Commutant of the Clifford Group

Nikolay Sheshko
Dheeran E. Wiggins

Representation-theoretic Methods in QIT

December 09, 2025

University of Illinois at Urbana-Champaign

Overview

Q: Why should we be interested in computing the commutant of the Clifford group?

A: The image of Clifford twirling is contained in the commutant.

Pauli Group

The Pauli matrices are

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In $\mathcal{U}_2$, they generate the 1-qubit Pauli group $\mathcal{P}_1$. Taking all n-fold tensor products

$$\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n, \quad \sigma_j \in \mathcal{P}_1,$$

we obtain the n-qubit Pauli group.

Pauli Group

Quotienting by phases $\langle iI \rangle$ yields a group

$$\mathcal{P}_n = \{I, X, Y, Z\}^{\otimes n}.$$

Denote all m-tuples of operators in $\mathcal{P}_n$ by $\mathcal{P}_n^m$.

Stabilizer Codes

The fixed subspace of abelian subgroups (without $-I^{\otimes n}$) of the n-qubit Pauli group give rise to stabilizer codes–the quintessential sort of error-correcting code.

Clifford Group

The Clifford group $\mathcal{C}_n$ is the subgroup of $\mathcal{U}_{2^n}$ given by

$$\mathcal{C}_n = \left\{ C \in \mathcal{U}_{2^n} : C\sigma C^\dagger \in \mathcal{P}_n \text{ for all } \sigma \in \mathcal{P}_n, \text{ up to phases} \right\}.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Random Clifford Gates

To study the effects of applying random Clifford gates to a system, we characterize averaging over the Clifford group using k-fold twirling.

The Haar measure allows us to define k-fold twirling for any subgroup $G \subseteq \mathcal{U}_{2^n}$. We focus on $\mathcal{C}_n$.

Let k be a number, $G \subseteq \mathcal{U}_{2^n}$ be a subgroup, and $\mathcal{K}$ be k copies of an n-qubit Hilbert space (i.e., of dimension 2^{nk}).

Commutant

The k-fold commutant of G is the $\mathbb{C}$-algebra

$$\mathrm{Com}(G^{\otimes k}) = \left\{ \rho \in \mathbb{B}\left(\mathcal{K}\right) : U^{\dagger \otimes k} \rho U^{\otimes k} = \rho \text{ for all } U \in G \right\}.$$

Clifford Twirling

The Clifford twirling (super)operator is

$$\Phi_{\mathrm{Cl}}^{(k)}(-) = \frac{1}{|\mathcal{C}_n|} \sum_{C \in \mathcal{C}_n} C^{\otimes k}(-) C^{\dagger \otimes k}.$$

Clifford Twirling

Lemma

Let $U \in \mathcal{C}_n$ be an arbitrary Clifford operator. Then, for all $X \in \mathbb{B}(\mathcal{K})$

$$U^{\dagger \otimes k} \Phi_{\mathrm{Cl}}^{(k)}(X) U^{\otimes k} = \Phi_{\mathrm{Cl}}^{(k)}(X).$$

That is, the image $\Phi_{\mathrm{Cl}}^{(k)}(\mathbb{B}(\mathcal{K})) \subseteq \mathrm{Com}(\mathcal{C}_n^{\otimes k})$.

Clifford Twirling

Proof.

For any Clifford operator $C \in \mathcal{C}_n$,

$$U^{\dagger \otimes k} C^{\otimes k} X C^{\dagger \otimes k} U^{\otimes k} = (U^\dagger C)^{\otimes k} X (U^\dagger C)^{\dagger \otimes k}.$$

Left multiplication $U^\dagger \times - : \mathcal{C}_n \to \mathcal{C}_n$ is a bijection, so we have just reindexed the twirling sum. □

Twirling

In fact, the same holds for twirling (via the Haar measure) over any group $G \subseteq \mathcal{U}_{2^n}$. Just use the invariance properties.

Basis

If we can find a nice basis for $\mathrm{Com}(\mathcal{C}_n^{\otimes k})$, we can then write down any averaged Clifford operator in terms of this basis.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Basis

In [GNW21], a basis is found when $k \leq n+1$. This basis is built from operators of the form

$$r(T) = \sum_{(x,y)\in T} |x\rangle\langle y|\,,$$

where $T \subseteq \mathbb{F}_2^k \oplus \mathbb{F}_2^k$ is a *stochastic Lagrangian subspace* with respect to a symplectic form (see later on Robust Hudson Theorem).

Dimension

This construction tells us

$$\dim\left(\mathrm{Com}(\mathcal{C}_n^{\otimes k})\right) = \prod_{j=0}^{k-2}(2^j+1).$$

That is, when $k \leq n+1$, the dimension is independent of n.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Adjacency Matrix

Let $\Gamma = (V, E)$ be a finite graph with m vertices $v_1, \ldots, v_m$.

The adjacency matrix $\mathcal{A}(\Gamma)$ is an operator in $\mathbb{M}_m(\mathbb{F}_2)$ defined by

$$\mathcal{A}(\Gamma)_{i,j} = \begin{cases} 1, & (v_i, v_j) \in E \\ 0, & \text{otherwise.} \end{cases}$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Anticommutation Graph

Let $\mathbf{P} = (P_1, P_2, \ldots, P_m) \in \mathcal{P}_n^m$. The anticommutation graph of $\mathbf{P}$ has

(i) m vertices $P_1, \ldots, P_m$.

(ii) edges between anticommuting pairs (P_i, P_j).

Write $\mathcal{A}(\mathbf{P})$ for the adjacency matrix of the above graph.

Now, a useful fact:

Lemma ([BEL+25], Lemma 17)

Let $\mathbf{P} \in \mathcal{P}_n^m$ be algebraically independent. Let $\mathbf{Q} \in \pm\mathcal{P}_n^m$ be algebraically independent with signs. Then, there exists a Clifford $C \in \mathcal{C}_n$ such that

$$C\mathbf{P}C^\dagger = \mathbf{Q}.$$

if and only if

$$\mathcal{A}(\mathbf{P}) = \mathcal{A}(\mathbf{Q}).$$

Idea.

When $m = 2n$, the Clifford operator is given by

$$C(X) = \frac{1}{2} \sum_{\alpha \in \mathbb{F}_2^m} \operatorname{tr}\left(P_\alpha^\dagger X\right) Q_\alpha,$$

where

$$P_\alpha = \prod_{j=1}^{m} P_j^{\alpha_j}, \quad \alpha \in \mathbb{F}_2^m$$

and likewise for Q_α. □

Idea, continued.

If $m < 2n$, we can complete both **P** and **Q** with $2n - m$ algebraically independent Pauli operators while keeping the adjacency matrices agreeing.

That we can do this relies on the canonical graph form of any anticommutation graph. □

Independent Graph-based Pauli Monomials

Definition

Let $G \in \mathrm{Sym}_0(\mathbb{F}_2^{m\times m})$ be a symmetric binary matrix, and $V \in \mathrm{Even}(\mathbb{F}_2^{k\times m})$. We define independent graph-based Pauli monomials as

$$\mho_I([V,G]) = \frac{1}{|S_{[V,G]}|} \sum_{\substack{\mathbf{P}\in\mathcal{P}_n^{\times m} \\ \mathcal{A}(\mathbf{P})=G, \\ \mathbf{P} \text{ alg ind.}}} \prod_{j=1}^{m} P_j^{\otimes v_j}$$

i.e., the sum runs over the set of algebraically independent Pauli operators $\mathbf{P} = (P_1, \ldots, P_m)$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Orthogonal Basis of the Commutant

Theorem

The set of independent graph-based Pauli monomials $\{\mho_I([V,G])\}_{V\in \mathrm{Even}(\mathbb{F}_2^{k\times m}),G\in \mathrm{Sym}_0(\mathbb{F}_2^{m\times m})}$ *forms an orthogonal basis of the commutant* $\mathrm{Com}(\mathcal{C}_n^{\otimes k})$.

Proof Sketch. The commutant is precisely the image of the twirling map

$$\Phi_{\mathrm{Cl}}^{(k)}(P) = \frac{1}{|\mathcal{C}_n|}\sum_{C\in\mathcal{C}_n} C^{\otimes k} P C^{\dagger\otimes k}.$$

Now it can be shown that V and G are invariant under the action of C, so we can combine the monomials with equivalent V and G together.

Pauli Monomials

Definition

Let $M \in \mathrm{Sym}_0(\mathbb{F}_2^{m\times m})$, and $V \in \mathrm{Even}(\mathbb{F}_2^{k\times m})$. The Pauli monomial, denoted by $\Omega(V, M)$ is defined as

$$\Omega(V, M) := \frac{1}{d^m} \sum_{\boldsymbol{P}\in\mathcal{P}_n^m} P_1^{\otimes v_1} P_2^{\otimes v_2} \cdots P_m^{\otimes v_m} \times \left(\prod_{\substack{i,j\in[m] \\ i<j}} \chi(P_i, P_j)^{M_{i,j}} \right),$$

Graphical Calculus

$$\Omega\left(\begin{pmatrix}1&1&0\\1&1&0\\1&1&0\\1&1&0\\0&1&1\\0&1&1\end{pmatrix}, \begin{pmatrix}0&0&1\\0&0&1\\1&1&0\end{pmatrix}\right) =$$

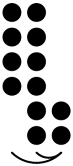

Figure: Graphical representation

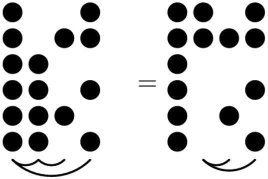

Figure: Adding first column to the second

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Graph-based Pauli Monomials

Definition

Let $G \in \mathrm{Sym}_0(\mathbb{F}_2^{m\times m})$, and $V \in \mathrm{Even}(\mathbb{F}_2^{k\times m})$. The graph-based Pauli monomials is defined as

$$\mho(V,G) := \frac{1}{d^m} \sum_{\substack{\boldsymbol{P}\in\mathcal{P}_n \\ \mathcal{A}(\boldsymbol{P})=G}} \prod_{j=1}^{m} P_j^{\otimes v_j},$$

where $\mathcal{A}(\boldsymbol{P})$ denotes the adjacency matrix of the anticommmutation graph associated with the set $\{P_1,\dots,P_m\}$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Connection Between Different Bases

Pauli monomials $\Omega(V, M)$ and graph-based Pauli monomials $\mho(V, G)$ are related via a linear Fourier transform:

$$\Omega(V, M) = \sum_{G \in \mathrm{Sym}_0(\mathbb{F}_2^{m \times m})} (-1)^{\sum_{i<j} M_{i,j} G_{i,j}} \mho(V, G).$$

Also there is a bijection between graph-based Pauli monomials and independent graph-based Pauli monomials.

Corollary

The sets $\{\Omega(V, M)\}_{V,M}$, $\{\mho(V, G)\}_{V,G}$, and $\{\mho_I(V, G)\}_{V,G}$ generate the same vector space.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Clifford-Weingarten Calculus

Theorem

Let $\Phi^{(k)}_{\mathrm{Cl}}(O)$ be the k-fold twirling operator $O \in \mathcal{B}(\mathcal{K})$ and let $\mathcal{P}$ be the set of (reduced) Pauli monomials. Then it reads

$$\Phi^{(k)}_{\mathrm{Cl}}(O) = \sum_{\Omega,\Omega' \in \mathcal{P}} (\mathcal{W}^{-1})_{\Omega,\Omega'} \operatorname{tr}(O\Omega)\Omega'$$

where we call the coefficients $(\mathcal{W}^{-1})_{\Omega,\Omega'}$ Clifford-Weingarten functions, which can be obtained as the (pseudo-)inverse of the Gram-Schmidt matrix $\mathcal{W}_{\Omega,\Omega'} := \operatorname{tr}\left(\Omega^{\dagger}\Omega'\right)$.

Clifford-Weingarten Calculus

Theorem

Let $\mathcal{W}$ the Gram-Schmidt matrix, and let $\mathcal{W}^{-1}$ be its inverse. Let $n \geq k^2 - 3k + 7$. Then the properties

$$\left|(\mathcal{W}^{-1})_{\Omega,\Omega} - \frac{1}{d^k}\right| \leq \frac{6|\mathcal{P}|^2}{d^{k+1}},$$

$$|(\mathcal{W}^{-1})_{\Omega,\Omega'}| \leq \frac{5|\mathcal{P}|^2}{d^{k+1}},$$

hold true.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

De Finetti Theorem for Stabilizer Symmetries

Recall the regular de Finetti theorem:

Theorem

Let ρ be a quantum state on $(\mathbb{C}^\ell)^{\otimes k}$ that commutes with all permutations. Then, there exists a probability measure μ on the space of mixed states on $\mathbb{C}^\ell$ such that

$$\frac{1}{2}\left\|\rho_{1\ldots s} - \int d\mu(\sigma)\sigma^{\otimes s}\right\|_1 \leq 2\ell^2 \frac{s}{k}$$

De Finetti Theorem for Stabilizer Symmetries

Let's add symmetries. For qudits with d being prime, consider the additional group of symmetries $O_k(d)$ consisting of $k \times k$- matrices with entries in $\mathbb{Z}_d$ which are orthogonal and such that the sum of elements in each row is equal to $1 \pmod{d}$. We call this group *stochastic orthogonal group*.

Theorem

Let d be a prime and ρ a quantum state on $((\mathbb{C}^d)^{\otimes n})^{\otimes k}$ that commutes with the action of $O_k(d)$. Then, there exists a probability distribution p on the (finite) set of mixed stabilizer states of n qudits, such that

$$\frac{1}{2}\left\|\rho_{1\ldots s} - \sum_{\sigma_S} p(\sigma_S)\sigma_S^{\otimes s}\right\|_1 \leq 2d^{\frac{1}{2}(2n+2)^2} d^{-\frac{1}{2}(k-s)}.$$

Robust Hudson Theorem

Let $x = (p, q) \in \mathbb{Z}^{2n}$. Define the *Weyl operator*

$$W_x = -\tau^{-p \cdot q}(Z^{p_1} X^{q_1}) \otimes \cdots \otimes (Z^{p_n} X^{q_n}).$$

Consider a symplectic form on $\mathbb{Z}^{2n}$ by $[x, x'] = p \cdot q' - q \cdot p'$. Then for any operator B on $(\mathbb{C}^d)^{\otimes n}$ one can define the *Wigner function* $w_B \colon \mathbb{Z}_d^{2n} \to \mathbb{C}$ by

$$w_B(x) = d^{-2n} \sum_y \omega^{-[x,y]} \operatorname{tr}(W_y^\dagger B)$$

where $\omega = e^{2\pi i/d}$.

Robust Hudson Theorem

For odd d, the Wigner function of a quantum state is real and $-d^{-n} \leq w_{\psi}(x) \leq d^{-n}$. Furthermore the Wigner function is a quasi-probability distribution, i.e., $\sum_x w_{\psi}(x) = 1$.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Robust Hudson Theorem

Theorem

A pure state $|\psi\rangle$ is a stabilizer state if and only if it has a nonnegative Wigner function.

For a quantitative version, define *sum-negativity* of ψ to be

$$\mathrm{sn}(\psi) = \sum_{w_\psi(x)<0} |w_\psi(x)|.$$

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Robust Hudson Theorem

Theorem

Let d be odd and ψ a pure quantum state of n qudits. Then there exists a stabilizer state $|S\rangle$, such that $|\langle S|\psi\rangle|^2 \geq 1 - 9d^2 \mathrm{sn}(\psi)$

Lennart Bittel, Jens Eisert, Lorenzo Leone, Antonio Mele, and Salvatore Oliviero.
A complete theory of the Clifford commutant, 2025.
arXiv preprint.

Sergey Bravyi and Alexei Kitaev.
Universal quantum computation with ideal Clifford gates and noisy ancillas.
Phys. Rev. A, 71, 2005.

D. Gross, K. Audenaert, and J. Eisert.
Evenly distributed unitaries: on the structure of unitary designs.
Journal of Mathematical Physics, 2007.

David Gross, Sepehr Nezami, and Michael Walter.
Schur-Weyl duality for the Clifford group with applications: Property testing, a robust Hudson theorem, and de Finetti representations.
Communications in Mathematical Physics, 385:1325–1393, 2021.

Daniel Gottesman.
Stabilizer Codes and Quantum Error Correction, 1997.

Daniel Gottesman.
Theory of fault-tolerant quantum computation.
Physical Review A, 57:127–137, 1998.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN