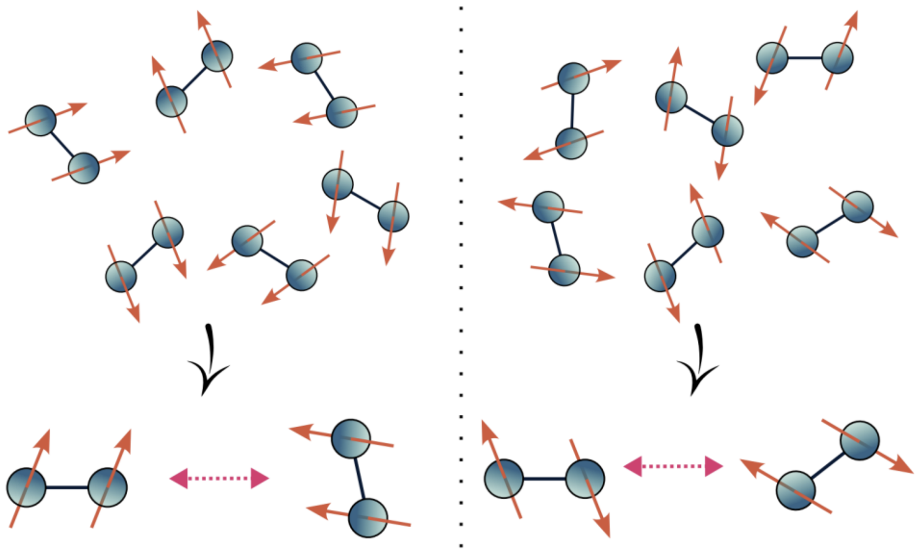
Exact finite unitary designs under symmetry

Christopher Vairogs and Felix Leditzky

Beyond IID
CUHK-Shenzhen, China
June 26, 2026

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN



Central question

- Randomness in QIS:
  - **Learning protocols**: tomography of channels, states, shadows
  - **Theoretical tool**: black-hole information paradox, thermalization

- Symmetry in QIS:
  - **Parameter reduction:** permutation symmetric states, covariant channels
  - **Physics:** SPT phases

- **What is the relationship between randomness and symmetry?**

Mitsuhashi and Yoshioka, PRX Quantum, ‘23
Arvind et al, Phys. Rev. Research 7, ‘25
Liu et al, arXiv:2408.14463, ‘24
Mitsuhashi et al, PRL 134, ‘25

Uniform randomness

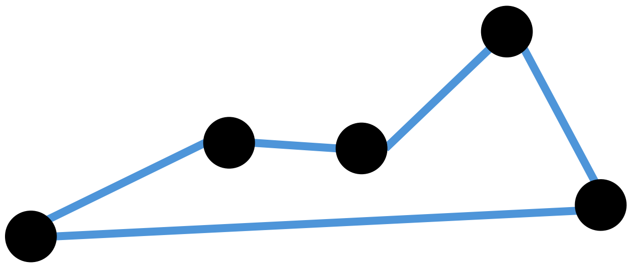
- Given Hilbert space $\mathcal{H}$ and compact group $K \le U(\mathcal{H})$, the group K has a unique normalized **unitarily-invariant** (Haar) measure μ_K.
- More practical to sample distributions that simply **mimic** Haar measure.
- Given finite set of unitaries $\mathcal{X} \subset K$ and distribution $p: \mathcal{X} \to [0,1]$ we say the ensemble $(\mathcal{X}, p)$ is **t-design in K** if

$$\sum_{g \in \mathcal{X}} p(g) g^{\otimes t} \otimes (g^\dagger)^{\otimes t} = \int_K d\mu_K(k) k^{\otimes t} \otimes (k^\dagger)^{\otimes t}.$$

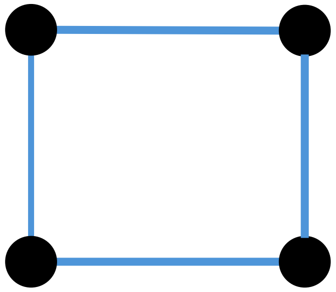
- $(\mathcal{X}, p)$ is t-design in $K \Longrightarrow (\mathcal{X}, p)$ is t'-design in K for $t' \le t$.
- Interested in **designs** for which moment equality holds **exactly** in this talk!

Symmetry in physics

- "When you do something to something and it stays the same."
- Operations preserving object of interest can form **symmetry group:**



no non-trivial symmetries
= **trivial** symmetry group



90° **rotations** + **reflections**
= **dihedral** group D_8

- Prominent feature of many quantum-mechanical problems:

Heisenberg *XXX* model:	$G = \{u^{\otimes N} : u \in \mathrm{SU}(2)\} \cong \mathrm{SU}(2)$	$H = \sum (X_j X_k + Y_j Y_k + Z_j Z_k)$	$g \in G \implies gHg^{-1} = H$
Multi-copy input state:	$G = \{P_d(\pi) : \pi \in S_N\} \cong S_N$	$\rho^{\otimes N}, \quad \rho \in (\mathbb{C}^{d\times d})^{\otimes N}$	$g \in G \implies g\rho^{\otimes N} g^{-1} = \rho^{\otimes N}$

Symmetries restrict realizable unitaries

- We want designs that mimic Haar measure over **realizable unitaries** under **symmetry constraints** instead of full unitary group (*symmetric* designs).

Symmetry group	$S \leq U(\mathcal{H})$
Set of unitaries	$\mathcal{X} \subset U(\mathcal{H})$
Symmetry-respecting subset	$\mathcal{X}_S \equiv \{g \in \mathcal{X} : sgs^\dagger = g, \forall s \in S\}$
Symmetry-respecting unitary group	$U(\mathcal{H})_S = \{u \in U(\mathcal{H}) : sus^\dagger = u, \forall s \in S\}$
Probability distribution	$p : \mathcal{X} \to [0,1]$
Symmetry-respecting distribution	$p_S : \mathcal{X}_S \to [0,1]$ $p_S(g) \equiv \frac{p(g)}{\sum_{g' \in \mathcal{X}_S} p(g)}$

$p_S(g)$ = probability of sampling g from $(\mathcal{X}, p)$ **conditioned** on g being **symmetric**

Maximum degree of designs

- Can consider **maximum degree** of t-design with and without symmetry:

$$t_{\max}(\mathcal{X}, p) \equiv \max\{t \geq 0 : (\mathcal{X}, p) \text{ is } t\text{-design in } U(\mathcal{H})\}$$

$$t_{\max}^{(S)}(\mathcal{X}, p) \equiv \max\{t \geq 0 : (\mathcal{X}_S, p_S) \text{ is } t\text{-design in } U(\mathcal{H})_S\}$$

- Consider the multi-qubit **Pauli** and **Clifford** groups

$$\mathcal{P}_N \equiv \{\pm 1, \pm i\}\{I, X, Y, Z\}^{\otimes N} \qquad \mathcal{C}_N \equiv \left\{u \in U((\mathbb{C}^2)^{\otimes N}) : u\mathcal{P}_N u^\dagger \subset \mathcal{P}_N\right\}$$

$$t_{\max}(\mathcal{P}_N, p^{\mathrm{unif}}) = 1 \qquad t_{\max}(\mathcal{C}_N, p^{\mathrm{unif}}) = 3$$

- For any finite-dimensional $\mathcal{H}$ and any $t \geq 0$, there exists a t-design in $U(\mathcal{H})$.
- However, if G is a **finite subgroup** of $U(\mathcal{H})$, then

$$\dim \mathcal{H} > 2 \implies t_{\max}(G, p^{\mathrm{unif}}) \leq 3.$$

- Group structure **throttles randomness** in t-design framework.

Bannai et al, J. Math. Soc. Japan 72, ‘18 Kaposi et al, Quantum 10, ‘26

Clifford group under symmetry

- How does a **symmetry** that restricts realizable **Clifford** gates affects the Clifford group's **maximum degree** as t-design?

$$t_{\max}^{(S)}((\mathcal{C}_N)_S, p_S^{\mathrm{unif}}) > 3 = t_{\max}(\mathcal{C}_N, p^{\mathrm{unif}})$$

$$\Longrightarrow \; U(\mathcal{H})_S = \left\{e^{i\theta} I : \theta \in \mathbb{R}\right\}$$

for any distribution p and any symmetry group S

$$t_{\max}^{(S)}((\mathcal{C}_N)_S, p_S^{\mathrm{unif}}) = 1 < t_{\max}(\mathcal{C}_N, p^{\mathrm{unif}})$$

for symmetry groups

$$S = \left\{(e^{i\theta Z})^{\otimes N} : \theta \in \mathbb{R}\right\} \cong U(1)$$

$$S = \left\{u^{\otimes N} : u \in \mathrm{SU}(2)\right\} \cong SU(2)$$

Mitsuhashi and Yoshioka, PRX Quantum, '23

$\Longrightarrow$ Symmetry **cannot increase** randomness of Clifford group in design sense

$\Longrightarrow$ Common **physical** symmetries **decrease** randomness of Clifford group

Our problems

- Do so by **generalizing** the Mitsuhashi and Yoshioka result beyond Clifford group.
- Can there exist a **symmetry group** S and **a $\boldsymbol{t}$-design** $(\mathcal{X}, p)$ in $U(\mathcal{H})$ such that

$$t_{\max}^{(S)}(\mathcal{X}_S, p_S) > t_{\max}(\mathcal{X}, p)?$$

- If so, then simply implementing $(\mathcal{X}, p)$ under symmetry constraints could allow us to produce **more powerful designs.**
- Also, can symmetry allow us to **break $\boldsymbol{t} = 4$ barrier** for group designs?

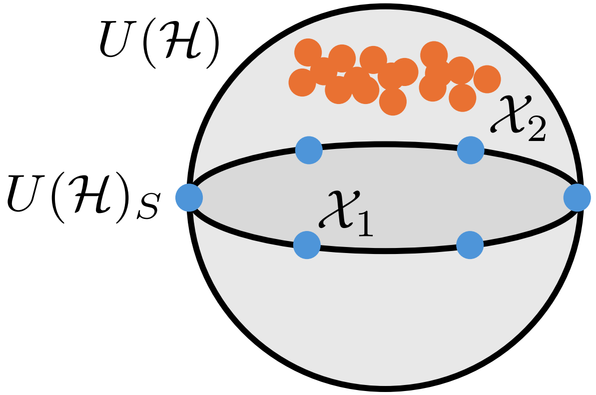
$$G \leq U(\mathcal{H}) \text{ and } t_{\max}^{(S)}(G_S, p_S) \geq 4?$$

Basic intuition

- **Naive intuition**: symmetry **orders things**, so symmetry generically decreases t?

$$t_{\max}^{(S)}(\mathcal{X}_S, p_S) \overset{?}{\leq} t_{\max}(\mathcal{X}, p)$$

- Indeed, this was the case for **Clifford group**.
- **Less naive intuition**: start with uniformly weighted t'-design in $U(\mathcal{H})_S$ and pad with many **asymmetric** operators **highly concentrated** in one region:



$$\mathcal{X} = \mathcal{X}_1 \sqcup \mathcal{X}_2 \qquad \mathcal{X}_S = \mathcal{X}_1$$

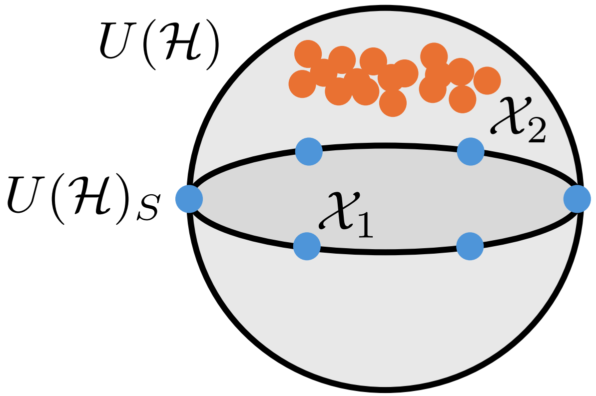
$$p^{\mathrm{unif},\mathcal{X}}(u) = \frac{1}{|\mathcal{X}_1| + |\mathcal{X}_2|} \qquad p_S^{\mathrm{unif},\mathcal{X}} = p^{\mathrm{unif},\mathcal{X}_1}$$

- If asymmetric operators **concentrated enough**, this suggests that

$$t_{\max}(\mathcal{X}, p) < t' \leq t_{\max}^{(S)}(\mathcal{X}_S, p_S).$$

The real difficulty in boosting design degree

- That $\mathcal{X}_1 \sqcup \mathcal{X}_2$ has any ***t*-design structure** for $\boldsymbol{t > 0}$ seems questionable.
- Similarly doubtful that $\mathcal{X}_1 \sqcup \mathcal{X}_2$ has **group structure**.
- $\mathcal{X}_1 \sqcup \mathcal{X}_2$ **simultaneously group** and ***t*-design** for $t > 0$ highly dubious.



$\Longrightarrow$ Design degree likely **can increase** under symmetry in simple way

$\Longrightarrow$ Unclear whether such ensembles are anything with **familiar structure**

A refinement of the problems

1. Does there exist a **finite group** $G \leq U(\mathcal{H})$ + symmetry $S \leq U(\mathcal{H})$ such that

$$t_{\max}^{(S)}(G_S, p_S^{\mathrm{unif}}) \geq 4?$$

2. Does there exist a **finite group design** $G \leq U(\mathcal{H})$ and $S \leq U(\mathcal{H})$ such that

$$0 < t_{\max}(G, p^{\mathrm{unif}}) < t_{\max}^{(S)}(G_S, p_S^{\mathrm{unif}})?$$

3. Does there exist a **finite design** $(\mathcal{X}, p)$ in $U(\mathcal{H})$ and $S \leq U(\mathcal{H})$ such that

$$0 < t_{\max}(\mathcal{X}, p) < t_{\max}^{(S)}(\mathcal{X}, p_S)?$$

Decomposing representations

- So how to establish whether **structured** t-designs boosted under symmetry?
- Use representation-theoretic description of symmetry group S:

$\mathcal{H}$ decomposes into **irreducible representations** V_λ of S
Isomorphic copies of **irrep $\boldsymbol{V_\lambda}$** occur **multiplicity** $m_\lambda = \dim W_\lambda$

$$\mathcal{H} \cong \bigoplus_{\lambda \in [n]} V_\lambda \otimes W_\lambda$$

Ex: $\dim V_1 = \dim V_3 = 1$ and $\dim V_2 = 2$

$$s \cong \bigoplus_{\lambda \in [n]} \rho_\lambda(s) \otimes I_{W_\lambda} \qquad s \in S$$

$$u \in U(\mathcal{H})_S \implies u \cong \begin{pmatrix} \sigma_1(u) & & & \\ & \sigma_2(u) & & \\ & & \sigma_2(u) & \\ & & & \sigma_3(u) \end{pmatrix}$$

- **Schur's lemma:** $[X, s] = 0 \text{ for all } s \in S \implies X \cong \bigoplus_{\lambda \in [n]} I_{V_\lambda} \otimes \sigma_\lambda(X)$

Structure of designs in $U(\mathcal{H})_S$

- What do the **diagonal blocks** of t-designs in $U(\mathcal{H})_S$ look like?
- Can check that σ_λ maps **unitaries** to **unitaries**, so

$$U(\mathcal{H})_S \ni u \cong \bigoplus_{\lambda \in [n]} I_{V_\lambda} \otimes \sigma_\lambda(u) \qquad\qquad \mathcal{X}_\lambda \equiv \sigma_\lambda(\mathcal{X}) \subset U(W_\lambda)$$

$$\frac{1}{|\mathcal{X}|} \sum_{u \in \mathcal{X}} u^{\otimes t} \otimes (u^\dagger)^{\otimes t} = \int_{U(\mathcal{H})_S} du \ u^{\otimes t} \otimes (u^\dagger)^{\otimes t}$$

$$\Downarrow$$

$$\frac{1}{|\mathcal{X}_\lambda|} \sum_{u \in \mathcal{X}_\lambda} u^{\otimes t} \otimes (u^\dagger)^{\otimes t} = \int_{U(W_\lambda)} du \ u^{\otimes t} \otimes (u^\dagger)^{\otimes t}$$

- **Fact:** $(\mathcal{X}, p^{\mathrm{unif}})$ is t-design in $U(\mathcal{H})_S \implies (\mathcal{X}_\lambda, p^{\mathrm{unif}})$ is t-design in $U(W_\lambda)$

Construction for symmetric designs

- So diagonal blocks of a design in $U(\mathcal{H})_S$ must form designs in $U(W_\lambda)$ for all λ.
- Is converse true?
- **Not quite**, but can **build designs** in $U(\mathcal{H})_S$ out of **group designs in** $U(W_\lambda)$:

$$\mathcal{H} \cong \bigoplus_{\lambda \in [n]} V_\lambda \otimes W_\lambda$$

$$s \cong \bigoplus_{\lambda \in [n]} \rho_\lambda(s) \otimes I_{W_\lambda}, \quad s \in S$$

$$\mathcal{X} \equiv \left\{ \bigoplus_{\lambda \in [n]} \exp\left(\frac{2\pi i}{t+1} j_\lambda\right) I_{V_\lambda} \otimes g_\lambda : g_\lambda \in G_\lambda, 0 \leq j_\lambda \leq t \right\}$$

- **Fact:** Suppose $G_\lambda \subset U(W_\lambda)$ are uniformly weighted **group t-designs in** $U(W_\lambda)$ and $\mathcal{X} \subset U(\mathcal{H})$ defined above. Then $\mathcal{X}$ **is uniformly weighted group t-design** in $U(\mathcal{H})_S$.

First problem

Does there exist a finite group $G \leq U(\mathcal{H})$ and symmetry $S \leq U(\mathcal{H})$ such that

$$t_{\max}^{(S)}(G_S, p_S^{\mathrm{unif}}) \geq 4?$$

Group designs under $U(1), SU(2)$ symmetry

- **Theorem**: Let $N > 3$ and assume $\mathcal{H} = (\mathbb{C}^d)^{\otimes N}$. Assume $G \leq U(\mathcal{H})$ is a finite group and let

$$S_1 = \{(e^{i\theta Z})^{\otimes N} : \theta \in \mathbb{R}\} \cong \mathrm{U}(1)$$
$$S_2 = \{u^{\otimes N} : u \in \mathrm{SU}(d)\} \cong \mathrm{SU}(d).$$

$$\implies \qquad t_{\max}^{(S_i)}(G_{S_i}, p_{S_i}^{\mathrm{unif}}) \leq 2$$

(Compare with Mitsuhashi-Yoshioka result for Clifford group)

$$d = 2: \qquad t_{\max}^{(S_i)}((\mathcal{C}_N)_{S_i}, p_{S_i}^{\mathrm{unif}}) = 1$$

- Group design $t = 4$ barrier **remains unbroken** for these symmetries.

Mitsuhashi and Yoshioka, PRX Quantum, '23

Group designs under $U(1), SU(d)$ symmetry

Proof sketch

- The images $\sigma_\lambda(G)$ **must be groups** because G is a group.
- The images $\sigma_\lambda(G)$ **must be 3-designs** in $U(W_\lambda)$ if G is a 3-design in $U(\mathcal{H})_S$.
- **Classification of finite group designs** allows only certain values of $\dim W_\lambda$.
- The **multiplicities** $\dim W_\lambda$ for S_i are given by simple **combinatorial formulas**:

$$S_1 \cong \mathrm{U}(1) \qquad \mathcal{H} \cong \bigoplus_{h=0}^{N} V_h \otimes W_h \qquad \dim W_h = \binom{N}{h}$$

$$S_2 \cong \mathrm{SU}(d) \qquad \mathcal{H} \cong \bigoplus_{\lambda \vdash_d N} V_\lambda \otimes W_\lambda \qquad \dim W_\lambda = \frac{N!}{\prod_{(i,j)} h(i,j)}$$

- Dimensions from the classification step **aren't equal** to formulas for $N > 3$.
- $\Longrightarrow G_{S_i}$ **can't be uniformly weighted 3-design** in $U(\mathcal{H})_S$ for $N > 3$.

$$t_{\max}^{(S_i)}(G_{S_i}, p_{S_i}^{\mathrm{unif}}) \leq 2$$

Bannai et al, J. Math. Soc. Japan 72, '18

Group designs under finite group symmetry

- Can extend to arbitrary finite symmetry groups using similar arguments.

- **Theorem**: Assume $G \leq U(\mathcal{H})$ is finite as before. Then

$$|S| \leq \frac{\dim \mathcal{H}}{2} \implies t_{\max}(G_S, p_S^{\mathrm{unif}}) \leq 3.$$

- **Theorem**: Let $S_0 \leq U(\mathbb{C}^d)$ be finite. Define

$$S = \left\{ s^{\otimes N} : s \in S_0 \right\}.$$

Then for all N sufficiently large, any finite group $G \leq U(\mathbb{C}^{dn})$ satisfies

$$t_{\max}(G_S, p^{\mathrm{unif}}) \leq 3.$$

Structure theorem for ≥4-designs

- **Theorem**: If S be arbitrary **closed symmetry group**. Recall that $\mathcal{H}$ decomposes

$$\mathcal{H} \cong \bigoplus_{\lambda\in[n]} V_\lambda \otimes W_\lambda$$

$$s \cong \bigoplus_{\lambda\in[n]} \rho_\lambda(s) \otimes I_{W_\lambda}, \;\; s \in S$$

and $G_S \leq U(\mathcal{H})_S$ is finite t-design in $U(\mathcal{H})_S$ for $\boldsymbol{t} \geq \mathbf{6}$, then H is **abelian**.

Furthermore, if $G_S \leq U(\mathcal{H})_S$ is finite t-design in $U(\mathcal{H})_S$ for $\boldsymbol{t} \geq \mathbf{4}$, then

$$H = Z(H)R$$

$$R \cong \mathrm{SL}(2,5)^{\times k}, \qquad 0 \leq k \leq n$$

$$\mathrm{SL}(2,5) \equiv \left\{M \in \mathbb{F}_5^{2\times 2} : \det(M) = 1\right\}.$$

Structure theorem for ≥4-designs

Proof sketch:

$$\mathcal{H} \cong \bigoplus_{\lambda\in[n]} V_\lambda \otimes W_\lambda$$

$$s \cong \bigoplus_{\lambda\in[n]} \rho_\lambda(s) \otimes I_{W_\lambda}, \;\; s \in S$$

- The images $\sigma_\lambda(G_S)$ are group designs on W_λ. Then use **CFGD**:
- $\dim W_\lambda = 1$: $\sigma_\lambda(G_S)$ is group of scalars $\langle \omega I_{W_\lambda} \rangle$.
- $\dim W_\lambda = 2$: $\sigma_\lambda(G_S)$ is set product of $\langle \omega_\lambda I_{W_\lambda} \rangle$ & isomorphic copy of $SL(2,5)$.
- **Note:** Does not automatically imply that G_S is ≅ to direct product of groups of the form $\langle \omega I_{W_\lambda} \rangle$ and $\langle \omega_\lambda I_{W_\lambda} \rangle SL(2,5)$. Matrices over W_λ might be correlated!
- Technical group-theoretic arguments used to conclude that this is the case.

Bannai et al, J. Math. Soc. Japan 72, '18

Second problem

Does there exist a finite group design $G \leq U(\mathcal{H})$ and symmetry $S \leq U(\mathcal{H})$ such that

$$0 < t_{\max}(G, p^{\mathrm{unif}}) < t_{\max}^{(S)}(G_S, p_S^{\mathrm{unif}})?$$

Group 1-designs under symmetry

- **Theorem**: Let $t > 1$. For all $C > 0$, there exists a
  - Hilbert space of dimension $\dim \mathcal{H} > C$,
  - a finite group $G \leq U(\mathcal{H})$,
  - a symmetry group $S \leq U(\mathcal{H})$

such that

$$U(\mathcal{H})_S \neq \{e^{i\theta} I : \theta \in \mathbb{R}\}$$

and

$$1 = t_{\max}(G, p^{\mathrm{unif}}) < t \leq t_{\max}(G_S, p^{\mathrm{unif}}).$$

Third problem and ongoing work

Does there exist a finite design $(\mathcal{X}, p)$ in $U(\mathcal{H})$ such that

$$0 < t_{\max}(\mathcal{X}, p) < t_{\max}(\mathcal{X}, p_S)?$$

Third problem and ongoing work

- **Claim:** Let $\dim \mathcal{H}$ be arbitrary and let $1 \leq t < t'$. Let $S \leq U(\mathcal{H})$ be **closed** symmetry group. Then there exists a set $\mathcal{X} \subset U(\mathcal{H})$ and distribution $p\colon \mathcal{X} \to [0,1]$ such that

$$t = t_{\max}(\mathcal{X}, p) < t' \leq t_{\max}(\mathcal{X}_S, p_S)$$

assuming the formula for unitarily-invariant measure over complex Grassmannian holds:

For any integrable function $f : G_{m,d} \to \mathbb{C}$ depending solely on the principal angles relative to the fixed subspace W, we then have

$$\int_{G_{m,d}} dp\ f(p) = \int_0^{\pi/2} d\theta_1 \cdots \int_0^{\theta_{m-1}} d\theta_m\ f(\theta_1, \ldots, \theta_m) \prod_{i=1}^{m} (\sin\theta_i)^{2(n-2m)} \prod_{1 \leq i < j \leq d} (\sin^2\theta_i - \sin^2\theta_j)^2. \tag{200}$$

Bannai et al, Adv. Math. 405, '22

- Formula appears to hold in complex case and apparently known as folklore.
- Similar orthogonally-invariant volume form derived for real Grassmannians explicitly.

James, Ann. Math. Stat. 25, '54

Summary and future work

- Studied interplay between **randomness** and **symmetry** in design context.
- Posed problem of how **symmetry influences max degree** of an exact t-design.
- Treated problem for three different **structures** imposed on the design:
  - group structure
  - group t-design with t strictly positive
  - t-design with t strictly positive (*ongoing*)
- **Extended** some results of **Mitsuhashi-Yoshioka** using algebraic methods.
- Did so **without** relying on long **Pauli matrix calculations**.
- Would be interesting to pursue problem for designs generated by **local gates**.
- Could consider other notions of randomness, such as **approximate unitary designs**.

Li et al, PRX Quantum 5, '24

Hearth et al, PRX, '24

Liu et al, arXiv:2408.14463, '24

Mitsuhashi et al, PRL 134, '25

Thanks for listening!

- Email: vairogs2@illinois.edu