Synthesis of Logical Clifford Operators via Symplectic Geometry

Narayanan Rengaswamy
Information Initiative at Duke (iiD), Duke University

Joint Work: Swanand Kadhe, Robert Calderbank, and Henry Pfister

2018 IEEE Intl. Symp. on Information Theory
Vail, Colorado, USA

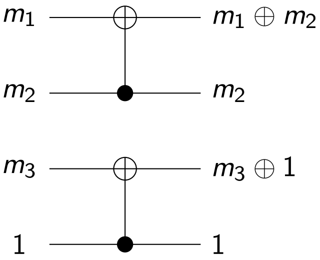
arXiv:1803.06987

June 19, 2018

Overview

Encoded Computation: An Example

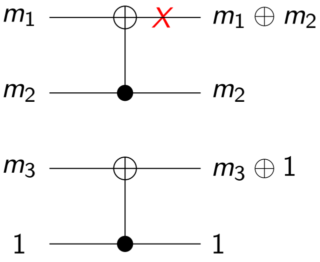
Uncoded: 3 bits



Coded: $[4, 3, 2]$ SPC

Encoded Computation: An Example

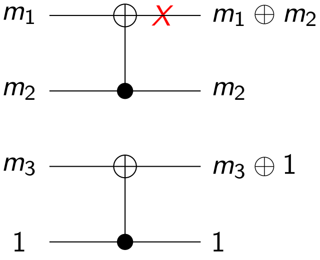
Uncoded: 3 bits



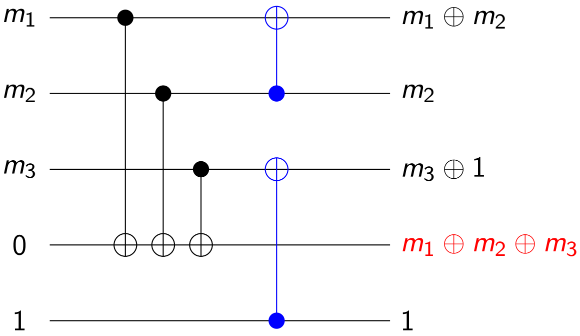
Coded: $[4, 3, 2]$ SPC

Encoded Computation: An Example

Uncoded: 3 bits

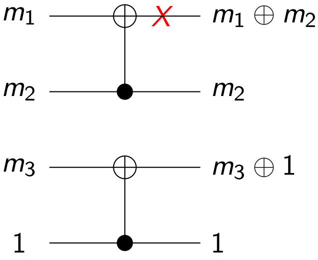


Coded: $[4, 3, 2]$ SPC

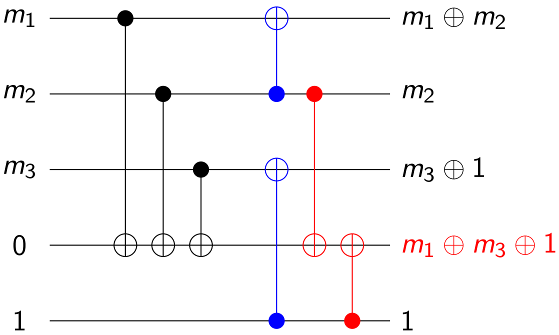


Encoded Computation: An Example

Uncoded: 3 bits

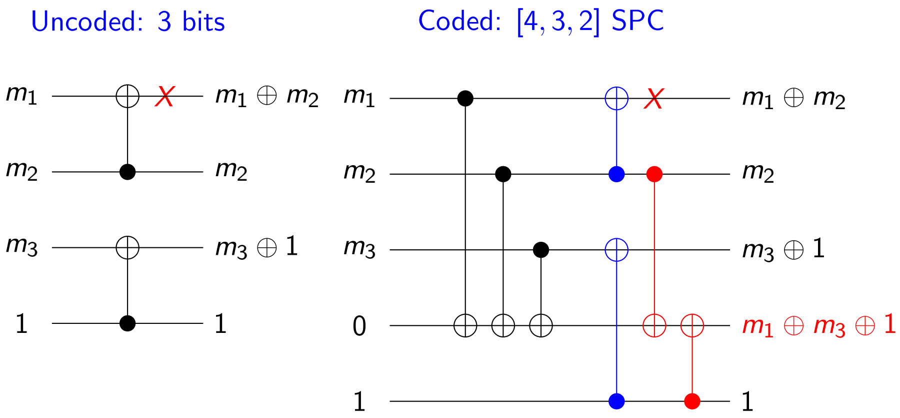


Coded: $[4, 3, 2]$ SPC



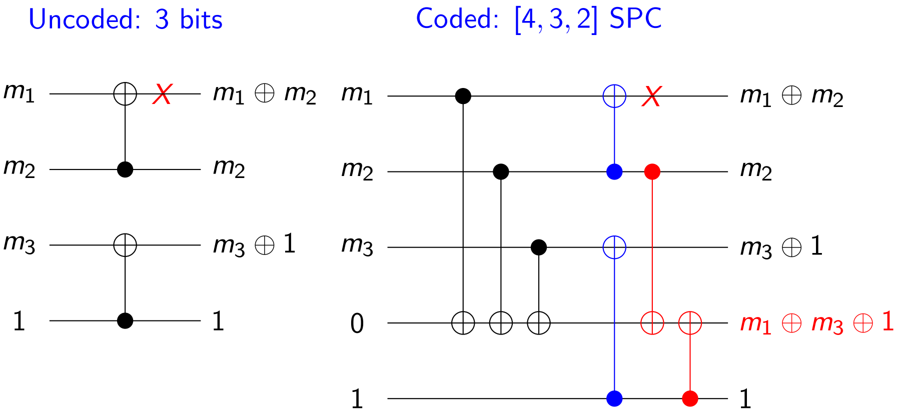
KEY: Physical circuit has to realize logical operation & preserve the code.

Encoded Computation: An Example



KEY: Physical circuit has to realize logical operation & preserve the code.

Encoded Computation: An Example



KEY: Physical circuit has to realize logical operation & preserve the code.

In the quantum analogue of this, we have arbitrary unitary operators!

Problem and Motivation

- Quantum systems are noisy - quantum error-correcting codes (QECCs) and quantum control are essential for reliable computation.
- QECCs encode logical information into physical states. Lots of interesting work on QECCs, their properties and efficient decoders.
- QECCs alone aren't enough; need to perform computation on the protected information stored in physical qubits.
- Synthesis of physical operators that realize such encoded computation seems to exist essentially for particular QECC examples.
- We propose a systematic framework for synthesizing a large class of such operators, called the Clifford group, for stabilizer QECCs.

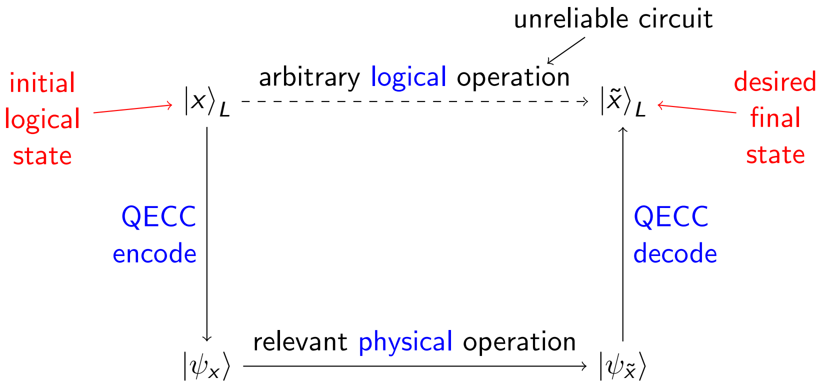
Problem and Motivation

- Quantum systems are noisy - quantum error-correcting codes (QECCs) and quantum control are essential for reliable computation.
- QECCs encode logical information into physical states. Lots of interesting work on QECCs, their properties and efficient decoders.
- QECCs alone aren't enough; need to perform computation on the protected information stored in physical qubits.
- Synthesis of physical operators that realize such encoded computation seems to exist essentially for particular QECC examples.
- We propose a systematic framework for synthesizing a large class of such operators, called the Clifford group, for stabilizer QECCs.

Problem and Motivation

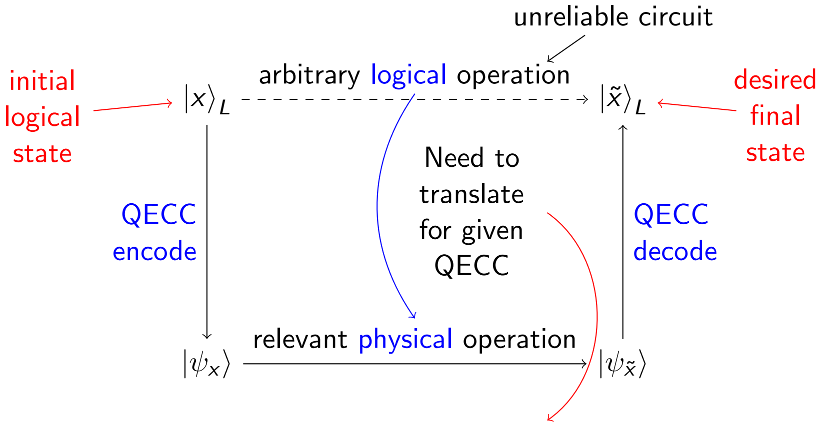
- Quantum systems are noisy - quantum error-correcting codes (QECCs) and quantum control are essential for reliable computation.
- QECCs encode logical information into physical states. Lots of interesting work on QECCs, their properties and efficient decoders.
- QECCs alone aren't enough; need to perform computation on the protected information stored in physical qubits.
- Synthesis of physical operators that realize such encoded computation seems to exist essentially for particular QECC examples.
- We propose a systematic framework for synthesizing a large class of such operators, called the Clifford group, for stabilizer QECCs.

Problem: Operations on Encoded Qubits



QECC: Quantum Error-Correcting Codes

Problem: Operations on Encoded Qubits

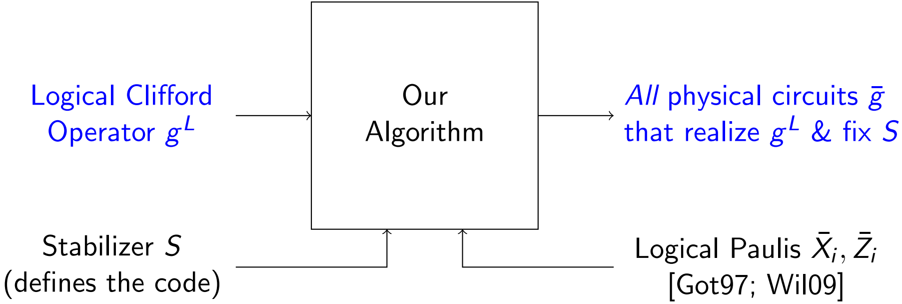


We do this for logical Clifford operations on stabilizer QECCs

QECC: Quantum Error-Correcting Codes

Algorithms on GitHub

Our algorithms are available open-source at:
https://github.com/nrenga/symplectic-arxiv18a



Overview

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) : $$|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle .$$

m Qubits: If qubit i is in the state $|v_i\rangle \in \{|0\rangle, |1\rangle\}$ then the Kronecker product $|v_1\rangle \otimes \cdots \otimes |v_m\rangle \triangleq |v\rangle$ describes the state of the system.

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

Pure state (m qubits): $|\phi\rangle = \sum_{v \in \mathbb{F}_2^m} \alpha_v |v\rangle$, $\alpha_v \in \mathbb{C}$, $\sum_{v \in \mathbb{F}_2^m} |\alpha_v|^2 = 1$.

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 $|\alpha|^2 + |\beta|^2 = 1$.

$$\text{Example } (m = 2 \text{ qubits}): \quad |0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle.$$

m Qubits: If qubit i is in the state $|v_i\rangle \in \{|0\rangle, |1\rangle\}$ then the Kronecker product $|v_1\rangle \otimes \cdots \otimes |v_m\rangle \triangleq |v\rangle$ describes the state of the system.

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

Pure state (m qubits): $|\phi\rangle = \sum_{v \in \mathbb{F}_2^m} \alpha_v |v\rangle$, $\alpha_v \in \mathbb{C}$, $\sum_{v \in \mathbb{F}_2^m} |\alpha_v|^2 = 1$.

Heisenberg-Weyl Group HW_N

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

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

Bit-Flip: $X \triangleq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \Rightarrow X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle.$

Phase-Flip: $Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle.$

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

Fact: $\{I_2, X, Z, Y\}$ forms an orthonormal basis for operators in $\mathbb{C}^{2\times 2}$.

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

Heisenberg-Weyl Group HW_N

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

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

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

$$\text{Phase-Flip}: \quad Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle.$$

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

Fact: $\{I_2, X, Z, Y\}$ forms an orthonormal basis for operators in $\mathbb{C}^{2\times 2}$.

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

Heisenberg-Weyl Group HW_N

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

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

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

$$\text{Phase-Flip}: \quad Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle.$$

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

Fact: $\{I_2, X, Z, Y\}$ forms an orthonormal basis for operators in $\mathbb{C}^{2\times 2}$.

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

Heisenberg-Weyl Group HW_N

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

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

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

$$\text{Phase-Flip}: \quad Z \triangleq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \Rightarrow Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle.$$

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

Fact: $\{I_2, X, Z, Y\}$ forms an orthonormal basis for operators in $\mathbb{C}^{2\times 2}$.

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

Hierarchy of the Unitary Group (m Qubits)

$\mathbb{U}_N \longrightarrow$ The group of all $2^m \times 2^m$ unitary matrices ($N = 2^m$)

$\text{Cliff}_N \longrightarrow$ Maps every HW_N element to another under conjugation
$\approx \text{Sp}(2m, \mathbb{F}_2)$: $2m \times 2m$ binary symplectic matrices

$HW_N \longrightarrow$ $HW_2 \otimes HW_2 \otimes \cdots \otimes HW_2$ (m times)
$\approx \mathbb{F}_2^{2m}$ under the symplectic inner product

$S \longrightarrow$ k-dimensional commutative subgroup of HW_N
– their common eigenspace defines a stabilizer code

$$V(S) \triangleq \{|\psi\rangle : g\,|\psi\rangle = |\psi\rangle \;\; \forall\, g \in S\}$$

Cliff_N: complexity reduced from $2^m \times 2^m$ (complex) to $2m \times 2m$ (binary)!

Hierarchy of the Unitary Group (m Qubits)

$\mathbb{U}_N \longrightarrow$ The group of all $2^m \times 2^m$ unitary matrices ($N = 2^m$)

$\text{Cliff}_N \longrightarrow$ Maps every HW_N element to another under conjugation
$\approx \text{Sp}(2m, \mathbb{F}_2)$: $2m \times 2m$ binary symplectic matrices

$HW_N \longrightarrow$ $HW_2 \otimes HW_2 \otimes \cdots \otimes HW_2$ (m times)
$\approx \mathbb{F}_2^{2m}$ under the symplectic inner product

$S \longrightarrow$ k-dimensional commutative subgroup of HW_N
– their common eigenspace defines a stabilizer code
$V(S) \triangleq \{|\psi\rangle : g|\psi\rangle = |\psi\rangle \ \forall g \in S\}$

Cliff_N: complexity reduced from $2^m \times 2^m$ (complex) to $2m \times 2m$ (binary)!

Hierarchy of the Unitary Group (m Qubits)

$\mathbb{U}_N \longrightarrow$ The group of all $2^m \times 2^m$ unitary matrices ($N = 2^m$)

$\mathrm{Cliff}_N \longrightarrow$ Maps every HW_N element to another under conjugation
$\approx \mathrm{Sp}(2m, \mathbb{F}_2)$: $2m \times 2m$ binary symplectic matrices

$HW_N \longrightarrow$ $HW_2 \otimes HW_2 \otimes \cdots \otimes HW_2$ (m times)
$\approx \mathbb{F}_2^{2m}$ under the symplectic inner product

$S \longrightarrow$ k-dimensional commutative subgroup of HW_N
– their common eigenspace defines a stabilizer code
$$V(S) \triangleq \{|\psi\rangle : g\,|\psi\rangle = |\psi\rangle \ \ \forall\, g \in S\}$$

Cliff_N: complexity reduced from $2^m \times 2^m$ (complex) to $2m \times 2m$ (binary)!

Hierarchy of the Unitary Group (m Qubits)

$\mathbb{U}_N \longrightarrow$ The group of all $2^m \times 2^m$ unitary matrices ($N = 2^m$)

$\text{Cliff}_N \longrightarrow$ Maps every HW_N element to another under conjugation

$\approx \text{Sp}(2m, \mathbb{F}_2)$: $2m \times 2m$ binary symplectic matrices

$HW_N \longrightarrow$ $HW_2 \otimes HW_2 \otimes \cdots \otimes HW_2$ (m times)

$\approx \mathbb{F}_2^{2m}$ under the symplectic inner product

$S \longrightarrow$ k-dimensional commutative subgroup of HW_N

– their common eigenspace defines a stabilizer code

$$V(S) \triangleq \{|\psi\rangle : g\,|\psi\rangle = |\psi\rangle \ \ \forall\, g \in S\}$$

Cliff_N: complexity reduced from $2^m \times 2^m$ (complex) to $2m \times 2m$ (binary)!

Heisenberg-Weyl and Clifford Groups

HW_N Elements $\approx \mathbb{F}_2^{2m}$: $\gamma(D(a,b)) \triangleq [a,b]$

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

$$D(a,b) \triangleq X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_m} Z^{b_m} \in \mathbb{U}_N \; ; N = 2^m.$$

- $D(a,b), D(a',b') \in HW_N$ commute iff $a^T b' + b^T a' = 0$.

Heisenberg-Weyl and Clifford Groups

HW_N Elements $\approx \mathbb{F}_2^{2m}$: $\gamma(D(a,b)) \triangleq [a,b]$

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

$$D(a,b) \triangleq X^{a_1} Z^{b_1} \otimes \cdots \otimes X^{a_m} Z^{b_m} \in \mathbb{U}_N \; ; N = 2^m.$$

- $D(a,b), D(a',b') \in HW_N$ commute iff $a^T b' + b^T a' = 0$.

Cliff_N Elements $\approx \text{Sp}(2m, \mathbb{F}_2)$: $\phi(g) \triangleq F_g$

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

$$gE(a,b)g^\dagger = \pm E\left([a,b]F_g\right), \text{ where } F_g \text{ is symplectic,}$$

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

Overview

Synthesizing Logical CZ_{12} for the $[\![6,4,2]\!]$ Code

Definition (partial) : $\overline{CZ}_{12}\bar{X}_1\overline{CZ}_{12}^{\dagger} \triangleq \bar{X}_1\bar{Z}_2$, $\overline{CZ}_{12}\bar{X}_2\overline{CZ}_{12}^{\dagger} \triangleq \bar{Z}_1\bar{X}_2$.

The process:

1. Generator matrices for the $[6,5,2]$ SPC code yield logical Paulis:

$$\bar{X}_1 = X_1X_2 = E(110000, 000000) \quad | \quad \bar{Z}_1 = Z_2Z_6 = E(000000, 010001)$$
$$\bar{X}_2 = X_1X_3 = E(101000, 000000) \quad | \quad \bar{Z}_2 = Z_3Z_6 = E(000000, 001001)$$

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

$$\bar{X}_1 = X_1X_2 \xmapsto{\overline{CZ}_{12}} X_1X_2Z_3Z_6 \xleftrightarrow{\gamma,\phi} [110000, 000000]F_{\overline{CZ}_{12}} = [110000, 001001]$$
$$\bar{X}_2 = X_1X_3 \xmapsto{\overline{CZ}_{12}} X_1X_3Z_2Z_6 \xleftrightarrow{\gamma,\phi} [101000, 000000]F_{\overline{CZ}_{12}} = [101000, 010001].$$

Synthesizing Logical CZ_{12} for the $[\![6,4,2]\!]$ Code

Definition (partial) : $\overline{\mathrm{CZ}}_{12}\bar{X}_1\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{X}_1\bar{Z}_2, \ \overline{\mathrm{CZ}}_{12}\bar{X}_2\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{Z}_1\bar{X}_2.$

The process:

1. Generator matrices for the $[6,5,2]$ SPC code yield logical Paulis:

$$\bar{X}_1 = X_1X_2 = E(110000, 000000) \quad \bar{Z}_1 = Z_2Z_6 = E(000000, 010001)$$
$$\bar{X}_2 = X_1X_3 = E(101000, 000000) \quad \bar{Z}_2 = Z_3Z_6 = E(000000, 001001)$$

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 $F_{\overline{\mathrm{CZ}}_{12}}$.

$$\bar{X}_1 = X_1X_2 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1X_2Z_3Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [110000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [110000, 001001]$$
$$\bar{X}_2 = X_1X_3 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1X_3Z_2Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [101000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [101000, 010001].$$

Synthesizing Logical CZ_{12} for the $[\![6,4,2]\!]$ Code

Definition (partial) : $\overline{\mathrm{CZ}}_{12}\bar{X}_1\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{X}_1\bar{Z}_2,\ \overline{\mathrm{CZ}}_{12}\bar{X}_2\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{Z}_1\bar{X}_2.$

The process:

1. Generator matrices for the $[6,5,2]$ SPC code yield logical Paulis:

$\bar{X}_1 = X_1X_2 = E(110000, 000000)$	$\bar{Z}_1 = Z_2Z_6 = E(000000, 010001)$
$\bar{X}_2 = X_1X_3 = E(101000, 000000)$	$\bar{Z}_2 = Z_3Z_6 = E(000000, 001001)$

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 $F_{\overline{\mathrm{CZ}}_{12}}$.

$$\bar{X}_1 = X_1X_2 \xmapsto{\overline{\mathrm{CZ}}_{12}} X_1X_2Z_3Z_6 \xLeftrightarrow{\gamma,\phi} [110000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [110000, 001001]$$

$$\bar{X}_2 = X_1X_3 \xmapsto{\overline{\mathrm{CZ}}_{12}} X_1X_3Z_2Z_6 \xLeftrightarrow{\gamma,\phi} [101000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [101000, 010001].$$

Synthesizing Logical CZ_{12} for the $[\![6,4,2]\!]$ Code

Definition (partial) : $\overline{\mathrm{CZ}}_{12}\bar{X}_1\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{X}_1\bar{Z}_2,\ \overline{\mathrm{CZ}}_{12}\bar{X}_2\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{Z}_1\bar{X}_2.$

The process:

1. Generator matrices for the $[6,5,2]$ SPC code yield logical Paulis:

$$\bar{X}_1 = X_1X_2 = E(110000,000000) \qquad \bar{Z}_1 = Z_2Z_6 = E(000000,010001)$$
$$\bar{X}_2 = X_1X_3 = E(101000,000000) \qquad \bar{Z}_2 = Z_3Z_6 = E(000000,001001)$$

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 $F_{\overline{\mathrm{CZ}}_{12}}$.

$$\bar{X}_1 = X_1X_2 \xmapsto{\overline{\mathrm{CZ}}_{12}} X_1X_2Z_3Z_6 \xLeftrightarrow{\gamma,\phi} [110000,000000]F_{\overline{\mathrm{CZ}}_{12}} = [110000,001001]$$

$$\bar{X}_2 = X_1X_3 \xmapsto{\overline{\mathrm{CZ}}_{12}} X_1X_3Z_2Z_6 \xLeftrightarrow{\gamma,\phi} [101000,000000]F_{\overline{\mathrm{CZ}}_{12}} = [101000,010001].$$

Synthesizing Logical CZ_{12} for the $[\![6,4,2]\!]$ Code

Definition (partial) : $\overline{\mathrm{CZ}}_{12}\bar{X}_1\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{X}_1\bar{Z}_2, \; \overline{\mathrm{CZ}}_{12}\bar{X}_2\overline{\mathrm{CZ}}_{12}^{\dagger} \triangleq \bar{Z}_1\bar{X}_2.$

The process:

1. Generator matrices for the $[6,5,2]$ SPC code yield logical Paulis:

$$\bar{X}_1 = X_1X_2 = E(110000, 000000) \qquad \bar{Z}_1 = Z_2Z_6 = E(000000, 010001)$$
$$\bar{X}_2 = X_1X_3 = E(101000, 000000) \qquad \bar{Z}_2 = Z_3Z_6 = E(000000, 001001)$$

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 $F_{\overline{\mathrm{CZ}}_{12}}$.

$$\bar{X}_1 = X_1X_2 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1X_2Z_3Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [110000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [110000, 001001]$$

$$\bar{X}_2 = X_1X_3 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1X_3Z_2Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [101000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [101000, 010001].$$

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

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

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

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

(Also include constraints to normalize the stabilizer S)

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

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

$$\bar{X}_1 = X_1X_2 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1X_2Z_3Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [110000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [110000, 001001]$$

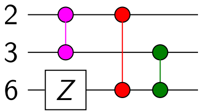
$$\bar{X}_2 = X_1X_3 \overset{\overline{\mathrm{CZ}}_{12}}{\longmapsto} X_1X_3Z_2Z_6 \overset{\gamma,\phi}{\Longleftrightarrow} [101000, 000000]F_{\overline{\mathrm{CZ}}_{12}} = [101000, 010001]$$

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

(Also include constraints to normalize the stabilizer S)

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

Algorithm to Synthesize Logical Clifford Operators

1. Determine the target $\bar{g}$ by specifying $\bar{g}\bar{X}_i\bar{g}^\dagger = \bar{X}_i', \bar{g}\bar{Z}_i\bar{g}^\dagger = \bar{Z}_i'$. Add conditions to normalize or centralize S [Got09].
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., $\bar{g}E(a,b)\bar{g}^\dagger = \pm E\left([a,b]F_{\bar{g}}\right) \Rightarrow [a,b] \mapsto [a,b]F_{\bar{g}}$.
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 the decomposition 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 $\bar{g}$ by an element from HW_N as necessary (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.

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. $x F_{h_1} F_{h_2} = y$.

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

Our Results

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

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

- Algorithm 1: Use symplectic transvections to find symplectic F s.t. $x_i F = y_i, \; i = 1, \ldots, t$.
- Algorithm 2: Use "nullspace-like" ideas for symplectic matrices to enumerate all symplectic solutions F.
- 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.

Future Work

- How to leverage this efficient enumeration during the process of computation? E.g., Quantum Compilers.
- What does this enumeration mean for topological codes?
- 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

[Got97] Daniel Gottesman. “Stabilizer codes and quantum error correction”. PhD thesis. California Institute of Technology, 1997.

[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.

[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.

Thank you!

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.