# Random stabilizer tensors – duality and applications

Michael Walter

joint work with David Gross and Sepehr Nezami

RUHR UNIVERSITÄT BOCHUM

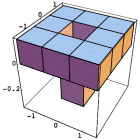
European Research Council
Established by the European Commission

Random Tensors @ IHP, October 2024

# Plan for today

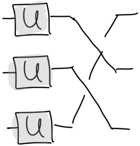
1. Introduction

   *Schur-Weyl, Paulis, Cliffords, stabilizers*



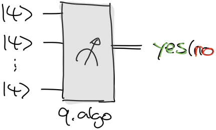

2. "Schur-Weyl" or Howe-Kashiwara-Vergne duality for the Clifford group

   *commutant of tensor power action*




2. Applications

   *property testing, de Finetti, ...*

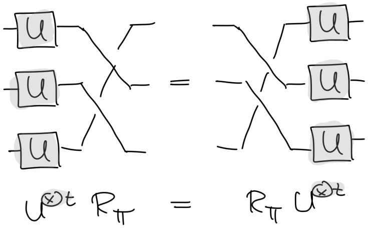


# Schur-Weyl duality

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

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

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



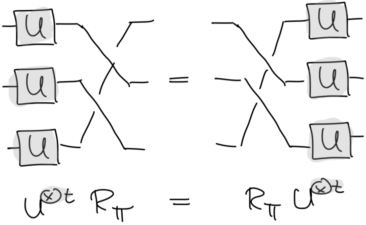

- i.i.d. quantum information: $[\rho^{\otimes t}, R_\pi] = 0$
- eigenvalues, entropies, ...: $\rho \equiv U\rho U^\dagger$
- randomized constructions: $E_{\text{Haar}}[|\psi\rangle\langle\psi|^{\otimes t}]$

# Schur-Weyl duality

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

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

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




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: $E_{\text{Haar}}[|\psi\rangle\langle\psi|^{\otimes t}] \propto \sum_{\pi \in S_t} R_\pi$

# 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 $\mathbb{P}(\mathbb{C}^D)$:

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

We now discuss a well-known source of $t$-designs (for small $t$)...

# 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 $\mathbb{P}(\mathbb{C}^D)$:

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

We now discuss a well-known source of $t$-designs (for small $t$)...

# 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: $P_{\boldsymbol{v}} P_{\boldsymbol{w}} = (-1)^{[\boldsymbol{v},\boldsymbol{w}]} P_{\boldsymbol{w}} P_{\boldsymbol{v}} \propto P_{\boldsymbol{v}+\boldsymbol{w} \bmod 2}$
- generate *Pauli group*
- orthogonal operator basis: can expand $\rho = \sum_{\boldsymbol{v}} c_{\boldsymbol{v}} P_{\boldsymbol{v}}$

*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: $\mathbb{F}_2^{2n} \ni \boldsymbol{v} = (\boldsymbol{q}, \boldsymbol{p})$.

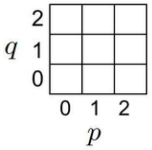
Pauli operators:

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

- commutation relations: $P_{\boldsymbol{v}} P_{\boldsymbol{w}} = (-1)^{[\boldsymbol{v},\boldsymbol{w}]} P_{\boldsymbol{w}} P_{\boldsymbol{v}} \propto P_{\boldsymbol{v}+\boldsymbol{w} \bmod 2}$
- generate *Pauli group*
- orthogonal operator basis: can expand $\rho = \sum_{\boldsymbol{v}} c_{\boldsymbol{v}} P_{\boldsymbol{v}}$

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

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



# Clifford unitaries and stabilizer states



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

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

Stabilizer states: States of the form $|S\rangle = U_C |0\rangle^{\otimes n}$.
Equivalently, stabilized by maximal commutative subgroup $G$ of Pauli group:

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

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

These are very widely used in quantum information (error correction, crypto, randomized constructions & protocols, topological order, scrambling, ...). Why?

- have rich algebraic structure and can be highly entangled
- efficient to compute with on *classical* computers [Gottesman-Knill]
- same low moments as Haar measure

# Clifford unitaries and stabilizer states



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

$$\text{CNOT}, \quad H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right), \quad S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right).$$

Stabilizer states: States of the form $|S\rangle = U_C |0\rangle^{\otimes n}$.
Equivalently, stabilized by maximal commutative subgroup $G$ of Pauli group:

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

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

These are very widely used in quantum information (error correction, crypto, randomized constructions & protocols, topological order, scrambling, ...). Why?

- have rich algebraic structure and can be highly entangled
- efficient to compute with on *classical* computers [Gottesman-Knill]
- same low moments as Haar measure

# Clifford unitaries and stabilizer states $(\mathbb{C}^d)^{\otimes n}$

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

$$\text{CNOT}, \quad H = \tfrac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right), \quad S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right).$$

Stabilizer states: States of the form $|S\rangle = U_C |0\rangle^{\otimes n}$.
Equivalently, stabilized by maximal commutative subgroup $G$ of Pauli group:

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

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

These are very widely used in quantum information (error correction, crypto, randomized constructions & protocols, topological order, scrambling, ...). Why?

- have rich algebraic structure and can be highly entangled
- efficient to compute with on *classical* computers [Gottesman-Knill]
- same low moments as Haar measure

# Cliffords and stabilizers in phase space $(\mathbb{C}^d)^{\otimes n}$

Clifford unitaries realize *classical dynamics* on discrete phase space:

- for any symplectic matrix $\Gamma$, exists Clifford $U_\Gamma$ s.th. $U_\Gamma P_{\boldsymbol{x}} U_\Gamma^\dagger \propto P_{\Gamma \boldsymbol{x}}$
- any Clifford unitary is of form $U_C \propto U_\Gamma P_{\boldsymbol{v}}$
- closely related to "oscillator" or Weil representation of $\mathrm{Sp}(2n, \mathbb{F}_d)$

Stabilizer states can also be described in phase space. For any state $|\psi\rangle$,

$$V = \{\boldsymbol{v} \in \mathbb{F}_d^{2n} \mid P_{\boldsymbol{v}} |\psi\rangle \propto |\psi\rangle\}$$

is an isotropic subspace ($[\boldsymbol{v}, \boldsymbol{w}] = 0$ for all $\boldsymbol{v}, \boldsymbol{w} \in V$). For stabilizer states, $V$ is of maximal dimension $n$, i.e., Lagrangian.

*This structure is at the heart of the theory and many applications...*

# Cliffords and stabilizers in phase space $(\mathbb{C}^d)^{\otimes n}$

Clifford unitaries realize *classical dynamics* on discrete phase space:

- for any symplectic matrix $\Gamma$, exists Clifford $U_\Gamma$ s.th. $U_\Gamma P_{\boldsymbol{x}} U_\Gamma^\dagger \propto P_{\Gamma \boldsymbol{x}}$
- any Clifford unitary is of form $U_C \propto U_\Gamma P_{\boldsymbol{v}}$
- closely related to "oscillator" or Weil representation of $\mathrm{Sp}(2n, \mathbb{F}_d)$

Stabilizer states can also be described in phase space. For any state $|\psi\rangle$,

$$V = \{\boldsymbol{v} \in \mathbb{F}_d^{2n} \mid P_{\boldsymbol{v}} |\psi\rangle \propto |\psi\rangle\}$$

is an isotropic subspace ($[\boldsymbol{v}, \boldsymbol{w}] = 0$ for all $\boldsymbol{v}, \boldsymbol{w} \in V$). For stabilizer states, $V$ is of maximal dimension $n$, i.e., Lagrangian.

*This structure is at the heart of the theory and many applications...*

# The result

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

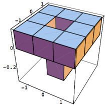
*Fewer unitaries $\rightsquigarrow$ larger commutant (more than permutations).*

Many applications by many authors:

- Higher moments of stabilizer states $E_S[|S\rangle\langle S|^{\otimes t}]$
- Random tensor networks and Clifford circuits [Nezami-W, Apel et al, Li et al, ...]
- Efficient constructions of unitary $t$-designs [Haferkamp et al]

- Property testing $|S\rangle^{\otimes t} \longleftrightarrow |\psi\rangle^{\otimes t}$
- Lower bounds on $T$-gates required for pseudorandomness [Grewal et al, ...]
- De Finetti theorems with increased symmetry $\Psi_s \approx \sum_S p_S \, |S\rangle\langle S|^{\otimes s}$

- Robust Hudson theorem



# Towards Schur-Weyl duality for the Clifford group

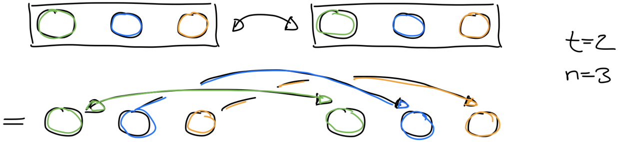
Plan:

1. Write down permutation action.
2. Generalize.
3. Prove that done!

# Towards Schur-Weyl duality for the Clifford group

1. Write down permutation action:

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

# Towards Schur-Weyl duality for the Clifford group

2. Generalize:

$$R_O = r_O^{\otimes n}, \quad r_O = \sum_{\boldsymbol{x}} |O\boldsymbol{x}\rangle \langle \boldsymbol{x}|$$

Allow all orthogonal and stochastic $t \times t$-matrices $O$ with entries in $\mathbb{F}_d$.

For qubits, an example is the $6 \times 6$ 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.

# Towards Schur-Weyl duality for the Clifford group

2. Generalize:

$$R_O = r_O^{\otimes n}, \quad r_O = \sum_{\boldsymbol{x}} |O\boldsymbol{x}\rangle \langle \boldsymbol{x}|$$

Allow all orthogonal and stochastic $t \times t$-matrices $O$ with entries in $\mathbb{F}_d$.

For qubits, an example is the $6 \times 6$ 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.

# Towards Schur-Weyl duality for the Clifford group

3. Generalize further:

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

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

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

$$T = \operatorname{rowspan}\begin{pmatrix} 1&1&1&1 & 0&0&0&0 \\ 0&0&0&0 & 1&1&1&1 \\ 1&1&0&0 & 1&1&0&0 \\ 1&0&1&0 & 1&0&1&0 \end{pmatrix},$$

$$R_T = 4^{-n}\left(I^{\otimes 4} + X^{\otimes 4} + Y^{\otimes 4} + Z^{\otimes 4}\right)^{\otimes n} = 4^{-n}\sum_P P^{\otimes 4}$$

The projector $R_T$ commutes with $U_C^{\otimes 4}$ for every $n$-qubit Clifford unitary.

# Towards Schur-Weyl duality for the Clifford group

3. Generalize further:

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

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

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

$$T = \text{rowspan}\begin{pmatrix} 1\,1\,1\,1 & 0\,0\,0\,0 \\ 0\,0\,0\,0 & 1\,1\,1\,1 \\ 1\,1\,0\,0 & 1\,1\,0\,0 \\ 1\,0\,1\,0 & 1\,0\,1\,0 \end{pmatrix},$$

$$R_T = 4^{-n}\left(I^{\otimes 4} + X^{\otimes 4} + Y^{\otimes 4} + Z^{\otimes 4}\right)^{\otimes n} = 4^{-n}\sum_P P^{\otimes 4}$$

The projector $R_T$ commutes with $U_C^{\otimes 4}$ for every $n$-qubit Clifford unitary.

# 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. $\boldsymbol{y} \cdot \boldsymbol{y}' = \boldsymbol{x} \cdot \boldsymbol{x}'$ and of maximal dimension $t$. Moreover, require $|\boldsymbol{y}| = |\boldsymbol{x}|$ (for qubits, modulo 4).

**Theorem (Gross-Nezami-W)**

For $n \geq t - 1$, the operators $R_T$ are a basis of the commutant of $\{U_C^{\otimes t}\}$. There are $\prod_{k=0}^{t-2}(d^k + 1)$ such operators.

- Commutant stabilizes for large $n$ (just like for ordinary Schur-Weyl)!
- For $n < t - 1$, still spans. [Nebe-Scheeren]
- Commutant only has *semigroup* structure!

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

*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? $(\mathbb{C}^2)^{\otimes n}$

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

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:

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

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

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

*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? $(\mathbb{C}^2)^{\otimes n}$

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

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

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

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

# 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 applies to *any* $t$-th moment!

*Many applications:* Improved bounds for randomized benchmarking [Helsen et al], low-rank matrix recovery [Kueng et al]; studies of dynamics in random Clifford circuits [Li et al, ...]; random tensor network toy models of holography [Nezami-W, Apel et al, ...]; analysis of thrifty shadow estimation [Helsen-W, Zhou-Liu]; ...

# Property testing and symmetry

Property testing asks us to decide if an unknown state $\rho$ has some property or is far from so. E.g., how can we test if a state is pure?

*Idea:* If $\rho = |\psi\rangle\langle\psi|$ is pure then $R_{(1\ 2)}\rho^{\otimes 2} = \rho^{\otimes 2}$, and only then.

This symmetry can be tested using the well-known swap test:

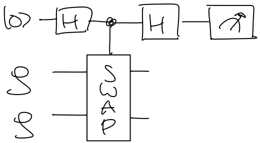
- We accept if we get "0". This happens with probability $\frac{1}{2}(1 + \operatorname{tr}\rho^2)$.
- This test uses only $t = 2$ copies and its power does *not* depend on the dimensionality – those are the best tests...

# Property testing and symmetry

Property testing asks us to decide if an unknown state $\rho$ has some property or is far from so. E.g., how can we test if a state is pure?

*Idea:* If $\rho = |\psi\rangle\langle\psi|$ is pure then $R_{(1\ 2)}\rho^{\otimes 2} = \rho^{\otimes 2}$, and only then.

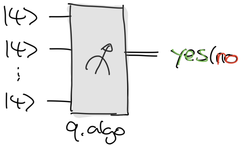
This symmetry can be tested using the well-known swap test:




- We accept if we get "0". This happens with probability $\frac{1}{2}(1 + \operatorname{tr}\rho^2)$.
- This test uses only $t = 2$ copies and its power does *not* depend on the dimensionality – those are the best tests...

# 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 $\varepsilon$-far from it.




*Idea:* Stabilizer tensor powers have an even larger symmetry:

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

E.g., for qubits have the anti-identity $\overline{\mathrm{id}}$. If we measure $R_{\overline{\mathrm{id}}}$ on $t = 6$ copies:

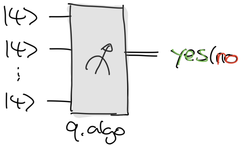
**Result**

Let $\psi$ be a pure state of $n$ qubits. If $\psi$ 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.

# 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 $\varepsilon$-far from it.




*Idea:* Stabilizer tensor powers have an even larger symmetry:

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

E.g., for qubits have the anti-identity $\overline{\mathrm{id}}$. If we measure $R_{\overline{\mathrm{id}}}$ on $t = 6$ copies:

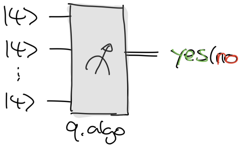
**Result**

Let $\psi$ be a pure state of $n$ qubits. If $\psi$ 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.

# 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 $\varepsilon$-far from it.




*Idea:* Stabilizer tensor powers have an even larger symmetry:

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

E.g., for qubits have the anti-identity $\overline{\mathrm{id}}$. If we measure $R_{\overline{\mathrm{id}}}$ on $t = 6$ copies:

**Result**

Let $\psi$ be a pure state of $n$ qubits. If $\psi$ 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.

# Stabilizer testing using Bell difference sampling

*Why does the preceding test work? How to implement it?*

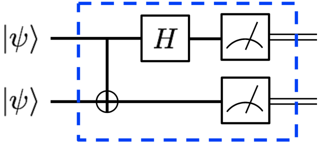
Any state $\psi$ can be expanded in Pauli basis:

$$\psi = \sum_{\boldsymbol{v}} c_{\boldsymbol{v}} P_{\boldsymbol{v}}$$

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

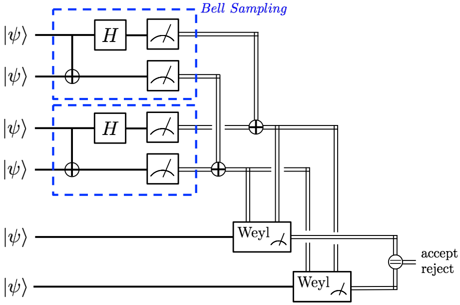
Key idea: Sample & verify!

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



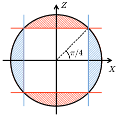
# Stabilizer testing using Bell difference sampling

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 and some symplectic Fourier analysis.



# Further applications to learning and testing

These techniques have found further applications in learning and testing properties of quantum states. Here is a fun one [Grewal-Iyer-Kretschmer-Liang]:

**Theorem**

Any Clifford+T quantum circuit family preparing a pseudorandom ensemble of quantum states must contain $\Omega(n)$ T-gates.

A pseudorandom ensemble is one that is indistinguishable from Haar random states by any polynomial-time algorithm. Their result is proved as follows:

- The initial state $|0\rangle^{\otimes n}$ has a stabilizer group of cardinality $2^n$.
- Each T-gate reduces size of stabilizer subgroup by at most a factor $\frac{1}{4}$.
- Hence, if $< \frac{n}{2}$ T-gates, output state $|\psi\rangle$ has nontrivial stabilizer group.
- Then $p_\psi$ is supported on a proper subspace (dual of isotropic subspace).

In contrast, for Haar random $|\psi\rangle$ it has weight $\leq \frac{2}{3}$ on any proper subspace. Bell sampling allows distinguishing these two cases.

# Further applications to learning and testing

These techniques have found further applications in learning and testing properties of quantum states. Here is a fun one [Grewal-Iyer-Kretschmer-Liang]:

**Theorem**

Any Clifford+T quantum circuit family preparing a pseudorandom ensemble of quantum states must contain $\Omega(n)$ T-gates.

A pseudorandom ensemble is one that is indistinguishable from Haar random states by any polynomial-time algorithm. Their result is proved as follows:

- The initial state $|0\rangle^{\otimes n}$ has a stabilizer group of cardinality $2^n$.
- Each T-gate reduces size of stabilizer subgroup by at most a factor $\frac{1}{4}$.
- Hence, if $< \frac{n}{2}$ T-gates, output state $|\psi\rangle$ has nontrivial stabilizer group.
- Then $p_\psi$ is supported on a proper subspace (dual of isotropic subspace).

In contrast, for Haar random $|\psi\rangle$ it has weight $\leq \frac{2}{3}$ on any proper subspace. Bell sampling allows distinguishing these two cases.

# Further applications to learning and testing

These techniques have found further applications in learning and testing properties of quantum states. Here is a fun one [Grewal-Iyer-Kretschmer-Liang]:

**Theorem**

Any Clifford+T quantum circuit family preparing a pseudorandom ensemble of quantum states must contain $\Omega(n)$ T-gates.

A pseudorandom ensemble is one that is indistinguishable from Haar random states by any polynomial-time algorithm. Their result is proved as follows:

- The initial state $|0\rangle^{\otimes n}$ has a stabilizer group of cardinality $2^n$.
- Each T-gate reduces size of stabilizer subgroup by at most a factor $\frac{1}{4}$.
- Hence, if $< \frac{n}{2}$ T-gates, output state $|\psi\rangle$ has nontrivial stabilizer group.
- Then $p_\psi$ is supported on a proper subspace (dual of isotropic subspace).

In contrast, for Haar random $|\psi\rangle$ it has weight $\leq \frac{2}{3}$ on any proper subspace. Bell sampling allows distinguishing these two cases.

# 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 $s \ll t$.

As mentioned, 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 and by stabilizer tensor powers.
- 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 $s \ll t$.

As mentioned, 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 and by stabilizer tensor powers.
- Similar to Gaussian de Finetti [Leverrier et al]. Applications to QKD?

*Can reduce symmetry requirements at expense of goodness.*

# Why does it work? Asymptotic orthogonality

The ordinary de Finetti theorem can be seen using the following facts:

- If $|\Psi\rangle$ is permutation symmetric, it is supported on $\mathrm{span}\{|\psi\rangle^{\otimes t}\}$.
- Tensor powers of distinct states become "asymptotically orthogonal".

Our stabilizer de Finetti theorem is proved similarly:

- If $|\Psi\rangle$ has ortho-stochastic symmetry, it is supported on $\mathrm{span}\{|S\rangle^{\otimes t}\}$.
- For any two distinct *stabilizer* states, it holds that $|\langle S|S'\rangle|^2 \leq \frac{1}{d}$.

*Here we used asymptotic orthogonality for large $t$. How about large $D/n$?*

# Why does it work? Asymptotic orthogonality

The ordinary de Finetti theorem can be seen using the following facts:

- If $|\Psi\rangle$ is permutation symmetric, it is supported on $\mathrm{span}\{|\psi\rangle^{\otimes t}\}$.
- Tensor powers of distinct states become "asymptotically orthogonal".

Our stabilizer de Finetti theorem is proved similarly:

- If $|\Psi\rangle$ has ortho-stochastic symmetry, it is supported on $\mathrm{span}\{|S\rangle^{\otimes t}\}$.
- For any two distinct *stabilizer* states, it holds that $|\langle S|S'\rangle|^2 \leq \frac{1}{d}$.

*Here we used asymptotic orthogonality for large $t$. How about large $D/n$?*

# Towards a Weingarten calculus for the Clifford group?

Any *t-th moment* of compact $G \subseteq U(D)$ is captured by the superoperator

$$\mathcal{M}_{G,t}(\rho) := \int_G U^{\otimes t} \rho U^{\otimes t,\dagger}.$$

This is the orthogonal projection onto the commutant.

- For the *unitary group*, commutant is spanned by $R_\pi$ for $\pi \in S_t$, and

$$\operatorname{tr} R_\pi^\dagger R_\sigma = D^{\#\text{cycles}(\pi^{-1}\sigma)} = D^{t-\delta_{\text{Cayley}}(\pi,\sigma)}.$$

- For the *Clifford group*, it is spanned by $R_T$ for certain $T \subseteq \mathbb{F}_d^{2t}$, and

$$\operatorname{tr} R_T^\dagger R_{T'} = D^{\dim(T \cap T')}.$$

The off-diagonal entries are $1/D$ suppressed also in the latter. This allows evaluating $t$-th moments in leading order [Haferkamp et al, Helsen-W, ...].

For the unitary group, Weingarten calculus inverts the Gram matrix exactly, using representation theory [Collins]. How about the Clifford group?

# Towards a Weingarten calculus for the Clifford group?

Any *t-th moment* of compact $G \subseteq U(D)$ is captured by the superoperator

$$\mathcal{M}_{G,t}(\rho) := \int_G U^{\otimes t} \rho U^{\otimes t,\dagger}.$$

This is the orthogonal projection onto the commutant.

- For the *unitary group*, commutant is spanned by $R_\pi$ for $\pi \in S_t$, and

$$\operatorname{tr} R_\pi^\dagger R_\sigma = D^{\#\text{cycles}(\pi^{-1}\sigma)} = D^{t-\delta_{\text{Cayley}}(\pi,\sigma)}.$$

- For the *Clifford group*, it is spanned by $R_T$ for certain $T \subseteq \mathbb{F}_d^{2t}$, and

$$\operatorname{tr} R_T^\dagger R_{T'} = D^{\dim(T \cap T')}.$$

The off-diagonal entries are $1/D$ suppressed also in the latter. This allows evaluating $t$-th moments in leading order [Haferkamp et al, Helsen-W, ...].

For the unitary group, Weingarten calculus inverts the Gram matrix exactly, using representation theory [Collins]. How about the Clifford group?

# Towards a Weingarten calculus for the Clifford group?

Any $t$-th moment of compact $G \subseteq U(D)$ is captured by the superoperator

$$\mathcal{M}_{G,t}(\rho) := \int_G U^{\otimes t} \rho U^{\otimes t,\dagger}.$$

This is the orthogonal projection onto the commutant.

- For the *unitary group*, commutant is spanned by $R_\pi$ for $\pi \in S_t$, and

$$\operatorname{tr} R_\pi^\dagger R_\sigma = D^{\#\text{cycles}(\pi^{-1}\sigma)} = D^{t-\delta_{\text{Cayley}}(\pi,\sigma)}.$$

- For the *Clifford group*, it is spanned by $R_T$ for certain $T \subseteq \mathbb{F}_d^{2t}$, and

$$\operatorname{tr} R_T^\dagger R_{T'} = D^{\dim(T\cap T')}.$$

The off-diagonal entries are $1/D$ suppressed also in the latter. This allows evaluating $t$-th moments in leading order [Haferkamp et al, Helsen-W, …].

For the unitary group, Weingarten calculus inverts the Gram matrix exactly, using representation theory [Collins]. How about the Clifford group?

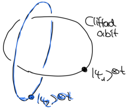
# Application 4: $t$-designs from Cliffords

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]. We find:

**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 $n$!




Relatedly, Haferkamp et al proved the following beautiful result:

**Theorem**

One obtains an $\varepsilon$-approximate unitary design by alternating $\tilde{O}(t^4)$ T-gates with random Clifford unitaries.

Proof uses techniques from the previous slide to control spectral gaps. A recent breakthrough achieves linear depth $O(t)$ using different techniques.

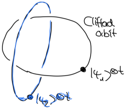
# Application 4: $t$-designs from Cliffords

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]. We find:

**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 $n$!



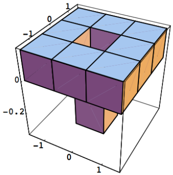

Relatedly, Haferkamp et al proved the following beautiful result:

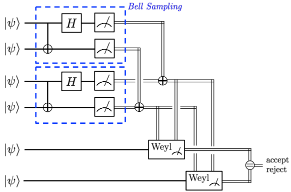
**Theorem**

One obtains an $\varepsilon$-approximate unitary design by alternating $\tilde{O}(t^4)$ T-gates with random Clifford unitaries.

Proof uses techniques from the previous slide to control spectral gaps. A recent breakthrough achieves linear depth $O(t)$ using different techniques.

# Summary and outlook




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

- best understood via finite geometries in $\mathbb{F}_d^{2n}$

Schur-Weyl duality for the Clifford group:

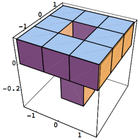
- clean algebraic description in terms of self-dual codes
- new tools for widely used objects and associated random ensembles
- already found some exciting applications, let's find more

*Thank you for your attention!*

# Application 5: Robust Hudson theorem

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

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



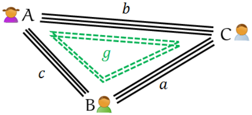
- Quasi-probability distribution on phase space $\mathbb{F}_d^{2n}$
- Discrete Hudson theorem: For pure states, $W_\psi \geq 0$ iff $\psi$ stabilizer
- Wigner negativity $\operatorname{sn}(\psi) = \sum_{\boldsymbol{v}: W_\rho(\boldsymbol{v})<0} |W_\rho(\boldsymbol{v})|$: monotone in resource theory of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

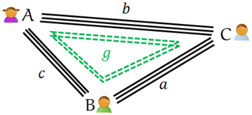
**Result (Nezami-W)**

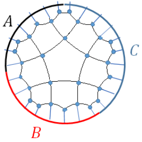
In random stabilizer tensor network states: $g = O(1)$ *w.h.p.*

- 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?*

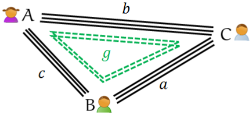
**Result (Nezami-W)**

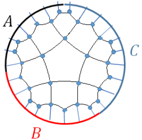
In random stabilizer tensor network states: $g = O(1)$ *w.h.p.*

- 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:



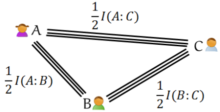




*How about typical stabilizer states? Or even tensor networks?*

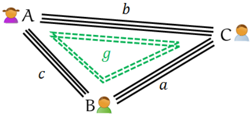
**Result (Nezami-W)**

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

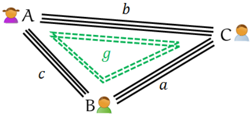
$$\operatorname{tr}(\rho_{AB}^{T_B})^3 = \operatorname{tr} |S\rangle\langle S|_{ABC}^{\otimes 3} \left( R_{\zeta,A} \otimes R_{\zeta^{-1},B} \otimes R_{\mathrm{id},C} \right)$$

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

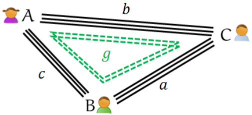
$$\operatorname{tr}(\rho_{AB}^{T_B})^3 = \operatorname{tr} |S\rangle\langle S|_{ABC}^{\otimes 3} \left( R_{\zeta,A} \otimes R_{\zeta^{-1},B} \otimes R_{\mathrm{id},C} \right)$$

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!*