Kerdock Codes Determine Unitary 2-Designs

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

Joint Work: Trung Can, Robert Calderbank, and Henry Pfister

2019 IEEE Intl. Symposium on Information Theory
Paris, France

arXiv: 1904.07842, 1907.00310

July 12, 2019

Overview

Overview

Problem and Motivation

- Randomized Benchmarking: Procedure to estimate the quality of gates on a quantum computer.
  - Twirl the noise channel through a randomized sequence of gates and induce a depolarizing channel.
  - Noise fidelity is invariant under twirling, so suffices to estimate the fidelity of the depolarizing channel.
- Unitary 2-design: The gates must be chosen from an ensemble of unitary matrices $\mathcal{E} = \{p_i, U_i\}_{i=1}^{t}$ such that

$$\sum_{i=1}^{t} p_i (U_i \otimes U_i) X (U_i^\dagger \otimes U_i^\dagger) = \int_{\mathbb{U}_N} d\mu \, (U \otimes U) X (U^\dagger \otimes U^\dagger),$$

where X is any linear operator on $\mathbb{C}^N \otimes \mathbb{C}^N$ and $d\mu$ is the Haar measure on $\mathbb{U}_N$, the unitary group on $m = \log_2(N)$ qubits.

Problem and Motivation

- Randomized Benchmarking: Procedure to estimate the quality of gates on a quantum computer.
  - Twirl the noise channel through a randomized sequence of gates and induce a depolarizing channel.
  - Noise fidelity is invariant under twirling, so suffices to estimate the fidelity of the depolarizing channel.

- Unitary 2-design: The gates must be chosen from an ensemble of unitary matrices $\mathcal{E} = \{p_i, U_i\}_{i=1}^{t}$ such that

$$\sum_{i=1}^{t} p_i (U_i \otimes U_i) X (U_i^{\dagger} \otimes U_i^{\dagger}) = \int_{\mathbb{U}_N} d\mu \, (U \otimes U) X (U^{\dagger} \otimes U^{\dagger}),$$

where X is any linear operator on $\mathbb{C}^N \otimes \mathbb{C}^N$ and $d\mu$ is the Haar measure on $\mathbb{U}_N$, the unitary group on $m = \log_2(N)$ qubits.

Main Contributions

Implementation Online:
https://github.com/nrenga/symplectic-arxiv18a

- The permutation automorphism group of the $\mathbb{Z}_4$-linear Kerdock codes produces a unitary 2-design, of almost optimal size.
- A simple derivation of the weight distribution of Kerdock codes.

Key Classical-Quantum Connection:

Exponentiated Kerdock codewords are stabilizer states.

Hamming Distance $\longleftrightarrow$ Inner Products

Permutations $\longleftrightarrow$ Clifford Symmetries

Main Contributions

Implementation Online:
https://github.com/nrenga/symplectic-arxiv18a

- The permutation automorphism group of the $\mathbb{Z}_4$-linear Kerdock codes produces a unitary 2-design, of almost optimal size.
- A simple derivation of the weight distribution of Kerdock codes.

Key Classical-Quantum Connection:

Exponentiated Kerdock codewords are stabilizer states.

Hamming Distance $\longleftrightarrow$ Inner Products

Permutations $\longleftrightarrow$ Clifford Symmetries

Overview

Heisenberg-Weyl Group HW_N

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

$$HW_2 \triangleq \langle \imath^\kappa I_2, X, Z, Y \rangle,\ \imath \triangleq \sqrt{-1},\ \kappa \in \mathbb{Z}_4,\ I_2, X, Y, Z \in \mathbb{C}^{2\times 2}.$$

$$\begin{aligned} \text{Bit-Flip}: &\quad X|0\rangle = |1\rangle,\ X|1\rangle = |0\rangle. \\ \text{Phase-Flip}: &\quad Z|0\rangle = |0\rangle,\ Z|1\rangle = -|1\rangle. \\ \text{Bit-Phase Flip}: &\quad Y \triangleq \imath \cdot XZ \Rightarrow Y|x\rangle = \imath \cdot (-1)^x |x \oplus 1\rangle. \end{aligned}$$

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

Binary Representation: $X \otimes Z \otimes Y = E(101, 011) = E(a, b), a, b \in \mathbb{F}_2^m$.

$XZ = -ZX$: $E(a, b), E(c, d)$ commute iff $\underbrace{ad^T + bc^T = 0}_{\text{symplectic inner product}}$.

Heisenberg-Weyl Group HW_N

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

$$HW_2 \triangleq \langle \imath^\kappa I_2, X, Z, Y \rangle, \ \imath \triangleq \sqrt{-1}, \ \kappa \in \mathbb{Z}_4, \ I_2, X, Y, Z \in \mathbb{C}^{2\times 2}.$$

$$\begin{aligned} \text{Bit-Flip}: &\quad X|0\rangle = |1\rangle, \ X|1\rangle = |0\rangle. \\ \text{Phase-Flip}: &\quad Z|0\rangle = |0\rangle, \ Z|1\rangle = -|1\rangle. \\ \text{Bit-Phase Flip}: &\quad Y \triangleq \imath \cdot XZ \Rightarrow Y|x\rangle = \imath \cdot (-1)^x |x \oplus 1\rangle. \end{aligned}$$

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

Binary Representation: $X \otimes Z \otimes Y = E(1\,0\,1, 0\,1\,1) = E(a, b), a, b \in \mathbb{F}_2^m$.

$XZ = -ZX$: $E(a, b), E(c, d)$ commute iff $\underbrace{ad^T + bc^T = 0}_{\text{symplectic inner product}}$.

Clifford Group and Symplectic Matrices

Binary Representation: $X \otimes Z \otimes Y = E(1\,0\,1,\ 0\,1\,1) = E(a,b), a,b \in \mathbb{F}_2^m$.

Paulis: $E(a,b) = \left(\imath^{a_1 b_1} X^{a_1} Z^{b_1}\right) \otimes \left(\imath^{a_2 b_2} X^{a_2} Z^{b_2}\right) \otimes \cdots \otimes \left(\imath^{a_m b_m} X^{a_m} Z^{b_m}\right)$.

Clifford Group: All unitaries that map Paulis to Paulis under conjugation.

Symplectic Matrices: If $g \in \text{Cliff}_N$ (Cliffords on $m = \log_2 N$ qubits) then

$$g\, E(a,b)\, g^{\dagger} = \pm E\left([a,b] F_g\right), \text{ where } F_g \Omega F_g^T = \Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}.$$

$F_g \in \mathbb{F}_2^{2m \times 2m}$ is symplectic: preserves symplectic inner products.

The Clifford group is a unitary 2-design but is too big ($2^{O(m^2)}$)!

Clifford Group and Symplectic Matrices

Binary Representation: $X \otimes Z \otimes Y = E(1\,0\,1,\, 0\,1\,1) = E(a,b), a, b \in \mathbb{F}_2^m$.

Paulis: $E(a,b) = \left(\imath^{a_1 b_1} X^{a_1} Z^{b_1}\right) \otimes \left(\imath^{a_2 b_2} X^{a_2} Z^{b_2}\right) \otimes \cdots \otimes \left(\imath^{a_m b_m} X^{a_m} Z^{b_m}\right)$.

Clifford Group: All unitaries that map Paulis to Paulis under conjugation.

Symplectic Matrices: If $g \in \mathrm{Cliff}_N$ (Cliffords on $m = \log_2 N$ qubits) then

$$g\, E(a,b)\, g^{\dagger} = \pm E\left([a,b]F_g\right), \text{ where } F_g \Omega F_g^T = \Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}.$$

$F_g \in \mathbb{F}_2^{2m \times 2m}$ is symplectic: preserves symplectic inner products.

The Clifford group is a unitary 2-design but is too big ($2^{O(m^2)}$)!

Elementary Symplectic Matrices

Symplectic Matrix F_g	Physical Operator g	Clifford Element
$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$	$H_N = H_2^{\otimes m} = \frac{1}{\sqrt{2^m}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{\otimes m}$	Transversal Hadamard
$A_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix}$	$a_Q = \sum_{v \in \mathbb{F}_2^m} \lvert vQ \rangle \langle v \rvert$	CNOTs, Permutations
$T_P = \begin{bmatrix} I_m & P \\ 0 & I_m \end{bmatrix}$ with P symmetric	$t_P = \sum_{v \in \mathbb{F}_2^m} \imath^{vPv^T \bmod 4} \lvert v \rangle \langle v \rvert$	Phase Gates, Controlled-Z (CZ)
$G_k = \begin{bmatrix} L_{m-k} & U_k \\ U_k & L_{m-k} \end{bmatrix}$ $U_k = \mathrm{diag}(I_k, O_{m-k})$ $L_{m-k} = \mathrm{diag}(O_k, I_{m-k})$	$g_k = H_{2^k} \otimes I_{2^{m-k}}$	Partial Hadamards

Elementary Symplectic Matrices

Symplectic Matrix F_g	Physical Operator g	Clifford Element
$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$	$H_N = H_2^{\otimes m} = \frac{1}{\sqrt{2^m}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}^{\otimes m}$	Transversal Hadamard
$A_Q = \begin{bmatrix} Q & 0 \\ 0 & Q^{-T} \end{bmatrix}$	$a_Q = \sum_{v \in \mathbb{F}_2^m} \lvert vQ \rangle \langle v \rvert$	CNOTs, Permutations
$T_P = \begin{bmatrix} I_m & P \\ 0 & I_m \end{bmatrix}$ with P symmetric	$t_P = \sum_{v \in \mathbb{F}_2^m} \imath^{vPv^T \bmod 4} \lvert v \rangle \langle v \rvert$	Phase Gates, Controlled-Z (CZ)
$G_k = \begin{bmatrix} L_{m-k} & U_k \\ U_k & L_{m-k} \end{bmatrix}$ $U_k = \mathrm{diag}(I_k, O_{m-k})$ $L_{m-k} = \mathrm{diag}(O_k, I_{m-k})$	$g_k = H_{2^k} \otimes I_{2^{m-k}}$	Partial Hadamards

Stabilizer States (SS)

Paulis: $E(a,b) = \left(\imath^{a_1 b_1} X^{a_1} Z^{b_1}\right) \otimes \left(\imath^{a_2 b_2} X^{a_2} Z^{b_2}\right) \otimes \cdots \otimes \left(\imath^{a_m b_m} X^{a_m} Z^{b_m}\right)$.

Cliffords: If $g \in \text{Cliff}_N$, then $g\, E(a,b)\, g^{\dagger} = \pm E\left([a,b]F_g\right)$, F_g symplectic.

- Stabilizer: Commutative subgroup of the Pauli group HW_N.
- SS: The common eigenvectors of maximal (size) stabilizers.
- $Z\,|0\rangle = |0\rangle \Rightarrow E(0,b)\,|0\rangle^{\otimes m} = |0\rangle^{\otimes m} \Rightarrow \pm E([0,b]F_g) \cdot g\,|0\rangle^{\otimes m} = g\,|0\rangle^{\otimes m}$.
- SS $g\,|0\rangle^{\otimes m} \longleftrightarrow$ maximal stabilizer $\{\pm E([0,b]F_g),\ b \in \mathbb{F}_2^m\}$.

Example:

$$g = \left(\sum_{v \in \mathbb{F}_2^m} \imath^{vPv^T} |v\rangle\langle v|\right) \cdot H_N \cdot E(w,0) \Rightarrow g\,|0\rangle^{\otimes m} \propto \sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle$$

$\updownarrow$ eigenvector

$(P = P^T \in \mathbb{F}_2^{m \times m},\ w \in \mathbb{F}_2^m)$ $\qquad E([I_m \,|\, P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$

Stabilizer States (SS)

Paulis: $E(a, b) = \left(\imath^{a_1 b_1} X^{a_1} Z^{b_1}\right) \otimes \left(\imath^{a_2 b_2} X^{a_2} Z^{b_2}\right) \otimes \cdots \otimes \left(\imath^{a_m b_m} X^{a_m} Z^{b_m}\right)$.

Cliffords: If $g \in \text{Cliff}_N$, then $g\, E(a, b)\, g^\dagger = \pm E\left([a, b] F_g\right)$, F_g symplectic.

- Stabilizer: Commutative subgroup of the Pauli group HW_N.
- SS: The common eigenvectors of maximal (size) stabilizers.
- $Z\,|0\rangle = |0\rangle \Rightarrow E(0, b)\,|0\rangle^{\otimes m} = |0\rangle^{\otimes m} \Rightarrow \pm E([0, b] F_g) \cdot g\,|0\rangle^{\otimes m} = g\,|0\rangle^{\otimes m}$.
- SS $g\,|0\rangle^{\otimes m} \longleftrightarrow$ maximal stabilizer $\{\pm E([0, b] F_g),\ b \in \mathbb{F}_2^m\}$.

Example:

$$g = \left(\sum_{v \in \mathbb{F}_2^m} \imath^{v P v^T} |v\rangle \langle v|\right) \cdot H_N \cdot E(w, 0) \Rightarrow g\,|0\rangle^{\otimes m} \propto \sum_{v \in \mathbb{F}_2^m} \imath^{(v P v^T + 2 v w^T) \bmod 4} |v\rangle$$

eigenvector

$(P = P^T \in \mathbb{F}_2^{m \times m},\ w \in \mathbb{F}_2^m)$ $\quad E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$

Stabilizer States (SS)

Paulis: $E(a, b) = \left(\imath^{a_1 b_1} X^{a_1} Z^{b_1}\right) \otimes \left(\imath^{a_2 b_2} X^{a_2} Z^{b_2}\right) \otimes \cdots \otimes \left(\imath^{a_m b_m} X^{a_m} Z^{b_m}\right)$.

Cliffords: If $g \in \text{Cliff}_N$, then $g\, E(a, b)\, g^\dagger = \pm E\left([a, b] F_g\right)$, F_g symplectic.

- Stabilizer: Commutative subgroup of the Pauli group HW_N.
- SS: The common eigenvectors of maximal (size) stabilizers.
- $Z\,|0\rangle = |0\rangle \Rightarrow E(0, b)\,|0\rangle^{\otimes m} = |0\rangle^{\otimes m} \Rightarrow \pm E([0, b] F_g) \cdot g\,|0\rangle^{\otimes m} = g\,|0\rangle^{\otimes m}$.
- SS $g\,|0\rangle^{\otimes m} \longleftrightarrow$ maximal stabilizer $\{\pm E([0, b] F_g),\ b \in \mathbb{F}_2^m\}$.

Example:

$$g = \left(\sum_{v \in \mathbb{F}_2^m} \imath^{vPv^T} |v\rangle \langle v|\right) \cdot H_N \cdot E(w, 0) \Rightarrow g\,|0\rangle^{\otimes m} \propto \sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle$$

$\updownarrow$ eigenvector

$(P = P^T \in \mathbb{F}_2^{m \times m},\ w \in \mathbb{F}_2^m)$ $\qquad E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$

Stabilizer States (SS)

Paulis: $E(a, b) = (\imath^{a_1 b_1} X^{a_1} Z^{b_1}) \otimes (\imath^{a_2 b_2} X^{a_2} Z^{b_2}) \otimes \cdots \otimes (\imath^{a_m b_m} X^{a_m} Z^{b_m})$.

Cliffords: If $g \in \text{Cliff}_N$, then $g\, E(a, b)\, g^\dagger = \pm E([a, b] F_g)$, F_g symplectic.

- Stabilizer: Commutative subgroup of the Pauli group HW_N.
- SS: The common eigenvectors of maximal (size) stabilizers.
- $Z\,|0\rangle = |0\rangle \Rightarrow E(0, b)\,|0\rangle^{\otimes m} = |0\rangle^{\otimes m} \Rightarrow \pm E([0, b]F_g) \cdot g\,|0\rangle^{\otimes m} = g\,|0\rangle^{\otimes m}$.
- SS $g\,|0\rangle^{\otimes m} \longleftrightarrow$ maximal stabilizer $\{\pm E([0, b]F_g),\ b \in \mathbb{F}_2^m\}$.

Example:

$$g = \left(\sum_{v \in \mathbb{F}_2^m} \imath^{vPv^T} |v\rangle \langle v|\right) \cdot H_N \cdot E(w, 0) \Rightarrow g\,|0\rangle^{\otimes m} \propto \sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle$$

$\updownarrow$ eigenvector

$$(P = P^T \in \mathbb{F}_2^{m \times m},\ w \in \mathbb{F}_2^m) \qquad E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$$

Overview

Connecting Quantum and Classical Worlds

$$E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$$

↕ eigenvector

$$\sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle \in \{\pm 1, \pm \imath\}^N$$

↕ exponentiation

$$\sum_{v \in \mathbb{F}_2^m} \left[(vPv^T + 2vw^T) \bmod 4 \right] |v\rangle \in \mathbb{Z}_4^N$$

Orthonormal Basis of Stabilizer States

↑ Exponentiation!

$\mathbb{Z}_4$-Linear Kerdock Code

Squared Euclidean Distance $=$ 2 $\times$ Hamming Distance

Gray Map: $\mathbb{Z}_4^N \to \mathbb{F}_2^{2N}$

$$\sum_{v \in \mathbb{F}_2^m} |v\rangle \otimes \left[\mathfrak{g}(vPv^T + 2vw^T) \right]^T \in \mathbb{F}_2^{2N}$$

Binary Kerdock Code

Connecting Quantum and Classical Worlds

$E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$

↕ eigenvector

$\sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle \in \{\pm 1, \pm \imath\}^N$

↕ exponentiation

$\sum_{v \in \mathbb{F}_2^m} \left[(vPv^T + 2vw^T) \bmod 4\right] |v\rangle \in \mathbb{Z}_4^N$

Orthonormal Basis of Stabilizer States

↕ Exponentiation!

$\mathbb{Z}_4$-Linear Kerdock Code

Squared Euclidean Distance $= 2 \times$ Hamming Distance

Gray Map: $\mathbb{Z}_4^N \to \mathbb{F}_2^{2N}$

$\sum_{v \in \mathbb{F}_2^m} |v\rangle \otimes \left[\mathfrak{g}(vPv^T + 2vw^T)\right]^T \in \mathbb{F}_2^{2N}$

Binary Kerdock Code

Connecting Quantum and Classical Worlds

$$E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$$

↕ eigenvector

$$\sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle \in \{\pm 1, \pm \imath\}^N$$

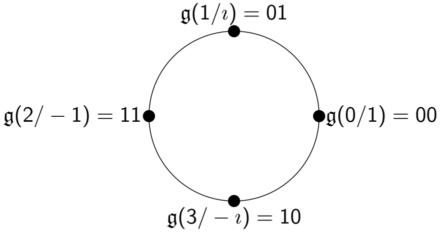
↕ exponentiation

$$\sum_{v \in \mathbb{F}_2^m} \left[(vPv^T + 2vw^T) \bmod 4 \right] |v\rangle \in \mathbb{Z}_4^N$$

Orthonormal Basis of Stabilizer States

Exponentiation!

$\mathbb{Z}_4$-Linear Kerdock Code



Squared Euclidean Distance = 2 × Hamming Distance

Gray Map: $\mathbb{Z}_4^N \rightarrow \mathbb{F}_2^{2N}$

$$\sum_{v \in \mathbb{F}_2^m} |v\rangle \otimes \left[\mathfrak{g}(vPv^T + 2vw^T) \right]^T \in \mathbb{F}_2^{2N}$$

Binary Kerdock Code

Connecting Quantum and Classical Worlds

$$E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$$

↕ eigenvector

$$\sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle \in \{\pm 1, \pm \imath\}^N$$

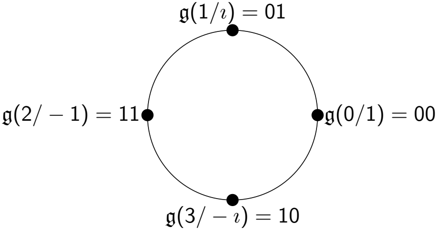
↕ exponentiation

$$\sum_{v \in \mathbb{F}_2^m} \left[(vPv^T + 2vw^T) \bmod 4 \right] |v\rangle \in \mathbb{Z}_4^N$$

Orthonormal Basis of Stabilizer States

Exponentiation!

$\mathbb{Z}_4$-Linear Kerdock Code



Squared Euclidean Distance
$= \; 2 \times$ Hamming Distance

Gray Map: $\mathbb{Z}_4^N \to \mathbb{F}_2^{2N}$

$$\sum_{v \in \mathbb{F}_2^m} |v\rangle \otimes \left[\mathfrak{g}(vPv^T + 2vw^T) \right]^T \in \mathbb{F}_2^{2N}$$

Binary Kerdock Code

Connecting Quantum and Classical Worlds

$E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$

↕ eigenvector

$\sum_{v \in \mathbb{F}_2^m} \imath^{(vPv^T + 2vw^T) \bmod 4} |v\rangle \in \{\pm 1, \pm \imath\}^N$

↕ exponentiation

$\sum_{v \in \mathbb{F}_2^m} \left[(vPv^T + 2vw^T) \bmod 4 \right] |v\rangle \in \mathbb{Z}_4^N$

Orthonormal Basis of Stabilizer States

↕ Exponentiation!

$\mathbb{Z}_4$-Linear Kerdock Code

Squared Euclidean Distance $= 2 \times$ Hamming Distance

Gray Map: $\mathbb{Z}_4^N \to \mathbb{F}_2^{2N}$

$\sum_{v \in \mathbb{F}_2^m} |v\rangle \otimes \left[\mathfrak{g}(vPv^T + 2vw^T) \right]^T \in \mathbb{F}_2^{2N}$

Binary Kerdock Code

Overview

Clifford Symmetries of Kerdock SSs

$$g_{P,w} = \left(\sum_{v\in\mathbb{F}_2^m} \imath^{vPv^T} |v\rangle\langle v|\right) \cdot H_N \cdot E(w,0) \Rightarrow g_{P,w}|0\rangle^{\otimes m} \propto \sum_{v\in\mathbb{F}_2^m} \imath^{(vPv^T+2vw^T) \bmod 4} |v\rangle$$

$\updownarrow$ eigenvector

$$(P = P^T \in \mathbb{F}_2^{m\times m},\ w \in \mathbb{F}_2^m) \qquad E([I_m \mid P]) = \{\pm E(b, bP), b \in \mathbb{F}_2^m\}$$

$Z_N = E([0 \mid I_m])$	$X_N = E([I_m \mid 0])$	$Y_P = E([I_m \mid P])$
$\updownarrow$	$\updownarrow$	$\updownarrow$
$E(w,0)\|0\rangle^{\otimes m} = \|w\rangle$	$H_N\|w\rangle \propto \sum_{v\in\mathbb{F}_2^m}(-1)^{vw^T}\|v\rangle$	$t_P H_N\|w\rangle \propto \sum_{v\in\mathbb{F}_2^m} \imath^{vPv^T+2vw^T}\|v\rangle$

Unitary Operator	H_N	$t_P = \sum_{v\in\mathbb{F}_2^m} \imath^{vPv^T} \|v\rangle\langle v\|$	Kerdock Set of Matrices P: $P \neq Q \Rightarrow P+Q$ non-singular
Symplectic Matrix	$\Omega = \begin{bmatrix} 0 & I_m \\ I_m & 0 \end{bmatrix}$	$T_P = \begin{bmatrix} I_m & P \\ 0 & I_m \end{bmatrix}$	Associate $z \in \mathbb{F}_{2^m} \leftrightarrow P_z$

Kerdock Symmetries

Col. of M_z indexed by $w \in \mathbb{F}_2^m$: $|\psi_{P_z,w}\rangle \propto \sum_{v \in \mathbb{F}_2^m} \imath^{(vP_z v^T + 2vw^T) \bmod 4} |v\rangle$.

Cols. of M_z form the eigenbasis of $E([I_m \mid P_z]) = \{\pm E(b, bP_z), b \in \mathbb{F}_2^m\}$.

Form the $N \times N(N+1)$ matrix $M \triangleq [\ M_\infty \ \mid \ M_0 \ \mid \ \cdots \ \mid \ M_z \ \mid \ \cdots\ ]$.

- Each of the $N+1$ blocks of M correspond to a stabilizer $E([I_m \mid P_z])$.
- Symmetry of M: A pair (U, G) s.t. $UMG = M$, where $U \in \mathbb{U}_N$ and G is a generalized permutation matrix with entries in $\{1, \imath, -1, -\imath\}$.
- Lemma: For any symmetry (U, G) of M, $U \in \text{Cliff}_N$.
- Proof Idea: U permutes the stabilizers $E([I_m \mid P_z])$, so $U \in \text{Cliff}_N$.

Kerdock Symmetries form a Unitary 2-Design

Col. of M_z indexed by $w \in \mathbb{F}_2^m$: $|\psi_{P_z,w}\rangle \propto \sum_{v\in\mathbb{F}_2^m} \imath^{(vP_zv^T+2vw^T) \bmod 4} |v\rangle$.

Cols. of M_z form the eigenbasis of $E([I_m \mid P_z]) = \{\pm E(b, bP_z), b \in \mathbb{F}_2^m\}$.

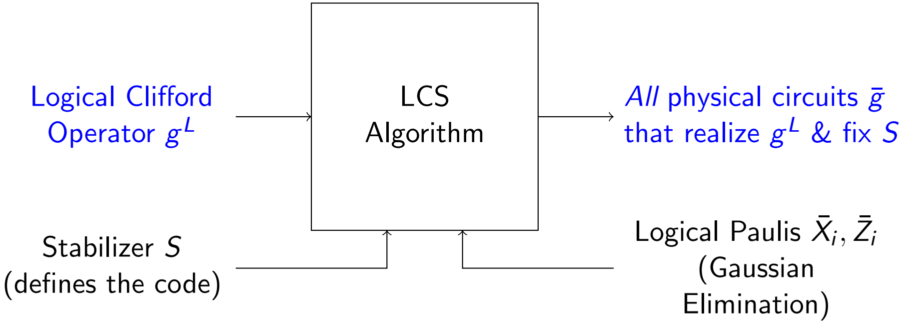
Form the $N \times N(N+1)$ matrix $M \triangleq [\ M_\infty \ \mid\ M_0 \ \mid\ \cdots \ \mid\ M_z \ \mid\ \cdots\ ]$.

- Pauli Mixing: Transitivity on Paulis, implies unitary 2-design (Webb).
- Symmetry Group $\mathfrak{P}_{\mathrm{K},m}$ of M: Generated as a product of 3 subgroups, each of which is one-to-one with a generator of the projective special linear group $\mathrm{PSL}(2, N)$. (Use symplectic matrices for this connection.)
- $\mathfrak{P}_{\mathrm{K},m} \cong \mathrm{PSL}(2, N)$: Size $(N+1)N(N-1) \approx 2^{3m} \ll |\mathrm{Cliff}_N| \approx 2^{O(m^2)}$.
- $\mathfrak{P}_{\mathrm{K},m}$ is Pauli mixing and hence forms a unitary 2-design!

Logical Unitary 2-Designs

Combining with our Logical Clifford Synthesis (LCS) algorithm (arXiv:1907.00310), we can synthesize unitary 2-designs on the qubits protected by a (quantum) stabilizer error-correcting code.

Code: `https://github.com/nrenga/symplectic-arxiv18a`



Summary and Future Work

- Exponentiated Kerdock codewords are stabilizer states (SS).
- Connection simplifies derivation of the Kerdock weight distribution.
- Clifford symmetries of Kerdock SS form a small unitary 2-design.
  - The design is isomorphic to Cleve et al. (arXiv:1501.04592), but the classical coding connection is new and makes the description simple.
- The isomorphism to $\mathrm{PSL}(2, N)$ makes sampling from the design easy.
- Using LCS algorithm, produced logical unitary 2-designs. Application in logical randomized benchmarking protocol (arXiv:1702.03688).
- Make an approximate unitary 2-design with lower circuit complexity?
- Use coding connection to synthesize unitary t-designs for $t > 2$?

Thank you!

For details see http://arxiv.org/abs/1904.07842
and http://arxiv.org/abs/1907.00310

(Logical/Physical) Unitary 2-Design Implementation:
https://github.com/nrenga/symplectic-arxiv18a

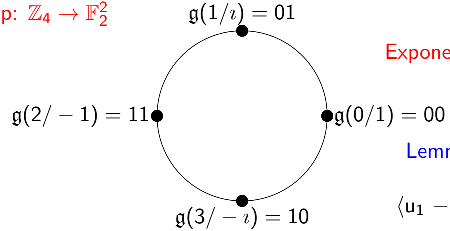
Any feedback is much appreciated!
narayanan.rengaswamy@duke.edu

Weight Distribution of (Binary) Kerdock Codes

Kerdock codewords: $\sum_{v \in \mathbb{F}_2^m} \left[(vPv^T + 2vw^T + \kappa) \bmod 4 \right] |v\rangle \in \mathbb{Z}_4^N$

Subtracting two codewords $\longleftrightarrow$ Inner product of corresponding SS!

Gray Map: $\mathbb{Z}_4 \to \mathbb{F}_2^2$



Exponentiated Kerdock Codeword

Lemma: For $\mathrm{u}_1, \mathrm{u}_2 \in \{1, \imath, -1, -\imath\}^N$,

$$\langle \mathrm{u}_1 - \mathrm{u}_2, \mathrm{u}_1 - \mathrm{u}_2 \rangle = 2d_H(\mathfrak{g}(\mathrm{u}_1), \mathfrak{g}(\mathrm{u}_2))$$

Lemma: For $P_1, P_2 \in P_K(m)$, $|\langle \mathrm{u}_1, \mathrm{u}_2 \rangle|^2 = \begin{cases} 0 & \text{if } P_1 = P_2 \text{ and } \mathrm{u}_1 \neq \mathrm{u}_2 \\ 2^m & \text{if } P_1 \neq P_2, \\ 2^{2m} & \text{if } (P_1 = P_2 \text{ and}) \ \mathrm{u}_1 = \mathrm{u}_2. \end{cases}$

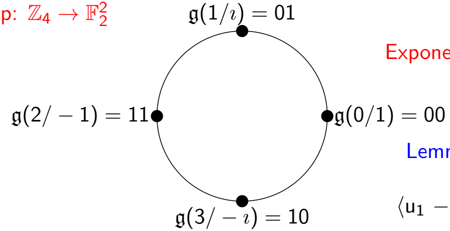
Proof Idea: $|\langle \mathrm{u}_1, \mathrm{u}_2 \rangle|^2 = \mathrm{Tr}\left[(\mathrm{u}_1 \mathrm{u}_1^\dagger)(\mathrm{u}_2 \mathrm{u}_2^\dagger) \right]$, $\mathrm{u}_i \mathrm{u}_i^\dagger =$ Projector onto $\mathrm{u}_i \longleftrightarrow E([I_m \,|\, P_i])$.

Weight Distribution of (Binary) Kerdock Codes

Kerdock codewords: $\sum_{v \in \mathbb{F}_2^m} \left[(vPv^T + 2vw^T + \kappa) \bmod 4 \right] |v\rangle \in \mathbb{Z}_4^N$

Subtracting two codewords $\longleftrightarrow$ Inner product of corresponding SS!

Gray Map: $\mathbb{Z}_4 \to \mathbb{F}_2^2$



Exponentiated Kerdock Codeword

$\updownarrow$

Lemma: For $u_1, u_2 \in \{1, \imath, -1, -\imath\}^N$,

$$\langle u_1 - u_2, u_1 - u_2 \rangle = 2 d_H(\mathfrak{g}(u_1), \mathfrak{g}(u_2))$$

Lemma: For $P_1, P_2 \in P_K(m)$, $|\langle u_1, u_2 \rangle|^2 = \begin{cases} 0 & \text{if } P_1 = P_2 \text{ and } u_1 \neq u_2 \\ 2^m & \text{if } P_1 \neq P_2, \\ 2^{2m} & \text{if } (P_1 = P_2 \text{ and}) \ u_1 = u_2. \end{cases}$

Proof Idea: $|\langle u_1, u_2 \rangle|^2 = \mathrm{Tr}\left[(u_1 u_1^\dagger)(u_2 u_2^\dagger) \right]$, $u_i u_i^\dagger =$ Projector onto $u_i \longleftrightarrow E([I_m \mid P_i])$.