An introduction to discrete phase space and Schur-Weyl duality for the Clifford group

Michael Walter

UNIVERSITY OF AMSTERDAM

QuSoft
Research Center for Quantum Software

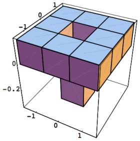
Bad Honnef, August 2018

joint work with David Gross (Cologne) and Sepehr Nezami (Stanford)

Plan for today

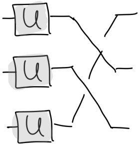
1. Introduction to discrete phase space

   Pauli & Clifford group, stabilizer states, motivation



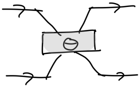
2. Schur-Weyl duality for the Clifford group

   higher moments, property testing, de Finetti, ...



Quantum optics motivation $[Q, P] = i$

Linear quantum optics described by Gaussian unitaries U_G (beam splitters, squeezing...), generate Gaussian states $|\psi\rangle = U_G |0\rangle$ (coherent, squeezed states...)

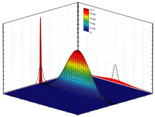


Phase space for n optical modes: $\mathbb{R}^{2n} \ni \boldsymbol{v} = (\boldsymbol{q}, \boldsymbol{p})$

- displacement operators $D_{\boldsymbol{v}} = e^{\mathrm{i}(\boldsymbol{pQ} - \boldsymbol{qP})}$
- commutation relations: $D_{\boldsymbol{v}} D_{\boldsymbol{w}} = e^{\mathrm{i}[\boldsymbol{v},\boldsymbol{w}]} D_{\boldsymbol{w}} D_{\boldsymbol{v}} \propto D_{\boldsymbol{v}+\boldsymbol{w}}$
- Gaussian unitaries act by symplectic transformations: $U_G D_{\boldsymbol{v}} U_G^\dagger \propto D_{\Gamma \boldsymbol{v}}$

Phase space distributions:

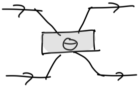
- *characteristic fn.* $\chi_\rho(\boldsymbol{v}) = \mathrm{tr}[\rho D_{\boldsymbol{v}}]$ and *Wigner function*
- Gaussian for Gaussian states $\rightsquigarrow$ mean & covariance



Highly useful – let's find a similar formalism in finite dimensions!

Quantum optics motivation $[Q, P] = i$

Linear quantum optics described by Gaussian unitaries U_G (beam splitters, squeezing...), generate Gaussian states $|\psi\rangle = U_G |0\rangle$ (coherent, squeezed states...)

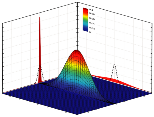


Phase space for n optical modes: $\mathbb{R}^{2n} \ni \boldsymbol{v} = (\boldsymbol{q}, \boldsymbol{p})$

- displacement operators $D_{\boldsymbol{v}} = e^{\mathrm{i}(\boldsymbol{p}\boldsymbol{Q} - \boldsymbol{q}\boldsymbol{P})}$
- commutation relations: $D_{\boldsymbol{v}} D_{\boldsymbol{w}} = e^{\mathrm{i}[\boldsymbol{v},\boldsymbol{w}]} D_{\boldsymbol{w}} D_{\boldsymbol{v}} \propto D_{\boldsymbol{v}+\boldsymbol{w}}$
- Gaussian unitaries act by symplectic transformations: $U_G D_{\boldsymbol{v}} U_G^\dagger \propto D_{\Gamma \boldsymbol{v}}$

Phase space distributions:

- *characteristic fn.* $\chi_\rho(\boldsymbol{v}) = \mathrm{tr}[\rho D_{\boldsymbol{v}}]$ and *Wigner function*
- Gaussian for Gaussian states $\rightsquigarrow$ mean & covariance



Highly useful – let's find a similar formalism in finite dimensions!

Pauli operators and discrete phase space $(\mathbb{C}^2)^{\otimes n}$

Discrete phase space for n qubits: $\mathbb{F}_2^{2n} \ni \boldsymbol{v} = (\boldsymbol{q}, \boldsymbol{p})$.

Pauli operators:

$$P_{\boldsymbol{v}} = P_{v_1} \otimes \ldots \otimes P_{v_n} \text{ where } P_{00} = I,\ P_{01} = X,\ P_{10} = Z,\ P_{11} = Y$$

- commutation relations: $P_{\boldsymbol{v}} P_{\boldsymbol{w}} = (-1)^{[\boldsymbol{v}, \boldsymbol{w}]} P_{\boldsymbol{w}} P_{\boldsymbol{v}} \propto P_{\boldsymbol{v}+\boldsymbol{w} \pmod 2}$
- generate *Pauli group*
- orthogonal operator basis: can expand $\rho = \sum_{\boldsymbol{v}} \chi_\rho(\boldsymbol{v}) P_{\boldsymbol{v}}$, where $\chi_\rho(\boldsymbol{v}) = 2^{-n} \operatorname{tr}[\rho P_{\boldsymbol{v}}]$ *characteristic function*

Qudits: phase space $\mathbb{F}_d^{2n}$ corresponding to 'shift' and 'clock' operators:

$$X|q\rangle = |q + 1 \pmod d\rangle$$
$$Z|q\rangle = e^{2\pi i q/d} |q\rangle$$

Pauli operators and discrete phase space $(\mathbb{C}^d)^{\otimes n}$

Discrete phase space for n qubits: $\mathbb{F}_2^{2n} \ni \boldsymbol{v} = (\boldsymbol{q}, \boldsymbol{p})$.

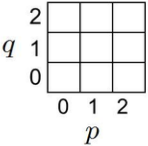
Pauli operators:

$$P_{\boldsymbol{v}} = P_{v_1} \otimes \ldots \otimes P_{v_n} \text{ where } P_{00} = I,\ P_{01} = X,\ P_{10} = Z,\ P_{11} = Y$$

- commutation relations: $P_{\boldsymbol{v}} P_{\boldsymbol{w}} = (-1)^{[\boldsymbol{v},\boldsymbol{w}]} P_{\boldsymbol{w}} P_{\boldsymbol{v}} \propto P_{\boldsymbol{v}+\boldsymbol{w} \,(\text{mod } 2)}$
- generate *Pauli group*
- orthogonal operator basis: can expand $\rho = \sum_{\boldsymbol{v}} \chi_\rho(\boldsymbol{v}) P_{\boldsymbol{v}}$, where $\chi_\rho(\boldsymbol{v}) = 2^{-n}\,\mathrm{tr}[\rho P_{\boldsymbol{v}}]$ *characteristic function*

Qudits: phase space $\mathbb{F}_d^{2n}$ corresponding to 'shift' and 'clock' operators:

$$X\,|q\rangle = |q + 1 \ (\text{mod } d)\rangle$$
$$Z\,|q\rangle = e^{2\pi i q/d}\,|q\rangle$$



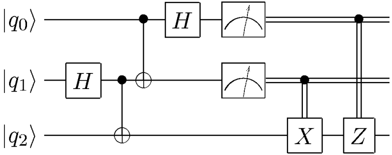
Clifford unitaries

$(\mathbb{C}^d)^{\otimes n}$

Clifford group: Unitaries U_C such that P Pauli $\Rightarrow U_C P U_C^\dagger \propto$ Pauli.
For qubits, generated by

$$\text{CNOT}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

E.g.,



Clifford unitaries = classical dynamics on discrete phase space

- for any symplectic matrix Γ, exists Clifford U_Γ with $U_\Gamma P_{\mathbf{x}} U_\Gamma^\dagger \propto P_{\Gamma \mathbf{x}}$
- conversely, any Clifford unitary is of form $U_C \propto U_\Gamma P_{\mathbf{v}}$

Clifford circuits can be simulated efficiently on a classical computer (Gottesman-Knill)

Stabilizer states

Stabilizer states: States of the form $|S\rangle = U_C |0\rangle^{\otimes n}$.

- computational basis states, maximally entangled states, GHZ states...
- QEC, MBQC, topological order, ...

Equivalently, stabilized by maximal commutative subgroup G of Paulis:

$$|S\rangle\langle S| = d^{-n} \sum_{P \in G} P$$

E.g., $|00\rangle + |11\rangle$ defined by $G = \langle XX, ZZ\rangle$.

Stabilizer states $(\mathbb{C}^d)^{\otimes n}$

Stabilizer states: States of the form $|S\rangle = U_C |0\rangle^{\otimes n}$.

- computational basis states, maximally entangled states, GHZ states...
- QEC, MBQC, topological order, ...

Equivalently, stabilized by maximal commutative subgroup G of Paulis:

$$|S\rangle\langle S| = d^{-n} \sum_{P \in G} P$$

In terms of discrete phase space: $G = \{e^{2\pi i f(\mathbf{v})/d} P_{\mathbf{v}} \mid \mathbf{v} \in V\}$, where

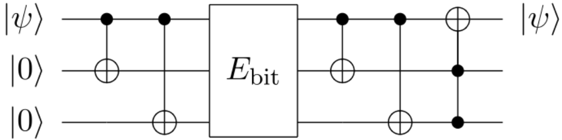
- $V \subseteq \mathbb{F}_d^{2n}$ isotropic: $[\mathbf{v}, \mathbf{w}] = 0$ for all $\mathbf{v}, \mathbf{w} \in V$
- maximal dimension: $\dim V = n$

E.g., $|00\rangle + |11\rangle$ defined by $G = \langle XX, ZZ\rangle$, $V = \langle (0011), (1100)\rangle$.

Stabilizer codes and quantum error correction

Obtain stabilizer *codes* if V isotropic but not of maximal dimension. E.g.,

- $1 \to 3$ *bit flip code* is defined by ZZI, IZZ



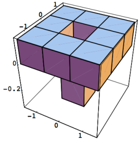
- $1 \to 5$ *qubit code* has stabilizers $XZZXI$, $IXZZX$, $XIXZZ$, $ZXIXZ$

Useful properties:

- 'stabilizers = syndrome'
- encoding and error correction circuits are Clifford
- q. error correction condition only depends on V (for Pauli errors)!

Wigner function and classical simulation

For odd d, every quantum state has a discrete Wigner function:



$$W_\rho(\boldsymbol{v}) = \hat{\chi}_\rho(\boldsymbol{v}) = d^{-2n} \sum_{\boldsymbol{w}} e^{-2\pi i [\boldsymbol{v},\boldsymbol{w}]/d} \operatorname{tr}[\rho P_{\boldsymbol{v}}]$$

- quasi-probability distribution on phase space $\mathbb{F}_d^{2n}$
- Clifford-covariant
- *discrete Hudson theorem* (Gross): for pure states, $W_\psi \geq 0$ iff stabilizer

Non-negative Wigner function $\Rightarrow$ efficient classical simulation

- Wigner negativity $\operatorname{sn}(\psi) = \sum_{\boldsymbol{v}: W_\rho(\boldsymbol{v})<0} |W_\rho(\boldsymbol{v})|$
- resource theory of stabilizer computation, contextuality, ...
- see work by Veitch *et al*, Pashayan *et al*, Raussendorf *et al*, Howard-Campbell, ...

Derandomization and designs

Randomized constructions often rely on *Haar measure*. Simple to analyze, often near-optimal – but inefficient!

A unitary t-design $\{U_j\}$ has same t-th moments as Haar measure on $U(D)$:

$$E_j[(U_j \otimes U_j^\dagger)^{\otimes t}] = E_{\text{Haar}}[(U \otimes U^\dagger)^{\otimes t}]$$

A state t-design $\{\psi_j\}$ has same t-th moments as 'Haar measure' on pure states:

$$E_j[|\psi_j\rangle\langle\psi_j|^{\otimes t}] = E_{\text{Haar}}[|\psi\rangle\langle\psi|^{\otimes t}]$$

- Clifford unitaries and stabilizer states are 2-design; 3-design for qubits (Küng-Gross, Zhu, Webb)
- many applications: randomized benchmarking, phase retrieval, low-rank matrix recovery, ...

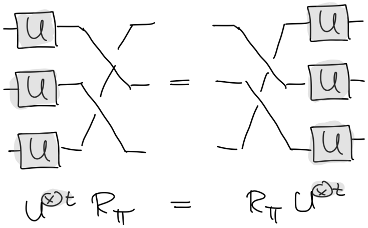
Schur-Weyl duality for the Clifford group

Schur-Weyl duality

$(\mathbb{C}^D)^{\otimes t}$

Two *symmetries* that are ubiquitous in quantum information theory:

$$U^{\otimes t} |x_1, \ldots, x_t\rangle = U |x_1\rangle \otimes \ldots \otimes U |x_t\rangle$$
$$R_\pi |x_1, \ldots, x_t\rangle = |x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(t)}\rangle$$



- i.i.d. quantum information: $[\rho^{\otimes t}, R_\pi] = 0$
- eigenvalues, entropies, ...: $\rho \equiv U \rho U^\dagger$
- randomized constructions: $E_{\text{Haar}}[|\psi\rangle\langle\psi|^{\otimes t}]$

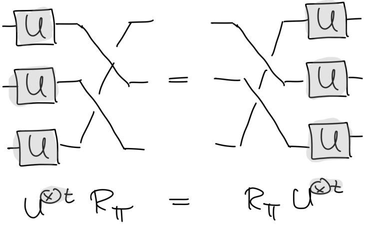
Would like a version for Clifford unitaries U_C!

Schur-Weyl duality

$(\mathbb{C}^D)^{\otimes t}$

Two *symmetries* that are ubiquitous in quantum information theory:

$$U^{\otimes t}\,|x_1,\dots,x_t\rangle = U\,|x_1\rangle \otimes \dots \otimes U\,|x_t\rangle$$
$$R_\pi\,|x_1,\dots,x_t\rangle = |x_{\pi^{-1}(1)},\dots,x_{\pi^{-1}(t)}\rangle$$



Schur-Weyl duality: These actions generate each other's commutant.

- i.i.d. quantum information: $[\rho^{\otimes t}, R_\pi] = 0$
- eigenvalues, entropies, ...: $\rho \equiv U \rho U^\dagger$
- randomized constructions: $E_{\text{Haar}}[|\psi\rangle\langle\psi|^{\otimes t}] \propto \sum_{\pi \in S_t} R_\pi$

Would like a version for Clifford unitaries U_C!

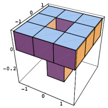
Our results

"Schur-Weyl duality" for the Clifford group: We characterize precisely which operators commute with $U_C^{\otimes t}$ for all Clifford unitaries U_C.

Fewer unitaries $\rightsquigarrow$ larger commutant (more than permutations).

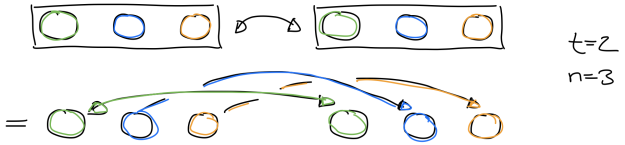
Applications:

- Property testing $\quad |S\rangle^{\otimes t} \longleftrightarrow |\psi\rangle^{\otimes t}$
- De Finetti theorems with increased symmetry $\quad \Psi_s \approx \sum_S p_S \, |S\rangle\langle S|^{\otimes s}$
- Higher moments of stabilizer states $\quad E_S[|S\rangle\langle S|^{\otimes t}]$
- t-designs from Clifford orbits
- Robust Hudson theorem



Permuting blocks

Permutation of t copies of $(\mathbb{C}^d)^{\otimes n}$:



$$R_\pi = r_\pi^{\otimes n}, \quad r_\pi = \sum_{\boldsymbol{x}} |\pi \boldsymbol{x}\rangle \langle \boldsymbol{x}|$$

Here, we think of π as $t \times t$-permutation matrix, and $|\boldsymbol{x}\rangle = |x_1, \ldots, x_t\rangle$ is computational basis of $(\mathbb{C}^d)^{\otimes t}$.

The commutant of $\{U_C^{\otimes t}\}$ is given by a straightforward generalization...

Schur-Weyl duality for the Clifford group $(\mathbb{C}^d)^{\otimes n}$

$$R_T = r_T^{\otimes n}, \quad r_T = \sum_{(\boldsymbol{y},\boldsymbol{x}) \in T} |\boldsymbol{y}\rangle \langle \boldsymbol{x}|$$

Allow all subspaces $T \subseteq \mathbb{F}_d^{2t}$ that are self-dual codes, i.e. $\boldsymbol{y} \cdot \boldsymbol{y}' \equiv \boldsymbol{x} \cdot \boldsymbol{x}'$ and of maximal dimension t. Moreover, require $|\boldsymbol{y}| \equiv |\boldsymbol{x}|$ (for qubits, modulo 4).

Theorem

For $n \geq t-1$, the operators R_T are $\prod_{k=0}^{t-2}(d^k+1)$ many linearly independent operators that span the commutant of $\{U_C^{\otimes t}\}$.

Independent of n (just like in ordinary Schur-Weyl duality)! Rich algebraic structure (see paper).

Examples of commutant

Want subspaces $T \subseteq \mathbb{F}_d^{2t}$ that are self-dual codes, i.e. $\boldsymbol{y} \cdot \boldsymbol{y}' \equiv \boldsymbol{x} \cdot \boldsymbol{x}'$ and of maximal dimension t. Moreover, require $|\boldsymbol{y}| \equiv |\boldsymbol{x}|$ (for qubits, modulo 4).

For qubits, an example is the following code for $t = 4$:

$$T = \operatorname{ran}\begin{pmatrix} 1\,1\,1\,1 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 1\,1\,1\,1 \\ 1\,1\,0\,0 & 1\,1\,0\,0 \\ 1\,0\,1\,0 & 1\,0\,1\,0 \end{pmatrix},$$
$$R_T = 2^{-n}\left(I^{\otimes 4} + X^{\otimes 4} + Y^{\otimes 4} + Z^{\otimes 4}\right)$$

The projector R_T commutes with $U_C^{\otimes 4}$ for every n-qubit Clifford unitary. Central to 4-th moments of multiqubit stabilizer states (Zhu *et al*, later).

Examples of commutant

Can also obtain subspaces as graphs $T = \{(O\boldsymbol{x}, \boldsymbol{x})\}$ of $t \times t$ orthogonal stochastic matrices. Then $R_O = r_O^{\otimes n}$, $r_O = \sum_{\boldsymbol{x}} |O\boldsymbol{x}\rangle \langle \boldsymbol{x}|$ is in commutant.

For qubits, an example is the 6×6 anti-identity:

$$\overline{\mathrm{id}} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

$$R_{\overline{\mathrm{id}}} |\boldsymbol{x}_1, \ldots, \boldsymbol{x}_6\rangle = |\boldsymbol{x}_2 + \ldots + \boldsymbol{x}_6, \ldots, \boldsymbol{x}_1 + \ldots + \boldsymbol{x}_5\rangle$$

The unitary $R_{\overline{\mathrm{id}}}$ commutes with $U_C^{\otimes 6}$ for every n-qubit Clifford unitary.

The $\{R_O\}$ are symmetries of stabilizer tensor powers $\rightsquigarrow$ de Finetti (later).

Why should the theorem be true?

$$R_T = r_T^{\otimes n}, \quad r_T = \sum_{(\boldsymbol{y},\boldsymbol{x}) \in T} |\boldsymbol{y}\rangle \langle \boldsymbol{x}|$$

When is R_T in the commutant? Need that $T \subseteq \mathbb{F}_2^{2t}$ is...

- subspace: $\mathrm{CNOT}^{\otimes t} \, r_T^{\otimes 2} \, \mathrm{CNOT}^{\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x}),(\boldsymbol{y}',\boldsymbol{x}') \in T} |\boldsymbol{y}\rangle\langle\boldsymbol{x}| \otimes |\boldsymbol{y}+\boldsymbol{y}'\rangle\langle\boldsymbol{x}+\boldsymbol{x}'| = r_T^{\otimes 2}$
- self-dual: $H^{\otimes t} \, r_T \, H^{\otimes t} = \sum_{(\boldsymbol{y}',\boldsymbol{x}') \in T^\perp} |\boldsymbol{y}'\rangle \langle \boldsymbol{x}'| = r_T$
- modulo 4: $P^{\otimes t} \, r_T \, P^{\dagger,\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x}) \in T} i^{|\boldsymbol{y}|-|\boldsymbol{x}|} |\boldsymbol{y}\rangle \langle \boldsymbol{x}| = r_T$

Remainder of proof: Show that R_T's linearly independent. Compute dimension of commutant (#group orbits) & number of subspaces as above (Witt's lemma). □

Why should the theorem be true?

$$R_T = r_T^{\otimes n}, \quad r_T = \sum_{(\boldsymbol{y},\boldsymbol{x})\in T} |\boldsymbol{y}\rangle\langle\boldsymbol{x}|$$

When is R_T in the commutant? Need that $T \subseteq \mathbb{F}_2^{2t}$ is...

- subspace: $\text{CNOT}^{\otimes t}\, r_T^{\otimes 2}\, \text{CNOT}^{\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x}),(\boldsymbol{y}',\boldsymbol{x}')\in T} |\boldsymbol{y}\rangle\langle\boldsymbol{x}| \otimes |\boldsymbol{y}+\boldsymbol{y}'\rangle\langle\boldsymbol{x}+\boldsymbol{x}'| = r_T^{\otimes 2}$
- self-dual:

$$H^{\otimes t}\, r_T\, H^{\otimes t} = \sum_{\boldsymbol{y}',\boldsymbol{x}'} |\boldsymbol{y}'\rangle\langle\boldsymbol{x}'|\, 2^{-t} \sum_{(\boldsymbol{y},\boldsymbol{x})\in T} (-1)^{\boldsymbol{y}\cdot\boldsymbol{y}'+\boldsymbol{x}\cdot\boldsymbol{x}'} = \sum_{(\boldsymbol{y}',\boldsymbol{x}')\in T^\perp} |\boldsymbol{y}'\rangle\langle\boldsymbol{x}'| = r_T$$

- modulo 4: $P^{\otimes t}\, r_T\, P^{\dagger,\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x})\in T} i^{|\boldsymbol{y}|-|\boldsymbol{x}|} |\boldsymbol{y}\rangle\langle\boldsymbol{x}| = r_T$

Remainder of proof: Show that R_T's linearly independent. Compute dimension of commutant (#group orbits) & number of subspaces as above (Witt's lemma). □

Why should the theorem be true?

$$R_T = r_T^{\otimes n}, \quad r_T = \sum_{(\boldsymbol{y},\boldsymbol{x})\in T} |\boldsymbol{y}\rangle\langle\boldsymbol{x}|$$

When is R_T in the commutant? Need that $T \subseteq \mathbb{F}_2^{2t}$ is...

- subspace: $\mathrm{CNOT}^{\otimes t}\, r_T^{\otimes 2}\, \mathrm{CNOT}^{\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x}),(\boldsymbol{y}',\boldsymbol{x}')\in T} |\boldsymbol{y}\rangle\langle\boldsymbol{x}| \otimes |\boldsymbol{y}+\boldsymbol{y}'\rangle\langle\boldsymbol{x}+\boldsymbol{x}'| = r_T^{\otimes 2}$
- self-dual: $H^{\otimes t}\, r_T\, H^{\otimes t} = \sum_{(\boldsymbol{y}',\boldsymbol{x}')\in T^\perp} |\boldsymbol{y}'\rangle\langle\boldsymbol{x}'| = r_T$
- modulo 4: $P^{\otimes t}\, r_T\, P^{\dagger,\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x})\in T} i^{|\boldsymbol{y}|-|\boldsymbol{x}|} |\boldsymbol{y}\rangle\langle\boldsymbol{x}| = r_T$

Remainder of proof: Show that R_T's linearly independent. Compute dimension of commutant (#group orbits) & number of subspaces as above (Witt's lemma). □

Why should the theorem be true?

$$R_T = r_T^{\otimes n}, \quad r_T = \sum_{(\boldsymbol{y},\boldsymbol{x})\in T} |\boldsymbol{y}\rangle\langle\boldsymbol{x}|$$

When is R_T in the commutant? Need that $T \subseteq \mathbb{F}_2^{2t}$ is...

- subspace: $\mathrm{CNOT}^{\otimes t}\, r_T^{\otimes 2}\, \mathrm{CNOT}^{\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x}),(\boldsymbol{y}',\boldsymbol{x}')\in T} |\boldsymbol{y}\rangle\langle\boldsymbol{x}| \otimes |\boldsymbol{y}+\boldsymbol{y}'\rangle\langle\boldsymbol{x}+\boldsymbol{x}'| = r_T^{\otimes 2}$
- self-dual: $H^{\otimes t}\, r_T\, H^{\otimes t} = \sum_{(\boldsymbol{y}',\boldsymbol{x}')\in T^\perp} |\boldsymbol{y}'\rangle\langle\boldsymbol{x}'| = r_T$
- modulo 4: $P^{\otimes t}\, r_T\, P^{\dagger,\otimes t} = \sum_{(\boldsymbol{y},\boldsymbol{x})\in T} i^{|\boldsymbol{y}|-|\boldsymbol{x}|} |\boldsymbol{y}\rangle\langle\boldsymbol{x}| = r_T$

Remainder of proof: Show that R_T's linearly independent. Compute dimension of commutant (#group orbits) & number of subspaces as above (Witt's lemma). □

Application 1: Higher moments of stabilizer states

Result (t-th moment)

$E[|S\rangle\langle S|^{\otimes t}] \propto \sum_T R_T$

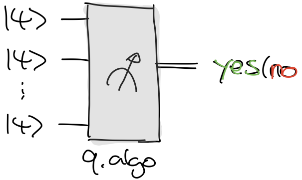
- When stabilizer states form t-design, reduces to $\sum_\pi R_\pi$ (Haar average)
- Summarizes all previous results on statistical properties
- ... but works for *any* t-th moment!

Many applications: Improved bounds for randomized benchmarking (Helsen et al, Bas' poster!), low-rank matrix recovery (Kueng et al); analytical studies of scrambling in Clifford circuits; toy models of holography (Nezami-W); ...

We can also write t-th moment as weighted sum of certain CSS codes.

Application 2: Stabilizer testing

Given t copies of an unknown state in $(\mathbb{C}^d)^{\otimes n}$, decide if it is a stabilizer state or ε-far from it.



Idea: Use the anti-identity. Measure POVM element $\frac{1+R_{\overline{\text{id}}}}{2}$ on $t = 6$ copies.

Result

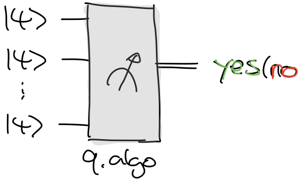
Let ψ be a pure state of n qubits. If ψ is a stabilizer state then this accepts always. But if $\max_S |\langle\psi|S\rangle|^2 \leq 1 - \varepsilon^2$, acceptance probability $\leq 1 - \varepsilon^2/4$.

- Power of test independent of n. Answers q. by Montanaro & de Wolf.
- Similar result for qudits & for testing if blackbox unitary is Clifford.

Why does it work? How to implement?

Application 2: Stabilizer testing

Given t copies of an unknown state in $(\mathbb{C}^d)^{\otimes n}$, decide if it is a stabilizer state or ε-far from it.



Idea: Use the anti-identity. Measure POVM element $\frac{1+R_{\overline{\mathrm{id}}}}{2}$ on $t = 6$ copies.

Result

Let ψ be a pure state of n qubits. If ψ is a stabilizer state then this accepts always. But if $\max_S |\langle\psi|S\rangle|^2 \leq 1 - \varepsilon^2$, acceptance probability $\leq 1 - \varepsilon^2/4$.

- Power of test independent of n. Answers q. by Montanaro & de Wolf.
- Similar result for qudits & for testing if blackbox unitary is Clifford.

Why does it work? How to implement?

Stabilizer testing using Bell difference sampling

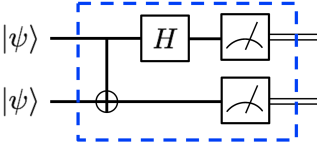
Any state ψ can be expanded in Pauli basis[†]:

$$\psi = \sum_{\boldsymbol{v}} \chi_\psi(\boldsymbol{v}) P_{\boldsymbol{v}}$$

- If pure, then $p_\psi(\boldsymbol{v}) = 2^n |\chi_\psi(\boldsymbol{v})|^2$ is a probability distribution.
- If stabilizer state, then support of p_ψ is stabilizer group (up to sign).

Key idea: Sample & verify!

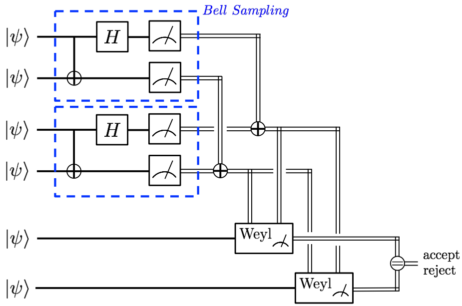
How to sample? If ψ is real, can simply measure in Bell basis $(P_{\boldsymbol{v}} \otimes I) |\Phi^+\rangle$ (Bell sampling; Montanaro, Zhao *et al*).



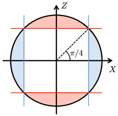
[†]recall $P_{\boldsymbol{v}} = P_{v_1} \otimes \ldots \otimes P_{v_n}$ where $P_{00} = I$, $P_{01} = X$, $P_{10} = Z$, $P_{11} = Y$

Stabilizer testing using Bell difference sampling

In general, need to take 'difference' of two Bell measurement outcomes:



- Fully transversal circuit, only need coherent two-qubit operations.
- Circuit is equivalent to measuring the anti-identity!



Proof of converse uses uncertainty relation.

How to test stabilizer rank?

Application 3: Stabilizer de Finetti theorems

Any tensor power $|\psi\rangle^{\otimes t}$ has S_t-symmetry. De Finetti theorems provide 'partial' converse: If $|\Psi\rangle$ has S_t-symmetry, $\Psi_s \approx \int d\mu(\psi)\psi^{\otimes s}$ for $s \ll t$.

Stabilizer tensor powers have increased symmetry:

$$R_O |S\rangle^{\otimes t} = |S\rangle^{\otimes t} \qquad \text{for all orthogonal and stochastic } O$$

Result

Assume that $|\Psi\rangle \in ((\mathbb{C}^d)^{\otimes n})^{\otimes t}$ has this symmetry. Then:

$$\|\Psi_s - \sum_S p_S |S\rangle\langle S|^{\otimes s}\|_1 \lesssim d^{2n(n+2)} d^{-(t-s)/2}$$

- Approximation is exponentially good, by *bona fide* stabilizer states.
- Similar to Gaussian de Finetti (Leverrier *et al*). Applications to QKD?

Can reduce symmetry requirements at expense of goodness.

Application 3: Stabilizer de Finetti theorems

Any tensor power $|\psi\rangle^{\otimes t}$ has S_t-symmetry. De Finetti theorems provide 'partial' converse: If $|\Psi\rangle$ has S_t-symmetry, $\Psi_s \approx \int d\mu(\psi)\psi^{\otimes s}$ for $s \ll t$.

Stabilizer tensor powers have increased symmetry:

$$R_O \, |S\rangle^{\otimes t} = |S\rangle^{\otimes t} \qquad \text{for all orthogonal and stochastic } O$$

Result

Assume that $|\Psi\rangle \in ((\mathbb{C}^d)^{\otimes n})^{\otimes t}$ has this symmetry. Then:

$$\|\Psi_s - \sum_S p_S \, |S\rangle\langle S|^{\otimes s}\|_1 \lesssim d^{2n(n+2)} d^{-(t-s)/2}$$

- Approximation is exponentially good, by *bona fide* stabilizer states.
- Similar to Gaussian de Finetti (Leverrier *et al*). Applications to QKD?

Can reduce symmetry requirements at expense of goodness.

Application 4: t-designs from Clifford orbits

When $t > 2$ or 3 (qubits), stabilizer states fail to be t-design. Yet, hints in the literature that this failure is relatively *graceful* (Zhu *et al*, Nezami-W). E.g., Clifford orbit of non-stabilizer qutrit states can be 3-design!

We prove in general:

Result

For every t, there exists ensemble of $N = N(d, t)$ many fiducial states in $(\mathbb{C}^d)^{\otimes n}$ such that corresponding Clifford orbits form t-design.

- Number of fiducials does not depend on n!
- Efficient construction?

Application 4: t-designs from Clifford orbits

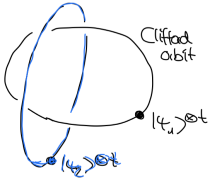
When $t > 2$ or 3 (qubits), stabilizer states fail to be t-design. Yet, hints in the literature that this failure is relatively *graceful* (Zhu *et al*, Nezami-W). E.g., Clifford orbit of non-stabilizer qutrit states can be 3-design!

We prove in general:

Result

For every t, there exists ensemble of $N = N(d,t)$ many fiducial states in $(\mathbb{C}^d)^{\otimes n}$ such that corresponding Clifford orbits form t-design.

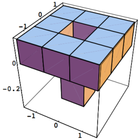
- Number of fiducials does not depend on n!
- Efficient construction?



Application 5: Robust Hudson theorem

Recall: For odd d, every quantum state has a discrete Wigner function:

$$W_\rho(\boldsymbol{v}) = d^{-2n} \sum_{\boldsymbol{w}} e^{-2\pi i[\boldsymbol{v},\boldsymbol{w}]/d} \operatorname{tr}[\rho P_{\boldsymbol{v}}]$$



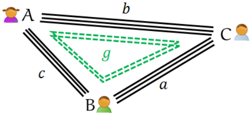
- Quasi-probability distribution on phase space $\mathbb{F}_d^{2n}$
- Discrete Hudson theorem: For pure states, $W_\psi \geq 0$ iff ψ stabilizer
- Wigner negativity $\operatorname{sn}(\psi) = \sum_{\boldsymbol{v}:W_\rho(\boldsymbol{v})<0} |W_\rho(\boldsymbol{v})|$: monotone in resource theory of stabilizer computation; witness for contextuality

Result (Robust Hudson)

There exists a stabilizer state $|S\rangle$ such that $|\langle S|\psi\rangle|^2 \geq 1 - 9d^2 \operatorname{sn}(\psi)$.

Application 6: Typical entanglement of stabilizer states

Tripartite stabilizer states decompose into EPR and GHZ entanglement:



How about typical stabilizer states? *Or even tensor networks?*

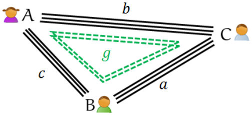
Result (Nezami-W)

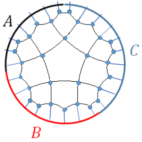
In random stabilizer tensor network states: $g = O(1)$ *w.h.p.*

- can distill $\simeq \frac{1}{2} I(A:B)$ EPR pairs
- mutual information is entanglement measure
- generalizes result by Leung & Smith (qubits, single tensor)

Application 6: Typical entanglement of stabilizer states

Tripartite stabilizer states decompose into EPR and GHZ entanglement:





How about typical stabilizer states? Or even tensor networks?

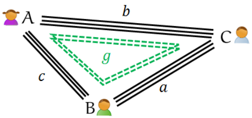
Result (Nezami-W)

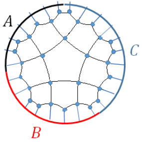
In random stabilizer tensor network states: $g = O(1)$ *w.h.p.*

- can distill $\simeq \frac{1}{2} I(A:B)$ EPR pairs
- mutual information is entanglement measure
- generalizes result by Leung & Smith
  (qubits, single tensor)

Application 6: Typical entanglement of stabilizer states

Tripartite stabilizer states decompose into EPR and GHZ entanglement:



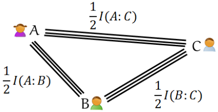


How about typical stabilizer states? Or even tensor networks?

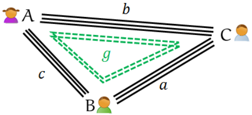
Result (Nezami-W)

In random stabilizer tensor network states: $g = O(1)$ *w.h.p.*

- can distill $\simeq \frac{1}{2} I(A:B)$ EPR pairs
- mutual information is entanglement measure
- generalizes result by Leung & Smith (qubits, single tensor)



Bounding the amount of GHZ entanglement



$$I(A:B) = 2c + g$$

Diagnose via third moment of *partial transpose*:

$$g \log d = S(A) + S(B) + S(C) + \log \operatorname{tr}(\rho_{AB}^{T_B})^3$$

Compute via *replica trick*: For single stabilizer state

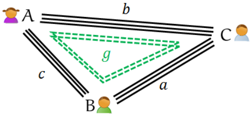
$$\operatorname{tr}(\rho_{AB}^{T_B})^3 = \operatorname{tr} |S\rangle\langle S|_{ABC}^{\otimes 3} \left(R_{\zeta,A} \otimes R_{\zeta^{-1},B} \otimes R_{\mathrm{id},C} \right)$$

where $\zeta = (1\ 2\ 3)$ three-cycle, hence

$$\mathbb{E}[\operatorname{tr}(\rho_{AB}^{T_B})^3] \propto \sum_T \left(\operatorname{tr} r_T r_\zeta\right)^{n_A} \left(\operatorname{tr} r_T r_{\zeta^{-1}}\right)^{n_B} \left(\operatorname{tr} r_T r_{\mathrm{id}}\right)^{n_C}$$

Similarly for tensor networks $\rightsquigarrow$ *classical statistical model!*

Bounding the amount of GHZ entanglement



$$I(A:B) = 2c + g$$

Diagnose via third moment of *partial transpose*:

$$g \log d = S(A) + S(B) + S(C) + \log \operatorname{tr}(\rho_{AB}^{T_B})^3$$

Compute via *replica trick*: For single stabilizer state

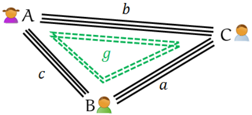
$$\operatorname{tr}(\rho_{AB}^{T_B})^3 = \operatorname{tr} |S\rangle\langle S|_{ABC}^{\otimes 3} \left(R_{\zeta,A} \otimes R_{\zeta^{-1},B} \otimes R_{\mathrm{id},C} \right)$$

where $\zeta = (1\ 2\ 3)$ three-cycle, hence

$$\mathbb{E}[\operatorname{tr}(\rho_{AB}^{T_B})^3] \propto \sum_T \left(\operatorname{tr} r_T r_\zeta\right)^{n_A} \left(\operatorname{tr} r_T r_{\zeta^{-1}}\right)^{n_B} \left(\operatorname{tr} r_T r_{\mathrm{id}}\right)^{n_C}$$

Similarly for tensor networks $\rightsquigarrow$ *classical statistical model!*

Bounding the amount of GHZ entanglement



$$I(A:B) = 2c + g$$

Diagnose via third moment of *partial transpose*:

$$g \log d = S(A) + S(B) + S(C) + \log \operatorname{tr}(\rho_{AB}^{T_B})^3$$

Compute via *replica trick*: For single stabilizer state

$$\operatorname{tr}(\rho_{AB}^{T_B})^3 = \operatorname{tr} |S\rangle\langle S|_{ABC}^{\otimes 3} \left(R_{\zeta,A} \otimes R_{\zeta^{-1},B} \otimes R_{\mathrm{id},C} \right)$$

where $\zeta = (1\ 2\ 3)$ three-cycle, hence

$$\mathbb{E}[\operatorname{tr}(\rho_{AB}^{T_B})^3] \propto \sum_T \left(\operatorname{tr} r_T r_\zeta\right)^{n_A} \left(\operatorname{tr} r_T r_{\zeta^{-1}}\right)^{n_B} \left(\operatorname{tr} r_T r_{\mathrm{id}}\right)^{n_C}$$

Similarly for tensor networks $\rightsquigarrow$ *classical statistical model!*

Bounding the amount of GHZ entanglement

For simplicity, assume A, B, C each n qubits.

$$\mathbb{E}[g] \leq 3n + \log \mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3]$$

Since qubit stabilizers are three-design:

$$\mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3] = \sum_{\pi \in S_3} 2^{-n\left(d(\zeta,\pi) + d(\zeta^{-1},\pi) + d(\mathrm{id},\pi)\right)}$$

where $d(\pi,\tau)$ = minimum number of swaps needed for $\pi \leftrightarrow \tau$. Thus:

$$\mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3] \leq 3 \cdot \underbrace{2^{-3n}}_{\text{swaps}} + 3 \cdot \underbrace{2^{-4n}}_{\mathrm{id},\zeta,\zeta^{-1}} \quad \Rightarrow \quad \mathbb{E}[g] \lesssim \log 3 \quad \square$$

For $d > 2$, $\{T\} = \{even\} \cup \{odd\}$. Calculation completely analogous!

Bounding the amount of GHZ entanglement

For simplicity, assume A, B, C each n qubits.

$$\mathbb{E}[g] \leq 3n + \log \mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3]$$

Since qubit stabilizers are three-design:

$$\mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3] = \sum_{\pi \in S_3} 2^{-n\left(d(\zeta,\pi) + d(\zeta^{-1},\pi) + d(\mathrm{id},\pi)\right)}$$

where $d(\pi, \tau)$ = minimum number of swaps needed for $\pi \leftrightarrow \tau$. Thus:

$$\mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3] \leq 3 \cdot \underbrace{2^{-3n}}_{\text{swaps}} + 3 \cdot \underbrace{2^{-4n}}_{\mathrm{id},\zeta,\zeta^{-1}} \quad \Rightarrow \quad \mathbb{E}[g] \lesssim \log 3 \quad \square$$

For $d > 2$, $\{T\} = \{even\} \cup \{odd\}$. Calculation completely analogous!

Bounding the amount of GHZ entanglement

For simplicity, assume A, B, C each n qubits.

$$\mathbb{E}[g] \leq 3n + \log \mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3]$$

Since qubit stabilizers are three-design:

$$\mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3] = \sum_{\pi \in S_3} 2^{-n\left(d(\zeta,\pi) + d(\zeta^{-1},\pi) + d(\mathrm{id},\pi) \right)}$$

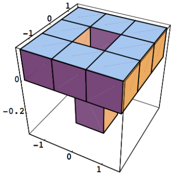
where $d(\pi,\tau) =$ minimum number of swaps needed for $\pi \leftrightarrow \tau$. Thus:

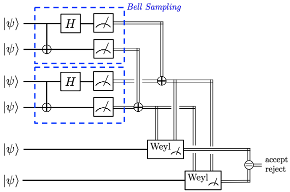
$$\mathbb{E}[\mathrm{tr}(\rho_{AB}^{T_B})^3] \leq 3 \cdot \underbrace{2^{-3n}}_{\text{swaps}} + 3 \cdot \underbrace{2^{-4n}}_{\mathrm{id},\zeta,\zeta^{-1}} \quad \Rightarrow \quad \mathbb{E}[g] \lesssim \log 3 \quad \square$$

For $d > 2$, $\{T\} = \{even\} \cup \{odd\}$. Calculation completely analogous!

Summary and outlook

arXiv:1712.08628





Pauli & Clifford unitaries, stabilizer states in $(\mathbb{C}^d)^{\otimes n}$:

- best understood via discrete phase space $\mathbb{F}_d^{2n}$

Schur-Weyl duality for the Clifford group:

- clean algebraic description in terms of self-dual codes
- resolve open question in quantum property testing
- new tools for stabilizer states: moments, de Finetti, Hudson, ...

Thank you for your attention!