Constructing Generalized Unitary Group Designs

Ágoston Kaposi[1,2][0009-0007-7604-1449], Zoltán Kolarovszki[1,2][0009-0001-9837-5534], Adrian Solymos[2,3][0009-0008-5734-4871], Tamás Kozsik[1][0000-0003-4484-9172], and Zoltán Zimborás[1,2,4][0000-0002-2184-526X]

[1] Faculty of Informatics, Eötvös Loránd University, Budapest, Hungary
[2] Quantum Computing and Quantum Information Research Group, Department of Computer Sciences, Wigner Research Centre for Physics, Budapest, Hungary
[3] Institute of Physics, Eötvös Loránd University, Budapest, Hungary
[4] Algorithmiq Ltd, Helsinki, Finland

Abstract. Unitary designs are essential tools in several quantum information protocols. Similarly to other design concepts, unitary designs are mainly used to facilitate averaging over a relevant space, in this case, the unitary group $U(d)$. The most appealing case is when the elements of the design form a group, which in turn is called a unitary group design. However, the application of group designs as a tool is limited by the fact that there is no trivial construction method to get even a group 2-design for arbitrary dimensions. In this paper, we present novel construction methods, based on the representation theory of the unitary group and its subgroups, that allow the building of higher-order unitary designs from group designs.

Keywords: Quantum information theory · Unitary t-designs · Representation theory

1 Introduction

Ever since their introduction, *unitary t-designs* have played a ubiquitous role in quantum information science. These finite sets of d-degree unitary operators have the property that averaging an operator over the t-fold tensor products of them equals the same type of averaging over the *entire* unitary group $U(d)$ with respect to the Haar measure. Unitary designs were proved to be useful in particular for the construction of unitary codes [13], the realization of quantum information protocols [6], the derandomization of probabilistic constructions [9], the study of SIC-POVMs [5], the detection of entanglement [2], process tomography [14], randomized benchmarking [17] and for shadow estimation [1,11].

E-mails: kaposiagoston@inf.elte.hu, kolarovszki.zoltan@wigner.hu, solymos.adrian@wigner.hu, kto@elte.hu, zimboras.zoltan@wigner.hu

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

The most well-known example of a unitary t-design is that of the multi-partite Clifford group which forms a unitary 3-design for qubit systems and a unitary 2-design for qudit systems when the local dimension d is an odd prime [19,18,12]. It is a well-established fact, that t-designs for $U(d)$ always exist for any t and d [15], but the actual construction of these designs is usually a mathematically challenging task. Evidently, this limits their use in concrete applications.

One of the most elegant ways of constructing them goes through representation theory. From unitary irreducible representations of finite groups, one can get a unitary 1-design, and with additional extra properties, the represented group elements can form a unitary 2-design or even a unitary 3-design. However, it has been shown that a representation of a finite group cannot be a unitary t-design for arbitrary $t \geq 4$ and $d > 2$ [10,3]. Moreover, there is no generic construction to find these so-called group 2- and 3-designs for an arbitrary dimension d.

In this paper, a generalization of the aforementioned group design construction is presented which provides methods to construct unitary 2- and possibly higher designs. Concrete examples are also provided in most cases.

The structure of the paper is as follows: Section 2 contains some basic definitions and statements regarding t-designs; in Section 3 a construction of t-designs from finite unitary subgroups is provided for $t = 2$ and 3 and some examples for the construction is presented; Section 4 presents a different construction with which a unitary design can be created from an orthogonal or unitary symplectic design and some examples.

2 Background and Notation

Several different definitions for unitary designs and group designs can be found in the literature [15,4,7]. The following section introduces the ones used in this paper. Most importantly, this paper only considers exact designs.

Definition 1 (t-design of a group). *Let $\mathcal{G} \subseteq U(d)$ be a compact matrix Lie group. A finite set $\mathcal{V} \subseteq \mathcal{G}$ with weight function $w : \mathcal{V} \to [0,1]$ is called a weighted t-design of the group $\mathcal{G}$ if the following equation holds for any linear transformation M on $(\mathbb{C}^d)^{\otimes t}$:*

$$\sum_{V \in \mathcal{V}} w(V)\, V^{\otimes t} M \left(V^{\otimes t}\right)^{\dagger} = \int_{g \in \mathcal{G}} g^{\otimes t} M \left(g^{\otimes t}\right)^{\dagger} \mathrm{d}g. \tag{1}$$

where the integral on the right-hand side is taken over all elements in $\mathcal{G}$ with respect to the Haar measure. The number t is called the order of the design.

Remark 1. In this definition and in the rest of the paper $\mathcal{G}$ can be naturally identified with its defining representation. Therefore, $g^{\otimes t} = \Pi(g)^{\otimes t}$, where Π is the defining representation of $\mathcal{G}$.

Definition 2 (Unitary t-design). *A t-design $\mathcal{V}$ (with weight function w) of a group $\mathcal{G}$ is called a weighted unitary t-design if $\mathcal{G} = U(d)$. If $\mathcal{V}$ forms a group, then it is called a unitary t-group or group t-design.*

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

Remark 2. The weight function of a t-design $\mathcal{V}$ is the constant function $w \equiv 1/|\mathcal{V}|$ unless otherwise stated.

An alternative characterization of unitary designs can be given through the representation theory of $U(d)$. Considering the t-fold tensor product of the defining representation of $U(d)$, the underlying vector space $(\mathbb{C}^d)^{\otimes t}$ splits up into the different irreducible sectors of $U(d)$ labelled by Young diagrams

$$(\mathbb{C}^d)^{\otimes t} \cong \bigoplus_{\gamma \in \Gamma} \mathcal{K}_\gamma \otimes \mathcal{H}_\gamma, \tag{2}$$

where Γ is the set of Young diagrams containing at most d rows and t number of boxes, $\mathcal{H}_\gamma$ carries the $U(d)$ irrep labelled by the Young diagram γ and $\mathcal{K}_\gamma$ is the multiplicity space (where $U(d)$ acts trivially). Let us denote by $P_\gamma = P_\gamma^{\mathcal{K}} \otimes P_\gamma^{\mathcal{H}}$ the projections corresponding to the $V_\gamma = \mathcal{K}_\gamma \otimes \mathcal{H}_\gamma$ subspaces.

Proposition 1. *A finite set $\mathcal{V} \subset U(d)$ forms a unitary t-design if and only if the following equation is true for all linear transformations M on $(\mathbb{C}^d)^{\otimes t}$:*

$$\sum_{V \in \mathcal{V}} w\left(V\right) V^{\otimes t} M \left(V^{\otimes t}\right)^\dagger = \sum_{\gamma \in \Gamma} \frac{\mathrm{Tr}_\gamma^{\mathcal{H}}(P_\gamma M P_\gamma) \otimes P_\gamma^{\mathcal{H}}}{\mathrm{Tr}(P_\gamma)}, \tag{3}$$

where we used the notation as before, and $\mathrm{Tr}_\gamma^{\mathcal{H}}$ is the partial trace over $\mathcal{H}_\gamma$ of operators supported on the subspace $\mathcal{K}_\gamma \otimes \mathcal{H}_\gamma$.

This proposition can be proven using Schur's lemma, since the left hand side of Eq. (3) commutes with all $U^{\otimes t}$ (this follows from Eq. (1)). Schur's lemma can be invoked after decomposing the tensor product of representations into irreps. If an irrep's multiplicity is one, the resulting intertwining map is simply a constant multiple of the projection to the support, the constant being given by the appropriate proportion of the M operator's trace. If the irrep has higher multiplicity the resulting multiplicity is as indicated on the right hand side of Eq. (3):

A particular set of exact t-designs (for low t) can be constructed using finite groups [8].

Proposition 2. *Let $\mathcal{G}$ be a compact matrix Lie group and $\mathcal{V} < \mathcal{G}$ a finite subgroup. $\mathcal{V}$ is a group t-design if and only if the irreducible subspaces of the defining representation of $\mathcal{G}$ at the t-fold tensor product are equivalent to the irreducible subspaces of the representations' restrictions to the subgroup $\mathcal{V}$.*

3 Constructing Higher Order Designs from Lower Ones

In this section, we want to show a construction method that creates higher-order designs from lower-order ones. The main idea is based on examining the behaviours of representations of finite groups on the relevant invariant subspaces

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

of the t-fold tensor product of the defining representation of the unitary group $U(d)$.

The defining representation of $U(d)$ is the most straightforward one, denoted by $\Pi_{\ydiagram{1}}$ and given by

$$\Pi_{\ydiagram{1}}(U) = U, \qquad U \in U(d). \tag{4}$$

One can easily verify that this representation is irreducible. In contrast, the t-fold tensor product of this representation $\Pi_{\ydiagram{1}}^{\otimes t}$ acting on $\left(\mathbb{C}^d\right)^{\otimes t}$ is reducible for $t \geq 2$. The irreducible decomposition of the t-fold tensor product can be described through Young diagrams and the Schur-Weyl duality. For this paper, one only needs to consider the 2- and 3-fold tensor products of $\Pi_{\ydiagram{1}}$, which decompose using the Schur-Weyl duality as

$$\Pi_{\ydiagram{1}}^{\otimes 2} \cong \Pi_{\ydiagram{2}} \oplus \Pi_{\ydiagram{1,1}}, \tag{5}$$
$$\Pi_{\ydiagram{1}}^{\otimes 3} \cong \Pi_{\ydiagram{3}} \oplus \Pi_{\ydiagram{2,1}}^{\oplus 2} \oplus \Pi_{\ydiagram{1,1,1}}, \tag{6}$$

where the irreducible representations are labelled by their Young diagrams. Evidently Eq. (5) holds for $d > 1$ and Eq. (6) for $d > 2$. It is known from basic representation theory that the irreducible representations $\Pi_{\ydiagram{2}}$ and $\Pi_{\ydiagram{1,1}}$ are supported on the symmetric and antisymmetric subspaces, respectively, and will be referred to as such in the following.

3.1 Constructing 2-designs

A unitary 2-design can be constructed from a unitary representation of a finite group if the irreducible subspaces of the 2-fold tensor product are equivalent to the irreducible subspaces of the 2-fold tensor product of the unitary group according to Proposition 2. In general, the decomposition may not be preserved after restricting to a finite subgroup, but there may exist certain subgroups, for which the decomposition is preserved on some irreducible subspace(s). The current section investigates the possibility of creating 2-designs from such subgroups. This can be done by the construction method stated by the following theorem:

Theorem 1. *Let $d > 1$ and $H, K < U(d)$ be finite subgroups with $\Pi_{\ydiagram{2}}|_K$ and $\Pi_{\ydiagram{1,1}}|_H$ being irreducible representations, then the sets of unitaries $HK = \{hk : h \in H, k \in K\}$ and $KH = \{kh : k \in K, h \in H\}$ both form a weighted unitary 2-design with weights*

$$w_{HK}(U) = w_{KH}(U^\dagger) = \frac{|\{(h,k) \in H \times K \, : hk = U\}|}{|H|\,|K|}. \tag{7}$$

Proof. According to Proposition 3 found in the Appendix, if the statement is true for HK, the same statement is automatically true for KH as well, therefore only proof for HK is needed.

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

Let M be an arbitrary matrix of dimension $d^2 \times d^2$. Consider the averaging over the elements of HK, taking into account the possibly non-equal weights given by Eq. (7):

$$\sum_{V \in HK} w_{HK}(V)\, V^{\otimes 2} M (V^{\otimes 2})^\dagger = \frac{1}{|H|} \sum_{h \in H} h^{\otimes 2} \left(\frac{1}{|K|} \sum_{k \in K} k^{\otimes 2} M (k^{\otimes 2})^\dagger \right) (h^{\otimes 2})^\dagger. \tag{8}$$

The irrep $\Pi_{\square\!\square}|_K$ appears with multiplicity one in the irrep decomposition of the 2-fold tensor product representation of K by dimensional arguments. By Proposition 1, when performing the averaging with respect to K one acquires

$$\overline{M^K} := \frac{1}{|K|} \sum_{k \in K} k^{\otimes 2} M (k^{\otimes 2})^\dagger = c_{\square\!\square} P_{\square\!\square} + N, \tag{9}$$

where $c_{\square\!\square} = \mathrm{Tr}(P_{\square\!\square} M)$ and N is some operator such that $N = P_{\substack{\square\\\square}} N P_{\substack{\square\\\square}}$. The averaging of $\overline{M^K}$ with respect to H can be done with respect to the splitting $V_{\square\!\square} \oplus V_{\substack{\square\\\square}}$ since the off-diagonal blocks are zero. The block corresponding to $V_{\square\!\square}$ remains the same since it commutes with any operator. On the other hand, the block corresponding to $V_{\substack{\square\\\square}}$ after the averaging becomes $c_{\substack{\square\\\square}} P_{\substack{\square\\\square}}$ based on Schur's lemma since $\Pi_{\substack{\square\\\square}}|_H$ is an irreducible representation. As a result, we get

$$\frac{1}{|H|} \sum_{h \in H} h^{\otimes 2} \overline{M^K} (h^{\otimes 2})^\dagger = c_{\square\!\square} P_{\square\!\square} + c_{\substack{\square\\\square}} P_{\substack{\square\\\square}}, \tag{10}$$

which proves the theorem by Proposition 1. □

Using the GAP system [16] we have found groups which have the property as described in Theorem 1:

Example 1. A 6-dimensional unitary 2-design can be constructed from the groups $PSU(3,3)$ and A_7. The first group, $PSU(3,3)$, has a unitary irreducible representation in 6 dimensions for which the symmetric irreducible representation on the 2-fold tensor product of the unitary group restricted to this representation of $PSU(3,3)$ remains irreducible while the antisymmetric does not. On the other hand, the alternating group on 7 elements has a 6 dimensional unitary irreducible representation that remains irreducible on the antisymmetric subspace of the 2-fold tensor product while being reducible on the symmetric subspace. As a result, we can construct a weighted unitary 2-design in 6 dimensions with weights given by Eq. (7) based on Theorem 1.

Example 2. Similarly to Example 1, a 4-dimensional unitary 2-design can be constructed from two groups found in the `SmallGroup` library of GAP. The group K which is obtained from the 6-th irreducible representation of `SmallGroup(640,21454)` and the group H which is obtained from the 2-nd irreducible representation of `SmallGroup(120,34)` behave as described in Theorem 1. This means that the representation $\Pi_{\square}^{\otimes 2}$ restricted to group K remains irreducible on the symmetric subspace and restricted to group H remains irreducible on the antisymmetric subspace (however, they are reducible on their respective complement).

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

3.2 Possible Construction of Higher Designs

As in the previous construction described in Section 3.1 for the $t = 2$ case, a similar method is expected to work for $t = 3$ or higher-order designs. However, for $t \geq 3$, the irreducible decomposition of the t-fold tensor product of $\Pi_{\square}$ contains at least a subspace with multiplicity 2 or higher, which results in different behaviour when averaging over the unitary group, as described in Proposition 1. Luckily, the following theorem asserts that the previous construction generalizes:

Theorem 2. *Let $d > 2$ such that $d \neq 4$ and $H, K < U(d)$ finite subgroups such that for each $\gamma = \square\square\square, \substack{\square\square\\ \square}, \substack{\square\\ \square\\ \square}$ either $\Pi_\gamma|_K$ or $\Pi_\gamma|_H$ is irreducible. Then the sets of unitaries $HK = \{hk : h \in H, k \in K\}$ and $KH = \{kh : h \in H, k \in K\}$ both form a weighted unitary 3-design with weights given by*

$$w_{HK}(U) = w_{KH}(U^\dagger) = \frac{|\{(h,k) \in H \times K : hk = U\}|}{|H|\,|K|}. \tag{11}$$

Remark 3. In case of $d = 4$ the dimensions of $\Pi_{\square\square\square}$ and $\Pi_{\substack{\square\square\\ \square}}$ are equal which would result in a different condition for this Theorem which will not be discussed here.

Proof. According to Proposition 3 found in the Appendix, if the statement is true for HK, the same statement is automatically true for KH as well, therefore only proof for HK is needed.

Let M be an arbitrary matrix of dimension $d^3 \times d^3$. One can write

$$\sum_{V \in HK} w_{HK}(V) V^{\otimes 3} M \left(V^\dagger\right)^{\otimes 3} = \frac{1}{|H|} \sum_{h \in H} h^{\otimes 3} \left(\frac{1}{|K|} \sum_{k \in K} k^{\otimes 3} M \left(k^\dagger\right)^{\otimes 3} \right) \left(h^\dagger\right)^{\otimes 3}, \tag{12}$$

where the appearance of w_{HK} follows from the fact that some elements in the product of groups H and K may coincide. For brevity the following is introduced:

$$\overline{M^K} := \frac{1}{|K|} \sum_{k \in K} k^{\otimes 3} M \left(k^\dagger\right)^{\otimes 3}, \tag{13}$$

$$\overline{M^{HK}} := \frac{1}{|H|} \sum_{h \in H} h^{\otimes 3} \overline{M^K} \left(h^\dagger\right)^{\otimes 3}. \tag{14}$$

To prove the theorem, we need to show that $\overline{M^{HK}}$ takes the form of the RHS in Eq. (3) from Proposition 1. This could be demonstrated by describing all the block elements of $\overline{M^{HK}}$ given by the projections corresponding to Eq. (6). Firstly, we investigate the block in the decomposition corresponding to the subspace $V_{\square\square\square}$. If the representation $\Pi_{\square\square\square}|_K$ remains irreducible on the subspace $V_{\square\square\square}$, one can write

$$\frac{1}{|K|} \sum_{k \in K} k^{\otimes 3} P_{\square\square\square} M P_{\square\square\square} (k^\dagger)^{\otimes 3} = \mathrm{Tr}(P_{\square\square\square} M) P_{\square\square\square}. \tag{15}$$

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

Consequently, the matrix $\overline{M^K}$ on the subspace $V_{\ydiagram{3}}$ acts as an identity matrix, therefore taking the average over H has no effect here. Moreover, if the representation $\Pi_{\ydiagram{3}}|_H$ remains irreducible then the average of $P_{\ydiagram{3}}\overline{M^K}P_{\ydiagram{3}}$ over H diagonalizes the matrix. As a consequence, by taking the average over HK with weights w_{HK}, the resulting transformation on the subspace $V_{\ydiagram{3}}$ acts as a unitary 3-design. The case of block $P_{\ydiagram{1,1,1}}MP_{\ydiagram{1,1,1}}$ is analogous to the case $V_{\ydiagram{3}}$.

According to the statement, $d \neq 4$, hence $\dim(V_\gamma) \neq \dim(V_{\gamma'})$ for $\gamma \neq \gamma'$. Consider a block described by $P_\gamma M P_{\gamma'}$ where $\gamma \neq \gamma'$. Let $\dim(V_\gamma) < \dim(V_{\gamma'})$, without loss of generality. By assumption, the representation restricted to either group H or K remains irreducible on $V_{\gamma'}$. By taking the average by H or K, the considered block may become zero, since it could only be an intertwiner between two different dimensional irreducible subspaces. After taking the average by both H and K consecutively, every off-diagonal block must vanish.

If the representation $\Pi_{\ydiagram{2,1}}|_K$ remains irreducible, then after averaging over K the matrix $P_{\ydiagram{2,1}}MP_{\ydiagram{2,1}}$ is by Proposition 2 and Proposition 1:

$$P_{\ydiagram{2,1}}\overline{M^K}P_{\ydiagram{2,1}} = \frac{1}{\mathrm{Tr}(P_{\ydiagram{2,1}})}\mathrm{Tr}^{\mathcal{H}}_{\ydiagram{2,1}}(P_{\ydiagram{2,1}}MP_{\ydiagram{2,1}}) \otimes P^{\mathcal{H}}_{\ydiagram{2,1}}. \tag{16}$$

Since for all $h \in H$ the $h^{\otimes 3}$ is block diagonal on the subspace corresponding to $V_{\ydiagram{2,1}}$, the matrix in Eq. (16) commutes with it.

If the representation $\Pi_{\ydiagram{2,1}}|_H$ remains irreducible, then the same happens to the matrix $\overline{M^K}$, and due to the cyclic property of the partial trace if tracing out over $\mathcal{H}_{\ydiagram{2,1}}$ it gives the same as partial trace for the matrix M:

$$\mathrm{Tr}^{\mathcal{H}}_{\ydiagram{2,1}}\left(P_{\ydiagram{2,1}}MP_{\ydiagram{2,1}}\right) = \mathrm{Tr}^{\mathcal{H}}_{\ydiagram{2,1}}\left(P_{\ydiagram{2,1}}\overline{M^K}P_{\ydiagram{2,1}}\right). \tag{17}$$

Consequently, all blocks are the same as in Proposition 1. $\square$

Example 3. Using the GAP system it can be shown that a 10-dimensional unitary 3-design can be constructed from two groups using Theorem 2. Let H be the 3-rd irreducible representation of the group `"(3xU5(2)).2"` and K the 36-th irreducible representation of the group `"2x2.M22"`. Then $H^{\otimes 3}|_{\ydiagram{3}}$ is irreducible and $K^{\otimes 3}|_{\ydiagram{2,1}}$ and $K^{\otimes 3}|_{\ydiagram{1,1,1}}$ are irreducible. Therefore the set of unitaries given by the product HK with weights given by Eq. (11) produces a 10-dimensional 3-design by Theorem 2.

4 Unitary 2-designs from Orthogonal and Symplectic 2-designs

In the previous section, we provided methods to build unitary designs from the irreducible representations of two finite unitary subgroups. Let us turn our attention to the scenario where one fixes a 2-design $\mathcal{V}$ of a subgroup $\mathcal{G}$ of the unitary group. This is then transformed resulting in a set of unitary matrices

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

also exhibiting design properties. Using this construction, *unitary* designs can be obtained from these two sets. In particular, the orthogonal and the unitary symplectic group (also called compact symplectic group) will be considered for $\mathcal{G}$. Note that using Definition 1, orthogonal and unitary symplectic t-designs are just t-designs of the groups $\mathcal{G} = O(d)$ and $\mathcal{G} = USp(d)$, respectively.

Theorem 3. *Let $\mathcal{V} \subset O(d)$ form an orthogonal 2-design, and consider the set $\mathcal{W}_\alpha := W_\alpha \mathcal{V} W_\alpha^\dagger$, where W_α is the unitary describing the basis transformation in Eq.* (18)*, then the set of unitaries $\mathcal{W}_\alpha \cdot \mathcal{V}$ forms a unitary 2-design.*

Proof. Let $\{|j\rangle\}_{j=0}^{d-1}$ be the basis of $\mathbb{C}^d$ with respect to which the representation of the orthogonal group is considered as real matrices. This leads to a basis on the tensor square $(\mathbb{C}^d)^{\otimes 2}$ defined by the tensor power of the elements: $\{|j\rangle \otimes |k\rangle\}_{j,k=0}^{d-1}$. Let W_α be the operation on the basis elements defined by

$$W_\alpha |j\rangle = (\tau_\alpha)^j |j\rangle \,, \tag{18}$$

where $\tau_\alpha = e^{\frac{2\pi i \alpha}{2d}}$.

Let $\Phi_{\square}$ denote the defining representation of the orthogonal group with respect to the basis $\{|j\rangle\}_{j=0}^{d-1}$. This can be embedded into the defining representation of the unitary group. The irreducible decomposition of $\Phi_{\square}^{\otimes 2}$ is the following:

$$\Phi_{\square}^{\otimes 2} \cong \Phi_{|\psi\rangle} \oplus \Phi_{|\psi\rangle}^c \oplus \Phi_{\begin{smallmatrix}\square\\\square\end{smallmatrix}}, \tag{19}$$

where $\Phi_{|\psi\rangle}$ is a 1-dimensional representation acting on the subspace spanned by $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \otimes |j\rangle$, $\Phi_{|\psi\rangle} \oplus \Phi_{|\psi\rangle}^c$ and $\Phi_{\begin{smallmatrix}\square\\\square\end{smallmatrix}}$ act on the symmetric subspace $V_{\square\square}$ and on the anti-symmetric subspace $V_{\begin{smallmatrix}\square\\\square\end{smallmatrix}}$, respectively, where the indices are used as in Eq. (5). The projections to these subspaces are $P_{|\psi\rangle} = |\psi\rangle\langle\psi|$, $P_{\square\square} - P_{|\psi\rangle}$ and $P_{\begin{smallmatrix}\square\\\square\end{smallmatrix}}$, respectively.

Let us now examine the set $\mathcal{W}_\alpha = W_\alpha \mathcal{V} W_\alpha^\dagger$. This also forms an orthogonal 2-design, however in this case for the representation $\Phi'_{\square}$ which is unitarily equivalent to $\Phi_{\square}$ but the matrices are considered real with respect to the basis $\{|W_\alpha j\rangle\}_{j=0}^{d-1}$. This means that in the irrep decomposition of the two-fold tensor product, the distinguished one-dimensional subspace is spanned by $|\psi'\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |W_\alpha j\rangle \otimes |W_\alpha j\rangle$.

One can take the scalar product $f(\alpha) := |\langle \psi, W_\alpha \otimes W_\alpha \psi\rangle|^2$. This gives $f(0) = 1$ and $f(1) = 0$ and, by the continuity of the scalar product, for arbitrary $q \in [0, 1]$ there is an $\alpha \in [0, 1]$ which gives $f(\alpha) = q$. This is used later to define the value of α for a given d. The main idea of this proof is, using the fact that when $\mathcal{V}$ and $\mathcal{W}_\alpha$ form an orthogonal 2-design, that the value of α can be determined in a way that the product $\mathcal{W}_\alpha \mathcal{V}$ also forms a unitary 2-design.

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

Let M be an arbitrary complex matrix of dimension $d^2 \times d^2$. According to Proposition 1, averaging with $\mathcal{V}$ results in

$$\begin{aligned}\overline{M} &:= \sum_{v \in \mathcal{V}} (v \otimes v) M (v \otimes v)^\dagger \\ &= \frac{\mathrm{Tr}\left(P_{|\psi\rangle} M\right)}{\mathrm{Tr}(P_{|\psi\rangle})} P_{|\psi\rangle} + \frac{\mathrm{Tr}\left(P_{\square\square} M - P_{|\psi\rangle} M\right)}{\mathrm{Tr}\left(P_{\square\square} - P_{|\psi\rangle}\right)} \left(P_{\square\square} - P_{|\psi\rangle}\right) + \frac{\mathrm{Tr}\left(P_{\substack{\square\\\square}} M\right)}{\mathrm{Tr}(P_{\substack{\square\\\square}})} P_{\substack{\square\\\square}}.\end{aligned} \tag{20}$$

Moreover, averaging $\overline{M}$ with $\mathcal{W}_\alpha$ one acquires

$$\begin{aligned}\overline{\overline{M}} &:= \sum_{w \in \mathcal{W}_\alpha} (w \otimes w)\, \overline{M} (w \otimes w)^\dagger \\ &= \frac{\mathrm{Tr}\left(P_{|\psi'\rangle} \overline{M}\right)}{\mathrm{Tr}(P_{|\psi'\rangle})} P_{|\psi'\rangle} + \frac{\mathrm{Tr}\left(P_{\square\square} \overline{M} - P_{|\psi'\rangle} \overline{M}\right)}{\mathrm{Tr}(P_{\square\square} - P_{|\psi'\rangle})} \left(P_{\square\square} - P_{|\psi'\rangle}\right) + \\ &+ \frac{\mathrm{Tr}\left(P_{\substack{\square\\\square}} \overline{M}\right)}{\mathrm{Tr}(P_{\substack{\square\\\square}})} P_{\substack{\square\\\square}}.\end{aligned} \tag{21}$$

On the antisymmetric subspace, the averaging acts like a unitary design since $\mathrm{Tr}\left(P_{\substack{\square\\\square}} \overline{\overline{M}}\right) = \mathrm{Tr}(P_{\substack{\square\\\square}} \overline{M}) = \mathrm{Tr}(P_{\substack{\square\\\square}} M)$. However, for it to act like a unitary design on the symmetric subspace, it is required that all diagonal elements are equal to each other. This means that in the remaining part of the proof it is enough to consider only the symmetric subspace so as to get this desired property.

Let the action of $\overline{M}$ on the unitary symmetric subspace be $D := \overline{M}|_{V_{\square\square}} = a \cdot P_{\square\square} + b \cdot P_{|\psi\rangle}$ for some $a, b \in \mathbb{C}$. By averaging it with $\mathcal{W}_\alpha$ this expression gets modified to

$$\frac{\mathrm{Tr}(P_{|\psi'\rangle} D)}{\mathrm{Tr}(P_{|\psi'\rangle})} P_{|\psi'\rangle} + \frac{\mathrm{Tr}\left(\left(P_{\square\square} - P_{|\psi'\rangle}\right) D\right)}{\mathrm{Tr}\left(P_{\square\square} - P_{|\psi'\rangle}\right)} \left(P_{\square\square} - P_{|\psi'\rangle}\right). \tag{22}$$

One can calculate the coefficient of the first term of Eq. (22) by

$$\mathrm{Tr}(P_{|\psi'\rangle} D) = \mathrm{Tr}(P_{|\psi'\rangle} a P_{\square\square} + P_{|\psi'\rangle} b P_{|\psi\rangle}) = a + bq. \tag{23}$$

Analogously, the coefficient of the second term is

$$\mathrm{Tr}\left(\left(P_{\square\square} - P_{|\psi'\rangle}\right) D\right) = \left(\frac{d(d+1)}{2} - 1\right) a + (1-q)b. \tag{24}$$

The two coefficients in equation (22) need to be equal for $\mathcal{W}_\alpha \mathcal{V}$ to form a unitary 2-design. Therefore the following condition needs to be met:

$$\left(\frac{d(d+1)}{2} - 1\right)(a + bq) = \left(\frac{d(d+1)}{2} - 1\right) a + (1-q)b, \tag{25}$$

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

which simplifies to

$$q = \frac{2}{d(d+1)}. \tag{26}$$

This can be achieved independently from the a and b values. $\square$

Using the GAP system [16] we have found groups which have the property as described in Theorem 3:

Example 4. The group `PSU(3,3)` has a 7-dimensional irreducible representation ($\texttt{PSU(3,3)}_{[3]}$ in GAP where the index denotes the third irrep) with which a 7-dimensional 2-design can be constructed using Theorem 3.

For constructing unitary 2-designs from symplectic 2-designs a similar theorem can be formulated:

Theorem 4. *Let $\mathcal{V} \subset USp(d)$ form a unitary symplectic 2-design, and consider the set $\mathcal{W}_\alpha = W_\alpha \mathcal{V} W_\alpha^\dagger$, where W_α is a unitary describing the basis transformation in Eq.* (27)*, then the set of unitaries $\mathcal{W}_\alpha \cdot \mathcal{V}$ forms a unitary 2-design.*

Proof. The proof is similar to the proof of Theorem 3 with the 1-dimensional subspace determined by $|\psi\rangle = \sum_{j=0}^{d-1} |j\rangle \otimes |j+d\rangle - |j+d\rangle \otimes |j\rangle$. The operator corresponding to the basis transformation is defined as

$$\begin{aligned} W_\alpha |j\rangle &= \tau^j |j\rangle \\ W_\alpha |j+d\rangle &= \tau^j |j+d\rangle \end{aligned} \tag{27}$$

for each $j = 0, \ldots, d-1$ and $\tau_\alpha = e^{\frac{2\pi i \alpha}{2d}}$. $\square$

Using the GAP system [16] we have found groups which have the property as described in Theorem 4:

Example 5. The group denoted as `SmallGroup(640,21454)` in GAP has 4-dimensional irreducible representation ($\texttt{SmallGroup(640,21454)}_{[6]}$ in GAP where the index denotes the sixth irrep) with which a 4-dimensional 2-design can be constructed using Theorem 4.

Example 6. The group `PSU(3,3)` has 6-dimensional irreducible representation ($\texttt{PSU(3,3)}_{[2]}$ in GAP) with which a 6-dimensional 2-design can be constructed using Theorem 4.

5 Summary and Outlook

The current paper establishes a procedure for constructing a weighted t-design using finite groups whose representation admits an easily verifiable property and some examples are shown to use this procedure to construct 2-designs. Furthermore, a method for constructing a unitary 2-design from an orthogonal or a unitary symplectic 2-design is proposed with some examples to demonstrate the working of construction. However, there are a plethora of possible research

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

directions regarding group representations based on these ideas. In particular, we plan to carry out a very thorough symbolic search through finite groups using GAP to identify cases, and perhaps even families of cases, when our current methods could be used successfully. We also aim to extended the basis change trick to cases beyond orthogonal and symplectic 2-designs, considering rather general examples of the splitting of the 2-fold tensor product representation of finite group families. On the more ambitious side, one of the goals could be to extend some of the results (or the ideas) in the paper to families of random circuits, which have different splitting and convergence properties in different irreducible subspaces of $U(d)$. Specifically, one may intend to study random circuits that are made of sequences of random orthogonal and random symplectic gates, and compare them with the convergence of other gate-set families.

Acknowledgement

This research was supported by the Ministry of Culture and Innovation and the National Research, Development and Innovation Office through the Quantum Information National Laboratory of Hungary (Grant No. 2022-2.1.1-NL-2022-00004) and OTKA grant No. FK 135220.

References

1. Arienzo, M., Heinrich, M., Roth, I., Kliesch, M.: Closed-form analytic expressions for shadow estimation with brickwork circuits. arXiv preprint (2022). https://doi.org/https://doi.org/10.48550/arXiv.2211.09835
2. Bae, J., Hiesmayr, B.C., McNulty, D.: Linking entanglement detection and state tomography via quantum 2-designs. New Journal of Physics **21**(1), 013012 (jan 2019). https://doi.org/10.1088/1367-2630/aaf8cf
3. Bannai, E., Navarro, G., Rizo, N., Tiep, P.H.: Unitary t-groups. Journal of the Mathematical Society of Japan **72**(3), 909 – 921 (2020). https://doi.org/10.2969/jmsj/82228222
4. Bengtsson, I., Życzkowski, K.: Geometry of quantum states: an introduction to quantum entanglement. Cambridge university press (2017)
5. Czartowski, J., Goyeneche, D., Grassl, M., Życzkowski, K.: Isoentangled mutually unbiased bases, symmetric quantum measurements, and mixed-state designs. Physical Review Letters **124**(9), 090503 (2020). https://doi.org/10.1103/physrevlett.124.090503
6. Dankert, C., Cleve, R., Emerson, J., Livine, E.: Exact and approximate unitary 2-designs and their application to fidelity estimation. Physical Review A **80**(1) (jul 2009). https://doi.org/10.1103/physreva.80.012304
7. Di Matteo, O.: A short introduction to unitary 2-designs. CS867/QIC890 (2014)
8. Gross, D., Audenaert, K., Eisert, J.: Evenly distributed unitaries: On the structure of unitary designs. Journal of Mathematical Physics **48**(5), 052104 (may 2007). https://doi.org/10.1063/1.2716992
9. Gross, D., Krahmer, F., Kueng, R.: A partial derandomization of PhaseLift using spherical designs. Journal of Fourier Analysis and Applications **21**(2), 229–266 (oct 2014). https://doi.org/10.1007/s00041-014-9361-2

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

10. Guralnick, R., Tiep, P.: Decompositions of small tensor powers and Larsen's conjecture. Representation Theory **9**(5), 138–208 (Feb 2005). https://doi.org/10.1090/S1088-4165-05-00192-5
11. Helsen, J., Walter, M.: Thrifty shadow estimation: re-using quantum circuits and bounding tails. arXiv preprint (2022). https://doi.org/https://doi.org/10.48550/arXiv.2212.06240
12. Kueng, R., Gross, D.: Qubit stabilizer states are complex projective 3-designs. arXiv preprint arXiv:1510.02767 (2015). https://doi.org/https://doi.org/10.48550/arXiv.1510.02767
13. Roy, A., Scott, A.J.: Unitary designs and codes. Designs, Codes and Cryptography **53**(1), 13–31 (apr 2009). https://doi.org/10.1007/s10623-009-9290-2
14. Scott, A.J.: Optimizing quantum process tomography with unitary 2-designs. Journal of Physics A: Mathematical and Theoretical **41**(5), 055308 (jan 2008). https://doi.org/10.1088/1751-8113/41/5/055308
15. Seymour, P., Zaslavsky, T.: Averaging sets: A generalization of mean values and spherical designs. Advances in Mathematics **52**(3), 213–240 (1984). https://doi.org/https://doi.org/10.1016/0001-8708(84)90022-7
16. The GAP Group: Gap–groups, algorithms, and programming (412 2 (2022)), https://www.gap-system.org
17. Wallman, J.J., Flammia, S.T.: Randomized benchmarking with confidence. New Journal of Physics **16**(10), 103032 (oct 2014). https://doi.org/10.1088/1367-2630/16/10/103032
18. Webb, Z.: The Clifford group forms a unitary 3-design. Quantum Information and Computation **16**, 1379–1400 (2015). https://doi.org/doi.org/10.26421/QIC16.15-16-8
19. Zhu, H.: Multiqubit Clifford groups are unitary 3-designs. Phys. Rev. A **96**, 062336 (Dec 2017). https://doi.org/10.1103/PhysRevA.96.062336

Appendix A: Symmetry of Product Designs

Proposition 3. *Let $H, K \subset U(d)$ be finite subsets invariant to the elementwise adjoint operation ($H^\dagger = H$, $K^\dagger = K$). If HK forms a t-design, then KH also forms a t-design, where $HK = \{hk : h \in H, k \in K\}$.*

Remark 4. H, K being finite subgroups of $U(d)$ is a special case.

Proof. It is easy to see from the properties of the adjoint that $(HK)^\dagger = KH$, where $(HK)^\dagger = \{(hk)^\dagger : h \in H, k \in K\}$. Starting from this observation, we now provide proof that for any t-design $\{V_i\}_{i=1}^n$ it follows that $\{V_i^\dagger\}_{i=1}^n$ is also a t-design, which then completes the proof of the theorem.

To see that the above-mentioned proposition is true, we will use the non-degeneracy of the Hilbert-Schmidt inner product $\langle A, B\rangle_{\mathrm{HS}} = \mathrm{Tr}(A^\dagger B)$, which implies that if $\mathrm{Tr}(AB) = \mathrm{Tr}(CB)$ for all $B \in \mathcal{B}(\mathbb{C}^d)$ then $A = C$. From this non-degeneracy statement it follows that given a t-design $\{V_i\}_{i=1}^n$, the set $\{V_i^\dagger\}_{i=1}^n$ is also a t-design if and only if

$$\mathrm{Tr}\left(\frac{1}{n}\sum_i (V_i^\dagger)^{\otimes t} X V_i^{\otimes t}\, Y\right) = \mathrm{Tr}\left(\int_{U(d)} U^{\otimes t} X (U^\dagger)^{\otimes t} \mathrm{d}U\, Y\right) \tag{28}$$

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19

holds for all $X, Y \in \mathcal{B}((\mathbb{C}^d)^{\otimes t})$. Using the linearity and the cyclic property of the trace one can write

$$\begin{aligned}
\mathrm{Tr}\left(\frac{1}{n}\sum_i (V_i^\dagger)^{\otimes t} X V_i^{\otimes t}\, Y\right) &= \mathrm{Tr}\left(\frac{1}{n}\sum_i V_i^{\otimes t}\, Y (V_i^\dagger)^{\otimes t} X\right) \\
&= \mathrm{Tr}\left(\int_{U(d)} U^{\otimes t} Y (U^\dagger)^{\otimes t} \mathrm{d}U\; X\right) \\
&= \mathrm{Tr}\left(\int_{U(d)} (U^\dagger)^{\otimes t} X U^{\otimes t} \mathrm{d}U\; Y\right) \\
&= \mathrm{Tr}\left(\int_{U(d)} U^{\otimes t} X (U^\dagger)^{\otimes t} \mathrm{d}U\; Y\right), \qquad (29)
\end{aligned}$$

where the last equality follows from the invariance of the Haar measure with respect to inversion, that is for any $X \in \mathcal{B}((\mathbb{C}^d)^{\otimes t})$:

$$\int_{U(d)} U^{\otimes t} X (U^\dagger)^{\otimes t} \mathrm{d}U = \int_{U(d)} (U^\dagger)^{\otimes t} X U^{\otimes t} \mathrm{d}U. \qquad (30)$$

Using this line of thought, Eq. 28 follows, which proves the theorem. □

ICCS Camera Ready Version 2023
To cite this paper please use the final published version:
DOI: 10.1007/978-3-031-36030-5_19