangleq$ Kronecker products of m HW_2 matrices $(N = 2^m)$.

Binary Representation of HW_N ($N = 2^m$)

E.g.: $$(XZ \otimes X \otimes Z \otimes XZ \otimes I_2)\left|10101\right\rangle = XZ\left|1\right\rangle \otimes X\left|0\right\rangle \otimes Z\left|1\right\rangle \otimes XZ\left|0\right\rangle \otimes I_2\left|1\right\rangle$$
$$= \left|01111\right\rangle.$$

Definition

Given binary m-tuples $a = (a_1, \ldots, a_m), b = (b_1, \ldots, b_m)$ define the matrix

$$D(a, b) \triangleq X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_m} Z^{b_m} \in \mathbb{C}^{N \times N}.$$

E.g.: $D(a, b) = D(11010, 10110) = XZ \otimes X \otimes Z \otimes XZ \otimes I_2 \equiv Y_1 X_2 Z_3 Y_4.$

$$D(a, b)\left|v\right\rangle = (-1)^{vb^T}\left|v + a\right\rangle \Rightarrow D(11010, 10110)\left|10101\right\rangle = \left|01111\right\rangle.$$

HW_N Group: All matrices of the form $\iota^\kappa D(a, b)$, $\kappa \in \{0, 1, 2, 3\}$.

Isomorphism: $\gamma(D(a, b)) \triangleq [a, b]$

Property: $D(a, b)D(a', b') = (-1)^{a' b^T} D(a + a', b + b')$.

- Multiplication of HW_N elements $\simeq$ addition of binary vectors.

Property: $D(a, b)D(a', b') = (-1)^{a' b^T + b' a^T} D(a', b')D(a, b)$.

Symplectic Inner Product [Cal+98]: For vectors $[a, b], [a', b'] \in \mathbb{F}_2^{2m}$, define

$$\langle [a, b], [a', b'] \rangle_s \triangleq a' b^T + b' a^T = [a, b] \, \Omega \, [a', b']^T,$$

where $\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$ is the symplectic form in $\mathbb{F}_2^{2m}$.

- $D(a, b), D(a', b') \in HW_N$ commute iff $\langle [a, b], [a', b'] \rangle_s = 0$.

Stabilizer Groups ($N = 2^m$)

k-dimensional stabilizer: commutative subgroup $S \subset HW_N$ generated by linearly independent Hermitian operators

$$E(a_j, b_j) \triangleq \iota^{ab^T} D(a_j, b_j),\ j = 1, \ldots, k.$$

Example: 2-dimensional subgroup of $HW_{2^6} (m = 6)$ generated by

$$\begin{aligned} g^X &= E(111111, 000000) = X^{\otimes 6} \ \text{ and} \\ g^Z &= E(000000, 111111) = Z^{\otimes 6}. \end{aligned}$$

Generator Matrix (using the isomorphism γ): $G = [a_j, b_j]_{j=1,\ldots,k}$.

Example: $G = \left[\begin{array}{cccccc|cccccc} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right]$.

Stabilizer Codes ($N = 2^m$)

k-dimensional stabilizer: commutative subgroup $S \subset HW_N$ generated by linearly independent Hermitian operators

$$E(a_j, b_j) \triangleq \iota^{ab^T} D(a_j, b_j), \ j = 1, \ldots, k.$$

$[\![m, m-k, d]\!]$ Stabilizer Code: The 2^{m-k} dimensional subspace $V(S)$ jointly fixed by all elements of the stabilizer S.

$$V(S) \triangleq \left\{ |\psi\rangle \in \mathbb{C}^N \mid g\,|\psi\rangle = |\psi\rangle \ \forall\, g \in S \right\}.$$

The $[\![6, 4, 2]\!]$ Code: $S \triangleq \langle g^X = X^{\otimes 6} = E(r, 0), g^Z = Z^{\otimes 6} = E(0, r) \rangle$, $r = [111111]$.

Example: The $[\![6,4,2]\!]$ CSS Code

Instance of Calderbank-Shor-Steane (CSS) construction [CS96; Ste96].

Built from the classical $[6,5,2]$ single-parity-check code $\mathcal{C}$.

Generator matrix: $G_{\mathcal{C}} = \begin{bmatrix} H_{\mathcal{C}} \\ G_{\mathcal{C}/\mathcal{C}^{\perp}} \end{bmatrix} = \begin{bmatrix} r \\ h_1 \\ h_2 \\ h_3 \\ h_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}.$

$V(S)$: stabilizer code spanned by the (basis) states $(x = (x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4)$

$$|x\rangle_L \equiv |\psi_x\rangle \triangleq \frac{1}{\sqrt{2}} \left| (000000) + \sum_{j=1}^{4} x_j h_j \right\rangle + \frac{1}{\sqrt{2}} \left| (111111) + \sum_{j=1}^{4} x_j h_j \right\rangle.$$

Note: $V(S)$ is preserved by $S = \langle X^{\otimes 6} = E(r,0), Z^{\otimes 6} = E(0,r) \rangle$.

Overview

$$
\begin{tikzcd}[column sep=huge, row sep=huge]
|x\rangle_L \arrow[r, "\text{logical } HW \text{ operation}"] \arrow[d, "{[\![6,4,2]\!]} \text{ QECC encode}"'] \arrow[dr, phantom, "\text{Need to translate for the } {[\![6,4,2]\!]} \text{ QECC}"] & |\tilde{x}\rangle_L \\
|\psi_x\rangle \arrow[r, "\text{relevant physical operation}"] & |\psi_{\tilde{x}}\rangle \arrow[u, "{[\![6,4,2]\!]} \text{ QECC decode}"']
\end{tikzcd}
$$

Notation: g from Heisenberg-Weyl

g^L is the logical operation and $\bar{g}$ is the corresponding physical operation.

Logical Pauli Operators $X_j^L, Z_j^L \in HW_{2^4}$

Defining Properties: $X_j^L \left|x\right\rangle_L = \left|\tilde{x}\right\rangle_L$, where $\tilde{x}_i = \begin{cases} x_j \oplus 1 & \text{, if } i = j \\ x_i & \text{, if } i \neq j \end{cases}$

and $Z_j^L \left|x\right\rangle_L = (-1)^{x_j} \left|x\right\rangle_L$.

These operators also satisfy $X_i^L Z_j^L = \begin{cases} -Z_j^L X_i^L & \text{if } i = j, \\ Z_j^L X_i^L & \text{if } i \neq j \end{cases}$.

$$\left|x_1 x_2 x_3 x_4\right\rangle_L \equiv \left|\psi_x\right\rangle \triangleq \frac{1}{\sqrt{2}} \left|(000000) + \sum_{j=1}^{4} x_j h_j\right\rangle + \frac{1}{\sqrt{2}} \left|(111111) + \sum_{j=1}^{4} x_j h_j\right\rangle.$$

Observe:

- Applying X_j^L to $\left|x\right\rangle_L \equiv$ Adding/removing h_j in each term of $\left|\psi_x\right\rangle$.
- Applying Z_j^L to $\left|x\right\rangle_L \equiv$ Multiplying $\left|\psi_x\right\rangle$ by (-1) iff h_j present in it.

Synthesizing X_j^L and Z_j^L

Synthesis refers to finding physical operators $\bar{X}_j$ and $\bar{Z}_j$ such that:

- $\bar{X}_j, \bar{Z}_j \in \mathbb{U}_N$ 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 so that, for $g \in S \; \exists \; g' \in S$ s.t.

$$\begin{aligned} \bar{X}_j |\psi_x\rangle &= \bar{X}_j g |\psi_x\rangle \\ &= (\bar{X}_j g \bar{X}_j^{\dagger}) \bar{X}_j |\psi_x\rangle \\ &= g' \bar{X}_j |\psi_x\rangle \;\; \text{(similarly for } \bar{Z}_j\text{)}. \end{aligned}$$

In other words, $\bar{X}_j, \bar{Z}_j$ preserve the code subspace.

Synthesizing X_j^L and Z_j^L

$$|x_1x_2x_3x_4\rangle_L \equiv |\psi_x\rangle \triangleq \frac{1}{\sqrt{2}}\left|(000000) + \sum_{j=1}^{4} x_j h_j\right\rangle + \frac{1}{\sqrt{2}}\left|(111111) + \sum_{j=1}^{4} x_j h_j\right\rangle .$$

Generator matrices $G^X_{\mathcal{C}/\mathcal{C}^\perp}$ and $G^Z_{\mathcal{C}/\mathcal{C}^\perp}$ satisfying $G^X_{\mathcal{C}/\mathcal{C}^\perp}\left(G^Z_{\mathcal{C}/\mathcal{C}^\perp}\right)^T = I_{m-k}$:

$$G^X_{\mathcal{C}/\mathcal{C}^\perp} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \text{ and } G^Z_{\mathcal{C}/\mathcal{C}^\perp} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

$\bar{X}_j$ and $\bar{Z}_j$ specified resp. by the j^{th} row of $G^X_{\mathcal{C}/\mathcal{C}^\perp}(h_j)$ and $G^Z_{\mathcal{C}/\mathcal{C}^\perp}(h'_j)$.

$$\bar{X}_j \triangleq D(h_j, 0),\ \bar{Z}_j \triangleq D(0, h'_j),\ \bar{X}_i\bar{Z}_j = \begin{cases} -\bar{Z}_j\bar{X}_i & \text{if } i = j, \\ \bar{Z}_j\bar{X}_i & \text{if } i \neq j \end{cases},\ \bar{X}_j S \bar{X}_j^\dagger = S, \bar{Z}_j S \bar{Z}_j^\dagger = S.$$

Overview

The Clifford Group Cliff_N

$\mathrm{Cliff}_N \triangleq \mathcal{N}_{\mathbb{U}_N}(HW_N)$: all $g \in \mathbb{U}_N$ for which $gHW_Ng^\dagger = HW_N$.

$$\mathrm{Cliff}_N = \langle HW_N, H, P, \mathrm{CNOT} \text{ or } \mathrm{CZ} \rangle$$

$$\begin{array}{c} \mathbb{U}_N \\ | \\ \mathrm{Cliff}_N \\ | \\ HW_N \\ | \\ S \\ | \\ \langle I_N \rangle \end{array}$$

Gate	Unitary Matrix	Action on Paulis
Hadamard	$H \triangleq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	$HX = ZH$ $HZ = XH$
Phase	$P \triangleq \begin{bmatrix} 1 & 0 \\ 0 & \iota \end{bmatrix}$	$PX = YP$ $PZ = ZP$
Controlled-NOT	$C_{1\to 2} \triangleq \begin{bmatrix} I_2 & 0 \\ 0 & X \end{bmatrix}$	$C_{1\to 2}(X \otimes I_2) = (X \otimes X)C_{1\to 2}$
Controlled-Z	$\mathrm{CZ}_{12} \triangleq \begin{bmatrix} I_2 & 0 \\ 0 & Z \end{bmatrix}$	$\mathrm{CZ}_{12}(X \otimes I_2) = (X \otimes Z)\mathrm{CZ}_{12}$

Cliff_N and Symplectic Geometry

$\mathbb{U}_N$

$\text{Cliff}_N = \{g \in \mathbb{U}_N \mid g HW_N g^\dagger = HW_N\} \simeq \text{Aut}(HW_N).$

Cliff_N

HW_N

S

$\langle I_N \rangle$

Symplectic Representation

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

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

is symplectic, i.e., satisfies $F_g \Omega F_g^T = \Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$.

$F_g \Omega F_g^T = \Omega$: $\langle [a,b], [a',b'] \rangle_s = \langle [a,b]F_g, [a',b']F_g \rangle_s$.

Example: The Controlled-Z Gate

$$g = \mathrm{CZ}_{12},\ F_g = \begin{bmatrix} I_2 & B_g \\ 0 & I_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ & & 1 & 0 \\ & & 0 & 1 \end{bmatrix},\ B_g = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Symplectic Representation: $gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right)$.

$$\begin{aligned} g(X \otimes I_2)g^\dagger &= gE(10,00)g^\dagger \\ &= E\left([10,00]F_g\right) \\ &= E(10,01) \\ &= X \otimes Z \\ \text{(or) } \mathrm{CZ}_{12}(X \otimes I_2) &= (X \otimes Z)\mathrm{CZ}_{12}. \end{aligned}$$

The Symplectic Group $\text{Sp}(2m, \mathbb{F}_2)$ [Cal+98]

Recollect that $D(a, b)D(a', b') = (-1)^{\langle [a,b],[a',b'] \rangle_s} D(a', b')D(a, b)$.

Hence, if g is a $D(a, b)$ then $F_g = I_{2m}$, since $gE(a, b)g^\dagger = \pm E(a, b)$.

$$\text{Sp}(2m, \mathbb{F}_2) \triangleq \{F \in \mathbb{F}_2^{2m \times 2m} \mid F \Omega F^T = \Omega\}.$$

- Map $\phi \colon \text{Cliff}_N \to \text{Sp}(2m, \mathbb{F}_2), \phi(g) \triangleq F_g$, is a group homomorphism with kernel HW_N, i.e., $\phi(g) = I_{2m}$ for $g \in HW_N$.
- Map $\gamma \colon HW_N \to \mathbb{F}_2^{2m}$, $\gamma(D(a, b)) \triangleq [a, b]$, is also a group homomorphism with kernel $\langle \iota^\kappa I_N \rangle$, i.e., $\gamma(h) = [0, 0]$ for $h \in \langle \iota^\kappa I_N \rangle$.

Elementary Symplectic Matrices

Symplectic Matrix F_g	Physical Operator g	Clifford Element
$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$	$H_N = H_2^{\otimes m}$	Full Hadamard
$A_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix}$	$a_Q : \lvert v \rangle \mapsto \lvert vQ \rangle$	CNOTs, Permutations
$T_R = \begin{bmatrix} I_m & R \\ 0 & I_m \end{bmatrix}$ with R symmetric	$t_R = \text{diag}\left(\iota^{vRv^T}\right)$	Phase (P), Controlled-Z (CZ)
$G_k = \begin{bmatrix} L_{m-k} & U_k \\ U_k & L_{m-k} \end{bmatrix}$ $U_k = \mathrm{diag}\left(I_k, O_{m-k}\right)$ $L_{m-k} = \mathrm{diag}\left(O_k, I_{m-k}\right)$	$g_k = H_{2^k} \otimes I_{2^{m-k}}$	Partial Hadamards

Recollect: Operations on Encoded Qubits

$$\begin{tikzcd}[column sep=huge, row sep=huge]
|x\rangle_L \arrow[r, "\text{logical Clifford operation}"] \arrow[d, "\begin{array}{c}[\![6,4,2]\!] \\ \text{QECC} \\ \text{encode}\end{array}"'] \arrow[dr, phantom, "\begin{array}{c}\text{Need to} \\ \text{translate} \\ \text{for the} \\ [\![6,4,2]\!] \\ \text{QECC}\end{array}"] & |\tilde{x}\rangle_L \\
|\psi_x\rangle \arrow[r, "\text{relevant physical operation}"] & |\psi_{\tilde{x}}\rangle \arrow[u, "\begin{array}{c}[\![6,4,2]\!] \\ \text{QECC} \\ \text{decode}\end{array}"']
\end{tikzcd}$$

Notation: g from Clifford

g^L is the logical operation and $\bar{g}$ is the corresponding physical operation.

Synthesis Problem

Find $\bar{g} \in \mathbb{U}_N$ for each $g^L \in \{P_1^L, \mathrm{CZ}_{12}^L, \mathrm{CNOT}_{2\to 1}^L, H_1^L\}$ such that:

- $\bar{g}$ realizes the action of g^L on the encoded qubits.
- $\bar{g}$ acts on HW_{2^6} the same way g^L acts on HW_{2^4} (under conjugation):

$$g^L h^L = (h')^L g^L \Rightarrow \bar{g}\bar{h} = \bar{h}'\bar{g}.$$

- $\bar{g}$ centralizes $S = \langle X^{\otimes 6}, Z^{\otimes 6} \rangle$ (commutes with every element of S).
  - stronger condition than normalize, but is always possible (see paper).

Synthesizing $g^L = \text{CNOT}^L_{2\to 1}$: flip x_1 if $x_2 = 1$

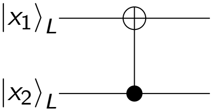
$$|x_1x_2x_3x_4\rangle_L \equiv |\psi_x\rangle \triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{c\in\mathcal{C}^\perp} \left| c + x \cdot G^X_{\mathcal{C}/\mathcal{C}^\perp} \right\rangle = \frac{1}{\sqrt{2}} \sum_{c\in\mathcal{C}^\perp} \left| c + \sum_{j=1}^{4} x_j h_j \right\rangle .$$

Implementing $\text{CNOT}^L_{2\to 1}$ on $|x\rangle_L \equiv x \mapsto x \cdot K$, $K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Then we find that $K \cdot G^X_{\mathcal{C}/\mathcal{C}^\perp} = G^X_{\mathcal{C}/\mathcal{C}^\perp} \cdot Q$, where Q fixes the code $\mathcal{C}^\perp$, i.e.,

$$\sum_{c\in\mathcal{C}^\perp} \left| c + xKG^X_{\mathcal{C}/\mathcal{C}^\perp} \right\rangle = \sum_{c\in\mathcal{C}^\perp} \left| c + xG^X_{\mathcal{C}/\mathcal{C}^\perp} Q \right\rangle = \sum_{c\in\mathcal{C}^\perp} \left| \left(c + xG^X_{\mathcal{C}/\mathcal{C}^\perp} \right) Q \right\rangle .$$

$\bar{g} =$

$\equiv$ 

$= g^L$

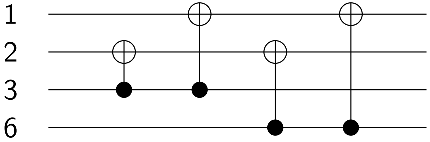
Synthesizing $g^L = \mathrm{CNOT}^L_{2\to1}$: flip x_1 if $x_2 = 1$

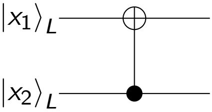
$$|x_1x_2x_3x_4\rangle_L \equiv |\psi_x\rangle \triangleq \frac{1}{\sqrt{|\mathcal{C}^\perp|}} \sum_{c\in\mathcal{C}^\perp} \left| c + x\cdot G^X_{\mathcal{C}/\mathcal{C}^\perp} \right\rangle = \frac{1}{\sqrt{2}} \sum_{c\in\mathcal{C}^\perp} \left| c + \sum_{j=1}^{4} x_j h_j \right\rangle .$$

Implementing $\mathrm{CNOT}^L_{2\to1}$ on $|x\rangle_L \equiv x \mapsto x\cdot K$, $K = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$.

Then we find that $K\cdot G^X_{\mathcal{C}/\mathcal{C}^\perp} = G^X_{\mathcal{C}/\mathcal{C}^\perp}\cdot Q$, where Q fixes the code $\mathcal{C}^\perp$, i.e.,

$$\sum_{c\in\mathcal{C}^\perp} \left| c + xKG^X_{\mathcal{C}/\mathcal{C}^\perp} \right\rangle = \sum_{c\in\mathcal{C}^\perp} \left| c + xG^X_{\mathcal{C}/\mathcal{C}^\perp} Q \right\rangle = \sum_{c\in\mathcal{C}^\perp} \left| \left(c + xG^X_{\mathcal{C}/\mathcal{C}^\perp} \right) Q \right\rangle .$$

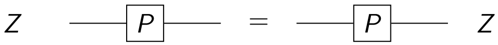
$\bar{g} =$ 

$\equiv$ 

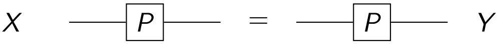
$= g^L$

Recollect Some Identities...

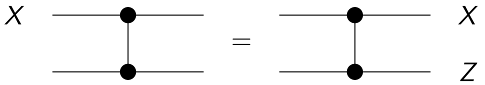
$$PZ = ZP$$



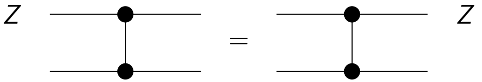
$$\color{red}{PX = YP}$$



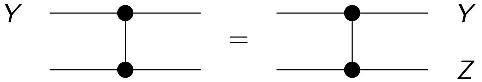
$$\mathrm{CZ}_{12}(X \otimes I_2) = (X \otimes Z)\mathrm{CZ}_{12}$$



$$\mathrm{CZ}_{12}(Z \otimes I_2) = (Z \otimes I_2)\mathrm{CZ}_{12}$$



$$\color{red}{\mathrm{CZ}_{12}(Y \otimes I_2) = (Y \otimes Z)\mathrm{CZ}_{12}}$$



Synthesizing $g^L = P_1^L$

Phase gate on the 1st logical qubit: (translate $P_1^L \mapsto \bar{P}_1$)

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

$$
\begin{array}{l|l}
\bar{X}_1 = X_1 X_2 \xmapsto{\bar{P}_1} \bar{X}_1' = X_1 Y_2 Z_6 & \bar{Z}_1 = Z_2 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_1' = Z_2 Z_6 \\
\bar{X}_2 = X_1 X_3 \xmapsto{\bar{P}_1} \bar{X}_2' = X_1 X_3 & \bar{Z}_2 = Z_3 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_2' = Z_3 Z_6 \\
\bar{X}_3 = X_1 X_4 \xmapsto{\bar{P}_1} \bar{X}_3' = X_1 X_4 & \bar{Z}_3 = Z_4 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_3' = Z_4 Z_6 \\
\bar{X}_4 = X_1 X_5 \xmapsto{\bar{P}_1} \bar{X}_4' = X_1 X_5 & \bar{Z}_4 = Z_5 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_4' = Z_5 Z_6
\end{array} .
$$

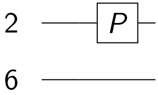
$\bar{P}_1 =$ 2 —— 6 —— $\equiv |x_1\rangle_L$ —$\boxed{P}$— $= P_1^L$

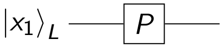
Synthesizing $g^L = P_1^L$

Phase gate on the 1st logical qubit: (translate $P_1^L \mapsto \bar{P}_1$)

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

$$\begin{array}{l|l} \bar{X}_1 = X_1 \color{red}{X_2} \xmapsto{\bar{P}_1} \bar{X}_1' = X_1 \color{red}{Y_2 Z_6} & \bar{Z}_1 = Z_2 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_1' = Z_2 Z_6 \\ \bar{X}_2 = X_1 X_3 \xmapsto{\bar{P}_1} \bar{X}_2' = X_1 X_3 & \bar{Z}_2 = Z_3 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_2' = Z_3 Z_6 \\ \bar{X}_3 = X_1 X_4 \xmapsto{\bar{P}_1} \bar{X}_3' = X_1 X_4 & \bar{Z}_3 = Z_4 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_3' = Z_4 Z_6 \\ \bar{X}_4 = X_1 X_5 \xmapsto{\bar{P}_1} \bar{X}_4' = X_1 X_5 & \bar{Z}_4 = Z_5 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_4' = Z_5 Z_6 \end{array}.$$

$\bar{P}_1 =$ 

$\equiv$ 

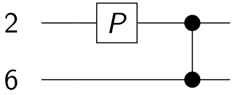
$= P_1^L$

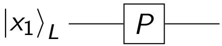
Synthesizing $g^L = P_1^L$

Phase gate on the 1st logical qubit: (translate $P_1^L \mapsto \bar{P}_1$)

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

$$\begin{array}{ll|ll}
\bar{X}_1 = X_1 X_2 \xmapsto{\bar{P}_1} \bar{X}_1' = X_1 Y_2 Z_6 & & \bar{Z}_1 = Z_2 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_1' = Z_2 Z_6 & \\
\bar{X}_2 = X_1 X_3 \xmapsto{\bar{P}_1} \bar{X}_2' = X_1 X_3 & & \bar{Z}_2 = Z_3 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_2' = Z_3 Z_6 & \\
\bar{X}_3 = X_1 X_4 \xmapsto{\bar{P}_1} \bar{X}_3' = X_1 X_4 & & \bar{Z}_3 = Z_4 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_3' = Z_4 Z_6 & . \\
\bar{X}_4 = X_1 X_5 \xmapsto{\bar{P}_1} \bar{X}_4' = X_1 X_5 & & \bar{Z}_4 = Z_5 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_4' = Z_5 Z_6 &
\end{array}$$

$\bar{P}_1 =$ 

$\equiv$ 

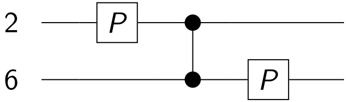
$= P_1^L$

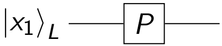
Synthesizing $g^L = P_1^L$

Phase gate on the 1st logical qubit: (translate $P_1^L \mapsto \bar{P}_1$)

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

$$
\begin{array}{l|l}
\bar{X}_1 = X_1 X_2 \xmapsto{\bar{P}_1} \bar{X}_1' = X_1 Y_2 Z_6 & \bar{Z}_1 = Z_2 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_1' = Z_2 Z_6 \\
\bar{X}_2 = X_1 X_3 \xmapsto{\bar{P}_1} \bar{X}_2' = X_1 X_3 & \bar{Z}_2 = Z_3 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_2' = Z_3 Z_6 \\
\bar{X}_3 = X_1 X_4 \xmapsto{\bar{P}_1} \bar{X}_3' = X_1 X_4 & \bar{Z}_3 = Z_4 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_3' = Z_4 Z_6 \\
\bar{X}_4 = X_1 X_5 \xmapsto{\bar{P}_1} \bar{X}_4' = X_1 X_5 & \bar{Z}_4 = Z_5 Z_6 \xmapsto{\bar{P}_1} \bar{Z}_4' = Z_5 Z_6
\end{array}
.
$$

$\bar{P}_1 =$ 

$\equiv$ 

$= P_1^L$

Synthesizing $g^L = \mathrm{CZ}_{12}^L$

Definition : $$\overline{\mathrm{CZ}}_{12}\bar{X}_j\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \begin{cases} \bar{X}_1\bar{Z}_2 & \text{if } j = 1, \\ \bar{Z}_1\bar{X}_2 & \text{if } j = 2, \\ \bar{X}_j & \text{if } j \neq 1, 2 \end{cases},$$

$$\overline{\mathrm{CZ}}_{12}\bar{Z}_j\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{Z}_j \ \forall\ j = 1, 2, 3, 4.$$

Recollect:

1. From rows of $G^X_{\mathcal{C}/\mathcal{C}^\perp}, G^Z_{\mathcal{C}/\mathcal{C}^\perp}$ we get the logical Paulis:

$$\begin{array}{l|l} \bar{X}_1 = X_1X_2 = E(110000, 000000) & \bar{Z}_1 = Z_2Z_6 = E(000000, 010001) \\ \bar{X}_2 = X_1X_3 = E(101000, 000000) & \bar{Z}_2 = Z_3Z_6 = E(000000, 001001) \\ \bar{X}_3 = X_1X_4 = E(100100, 000000) & \bar{Z}_3 = Z_4Z_6 = E(000000, 000101) \\ \bar{X}_4 = X_1X_5 = E(100010, 000000) & \bar{Z}_4 = Z_5Z_6 = E(000000, 000011) \end{array}$$

2. $\mathrm{Cliff}_{2^6} \cong \mathrm{Sp}(12, \mathbb{F}_2)$: $\overline{\mathrm{CZ}}_{12}E(a,b)\overline{\mathrm{CZ}}_{12}^{\dagger} = \pm E\left([a,b]F_{\overline{\mathrm{CZ}}_{12}}\right)$. Find $F_{\overline{\mathrm{CZ}}_{12}}$.

Finding $\overline{\mathrm{CZ}}_{12}$ via $\mathrm{Sp}(2m = 12, \mathbb{F}_2)$

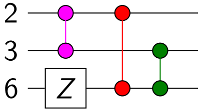
$$\bar{X}_1 = X_1 X_2 \xmapsto{\overline{\mathrm{CZ}}_{12}} X_1 X_2 Z_3 Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [110000, 000000] F_{\overline{\mathrm{CZ}}_{12}} = [110000, 001001]$$

$$\bar{X}_2 = X_1 X_3 \xmapsto{\overline{\mathrm{CZ}}_{12}} X_1 X_3 Z_2 Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [101000, 000000] F_{\overline{\mathrm{CZ}}_{12}} = [101000, 010001]$$

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

One possible solution

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



$$\Downarrow$$

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

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

Synthesizing $g^L = H_1^L$

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

One solution: (note that $F_{\bar{H}_1}$ is not of any elementary symplectic form)

$$F_{\bar{H}_1} = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \; A = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}, \; B = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix},$$

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

Decomposition of a Symplectic Matrix [Can17]

Symplectic Matrix $F = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$

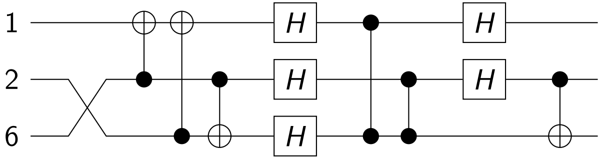
$$\begin{array}{c}
(A, B) \\
\Big\downarrow \quad A_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix} \\
\begin{bmatrix} I_k & 0 & R_k & 0 \\ 0 & 0 & 0 & I_{m-k} \end{bmatrix} \\
\Bigg\downarrow \quad T_{R_2} = \begin{bmatrix} I_m & R_2 \\ 0 & I_m \end{bmatrix} \text{ with } R_2 = \begin{bmatrix} R_k & 0 \\ 0 & 0 \end{bmatrix} \\
\begin{bmatrix} I_k & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{m-k} \end{bmatrix} \\
\Big\downarrow \quad G_k \Omega \\
(I_m, 0)
\end{array}$$

Finally, $A_{Q_1^{-1}} F A_{Q_2^{-1}} T_{R_2} G_k \Omega = \Omega \, T_{R_1} \Omega$.
So $F = A_{Q_1} \Omega \, T_{R_1} G_k T_{R_2} A_{Q_2}$.

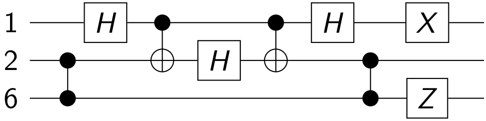
Translate each matrix to a Clifford element!

Synthesizing H_1^L for the $[\![6,4,2]\!]$ Code

Our solution using the above general decomposition:



Particular solution for this case from [CR17]:



Note: Both circuits correspond to the same symplectic solution $F_{\bar{H}_1}$.

Algorithm to Synthesize Logical Clifford Operators

1. Determine the target $\bar{g}$ by specifying its action on $\bar{X}_i, \bar{Z}_i$ [Got09]: $\bar{g}\bar{X}_i\bar{g}^\dagger = \bar{X}_i', \bar{g}\bar{Z}_i\bar{g}^\dagger = \bar{Z}_i'$. Add conditions to normalize or centralize S.
2. Using the maps γ, ϕ, transform these relations into linear equations on $F_{\bar{g}} \in \mathrm{Sp}(2m, \mathbb{F}_2)$, i.e., $\bar{g}E(a,b)\bar{g}^\dagger = \pm E\left([a,b]F_{\bar{g}}\right) \Rightarrow [a,b] \mapsto [a,b]F_{\bar{g}}$.
3. Find the feasible symplectic solution set $\mathcal{F}_{\bar{g}}$ using transvections.
4. Factor each $F_{\bar{g}} \in \mathcal{F}_{\bar{g}}$ using above decomposition [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 $S^\perp = \langle S, \bar{X}_i, \bar{Z}_i \rangle$).
6. Express $\bar{g}$ as a sequence of physical Clifford gates obtained from the factorization in step 4.

Overview

Symplectic Transvections

Definition: Given a vector $h \in \mathbb{F}_2^{2m}$, the transvection $Z_h : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ is

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

Fact: Transvections generate the binary symplectic group $\mathrm{Sp}(2m, \mathbb{F}_2)$.

Lemma ([SAF08; KS14])

Let $x, y \in \mathbb{F}_2^{2m}$. Then there exists at most two transvections F_{h_1}, F_{h_2} s.t. $xF_{h_1}F_{h_2} = y$.

We extend this to map a sequence of vectors x_i to y_i, $i = 1, \ldots, t$.

Solving for Symplectic F s.t. $x_i F = y_i, \;\; i = 1, \ldots, t$

Input: $x_i, y_i \in \mathbb{F}_2^{2m}$ s.t. $\langle x_i, x_j \rangle_s = \langle y_i, y_j \rangle_s \;\forall\; i, j \in \{1, \ldots, t\}$.
Output: $F \in \mathrm{Sp}(2m, \mathbb{F}_2)$ satisfying $x_i F = y_i \;\forall\; i \in \{1, \ldots, t\}$

if $\langle x_1, y_1 \rangle_s = 1$ **then**
  set $h_1 \triangleq x_1 + y_1$ and $F_1 \triangleq F_{h_1}$.
else
  $h_{11} \triangleq w_1 + y_1, h_{12} \triangleq x_1 + w_1$ and $F_1 \triangleq F_{h_{11}} F_{h_{12}}$.
end if
for $i = 2, \ldots, t$ **do**
  Calculate $\tilde{x}_i \triangleq x_i F_{i-1}$ and $\langle \tilde{x}_i, y_i \rangle_s$.
  if $\tilde{x}_i = y_i$ **then**
    Set $F_i \triangleq F_{i-1}$. **Continue**.
  end if
  if $\langle \tilde{x}_i, y_i \rangle_s = 1$ **then**
    Set $h_i \triangleq \tilde{x}_i + y_i, F_i \triangleq F_{i-1} F_{h_i}$.
  else
    Find a w_i s.t. $\langle \tilde{x}_i, w_i \rangle_s = \langle y_i, w_i \rangle_s = 1$ and $\langle y_j, w_i \rangle_s = \langle y_j, y_i \rangle_s \;\forall\; j < i$.
    Set $h_{i1} \triangleq w_i + y_i, h_{i2} \triangleq \tilde{x}_i + w_i, F_i \triangleq F_{i-1} F_{h_{i1}} F_{h_{i2}}$.
  end if
end for
return $F \triangleq F_t$.

Algorithm to Solve for all Symplectic Solutions

Input: $u_a, v_b \in \mathbb{F}_2^{2m}$ s.t. $\langle u_a, v_b \rangle_s = \delta_{ab}$ and $\langle u_a, u_b \rangle_s = \langle v_a, v_b \rangle_s = 0,\ a, b \in \{1, \ldots, m\}$.
$u_i', v_j' \in \mathbb{F}_2^{2m}$ s.t. $\langle u_{i_1}', u_{i_2}' \rangle_s = 0, \langle v_{j_1}', v_{j_2}' \rangle_s = 0, \langle u_i', v_j' \rangle_s = \delta_{ij}$, where
$i, i_1, i_2 \in \mathcal{I},\ j, j_1, j_2 \in \mathcal{J},\ \mathcal{I}, \mathcal{J} \subseteq \{1, \ldots, m\}$.

Output: $\mathcal{F} \subset \mathrm{Sp}(2m, \mathbb{F}_2)$ s.t. each $F \in \mathcal{F}$ satisfies $u_i F = u_i'\ \forall\ i \in \mathcal{I}$, & $v_j F = v_j'\ \forall\ j \in \mathcal{J}$.

Determine a particular symplectic solution F_0 for the linear system.
Form the matrix A whose a-th row is $u_a F_0$ and $(m + b)$-th row is $v_b F_0$, where $a, b \in \{1, \ldots, m\}$.
Compute the inverse of this matrix, A^{-1}, in $\mathbb{F}_2$.
Set $\mathcal{F} = \phi$ and $\alpha \triangleq |\bar{\mathcal{I}}| + |\bar{\mathcal{J}}|$, where $\bar{\mathcal{I}}, \bar{\mathcal{J}}$ denote the set complements of $\mathcal{I}, \mathcal{J}$ in $\{1, \ldots, m\}$, respectively.
for $\ell = 1, \ldots, 2^{\alpha(\alpha+1)/2}$ **do**
    Form a matrix $B_\ell = A$.
    For $i \notin \mathcal{I}$ and $j \notin \mathcal{J}$ replace the i-th and $(m+j)$-th rows of B_ℓ with arbitrary vectors such that $B_\ell \Omega B_\ell^T = \Omega$ and $B_\ell \neq B_{\ell'}$ for $1 \leq \ell' < \ell$.
    Compute $F' = A^{-1} B$.
    Add $F_\ell \triangleq F_0 F'$ to $\mathcal{F}$.
end for
return $\mathcal{F}$

More Results . . .

Given a stabilizer code with logical Paulis $\bar{X}_i, \bar{Z}_i$, we have the system

$$\begin{bmatrix} \gamma(\bar{X}) \\ \gamma(S) \\ \gamma(\bar{Z}) \end{bmatrix} F = \begin{bmatrix} \gamma(\bar{X}') \\ \gamma(S') \\ \gamma(\bar{Z}') \end{bmatrix}.$$

Theorem

For an $[\![m, m-k]\!]$ stabilizer code, the number of symplectic solutions for each logical Clifford operator is $2^{k(k+1)/2}$.

Theorem

For each logical Clifford operator of an $[\![m, m-k]\!]$ stabilizer code, one can always synthesize a solution that centralizes the stabilizer S.

Recap: In this talk...

- Synthesis of logical Pauli operators for CSS codes
  - Two popular algorithms in the literature: [Got97b; Wil09].
  - We provided a closely-related but classical coding-theoretic perspective.

- Synthesis of logical Clifford operators for stabilizer codes
  - Methods seem to exist only for particular QECCs and operations, e.g., [Got97a; Fow+12; GR13; CR17].
  - We proposed a systematic framework using symplectic geometry.
  - For an $[\![m, m-k]\!]$ stabilizer code, we showed that there are $2^{k(k+1)/2}$ symplectic solutions for a given logical Clifford operator.
  - Then enumerated these matrices efficiently using symplectic transvections, and translated them to physical operators (circuits).
  - Showed that any normalizing solution can be converted into a centralizing solution, i.e., commute with every stabilizer element.

Future Work

- How to leverage this efficient enumeration during the process of computation?
- Understand the geometry of the solution space of symplectic matrices.
- Optimization of solutions with respect to a useful metric.
- Decomposition of symplectic matrix motivated by practical constraints, e.g., circuit complexity, fault-tolerance.
- Extend the framework to accommodate non-Clifford gates, e.g., T.
- . . . etc.

References

[CS96] A. R. Calderbank and Peter W. Shor. "Good quantum error-correcting codes exist". In: *Phys. Rev. A* 54 (2 Aug. 1996), pp. 1098–1105.

[Ste96] A. M. Steane. "Simple quantum error-correcting codes". In: *Phys. Rev. A* 54.6 (1996), pp. 4741–4751. DOI: 10.1103/PhysRevA.54.4741.

[Got97a] Daniel Gottesman. "A Theory of Fault-Tolerant Quantum Computation". In: *arXiv preprint arXiv:quant-ph/9702029* (1997).

[Got97b] Daniel Gottesman. "Stabilizer codes and quantum error correction". PhD thesis. California Institute of Technology, 1997.

References

[Cal+98] A.R. Calderbank et al. "Quantum error correction via codes over GF(4)". In: *IEEE Trans. Inform. Theory* 44.4 (July 1998), pp. 1369–1387.

[DD03] Jeroen Dehaene and Bart De Moor. "Clifford group, stabilizer states, and linear and quadratic operations over GF(2)". In: *Phys. Rev. A* 68.4 (Oct. 2003), p. 042318. DOI: 10.1103/PhysRevA.68.042318.

[SAF08] A Salam, E Al-Aidarous, and A El Farouk. "Optimal symplectic Householder transformations for SR decomposition". In: *Lin. Algebra and its Appl.* 429 (2008), pp. 1334–1353. DOI: 10.1016/j.laa.2008.02.029.

[Got09] Daniel Gottesman. "An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation". In: *arXiv preprint arXiv:0904.2557* (2009).

References

[Wil09] Mark M Wilde. “Logical operators of quantum codes”. In: *Phys. Rev. A* 79.6 (2009), pp. 062322-1–062322-5. DOI: 10.1103/PhysRevA.79.062322.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[Fow+12] Austin G. Fowler et al. “Surface codes: Towards practical large-scale quantum computation”. In: *arXiv preprint arXiv:1208.0928* (2012). [Online]. Available: http://arxiv.org/abs/1208.0928.

[GR13] Markus Grassl and Martin Roetteler. “Leveraging automorphisms of quantum codes for fault-tolerant quantum computation”. In: *Proc. IEEE Int. Symp. Inform. Theory*. IEEE, July 2013, pp. 534–538.

[KMM13] Vadym Kliuchnikov, Dmitri Maslov, and Michele Mosca. "Asymptotically Optimal Approximation of Single Qubit Unitaries by Clifford and T Circuits Using a Constant Number of Ancillary Qubits". In: *Phys. Rev. Lett.* 110.19 (May 2013), p. 190502. DOI: 10.1103/PhysRevLett.110.190502.

[KS14] Robert Koenig and John A Smolin. "How to efficiently select an arbitrary Clifford group element". In: *J. Math. Phys.* 55.12 (Dec. 2014), p. 122202. DOI: 10.1063/1.4903507.

[Can17] Trung Can. "An Algorithm to Generate a Unitary Transformation from Logarithmically Many Random Bits". Research Independent Study Report, Duke Univeristy. 2017.

[CR17] Rui Chao and Ben W Reichardt. "Fault-tolerant quantum computation with few qubits". In: *arXiv preprint arXiv:1705.05365* (2017).

Thank you! Questions?

For details see https://arxiv.org/abs/1803.06987.

Have fun synthesizing Clifford circuits for your favorite stabilizer code, at https://github.com/nrenga/symplectic-arxiv18a :-).

Any feedback is much appreciated.