

Generalized group designs: constructing novel unitary 2-, 3- and 4-designs

Ágoston Kaposi^{1,2}, Zoltán Kolarovszki^{1,2}, Adrián Solymos^{1,3}, and Zoltán Zimborás^{1,2,4,5}

¹Quantum Computing and Quantum Information Research Group, HUN-REN Wigner Research Centre for Physics, Konkoly-Thege Miklós út 29-33, Budapest, H-1525, Hungary

²Department of Programming Languages and Compilers, Eötvös Loránd University, Pázmány Péter sétány 1/C, Budapest, H-1117, Hungary

³Department of Physics of Complex Systems, Eötvös Loránd University, Pázmány Péter sétány 1/A, Budapest, H-1117, Hungary

⁴Algorithmiq Ltd, Kanavakatu 3C, Helsinki, 00160, Finland

⁵University of Helsinki, Yliopistonkatu 4, Helsinki, 00100, Finland

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 $U(d)$. While it is known that exact unitary t -designs exist for any degree t and dimension d , the most appealing type of designs, group designs (in which the elements of the design form a group), can provide at most 3-designs. Moreover, even group 2-designs can exist only in limited dimensions. In this paper, we present novel construction methods for creating *exact generalized group designs* based on the representation theory of the unitary group and its finite subgroups that overcome the 4-design-barrier of unitary group designs. Furthermore, a construction is presented for creating generalized group 2-designs in arbitrary dimensions.

1 Introduction

Unitary t -designs were first introduced in Refs. [1, 2], and subsequently have become an essential tool within the field of quantum information science. These finite collections of $d \times d$ unitary matrices possess a unique property: By twirling (i.e., averaging) a certain matrix with the t -fold tensor products of these unitary matrices, the result is equal to the twirling over the *entire* unitary group $U(d)$ with respect to the Haar measure. This property makes them advantageous to use in protocols requiring unitaries sampled randomly from the Haar measure, thus potentially decreasing the resources needed, as generic Haar random unitaries are hard to implement. Hence, unitary designs have wide-ranging applications in quantum information science, in particular for quantum process tomography

Ágoston Kaposi: kaposiagoston@inf.elte.hu

Zoltán Kolarovszki: kolarovszki.zoltan@wigner.hun-ren.hu

Adrián Solymos: solymos.adrian@wigner.hun-ren.hu

Zoltán Zimborás: zimboras.zoltan@wigner.hun-ren.hu

and channel fidelity estimation [3, 2], the construction of unitary codes [4], derandomization of probabilistic constructions [5], entanglement detection [6], the study of quantum chaos [7, 8], randomized benchmarking [9, 10], and shadow estimation [11, 12, 13, 14].

One of the most elegant methods for constructing unitary designs involves delving into the representation theory of finite groups. The collection of unitaries derived from any unitary irreducible representation of a finite group constitutes a 1-design, and given additional properties, these elements can potentially form a higher-degree unitary design [15]. We call such collections of unitaries that form a group (such as those coming from representations) *unitary group designs*¹. Notably, some of the most renowned families of unitary t -designs fall under the category of group designs: The Clifford groups over finite fields, both in their multipartite and single-particle variants, provide elegant and practical 2-designs in prime power dimensions [18]. Consequently, they find applications in randomized benchmarking for both qubit and qudit systems [9, 10, 19]. The multipartite Clifford group for qubit systems even constitutes a unitary 3-design [20, 21, 22], proving to be advantageous, for instance, in single-shot shadow estimation [12, 13, 14].

The rotten apple that spoils the barrel is the fact that, in dimensions greater than 2, there do not exist group 4-designs (and thus higher-degree designs) [23]. Moreover, one can construct group 2-designs only for a few non-prime-power dimensions (in particular, one can define modular versions of the Clifford group for non-prime-power dimensions, however, these fail to be 2-designs [24]). This severely limits the use of group designs for tasks such as randomized benchmarking in these dimensions.

Constructing unitary t -designs using finite group representations will eventually fail because the t -fold tensor product of the chosen representation will decompose nontrivially on some of the $U(d)$ -irreducible subspaces of the t -fold tensor product space. Thus, our research was mainly focused on the behavior of the group representations on those $U(d)$ -irreducible subspaces. In this paper, we present novel construction methods for creating *generalized group designs* based on such representation theoretic considerations. This allows us to build higher-degree designs from lower ones and also enables us to define a procedure for constructing 2-designs in arbitrary dimensions.

The structure of the paper is as follows: Section 2 contains necessary basic definitions regarding unitary designs; Section 3 provides a construction of t -designs from finite unitary subgroups and presents some examples for the construction; Section 4 describes an explicit construction for generalized group 2-designs in arbitrary dimensions; finally, Section 5 outlines a method for constructing unitary 2- and 3-designs from orthogonal 2- and 3-designs, respectively.

2 Preliminaries

This section provides the essential definitions and statements employed in the proposed constructions. A basic familiarity with representation theory is assumed; a brief recap on the basic concepts is provided in Appendix B. It is important to note, that this paper is mainly concerned with the construction of exact designs, but we provide a statement for the construction of unitary 2- or 3-designs from orthogonal ones, which holds in the approximate case as well. For concrete constructions regarding approximate designs, see Refs. [2, 25, 26, 27].

Several different but equivalent definitions can be found for unitary designs and group

¹We note that the term group design is also used in the literature to denote a unitary ensemble that approximates the Haar measure restricted to a subgroup of the unitary group, see, e.g., Refs. [16, 17].

designs in the literature [28, 29, 15]. However, the notion of unitary t -designs, where the summation over the finite set is weighted with a certain weight function, is crucial for this paper since the constructions presented are generally of this type.

Definition 1 (Unitary t -design). A finite set $\mathcal{V} \subset \mathrm{U}(d)$ with weight function $w : \mathcal{V} \rightarrow [0, 1]$ is called a unitary t -design if the following equation holds for any linear transformation M on $(\mathbb{C}^d)^{\otimes t}$:

$$\sum_{V \in \mathcal{V}} w(V) V^{\otimes t} M (V^{\otimes t})^\dagger = \int_{U \in \mathrm{U}(d)} U^{\otimes t} M (U^{\otimes t})^\dagger dU, \quad (1)$$

where the integral on the right-hand side is taken over all elements in $\mathrm{U}(d)$ with respect to the Haar measure. The number t is called the degree of the design.

In this definition and the rest of the paper $\mathrm{U}(d)$ can be naturally identified with its defining representation. More concretely, $U^{\otimes t} = \Pi_\square(U)^{\otimes t}$ for $U \in \mathrm{U}(d)$, where $\Pi_\square$ is the defining representation of $\mathrm{U}(d)$. Moreover, the weight function of a t -design $\mathcal{V}$ is the constant function $w \equiv 1/|\mathcal{V}|$ unless otherwise stated. Finally, a unitary t -design is called a *unitary group t -design* when it possesses a group structure. In our proposals, however, we will construct t -designs which are generalizations of group t -designs in the sense that they are constructed from products of finite groups:

Definition 2 (Generalized group t -design). Let $\mathcal{V}_1, \dots, \mathcal{V}_\ell < \mathrm{U}(d)$ be finite subgroups. We call $\mathcal{V} := \mathcal{V}_1 \cdot \dots \cdot \mathcal{V}_\ell$ a generalized group t -design if $\mathcal{V}$ forms a unitary t -design with weight function given by

$$w(U) := \frac{\left| \left\{ (h_1, \dots, h_\ell) \in \mathcal{V}_1 \times \dots \times \mathcal{V}_\ell : \prod_{j=1}^\ell h_j = U \right\} \right|}{|\mathcal{V}_1| \cdots |\mathcal{V}_\ell|}. \quad (2)$$

Remark 1. The above careful definition of the weight function is needed as, in general, the product of finite subgroups of a group does not form a set whose cardinality is equal to the product of the cardinalities of the constituent subgroups.

3 Constructing higher-degree generalized group designs

Construction of unitary designs for general t and d is a mathematically challenging task [30]. A well-known example of a unitary design is the Clifford group, which constitutes a group 3-design for qubit systems [21, 20, 22], but this specific example does not generalize for higher-degree designs. Fortunately, using the representation theory of finite groups, one may discover group t -designs with $t = 1, 2, 3$ for specific dimensions. However, the construction of higher-degree group designs based on representation theory is impossible because of the nonexistence of group 4-designs in dimensions greater than 2 [23]. The resulting 4-design-barrier for group designs compelled us to search for higher-degree designs that are not group designs. In this section, we present a construction that pushes the 4-design-barrier further for unitary designs by introducing an extended notion of group designs, which we will refer to as generalized group designs (see Def. 2).

First, another characterization of unitary t -designs (equivalent to Def. 1) is presented based on representation theory (see also, Appendix of [15]). Consider the t -fold tensor product of the defining representation of $\mathrm{U}(d)$: the underlying vector space $(\mathbb{C}^d)^{\otimes t}$ splits up under the action of $\mathrm{U}(d)$ into the different isotypic components labeled by Young diagrams as

$$(\mathbb{C}^d)^{\otimes t} = \bigoplus_{\gamma \in \Gamma} \mathcal{K}_\gamma \otimes \mathcal{H}_\gamma, \quad (3)$$

where Γ is the set of Young diagrams with t number of boxes and at most d rows, $\mathcal{H}_\gamma$ carries the $U(d)$ -irrep labeled by the Young diagram γ and $\mathcal{K}_\gamma$ is the multiplicity space where $U(d)$ acts trivially [31]. Let us denote by P_γ the projection corresponding to the $\mathcal{W}_\gamma := \mathcal{K}_\gamma \otimes \mathcal{H}_\gamma$ subspace. As previously mentioned, we present another equivalent characterization of unitary t -designs, which may be easily justified using Schur's lemma:

Proposition 1. *A finite set $\mathcal{V} \subset U(d)$ and a weight function $w : \mathcal{V} \rightarrow [0, 1]$ forms a unitary t -design if and only if the following equation is true for all linear transformations M on $(\mathbb{C}^d)^{\otimes t}$:*

$$\sum_{V \in \mathcal{V}} w(V) V^{\otimes t} M (V^{\otimes t})^\dagger = \bigoplus_{\gamma \in \Gamma} \frac{\text{Tr}_{\mathcal{H}_\gamma}(P_\gamma M P_\gamma)}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma}, \quad (4)$$

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

Based on Proposition 1 the condition for a finite subgroup of the unitary group to be a unitary t -design can be reformulated to require that the appropriate irreducible subspaces of the unitary group remain irreducible when restricted to this finite subgroup. In light of this, the 4-design-barrier can be formulated in the following way: there is no finite subgroup of $U(d)$ such that all irreps of $U(d)$ labeled by Young diagrams with 4 boxes, restricted to this subgroup, remain irreducible if $d > 2$. The idea behind our construction is that for each Young diagram with t boxes and at most d rows we find a finite subgroup of $U(d)$, such that the irrep of $U(d)$ corresponding to this Young diagram remains irreducible when restricted to this subgroup. From these irreps, one can attempt to create a generalized unitary group t -design for $t \geq 4$. The fly in the ointment is that the irreducible subspace corresponding to such irreps might appear elsewhere in the irreducible decomposition of the t -fold tensor product of $U(d)$ upon restriction. This might lead to a non-trivial intertwiner between these irreducible subspaces when averaging, ruining the construction. To rescue this idea, we aim to exclude these situations, in a carefully crafted theorem.

Theorem 1. *Let $\Pi_\square$ denote the defining representation of the unitary group $U(d)$. Let Γ denote the set of all Young diagrams with t boxes and at most d rows, corresponding to the irreducible representations appearing in the irreducible decomposition of $\Pi_\square^{\otimes t}$. Let $G_1, \dots, G_\ell < U(d)$ be finite unitary subgroups such that:*

1. *For each Young diagram $\gamma \in \Gamma$, there is a $j \in \{1, \dots, \ell\}$ such that the representation $\Pi_\gamma|_{G_j}$ remains an irreducible representation;*
2. *For any $\gamma, \eta \in \Gamma$, there is a $j \in \{1, \dots, \ell\}$ such that there is no non-trivial intertwiner between the representations $\Pi_\gamma|_{G_j}$ and $\Pi_\eta|_{G_j}$.*

Then the product $G_1 \cdot \dots \cdot G_\ell$ forms a generalized group t -design.

Proof. Let us denote twirling with a subgroup $G < U(d)$ as

$$\mathcal{T}_G(X) := \int_G U^{\otimes t} X (U^{\otimes t})^\dagger dU, \quad (5)$$

where the integration is done over the Haar measure of G . Moreover, let us denote the consecutive twirls with $G_1, \dots, G_\ell$ by

$$\mathcal{T} := \mathcal{T}_{G_1} \dots \mathcal{T}_{G_\ell}, \quad (6)$$

and let us have the following notations

$$\mathcal{P}_{\gamma,\eta}(X) := P_\gamma X P_\eta, \quad \mathcal{P}_\gamma := \mathcal{P}_{\gamma,\gamma}, \quad (7)$$

where X is a linear operator on $(\mathbb{C}^d)^{\otimes t}$. Considering a fixed linear operator M on $(\mathbb{C}^d)^{\otimes t}$, we want to show that

$$\mathcal{T}(M) = \sum_{\gamma \in \Gamma} \frac{\text{Tr}_{\mathcal{H}_\gamma}(\mathcal{P}_\gamma(M))}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma}. \quad (8)$$

For this, let us decompose $\mathcal{T}(M)$ as

$$\mathcal{T}(M) = \sum_{\gamma, \eta \in \Gamma} \mathcal{P}_{\gamma,\eta} \mathcal{T}(M) = \sum_{\gamma \in \Gamma} \mathcal{P}_\gamma \mathcal{T}(M) + \sum_{\substack{\gamma, \eta \in \Gamma \\ \gamma \neq \eta}} \mathcal{P}_{\gamma,\eta} \mathcal{T}(M). \quad (9)$$

Let $\gamma, \eta \in \Gamma$. Firstly, we prove that $\mathcal{P}_{\gamma,\eta} \mathcal{T}(M) = 0$ if $\gamma \neq \eta$. We can use the fact that for all $\gamma, \eta \in \Gamma$ and any subgroup $G < \text{U}(d)$

$$\mathcal{P}_{\gamma,\eta} \mathcal{T}_G = \mathcal{P}_{\gamma,\eta} \mathcal{T}_G \mathcal{P}_{\gamma,\eta}, \quad (10)$$

which is trivial by using Schur's lemma. Hence, the following is true:

$$\mathcal{P}_{\gamma,\eta} \mathcal{T}(M) = \mathcal{P}_{\gamma,\eta} \mathcal{T}_{G_1} \mathcal{P}_{\gamma,\eta} \dots \mathcal{P}_{\gamma,\eta} \mathcal{T}_{G_\ell} \mathcal{P}_{\gamma,\eta}(M). \quad (11)$$

Let j be the index for which there is no non-trivial intertwiner between $\Pi_\gamma|_{G_j}$ and $\Pi_\eta|_{G_j}$ as required by the second condition. It is easy to see that $\mathcal{T}_{G_j}(X)$ is an intertwiner of the t -fold diagonal action of G_j for any linear operator X on $(\mathbb{C}^d)^{\otimes t}$. Furthermore, given that G_j is a subgroup of the unitary group, $P_\gamma \mathcal{T}_{G_j}(X) P_\eta$ is also an intertwiner for the same representation as the product of intertwiners is also an intertwiner. Given that $P_\gamma \mathcal{T}_{G_j}(X) P_\eta$ would be an intertwiner exactly between the subrepresentations $\Pi_\gamma|_{G_j}$ and $\Pi_\eta|_{G_j}$ (with multiplicities), it has to be zero by the second condition. Moreover, because of the linearity of the above equation, if it transforms into the zero map at any point it will stay zero after subsequent twirls.

Secondly, considering the case when $\gamma = \eta$, we can write Eq. (11) as

$$P_\gamma \mathcal{T}(M) P_\gamma = P_\gamma \mathcal{T}_{G_1} P_\gamma \dots \mathcal{T}_{G_\ell} P_\gamma(M). \quad (12)$$

By the first assumption in the Theorem, for each $\gamma \in \Gamma$, there exists a group G_j such that $\Pi_\gamma|_{G_j}$ is irreducible. Note that from Proposition 1 it follows that:

$$P_\gamma \mathcal{T}_{G_j}(X) = \mathbb{0} \oplus \frac{\text{Tr}_{\mathcal{H}_\gamma}(\mathcal{P}_\gamma(X))}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma}, \quad (13)$$

where X is any linear transformation on $(\mathbb{C}^d)^{\otimes t}$ and where we denoted the zero operator on the orthogonal complement of P_γ by $\mathbb{0}$.

As a consequence, it is clear that $\mathcal{P}_\gamma \mathcal{T}_{G_j} \mathcal{T}_{G_k} = \mathcal{P}_\gamma \mathcal{T}_{G_j}$ for $k = j+1, \dots, \ell$ since

$$\mathcal{P}_\gamma \mathcal{T}_{G_j} \mathcal{T}_{G_k}(X) = \mathbb{0} \oplus \frac{\int_{G_k} \text{Tr}_{\mathcal{H}_\gamma} \left([\mathbb{1}_{\mathcal{K}_\gamma} \otimes \Pi_\gamma(U)] \mathcal{P}_\gamma(X) [\mathbb{1}_{\mathcal{K}_\gamma} \otimes \Pi_\gamma(U)^\dagger] \right) dU}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma}, \quad (14)$$

where the integration is done over the Haar measure of G_k . The partial trace is cyclic on the vector space it is tracing over, i.e., $\mathcal{H}_\gamma$, and the operators on $\mathcal{K}_\gamma$ commute. Therefore this partial trace can be treated as cyclic to get

$$\mathcal{P}_\gamma \mathcal{T}_{G_j} \mathcal{T}_{G_k}(X) = \mathbb{0} \oplus \frac{\text{Tr}_{\mathcal{H}_\gamma}(\mathcal{P}_\gamma(X))}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma} = \mathcal{P}_\gamma \mathcal{T}_{G_j}(X). \quad (15)$$

Moreover, the twirlings $\mathcal{T}_{G_k}$ for $k = 1, \dots, j-1$ leave $\mathcal{T}_{G_j}(X)$ invariant, since the above operator is invariant to the adjoint action of any subgroup. More concretely, let $k \in \{1, \dots, j-1\}$. Then we can write for any linear transformation X on $(\mathbb{C}^d)^{\otimes t}$

$$\begin{aligned} \mathcal{P}_\gamma \mathcal{T}_{G_k} \mathcal{P}_\gamma \mathcal{T}_{G_j} \mathcal{P}_\gamma(X) &= \mathcal{P}_\gamma \mathcal{T}_{G_k} \left(\mathbb{0} \oplus \frac{\text{Tr}_{\mathcal{H}_\gamma}(\mathcal{P}_\gamma(X))}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma} \right) \\ &= \mathbb{0} \oplus \int_{G_k} (\mathbb{1}_{\mathcal{K}_\gamma} \otimes \Pi_\gamma(U)) \left(\frac{\text{Tr}_{\mathcal{H}_\gamma}(\mathcal{P}_\gamma(X))}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma} \right) (\mathbb{1}_{\mathcal{K}_\gamma} \otimes \Pi_\gamma(U))^\dagger dU \\ &= \mathbb{0} \oplus \frac{\text{Tr}_{\mathcal{H}_\gamma}(\mathcal{P}_\gamma(X))}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma}, \end{aligned} \quad (16)$$

hence, $\mathcal{P}_\gamma \mathcal{T}_{G_k} \mathcal{T}_{G_j} = \mathcal{P}_\gamma \mathcal{T}_{G_j}$. By combining this with the fact that

$$\mathcal{P}_\gamma \mathcal{T}_{G_j} \mathcal{T}_{G_k} = \mathcal{P}_\gamma \mathcal{T}_{G_j} \quad (k = j+1, \dots, \ell)$$

by Eq. (15), we get that

$$\mathcal{P}_\gamma \mathcal{T} = \mathcal{P}_\gamma \mathcal{T}_{G_j}. \quad (17)$$

As a result, one gets

$$\mathcal{T}(M) = \sum_{\gamma \in \Gamma} \frac{\text{Tr}_{\mathcal{H}_\gamma}(\mathcal{P}_\gamma(M))}{\dim \mathcal{H}_\gamma} \otimes \mathbb{1}_{\mathcal{H}_\gamma}. \quad (18)$$

which proves the Theorem by Proposition 1. $\square$

Theorem 1 enables us to search for examples of unitary t -designs using character theory. In particular, for some low-dimensional 2- and 3-design constructions a similar technique was used in Ref. [32]. To be explicit, given a finite unitary subgroup $G < \text{U}(d)$, one can examine if the representation labeled by the Young diagram γ with t boxes and at most d rows remains irreducible when restricted to G . Hence, one can search for a set of finite subgroups of $\text{U}(d)$ such that the first condition is fulfilled. For the second condition, consider two Young diagrams γ, η . When $\dim \Pi_\gamma \neq \dim \Pi_\eta$, consider $\dim \Pi_\gamma > \dim \Pi_\eta$ without loss of generality. By the first condition, there is a finite subgroup G for which the representation $\Pi_\gamma|_G$ remains irreducible, hence, the second condition is automatically fulfilled. When $\dim \Pi_\gamma = \dim \Pi_\eta$, further investigation is needed to verify that the representations are inequivalent when restricted to some finite subgroup G . To verify the irreducibility and inequivalence of the representations, the method described in Appendix B.1 is used. Using these methods, we have found the following examples of generalized group 4-designs in the GAP system (version 4.14.0) [33]:

Example 1 (A 6-dimensional 4-design). In this example, not all the groups are commonly referenced in the literature, hence, we employ the notation utilized within the GAP system to avoid ambiguity. Any of the 6-dimensional irreducible representations of the group "S3x6_1.U4(3).2_2" or the group "6.U6(2)M6" remain irreducible on the subspaces corresponding to $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$, $\begin{smallmatrix} \square & \square & \square \\ \square & \square & \square \end{smallmatrix}$, $\begin{smallmatrix} \square & \square & \square \\ \square & \square & \square \end{smallmatrix}$. Meanwhile, the 22nd irreducible representation of the group "2.J2" is irreducible when restricted to the subspace corresponding to $\begin{smallmatrix} \square & \square & \square \\ \square & \square & \square \end{smallmatrix}$. Finally, the irreps corresponding to $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$ and $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$ have the same dimension, but are inequivalent when restricted to the corresponding group, and thus, they also satisfy the second condition in Theorem 1.

Example 2 (A 12-dimensional 4-design). The Suzuki sporadic simple group Suz has a central extension of order 6 (denoted by "6.Suz" in GAP) which has an irreducible representation (the 153rd in GAP) which remains irreducible on the subspaces corresponding

to $\square\square\square, \square\square, \square$ and $\square$. Meanwhile, the standard representation of the alternating group on 13 elements is irreducible on the subspace corresponding to $\square$. Therefore, from these two unitary representations, a unitary 4-design can be constructed in 12 dimensions by Theorem 1.

Apart from the two examples presented so far, Theorem 1 can also be used to find other examples, e.g. for 3-designs. Without completeness, we present a few such examples here:

Example 3 (A 10-dimensional 3-design). The double cover of the Mathieu group M_{22} (denoted by 2.M22 in GAP) has a 10-dimensional representation which remains irreducible on subspaces corresponding to $\square$ and $\square$. Together with a 10-dimensional representation of the double cover of the Mathieu group M_{12} together with an outer automorphism of order 2 (denoted by 2.M12.2 in GAP) which remains irreducible on the subspace corresponding to $\square\square$. With these representations, a 10-dimensional 3-design can be constructed.

Example 4 (A 13-dimensional 3-design). The non-split double cover of the projective symplectic group $\text{PSp}_6(3)$ (denoted by 2.S6(3) in GAP) has a 13-dimensional representation which remains irreducible on subspaces corresponding to $\square\square$ and $\square$. Together with the standard representation of the alternating group on 14 elements, the concatenated product of these groups constitute a 13-dimensional 3-design.

Example 5 (A 18-dimensional 3-design). There is a central extension of the Janko group J_3 by a cyclic group of order 3 (denoted by 3.J3 in GAP) which has an 18-dimensional representation which is already a 3-design.

Note that in Examples 2–5, the dimensions of the subspaces are different, producing inequivalent representations on the subspaces.

4 Constructing 2-designs in arbitrary dimension

In prime power dimensions, the Clifford groups provide examples of unitary 2-designs [9, 10]. For arbitrary dimensions, an inductive construction for t -designs is provided in Ref. [30]. However, an explicit non-inductive construction for 2-designs is not known for every dimensions. In this section, we provide an explicit construction of generalized group 2-designs in arbitrary dimensions.

Lemma 1. *Consider a finite subgroup $G < \text{U}(d)$, and consider the defining representation of $\text{U}(d)$ restricted to this subgroup, denoted as $\Pi_{\square}|_G$. Suppose that the restriction of the representation $\Pi_{\square}$ to G remains irreducible, and that*

$$\Pi_{\square\square}|_G \cong \Pi_1 \oplus \Pi_2, \quad (19)$$

where Π_1 and Π_2 are two inequivalent irreducible representations of G , each also inequivalent to $\Pi_{\square}|_G$. Let P_1 and P_2 denote the corresponding projectors onto the subrepresentations Π_1 and Π_2 , respectively. Moreover, suppose that there exists $U \in \text{U}(d)$ such that

$$\text{Tr} \left(P_1^{U^{\otimes 2}} P_1 \right) = \frac{(\text{Tr} P_1)^2}{\text{Tr}(P_1 + P_2)}, \quad (20)$$

then the product $G^U \cdot G$ forms a unitary 2-design, where $G^U = \{UgU^\dagger \mid g \in G\}$.

Proof. Let $M \in (\mathbb{C}^{d \times d})^{\otimes 2}$ be an arbitrary matrix. The irreducible decomposition of $(\Pi_{\square}|_G)^{\otimes 2}$ is given by $\Pi_1 \oplus \Pi_2 \oplus \Pi_{\square}|_G$ and the projections to their supporting subspaces are denoted by $P_1, P_2, P_{\square}$, respectively. Twirling over G gives

$$M' := \mathcal{T}_G(M) = a_1 P_1 + a_2 P_2 + a_{\square} P_{\square}, \quad (21)$$

where $a_j := \frac{\text{Tr}(P_j M)}{\text{Tr}(P_j)}$ for $j \in \{1, 2, \square\}$. The second twirling yields

$$\mathcal{T}_{G^U}(M') = b_1 P_1^{U^{\otimes 2}} + b_2 P_2^{U^{\otimes 2}} + b_{\square} P_{\square}^{U^{\otimes 2}}, \quad (22)$$

where $b_j := \frac{\text{Tr}(P_j^{U^{\otimes 2}} M')}{\text{Tr}(P_j)}$ for $j \in \{1, 2, \square\}$. Since $P_{\square}^{U^{\otimes 2}} = P_{\square}$, their coefficients are the same $b_{\square} = a_{\square}$. Let $P_{\square\square} = P_1 + P_2$ denote the projection to the symmetric subspace, for which we also know that $P_{\square\square}^{U^{\otimes 2}} = P_{\square\square}$. Substituting $P_2 = P_{\square\square} - P_1$ into the expressions for the coefficients b_1 and b_2 , we find that b_1, b_2 are completely determined by the coefficients a_1, a_2 and the value of $\text{Tr}(P_1^{U^{\otimes 2}} P_1)$. The condition from Eq. (20) implies similar relations in the form of

$$\text{Tr}(P_i^{U^{\otimes 2}} P_j) = \frac{\text{Tr } P_i \text{Tr } P_j}{\text{Tr } P_{\square\square}} \quad (i, j = 1, 2). \quad (23)$$

This can be verified by

$$\text{Tr}(P_1^{U^{\otimes 2}} P_2) = \text{Tr}(P_1^{U^{\otimes 2}} P_{\square\square}) - \text{Tr}(P_1^{U^{\otimes 2}} P_1) = \text{Tr } P_1 - \frac{(\text{Tr } P_1)^2}{\text{Tr } P_{\square\square}} = \frac{\text{Tr } P_1 \text{Tr } P_2}{\text{Tr } P_{\square\square}}, \quad (24)$$

where we used the fact that $\text{Tr}(P_1^{U^{\otimes 2}} P_{\square\square}) = \text{Tr}(P_1) = d$. In a similar vein, we can show that

$$\text{Tr}(P_2^{U^{\otimes 2}} P_2) = \frac{(\text{Tr } P_2)^2}{\text{Tr } P_{\square\square}}. \quad (25)$$

The relation from Eq. (23) enables us to write the final coefficients as

$$b_1 = \frac{\text{Tr}(P_1^{U^{\otimes 2}} (a_1 P_1 + a_2 P_2))}{\text{Tr } P_1} = a_1 \frac{\text{Tr } P_1}{\text{Tr } P_{\square\square}} + a_2 \frac{\text{Tr } P_2}{\text{Tr } P_{\square\square}}, \quad (26a)$$

$$b_2 = \frac{\text{Tr}(P_2^{U^{\otimes 2}} (a_1 P_1 + a_2 P_2))}{\text{Tr } P_2} = a_1 \frac{\text{Tr } P_1}{\text{Tr } P_{\square\square}} + a_2 \frac{\text{Tr } P_2}{\text{Tr } P_{\square\square}} \stackrel{!}{=} b_1. \quad (26b)$$

As a result, we know that $b_1 = b_2 =: b_{\square\square}$, meaning that the second twirling results in a quantity that can be equivalently obtained using a unitary 2-design, i.e.,

$$\mathcal{T}_{G^U \cdot G}(M) = b_1 P_1 + b_2 P_2 + b_{\square} P_{\square} = b_{\square\square} P_{\square\square} + b_{\square} P_{\square}. \quad (27)$$

Therefore, using Proposition 1, the set $G^U \cdot G$ forms a unitary 2-design. $\square$

4.1 Monomial reflection group

The monomial reflection group $G(m, 1, d)$ is the group of $d \times d$ matrices with a single non-zero entry in each row and column, where the only possible values for the non-zero entries are the m -th root of unity. More generally, given p such that $p \mid m$, $G(m, p, d)$ is the subgroup of $G(m, 1, d)$ in which the product of the non-zero entries in each matrix is an $\frac{m}{p}$ -th root of unity. However, for the purposes of this paper, the group $G(3, 1, d)$ is sufficient. The group has also been utilized for randomized benchmarking in Ref. [34].

We know that $G(3, 1, d) \cong S_d \ltimes \mathbb{Z}_3^d$, since each element in $G(3, 1, d)$ can be completely characterized by

- an element in S_d corresponding to the places of the nonzero entries in the $d \times d$ matrix through its natural representation, and
- an element in $\mathbb{Z}_3^d$ (corresponding to the 3rd roots of unity in these entries).

The group product in $S_d \ltimes \mathbb{Z}_3^d$ is given by

$$(\omega_1, \alpha_1) \cdot (\omega_2, \alpha_2) = (\omega_1 \omega_2, \alpha_2 + \Gamma_{\text{nat}}(\omega_2) \alpha_1) \quad (\omega_1, \omega_2 \in S_d, \alpha_1, \alpha_2 \in \mathbb{Z}_3^d), \quad (28)$$

where Γ_{nat} is the natural representation of the symmetric group S_d defined by $\Gamma_{\text{nat}}(\omega) |j\rangle := |\omega(j)\rangle$.

In the following, we will consider the *natural representation* $\Gamma : G(3, 1, d) \cong S_d \ltimes \mathbb{Z}_3^d \rightarrow \text{GL}(d, \mathbb{C})$, defined as

$$\Gamma(\omega, \alpha) := \Gamma_{\text{nat}}(\omega) D(\alpha) \quad (\omega \in S_d, \alpha \in \mathbb{Z}_3^d), \quad (29)$$

where, as before, Γ_{nat} is the natural representation of the symmetric group S_d and

$$D(\alpha) := \bigoplus_{j=0}^{d-1} \zeta^{\alpha_j} \quad (30)$$

is the representation of $\mathbb{Z}_3^d$ with ζ being the principal 3rd root of unity. In this representation, the product of two elements is

$$\Gamma(\omega_1, \alpha_1) \Gamma(\omega_2, \alpha_2) = \Gamma_{\text{nat}}(\omega_1 \omega_2) D(\omega_2(\alpha_1)) D(\alpha_2) = \Gamma(\omega_1 \omega_2, \alpha_2 + \omega_2(\alpha_1)), \quad (31)$$

analogously to Eq. (28). The natural representation of the symmetric group decomposes into two irreducible representations; one of them is the trivial representation acting on the subspace spanned by the vector $\sum_{j=0}^{d-1} |j\rangle$. However, this subspace is not left invariant by $D(\alpha)$, making Γ irreducible.

Proposition 2. *Let $d \geq 2$. The 2-fold tensor power of the representation Γ has 3 non-trivial invariant subspaces, which we will denote by $V_1, V_2, V_{\square}$. Among these, $V_{\square}$ is the antisymmetric subspace, V_1 is spanned by the vectors $\{|j\rangle \otimes |j\rangle\}_{j=0}^{d-1}$ and V_2 is the complementary subspace of V_1 in the symmetric subspace $V_{\square\! \square}$.*

Proof. Trivially, V_1 is invariant under the action of $\Gamma \otimes \Gamma$. Hence, if we prove that the irreducible decomposition of the 2-fold tensor power of Γ consists of 3 inequivalent irreps, the rest of the statement follows trivially. To prove that $\Gamma \otimes \Gamma$ decomposes into three components, consider the character $\chi_{\Gamma \otimes \Gamma}$. We aim to show that $\langle \chi_{\Gamma \otimes \Gamma}, \chi_{\Gamma \otimes \Gamma} \rangle = 3$, i.e., $\Gamma \otimes \Gamma$ consists of three different irreducible components, resulting in 3 different irreducible characters. The character of Γ is

$$\chi_{\Gamma}(\Gamma_{\text{nat}}(\omega) D(\alpha)) = \sum_{j \in J(\omega)} \zeta^{\alpha_j}, \quad (32)$$

where $J(\omega)$ is the set of indices representing the fixed points of ω . With this equation, the inner product can be calculated as follows:

$$\begin{aligned} \langle \chi_{\Gamma^{\otimes 2}}, \chi_{\Gamma^{\otimes 2}} \rangle &= \langle \chi_{\Gamma}^2, \chi_{\Gamma}^2 \rangle = \frac{1}{|G(3, 1, d)|} \sum_{g \in G(3, 1, d)} \text{Tr}(\Gamma(g))^2 \overline{\text{Tr}(\Gamma(g))^2} \\ &= \frac{1}{d! 3^d} \sum_{\omega \in S_d} \sum_{\alpha \in \mathbb{Z}_3^d} \sum_{j, k \in J(\omega)} \sum_{\ell, m \in J(\omega)} \zeta^{\alpha_j + \alpha_k - \alpha_{\ell} - \alpha_m} \\ &= \frac{1}{3^d} \mathbb{E}_{\omega \in S_d} \left[\sum_{j, k, \ell, m \in J(\omega)} \sum_{\alpha \in \mathbb{Z}_3^d} \zeta^{\alpha_j + \alpha_k - \alpha_{\ell} - \alpha_m} \right]. \end{aligned} \quad (33)$$

It is clear that the innermost sum for fixed indices j, k, ℓ, m and fixed ω only depends on the equality of the indices $\{j, k\} = \{\ell, m\}$ as sets. We can write

$$\sum_{\alpha \in \mathbb{Z}_3^d} \zeta^{\alpha_j + \alpha_k - \alpha_\ell - \alpha_m} = \begin{cases} 3^d & \text{if } \{j, k\} = \{\ell, m\}, \\ 0 & \text{otherwise.} \end{cases} \quad (34)$$

Let $f(\omega) := |J(\omega)|$. Hence, for fix ω , we get the following:

$$\sum_{j, k, \ell, m \in J(\omega)} \sum_{\alpha \in \mathbb{Z}_3^d} \zeta^{\alpha_j + \alpha_k - \alpha_\ell - \alpha_m} = \sum_{\substack{j, k, \ell, m \in J(\omega) \\ \{j, k\} = \{\ell, m\}}} 3^d = \left(2f(\omega)^2 - f(\omega)\right) 3^d \quad (35)$$

Proceeding with Eq. (33), in order to evaluate the average over S_d , we define $\iota_j(\omega)$ to be the characteristic function of j being a fixed point of ω . Then, the number of fixed points can be written as $f(\omega) = \sum_{j=0}^{d-1} \iota_j(\omega)$. The expectation values of $f(\omega)$ and $f^2(\omega)$ are the following:

$$\mathbb{E}_{\omega \in S_d} \iota_j(\omega) = \frac{1}{d!} \sum_{\omega \in S_d} \iota_j(\omega) = \frac{(d-1)!}{d!} = \frac{1}{d}, \quad (36a)$$

$$\mathbb{E}_{\omega \in S_d} \iota_j(\omega) \iota_k(\omega) = \frac{(d-2)!}{d!} = \frac{1}{d(d-1)} \quad \text{for } j \neq k, \quad (36b)$$

$$\mathbb{E}_{\omega \in S_d} f(\omega) = \sum_{j=0}^{d-1} \mathbb{E}_{\omega \in S_d} \iota_j(\omega) = 1, \quad (36c)$$

$$\mathbb{E}_{\omega \in S_d} f^2(\omega) = \sum_{j, k=0}^{d-1} \mathbb{E}_{\omega \in S_d} \iota_j(\omega) \iota_k(\omega) = \sum_j \mathbb{E}_{\omega \in S_d} \iota_j(\omega) + \sum_{\substack{j, k=0 \\ j \neq k}}^{d-1} \mathbb{E}_{\omega \in S_d} \iota_j(\omega) \iota_k(\omega) = 2. \quad (36d)$$

Finally, the inner product of the character follows from Eq. (33) and Eq. (35), and can be calculated as

$$\langle \chi_{\Gamma^{\otimes 2}}, \chi_{\Gamma^{\otimes 2}} \rangle = \frac{1}{d!} \sum_{\omega \in S_d} \left(2f(\omega)^2 - f(\omega)\right) = 2 \cdot 2 - 1 = 3. \quad (37)$$

The only possible way to get 3 as the sum of positive integer squares is by three 1s, and hence, $\Gamma \otimes \Gamma$ decomposes into three inequivalent irreducible representations. $\square$

In the following sections, we will denote the irreducible representations appearing in $\Gamma^{\otimes 2}$ by $\Gamma_1, \Gamma_2, \Gamma_{\square}$, i.e.,

$$\Gamma^{\otimes 2} \cong \Gamma_1 \oplus \Gamma_2 \oplus \Gamma_{\square}. \quad (38)$$

4.2 Constructing generalized unitary 2-design

As a consequence of Schur's lemma, twirling over a finite unitary subgroup yields a quantity that depends on the irreducible subspaces of the subgroup. In this subsection, two consecutive twirlings are used to get the same result as twirling by the entire unitary group, resulting in an exact unitary 2-design by Proposition 1.

Theorem 2. *Let $d \geq 2$ and let $\mathcal{G}$ be the image of the representation Γ of the monomial reflection group $G(3, 1, d)$ and suppose that Q is a unitary matrix with the following property:*

$$\text{Tr} \left(P_1^{Q^{\otimes 2}} P_1 \right) = \frac{2d}{d+1}. \quad (39)$$

Then $\mathcal{G}^Q \cdot \mathcal{G}$ is a generalized unitary 2-design, where $\mathcal{G}^Q = \{QgQ^\dagger \mid g \in \mathcal{G}\}$.

Proof. Using that $\text{Tr } P_1 = d$ and $\text{Tr } P_{\square} = d(d+1)/2$, the statement is a trivial consequence of lemma 1. $\square$

Theorem 2 asserts the existence of a matrix Q which fulfills the relation given by Eq. (39). In the next part of this section, we construct a matrix that satisfies the required condition. The search for such a matrix follows the idea of defining the function

$$f : \text{U}(d) \rightarrow \mathbb{R} \quad (40)$$

$$U \mapsto \text{Tr} \left(P_1^{U^{\otimes 2}} P_1 \right), \quad (41)$$

whose maximum value is d , attained at the identity. The main idea is to find a matrix B such that $f(B) \leq 2d/(d+1)$, and then to search for the optimal matrix Q along a continuous path in $\text{U}(d)$ between the identity and B .

Let F denote the matrix of the (normalized) discrete Fourier transform (DFT), with matrix elements given by

$$F_{jk} = \frac{1}{\sqrt{d}} \exp \left(-\frac{2\pi i}{d} jk \right). \quad (42)$$

This is a well-known transformation, but it is difficult to connect with a continuous path to the identity which is also analytically tractable. In order to acquire a simpler matrix, we can transform the DFT matrix as follows:

$$B := \frac{1+i}{2} F + \frac{1-i}{2} F^\dagger, \quad (43)$$

which is real valued and its eigenvalues are ± 1 . Importantly, since $B^2 = \mathbb{1}$, we can give a parameterized path of unitaries that connects B to the identity in $\text{U}(d)$:

$$Q(t) := \exp(itB) = \cos(t)\mathbb{1} + i \sin(t)B. \quad (44)$$

According to the next proposition, the path $Q(t)$ will contain at least one specific matrix $Q(t^*)$ that satisfies Eq. (39). To keep this proposition compact, we define

$$q(d) := \begin{cases} 0, & d \equiv 1, 2, 4, 5 \pmod{8}, \\ \sqrt{d}, & d \equiv 7 \pmod{8}, \\ -\sqrt{d}, & d \equiv 3 \pmod{8}, \\ \sqrt{2d}, & d \equiv 0, 6 \pmod{8}. \end{cases} \quad (45)$$

Proposition 3. *The overlap of P_1 and $P_1^{Q(t)^{\otimes 2}}$ is given by the following formula:*

$$\text{Tr} \left(P_1 P_1^{Q(t)^{\otimes 2}} \right) = a(d) \sin^4(t) + b(d) \sin^2(t) + d, \quad (46)$$

where

$$a(d) := \frac{2d-1}{2} - \frac{2q(d)}{d} - \frac{\gcd(4, d)}{2d}, \quad (47a)$$

$$b(d) := -2(d-1) + \frac{2q(d)}{d}. \quad (47b)$$

The desired value $\frac{2d}{d+1}$ can be reached by a specific t given by

$$t = \pm \arcsin(\sqrt{x^*}) + k\pi, \quad k \in \mathbb{Z}, \quad (48a)$$

$$x^* = \frac{-b(d) - \sqrt{\Delta(d)}}{2a(d)}, \quad (48b)$$

with determinant $\Delta(d) = b(d)^2 - 4a(d)c(d)$ with $c(d) := d - \frac{2d}{d+1}$ the constant term in the 0-reduced quadratic polynomial.

Proof in Appendix A.

5 Constructing unitary designs from orthogonal designs

5.1 Orthogonal designs

The concept of a unitary t -design, which is based on the unitary group, may be naturally defined for other groups as well, see, e.g., Ref. [35]. For our purposes, the orthogonal group $O(d)$ will be of main concern.

Definition 3 (Orthogonal t -design). A finite set $\mathcal{V} \subset O(d)$ with weight function $w : \mathcal{V} \rightarrow [0, 1]$ is called a weighted orthogonal t -design if the following equation holds for any linear transformation M on $(\mathbb{C}^d)^{\otimes t}$:

$$\sum_{V \in \mathcal{V}} w(V) V^{\otimes t} M (V^{\otimes t})^\dagger = \int_{O \in O(d)} O^{\otimes t} M (O^{\otimes t})^\dagger dO, \quad (49)$$

where the integral on the right-hand side is taken over all elements in $O(d)$ with respect to the Haar measure. The number t is called the degree of the design.

In this section, let us use the notation

$$\begin{aligned} \mathcal{T}_{O(d)}^{(t)}(M) &:= \int_{O \in O(d)} O^{\otimes t} M (O^{\otimes t})^\dagger dO, \\ \mathcal{T}_{U(d)}^{(t)}(M) &:= \int_{U \in U(d)} U^{\otimes t} M (U^{\otimes t})^\dagger dU. \end{aligned} \quad (50)$$

Moreover, for a finite subset $\mathcal{V} \subset U(d)$ with weight function w , we define

$$\mathcal{F}_{\mathcal{V}}^{(t)}(M) := \sum_{U \in \mathcal{V}} w(U) U^{\otimes t} M (U^{\otimes t})^\dagger. \quad (51)$$

Here, we are considering approximate t -designs, since the main statement of this section holds in this general setting for $t \leq 3$. In this paper, we are considering approximate designs using the relative error as follows [36, 37].

Definition 4 (ϵ -approximate unitary t -design). We call a finite subset $\mathcal{V} \subset U(d)$ an ϵ -approximate unitary t -design for some $\epsilon > 0$ when

$$(1 - \epsilon) \mathcal{F}_{\mathcal{V}}^{(t)} \preceq \mathcal{T}_{U(d)}^{(t)} \preceq (1 + \epsilon) \mathcal{F}_{\mathcal{V}}^{(t)}, \quad (52)$$

where $\mathcal{A} \preceq \mathcal{A}'$ means that the $\mathcal{A}' - \mathcal{A}$ is a completely positive map.

Remark 2. The definition of ϵ -approximate unitary design can be generalized to ϵ -approximate orthogonal design naturally.

5.2 Representation theory of the orthogonal group

In this section, representation theoretic results are summarized, which are based on Appendix A of Ref. [38]. We denote by $\Pi_{\square}$ and $\Phi_{\square}$ the defining representations of the unitary group $U(d)$ and the orthogonal group $O(d)$, respectively, with respect to the standard basis $|j\rangle_{j=0}^{d-1}$. The representation $\Phi_{\square}$ can be embedded into $\Pi_{\square}$. The irreducible decomposition of $\Phi_{\square}^{\otimes 2}$ is the following [39]:

$$\Phi_{\square}^{\otimes 2} = \Phi_t \oplus \Phi_c \oplus \Phi_{\square}, \quad (53)$$

where Φ_t is the trivial representation acting on the subspace $\mathcal{W}_t$ spanned by

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \otimes |j\rangle. \quad (54)$$

The representations Φ_t, Φ_c and $\Phi_{\square}$ act on the subspaces $\mathcal{W}_t, \mathcal{W}_c$ and $\mathcal{W}_{\square}$, respectively, where $\mathcal{W}_c$ is the complementary subspace of $\mathcal{W}_t$ in $V_{\square}$. The projections to their subspaces are $P_t = |\psi\rangle\langle\psi|$, $P_c = P_{\square} - P_t$ and $P_{\square}$, respectively.

Let $\Pi_{\square}$ denote the defining representation of the unitary group $U(d)$. The irreducible decomposition of the third tensor power is

$$\Pi_{\square}^{\otimes 3} \cong \Pi_{\square\square\square} \oplus \Pi_{\square\square}^{\oplus 2} \oplus \Pi_{\square}, \quad (55)$$

where the underlying subspaces are denoted by $V_{\square\square\square}, V_{\square\square}, V_{\square}$. It is known that the subspace $V_{\square\square}$ supports two equivalent representations; hence, it can be written as $\tilde{V}_{\square\square} \otimes \mathbb{C}^2$ where the subspace $\tilde{V}_{\square\square}$ is the representation subspace and $\mathbb{C}^2$ is the multiplicity space. If we take the restriction of $\Pi_{\square}^{\otimes 3}$ to the orthogonal group $O(d)$, the prior two subspaces decompose into the following invariant subspaces:

$$V_{\square\square\square} = \mathcal{W}_{\square\square\square(0)} \oplus \mathcal{W}_{\square\square\square(1)}, \quad (56)$$

$$\tilde{V}_{\square\square} = \tilde{\mathcal{W}}_{\square\square(0)} \oplus \tilde{\mathcal{W}}_{\square\square(1)}, \quad (57)$$

where the traceless components are labeled by (0) and the traceful components are labeled with (1). The trace components correspond to d -dimensional representations. The irreducible decomposition of $\Phi_{\square}^{\otimes 3}$ is

$$\Phi_{\square}^{\otimes 3} \cong \Phi_{\square\square\square} \oplus \Phi_{\square\square}^{\oplus 2} \oplus \Phi_{\square} \oplus \Phi_{\square}^{\oplus 3}, \quad (58)$$

where $\Phi_{\square}^{\oplus 3}$ belongs to the subspace $\mathcal{W}_{\square\square\square(1)} \oplus \tilde{\mathcal{W}}_{\square\square(1)}^{\oplus 2}$. It is straightforward to see that the trace-component subspaces can be given by

$$\mathcal{W}_{\square\square\square(1)} = \text{span} \left\{ \sum_{j=0}^{d-1} (|kjj\rangle + |jkk\rangle + |jjk\rangle) \right\}_{k=0}^{d-1}, \quad (59)$$

$$\mathcal{W}_{\square\square\square(1)} \oplus \tilde{\mathcal{W}}_{\square\square(1)}^{\oplus 2} = \text{span} \left\{ \sum_{j=0}^{d-1} |kjj\rangle, \sum_{j=0}^{d-1} |jkk\rangle, \sum_{j=0}^{d-1} |jjk\rangle \right\}. \quad (60)$$

These facts are used to prove the statements of the following part of this paper.

5.3 Construction

In this section, a method is presented to construct a unitary 2- or 3-design from an orthogonal 2- or 3-design.

For the $t = 2$ and $t = 3$ cases, we give a relation between orthogonal t -designs and unitary t -designs. For technical reasons, we start with the $t = 2$ case:

Proposition 4. *Suppose that W is a unitary with the following property:*

$$\text{Tr} \left(P_t^{W^{\otimes 2}} P_t \right) = \frac{2}{d(d+1)}. \quad (61)$$

Twirling with the unitary group can be decomposed into two consecutive twirlings with the orthogonal group, i.e.,

$$\mathcal{T}_{\text{U}(d)}^{(2)} = \mathcal{T}_{\text{O}(d)^W}^{(2)} \circ \mathcal{T}_{\text{O}(d)}^{(2)}, \quad (62)$$

where $\text{O}(d)^W := \{WOW^\dagger : O \in \text{O}(d)\}$.

Proof. Using the notation from Section 5.2, the dimension of $\mathcal{W}_t$ is 1 and the dimension of $V_{\square}$ is $\frac{d(d+1)}{2}$. Based on the assumption Eq. (61) and Lemma 1, the proposition follows. $\square$

To show the existence of unitary W as assumed in Eq. (61), take the following diagonal matrix W :

$$W |j\rangle = \omega_{2d}^{j\alpha} |j\rangle \quad j = 0, \dots, d-1, \quad (63)$$

where $\omega_{2d} = \exp\left(\frac{2\pi i}{2d}\right)$ and α is the solution of the real equation

$$q(\alpha) = \left| \sum_{j=0}^{d-1} \omega_{2d}^{2\alpha j} \right|^2 = \frac{2d}{d+1}. \quad (64)$$

Although α is not explicit, we can use the fact that $q(0) = d^2$, $q(1) = 0$ and the continuity of q to efficiently find a solution of Eq. (64) for any dimension. To verify Eq. (61), with projection $P_t = |\psi\rangle\langle\psi|$, where $|\psi\rangle$ is defined as in Eq. (54), we show that

$$\begin{aligned} \text{Tr} \left(P_t^{W^{\otimes 2}} P_t \right) &= \text{Tr} \left(W^{\otimes 2} |\psi\rangle\langle\psi| \left(W^\dagger \right)^{\otimes 2} |\psi\rangle\langle\psi| \right)^2 = \left| \langle\psi| W^{\otimes 2} |\psi\rangle \right|^2 \\ &= \frac{1}{d^2} \left| \sum_{j,k=0}^{d-1} \langle j| W |k\rangle^2 \right|^2 = \frac{1}{d^2} \left| \sum_{j,k=0}^{d-1} \delta_{jk} \omega_{2d}^{2k\alpha} \right|^2 = \frac{1}{d^2} \left| \sum_{j=0}^{d-1} \omega_{2d}^{2\alpha j} \right|^2 = \frac{2}{d(d+1)}. \end{aligned} \quad (65)$$

Using the same unitary W , there is a similar connection between orthogonal and unitary 3-designs as well:

Proposition 5. *Let $d \geq 5$. For $t = 3$, twirling with the unitary group can be decomposed into two consecutive twirlings with the orthogonal group, i.e.,*

$$\mathcal{T}_{\text{U}(d)}^{(3)} = \mathcal{T}_{\text{O}(d)^W}^{(3)} \circ \mathcal{T}_{\text{O}(d)}^{(3)}, \quad (66)$$

where W is defined in Eq. (63).

Proof. In this proof, the notation as in Section 5.2 is used. The statement of the proposition follows by showing that the result of the twirlings with the defining and rotated representations of the orthogonal group coincides with twirling with the unitary group. To establish this, we verify that on the subspaces $\mathcal{W}_{\square\square(1)}$ and $\widetilde{\mathcal{W}}_{\square(1)}^{\oplus 2}$, the maps $\mathcal{T}_{\text{U}(d)}^{(3)}$ and $\mathcal{T}_{\text{O}(d)W}^{(3)} \circ \mathcal{T}_{\text{O}(d)}^{(3)}$ act identically. This follows from the fact that both actions can be expressed solely in terms of the Young projectors $P_{\square\square}, P_{\square}, P_{\square}$ together with the projectors onto the subspaces $\mathcal{W}_{\square\square(1)}$ and $\widetilde{\mathcal{W}}_{\square(1)}^{\oplus 2}$. We will show the effect of the twirlings with the different orthogonal group representations on one general element of the matrix acting on $\mathcal{W}_{\square\square(1)} \oplus \widetilde{\mathcal{W}}_{\square(1)}^{\oplus 2}$. Without loss of generality, let us consider the operator $\sum_{j,\ell=0}^{d-1} |jjk\rangle\langle m\ell\ell| \in \mathcal{W}_{\square\square(1)} \oplus \widetilde{\mathcal{W}}_{\square(1)}^{\oplus 2}$, and let $\mathbb{F}_{13}$ denote the flip between the first and third tensor components. It is known that the Bell state is invariant under the action of $(O \otimes O)$ for any $O \in \text{O}(d)$, i.e.,

$$(O \otimes O) \sum_{j=0}^{d-1} |jj\rangle = \sum_{j=0}^{d-1} |jj\rangle. \quad (67)$$

Using the statement of Proposition 4, one can show that the two consecutive orthogonal 3-twirlings give the same result as the unitary 3-twirling. The first 3-twirling gives

$$\begin{aligned} \mathcal{T}_{\text{O}(d)}^{(3)} \left(\sum_{j,\ell=0}^{d-1} |jjk\rangle\langle m\ell\ell| \right) &= \mathcal{T}_{\text{O}(d)}^{(3)} \left(\sum_{j,\ell=0}^{d-1} |jjk\rangle\langle \ell\ell m| \mathbb{F}_{13} \right) \\ &= \int_{O \in \text{O}(d)} (\mathbb{1} \otimes \mathbb{1} \otimes O) \sum_{j,\ell=0}^{d-1} (|jjk\rangle\langle \ell\ell m|) (\mathbb{1} \otimes \mathbb{1} \otimes O)^\dagger dO \mathbb{F}_{13} \\ &= \left(\sum_{j,\ell=0}^{d-1} (|jj\rangle\langle \ell\ell|) \otimes \frac{\delta_{km}}{d} \mathbb{1} \right) \mathbb{F}_{13}. \end{aligned} \quad (68)$$

A subsequent twirling with $\text{O}(d)^W$ yields

$$\begin{aligned} \mathcal{T}_{\text{O}(d)W}^{(3)} \left(\left(\sum_{j,\ell=0}^{d-1} (|jj\rangle\langle \ell\ell|) \otimes \frac{\delta_{km}}{d} \mathbb{1} \right) \mathbb{F}_{13} \right) &= \\ &= \left(\mathcal{T}_{\text{O}(d)W}^{(2)} \left(\sum_{j,\ell=0}^{d-1} (|jj\rangle\langle \ell\ell|) \right) \otimes \frac{\delta_{km}}{d} \mathbb{1} \right) \mathbb{F}_{13} \\ &= \left(\left(\mathcal{T}_{\text{O}(d)W}^{(2)} \circ \mathcal{T}_{\text{O}(d)}^{(2)} \right) \sum_{j,\ell=0}^{d-1} (|jj\rangle\langle \ell\ell|) \right) \otimes \frac{\delta_{km}}{d} \mathbb{1} \right) \mathbb{F}_{13} \\ &= \left(\mathcal{T}_{\text{U}(d)}^{(2)} \left(\sum_{j,\ell=0}^{d-1} (|jj\rangle\langle \ell\ell|) \right) \otimes \frac{\delta_{km}}{d} \mathbb{1} \right) \mathbb{F}_{13} \\ &= \left(\mathcal{T}_{\text{U}(d)}^{(3)} \circ \mathcal{T}_{\text{O}(d)}^{(3)} \right) \left(\sum_{j,\ell=0}^{d-1} |jjk\rangle\langle m\ell\ell| \right) \\ &= \mathcal{T}_{\text{U}(d)}^{(3)} \left(\sum_{j,\ell=0}^{d-1} |jjk\rangle\langle m\ell\ell| \right) \end{aligned} \quad (69)$$

In the last equality, we have exchanged the $\text{U}(d)$ - and $\text{O}(d)$ -integrals and used the Haar invariance to obtain a single integral over $\text{U}(d)$. Given that the action $\mathcal{T}_{\text{O}(d)W}^{(3)} \circ \mathcal{T}_{\text{O}(d)}^{(3)}$ gives

the same result as $\mathcal{T}_{U(d)}^{(3)}$ in the subspaces $V_{\square\square}, V_{\square\Box}, V_{\Box\Box}$ and in the subspaces $\mathcal{W}_{\square\square(1)}, \widetilde{\mathcal{W}}_{\square(1)}^{\oplus 2}$, the statement is proven. $\square$

Lemma 2. *Let $t \leq 3$. Consider an ϵ -approximate orthogonal t -design $\mathcal{V} \subset O(d)$. Then $\mathcal{V}^W \cdot \mathcal{V}$ is a $(2\epsilon + \epsilon^2)$ -approximate unitary t -design where $W \in U(d)$ is a concrete unitary described in Proposition 4.*

Proof. Note that throughout the proof we restrict to $t \leq 3$, although we keep the notation simply as t for readability. Since $\mathcal{V}$ is an ϵ -approximate orthogonal t -design, by definition we know that

$$(1 - \epsilon)\mathcal{F}_{\mathcal{V}}^{(t)} \preceq \mathcal{T}_{O(d)}^{(t)} \preceq (1 + \epsilon)\mathcal{F}_{\mathcal{V}}^{(t)}. \quad (70)$$

Our goal is to establish

$$(1 - 2\epsilon - \epsilon^2)\mathcal{F}_{\mathcal{V}^W \cdot \mathcal{V}}^{(t)} \preceq \mathcal{T}_{U(d)}^{(t)} \preceq (1 + 2\epsilon + \epsilon^2)\mathcal{F}_{\mathcal{V}^W \cdot \mathcal{V}}^{(t)}. \quad (71)$$

By Proposition 4 and Proposition 5, the unitary t -twirl decomposes as $\mathcal{T}_{U(d)}^{(t)} = \mathcal{T}_{O(d)W}^{(t)} \circ \mathcal{T}_{O(d)}^{(t)}$. Moreover, $\mathcal{F}_{\mathcal{V}^W \cdot \mathcal{V}}^{(t)} = \mathcal{F}_{\mathcal{V}^W}^{(t)} \circ \mathcal{F}_{\mathcal{V}}^{(t)}$. The inequalities in Eq. (70) also hold for $\mathcal{V}^W$ because conjugation by W preserves complete positivity and operator order. Since operator inequalities are preserved under left- and right-composition with completely positive maps, we obtain

$$\mathcal{T}_{U(d)}^{(t)} = \mathcal{T}_{O(d)W}^{(t)} \circ \mathcal{T}_{O(d)}^{(t)} \succeq (1 - \epsilon)\mathcal{T}_{O(d)W}^{(t)} \circ \mathcal{F}_{\mathcal{V}}^{(t)} \succeq (1 - \epsilon)^2 \mathcal{F}_{\mathcal{V}^W}^{(t)} \circ \mathcal{F}_{\mathcal{V}}^{(t)}, \quad (72a)$$

$$\mathcal{T}_{U(d)}^{(t)} = \mathcal{T}_{O(d)W}^{(t)} \circ \mathcal{T}_{O(d)}^{(t)} \preceq (1 + \epsilon)\mathcal{T}_{O(d)W}^{(t)} \circ \mathcal{F}_{\mathcal{V}}^{(t)} \preceq (1 + \epsilon)^2 \mathcal{F}_{\mathcal{V}^W}^{(t)} \circ \mathcal{F}_{\mathcal{V}}^{(t)}. \quad (72b)$$

The above inequalities give a strictly stronger lower bound than the one stated on the LHS of Eq. (71), while the corresponding upper bound coincides exactly with the RHS of Eq. (71). $\square$

As a special case, an exact orthogonal 2-design or 3-design yields an exact unitary 2-design or 3-design, respectively.

Theorem 3. *Let $t \leq 3$. Consider an orthogonal t -design $\mathcal{V} \subset O(d)$. Then there exists a unitary $W \in U(d)$ such that the set $\mathcal{V}^W \cdot \mathcal{V}$ forms a unitary generalized group t -design.*

Proof. Trivial based on Lemma 2 by taking $\epsilon \rightarrow 0$. $\square$

To showcase the use of Theorem 3, we present a number of examples. With GAP systems, it can be shown that several groups have orthogonal irreducible representations whose image constitutes a t -design with $t = 2$ or $t = 3$ (from several possible irreps, just one is selected). From these irreducible representations, exact unitary 2- or 3-designs can be constructed using Theorem 3. Since the Clifford group on four qubits forms a unitary 3-design in dimension 16, the example in the paper merely illustrates a direct application of the theorem.

6 Summary and Outlook

The current paper establishes the concept of a generalized group t -design and provides several construction methods. One such construction is enabled by Theorem 1, establishing a procedure for constructing a generalized group t -design using finite groups whose representations admit an easily verifiable property. Moreover, we mention some examples

Name of group in GAP	Index of irrep	Dimension	t
$(3^2:2 \times G_2(3)).2$	31	14	3
$(2 \times 2^{(1+8)}_+).08+(2)$	156	16	3
Co2	2	23	3
2.Co1	102	24	3
Isoclinic(2.F4(2).2)	92	52	3
2.U6(2)	2	22	2
S6(5)	2	63	2
Fi22	2	78	2
HN	2	133	2
Th	2	248	2

Table 1: Data extracted from GAP (group name, irrep index, dimension, and design degree t) for irreducible representations whose image yields orthogonal t -designs. (Wherever several possible irreps are available for our use, just one is selected.) These representations provide explicit examples that can be used in Theorem 3 to construct exact unitary 2- and 3-designs. All computations were carried out using GAP 4.14.0 [33].

of novel 3- and 4-design constructions using this procedure. Another notable construction is given in Theorem 2, which allows one to construct an explicit generalized group 2-design in arbitrary dimensions using the natural representation of the monomial reflection group. We have also described a method for converting orthogonal 2- or 3-designs into unitary designs in Theorem 3, together with several examples.

There is an abundance of possible research directions based on group representations and the ideas presented here. As a start, we plan to carry out a thorough search through the finite groups using the GAP system to identify cases where 5- or higher-degree-designs could be constructed using Theorem 1. On the more ambitious side, one could envision obtaining a construction for 3-designs for general dimensions in a similar way to Theorem 2. A further research direction is to examine the consequences of our 2- and higher-degree-design constructions in applications such as quantum process tomography, randomized benchmarking, and (thrifty) shadow estimation.

Acknowledgement

We thank David Amaro Alcalá for fruitful discussions. This research was supported by the Ministry of Culture and Innovation and the National Research, Development and Innovation Office (NKFIH) through the Quantum Information National Laboratory of Hungary (Grant No. 2022-2.1.1-NL-2022-00004), the AI4QT project Nr. 2020-1.2.3-EUREKA-2022-00029 and the Grant No. FK135220. The authors were also supported by the QuantERA project HQCC-101017733 and ZZ was partially supported by the Horizon Europe programme HORIZON-CL4-2022-QUANTUM-01-SGA via the project 101113946 OpenSuperQPlus100.

A Rotation of the d -dimensional irreducible representation of the monomial reflection group $G(3, 1, d)$

In this section, the proof of Proposition 3 is presented in detail. The first step describes the overlap of the projection P_1 and its rotation $P_1^{Q^{\otimes 2}}$ in terms of the matrix elements of Q :

Proposition 6. *Let P_1 be the projection onto the subspace spanned by $\{|j\rangle \otimes |j\rangle\}_{j=0}^{d-1}$. The trace of the product of P_1 and P_1 rotated by Q is given by the equation:*

$$\text{Tr}(P_1^{Q^{\otimes 2}} P_1) = \sum_{j,k=0}^{d-1} |\langle j|Q|k\rangle|^4 \quad (73)$$

Proof. By direct calculation, we get

$$\begin{aligned} \text{Tr}(P_1^{Q^{\otimes 2}} P_1) &= \sum_{\ell=0}^{d-1} \sum_{j=0}^{d-1} \sum_{k=0}^{d-1} \overbrace{\langle \ell\ell|jj\rangle}^{\delta_{\ell j}} \langle jj|Q^{\otimes 2}|kk\rangle \langle kk|Q^{\dagger\otimes 2}|\ell\ell\rangle \\ &= \sum_{j=0}^{d-1} \sum_{k=0}^{d-1} \langle jj|Q^{\otimes 2}|kk\rangle \langle kk|Q^{\dagger\otimes 2}|jj\rangle \\ &= \sum_{j,k=0}^{d-1} |\langle j|Q|k\rangle|^4. \end{aligned} \quad (74)$$

□

To proceed, let us introduce the notation

$$\tau_{jk} := \frac{2\pi jk}{d}, \quad (75)$$

for brevity. To obtain explicit formulas when we use Eq. (44) in Eq. (73), two quadratic Gauss sums have to be considered:

Proposition 7. *Using the previous notation, the following identities hold:*

$$\sum_{j=0}^{d-1} \sin(2\tau_{jj}) = \sum_{j=0}^{d-1} \sin\left(\frac{4\pi j^2}{d}\right) = q(d) := \begin{cases} 0, & d \equiv 1, 2, 4, 5 \pmod{8}, \\ \sqrt{d}, & d \equiv 7 \pmod{8}, \\ -\sqrt{d}, & d \equiv 3 \pmod{8}, \\ \sqrt{2d}, & d \equiv 0, 6 \pmod{8}, \end{cases} \quad (76)$$

$$\sum_{j,k=0}^{d-1} \cos(4\tau_{jk}) = \sum_{j,k=0}^{d-1} \cos\left(\frac{8\pi jk}{d}\right) = d \cdot \gcd(4, d), \quad (77)$$

where the function $q(d)$ is defined by Eq. (45).

Proof. We prove the two identities separately.

The sine diagonal-sum (Eq. (76)). Introducing the quadratic Gauss sum for any integer a and positive integer d :

$$g(a, d) := \sum_{j=0}^{d-1} e^{2\pi i \frac{aj^2}{d}}. \quad (78)$$

Then the function q can be written as

$$q(d) = \text{Im}(g(2, d)). \quad (79)$$

The following statements regarding Gauss sums follow from results in Ref. [40], in particular Equations (80)–(82). The quadratic Gauss sum can be evaluated for the case of $a = 1$:

$$\text{Im}(g(1, d)) = \begin{cases} 0 & \text{if } d \equiv 1, 2 \pmod{4}, \\ \sqrt{d} & \text{if } d \equiv 0, 3 \pmod{4}. \end{cases} \quad (80)$$

For odd d , the Gauss sum can be written as

$$g(2, d) = \epsilon_d \sqrt{d} (-1)^{\frac{d^2-1}{8}}, \quad (81)$$

where $\epsilon_d = 1$ if $d \equiv 1 \pmod{4}$ and $\epsilon_d = i$ if $d \equiv 3 \pmod{4}$. For odd d this results in the following

$$q(d) = \text{Im}(g(2, d)) = \begin{cases} 0 & \text{if } d \equiv 1, 5 \pmod{8}, \\ \sqrt{d} & \text{if } d \equiv 7 \pmod{8}, \\ -\sqrt{d} & \text{if } d \equiv 3 \pmod{8}, \end{cases} \quad (\text{for odd } d). \quad (82)$$

For even d , the greatest common divisor is $\gcd(2, d) = 2$. Using gcd reduction for even d we get

$$q(d) = \text{Im}(g(2, d)) = 2 \text{Im}(g(1, d/2)). \quad (83)$$

Using Eq. (80), for even d we acquire

$$q(d) = \begin{cases} 0 & \text{if } d \equiv 2, 4 \pmod{8}, \\ \sqrt{2d} & \text{if } d \equiv 0, 6 \pmod{8}, \end{cases} \quad (\text{for even } d). \quad (84)$$

Putting together the even and odd cases, we get Eq. (76).

The cosine double-sum (Eq. (77)). The double-sum can be written as the real part of an exponential sum:

$$\sum_{j,k=0}^{d-1} \cos\left(\frac{8\pi jk}{d}\right) = \text{Re}\left(\sum_{j,k=0}^{d-1} e^{2\pi i \frac{4jk}{d}}\right) = \text{Re}\left(\sum_{j=0}^{d-1} \sum_{k=0}^{d-1} e^{2\pi i \frac{(4j)k}{d}}\right). \quad (85)$$

For fixed j , the inner sum $\sum_{k=0}^{d-1} e^{2\pi i \frac{(4j)k}{d}} = d$ if $4j \equiv 0 \pmod{d}$ and equals 0 otherwise (geometric series). Thus the whole double sum equals

$$d \cdot \#\{j \in \{0, \dots, d-1\} : d \mid 4j\}. \quad (86)$$

The congruence $d \mid 4j$ has exactly $\gcd(4, d)$ solutions modulo d (indeed $4j \equiv 0 \pmod{d}$ if and only if j is a multiple of $d/\gcd(4, d)$, and there are $\gcd(4, d)$ residue classes of that form). This yields Eq. (77). $\square$

The preceding two propositions serve as a preliminary introduction to this Appendix. Their purpose is to prepare the ground for the proof of Proposition 3, which is the main objective of this section. We now present the proof of Proposition 3:

Proof of Proposition 3. The sum can be split into the diagonal values and the off-diagonal ones.

$$\sum_{j,k=0}^{d-1} |\langle j|Q(t)|k\rangle|^4 = \sum_{j,k=0}^{d-1} (Q(t)_{jk})^4 \quad (87)$$

$$= \sum_j^{d-1} (Q(t)_{jj})^4 + \sum_{\substack{j,k=0 \\ j \neq k}}^{d-1} (Q(t)_{jk})^4. \quad (88)$$

The elements of the matrix $Q(t)$ are

$$Q(t)_{jk} = \delta_{jk} \cos(t) + \frac{i}{\sqrt{d}} \sin(t) (\cos(\tau_{jk}) + \sin(\tau_{jk})), \quad (89)$$

where $\tau_{jk} = 2\pi jk/d$. The sum of all elements can be split into two different sums corresponding to the diagonal elements and the others.

$$\sum_{j,k=0}^{d-1} |Q(t)_{jk}|^4 = \sum_{j=0}^{d-1} |Q(t)_{jj}|^4 + \sum_{\substack{j,k=0 \\ j \neq k}}^{d-1} |Q(t)_{jk}|^4. \quad (90)$$

First, the first (diagonal) sum is expressed as

$$\sum_{j=0}^{d-1} |Q(t)_{jj}|^4 = \sum_{j=0}^{d-1} \left(\cos(t)^2 + \frac{1}{d} \sin(t)^2 (\cos(\tau_{jj}) + \sin(\tau_{jj}))^2 \right)^2 \quad (91)$$

$$= \sum_{j=0}^{d-1} \left(1 + \sin(t)^2 \overbrace{\left(\frac{1}{d} (\cos(\tau_{jj}) + \sin(\tau_{jj}))^2 - 1 \right)}^{\Theta_j} \right)^2 \quad (92)$$

$$= d + 2 \sin(t)^2 \sum_{j=0}^{d-1} \Theta_j + \sin(t)^4 \sum_{j=0}^{d-1} \Theta_j^2. \quad (93)$$

The second sum can be expressed as

$$\sum_{\substack{j,k=0 \\ j \neq k}}^{d-1} |Q(t)_{jk}|^4 = \frac{1}{d^2} \sin(t)^4 \sum_{\substack{j,k=0 \\ j \neq k}}^{d-1} |(\cos(\tau_{jk}) + \sin(\tau_{jk}))|^4. \quad (94)$$

The Eq (90) is a 2-degree polynomial in $\sin(t)^2$ with coefficients $a(d), b(d)$ and d . The following equations are used in the calculations:

$$(\cos(x) + \sin(x))^2 = 1 + \sin(2x), \quad (95a)$$

$$(\cos(x) + \sin(x))^4 = \frac{3}{2} + 2 \sin(2x) - \frac{1}{2} \cos(4x). \quad (95b)$$

The linear coefficient is

$$\begin{aligned} b(d) &= 2 \frac{1}{d} \sum_{j=0}^{d-1} (\cos(\tau_{jj}) + \sin(\tau_{jj}))^2 - 2 \sum_{j=0}^{d-1} 1 \\ &= \frac{2}{d} \sum_{j=0}^{d-1} (1 + \sin(2\tau_{jj})) - 2d \\ &= 2(1 - d) + \frac{2}{d} \sum_{j=0}^{d-1} \sin(2\tau_{jj}). \end{aligned} \quad (96)$$

The coefficient of $\sin(t)^4$ is

$$\begin{aligned}
a(d) &= \frac{1}{d^2} \sum_{j=0}^{d-1} \left((\cos(\tau_{jj}) + \sin(\tau_{jj}))^2 - d \right)^2 + \frac{1}{d^2} \sum_{\substack{j,k=0 \\ j \neq k}}^{d-1} (\cos(\tau_{jk}) + \sin(\tau_{jk}))^4 \\
&= \frac{1}{d^2} \sum_{j,k=0}^{d-1} (\cos(\tau_{jk}) + \sin(\tau_{jk}))^4 - \frac{2}{d} \sum_{j=0}^{d-1} (\cos(\tau_{jj}) + \sin(\tau_{jj}))^2 + d \\
&= \frac{1}{d^2} \sum_{j,k=0}^{d-1} \left(\frac{3}{2} + 2 \sin(2\tau_{jk}) - \frac{1}{2} \cos(4\tau_{jk}) \right) - \frac{2}{d} \sum_{j=0}^{d-1} (1 + \sin(2\tau_{jj})) + d \\
&= \frac{3}{2} + \frac{2}{d^2} \sum_{j,k=0}^{d-1} \sin(2\tau_{jk}) - \frac{1}{2d^2} \sum_{j,k=0}^{d-1} \cos(4\tau_{jk}) - 2 - \frac{2}{d} \sum_{j=0}^{d-1} \sin(2\tau_{jj}) + d \\
&= \frac{2d-1}{2} + \frac{2}{d^2} \overbrace{\sum_{j,k=0}^{d-1} \sin(2\tau_{jk})}^0 - \frac{1}{2d^2} \sum_{j,k=0}^{d-1} \cos(4\tau_{jk}) - \frac{2}{d} \sum_{j=0}^{d-1} \sin(2\tau_{jj}).
\end{aligned} \tag{97}$$

□

Proposition 8. Let $d \geq 2$ and let $a(d), b(d)$ be the coefficients in the displayed equation from Proposition 3:

$$\frac{2d}{d+1} = a(d) \sin^4 t + b(d) \sin^2 t + d, \tag{98}$$

so that with $x = \sin^2(t)$ we obtain the quadratic equation

$$f(x) = a(d)x^2 + b(d)x + c(d) = 0, \tag{99}$$

where $c(d) := d - \frac{2d}{d+1}$. Let $\Delta(d) := b(d)^2 - 4a(d)c(d)$. Then $\Delta(d) \geq 0$ and exactly one root of Eq. (99) lies in the interval $(0, 1)$. That root can be written in the form

$$x^* = \frac{-b(d) - \sqrt{\Delta(d)}}{2a(d)}, \tag{100}$$

and it satisfies $0 < x^* < 1$; conversely, any admissible solution for $\sin^2(t)$ is x^* .

Proof. We will prove three facts: (i) $f(0) = c(d) > 0$, (ii) $f(1) = a(d) + b(d) + c(d) < 0$, and (iii) $\Delta \geq 0$. The facts (i)–(iii) together imply there is exactly one real root in $(0, 1)$ and it is given by Eq. (100).

(i) *Positivity at 0.* Since the constant term is d , we have

$$c(d) = d - \frac{2d}{d+1} = \frac{d(d-1)}{d+1} > 0 \quad (\text{for } d \geq 2), \tag{101}$$

hence $f(0) = c(d) > 0$.

(ii) *Negativity at 1.* Compute $f(1) = a(d) + b(d) + c(d)$. Using the given explicit forms of $a(d)$ and $b(d)$ we get that

$$a(d) + b(d) = -\frac{2d-3}{2} - d \cdot \gcd(4, d) + \frac{2}{d}q(d) - \frac{2}{d}q(d) = -\frac{2d-3}{2} - d \cdot \gcd(4, d), \tag{102}$$

Hence, $f(1)$ is given by

$$\begin{aligned} f(1) &= a(d) + b(d) + c(d) = -\frac{2d-3}{2} - d \cdot \gcd(4, d) + \frac{d(d-1)}{d+1}. \\ &= \frac{3-d-2d(d+1) \cdot \gcd(4, d)}{2(d+1)} < 0 \quad \text{if } d \geq 2, \end{aligned} \quad (103)$$

since the numerator is less than 0 for any $d \geq 1$. As $f(x)$ is a quadratic polynomial, it can only contain one or two roots in the open interval $(0, 1)$.

(iii) *Discriminant and uniqueness.* We have already shown that there is at least one real root in $(0, 1)$; therefore $\Delta(d) > 0$ and there are real roots. Since $c(d) > 0$, the product of the two roots is $\frac{c(d)}{a(d)}$. Two cases occur depending on the sign of $a(d)$:

- If $a(d) > 0$, the parabola opens upwards. Then, the conditions $f(0) > 0$ and $f(1) < 0$ imply that the smaller root (the one with the minus sign in the standard formula) lies in the open interval $(0, 1)$. Concretely, the root in $(0, 1)$ has to be the one given by Eq. (100).
- If $a(d) < 0$, the parabola opens downward. In that case, the greater root has to be in the interval $(0, 1)$: the expression with the minus sign represents the greater root since $a(d) < 0$. Thus, the in-interval root can be written uniformly as

$$x^* = \frac{-b(d) - \sqrt{\Delta(d)}}{2a(d)}, \quad (104)$$

which coincides with Eq. (100).

Therefore, $t = \pm \arcsin(\sqrt{x^*}) + \pi k$ with some $k \in \mathbb{Z}$. □

B Recap of representation theory

The representation theory of finite and compact groups is a vast topic, and the interested reader is directed to [31, 41, 42, 43] for more thorough introductions. In this section, only the basic notions are presented.

In quantum theory, we are usually interested in operations that can be described by unitary matrices. Thus, every representation we encounter in this paper is a unitary representation, i.e., a representation $\Pi : G \rightarrow \text{U}(d)$. The dimension of the representation is the dimension of the underlying vector space $\mathbb{C}^d$ on which these matrices act, i.e., $\dim \Pi = d$.

Two unitary representations are considered the same (i.e., unitarily equivalent) if there is a unitary basis transformation that links them. In general, a group can have many different representations. Sometimes, one talks about *natural*, *standard* or *defining* representations when the representation is based on some native properties of the group itself. Thus, in the case of matrix groups such as $\text{U}(d)$, the defining representation is the representation when every unitary matrix in $\text{U}(d)$ is represented by itself.

To get a handle on representations, we usually turn to representations that are, in some sense, indivisible into smaller ones:

Definition 5 (Irreducible representation). A representation $\Pi : G \rightarrow \text{U}(d)$ is called *irreducible* (or irrep for short) if there is no non-trivial subspace in $\mathbb{C}^d$ such that every matrix $\Pi(g)$ leaves it invariant. That is, a non-trivial subspace $V \subset \mathbb{C}^d$ such that $\Pi(g)v \in V$ for all $g \in G$ and $v \in V$.

A nice property of unitary representations is the following:

Proposition 9. *Every unitary representation of any group G is completely reducible. That is, every unitary representation $\Pi : G \rightarrow \text{U}(d)$ can be written as the direct sum of irreducible representations. In such a direct sum decomposition we call the isotypic component of an irrep Π_γ the sum of all subrepresentations isomorphic to that given irrep.*

For example, if a unitary representation $\Pi : G \rightarrow \text{U}(d)$ splits up into four irreps, out of which two are isomorphic, then we have three isotypic components:

$$\Pi \cong \Pi_1 \oplus (\Pi_2 \oplus \Pi_2) \oplus \Pi_3. \quad (105)$$

This means, that the underlying vector space $\mathbb{C}^d$ splits into direct summands under the action of Π as:

$$\mathbb{C}^d \cong \mathbb{C}^{d_1} \oplus (\mathbb{C}^{d_2} \oplus \mathbb{C}^{d_2}) \oplus \mathbb{C}^{d_3} \cong \mathbb{C}^{d_1} \oplus (\mathbb{C}^2 \otimes \mathbb{C}^{d_2}) \oplus \mathbb{C}^{d_3}, \quad (106)$$

where on the right-hand side of the above equation we have used a simple transformation into tensor products.

Given two representations, one may ask about matrices that link them in a structure preserving way similar to how a matrix between two vector spaces preserves linearity.

Definition 6 (Intertwiner). Let $\Pi_1 : G \rightarrow \text{U}(d_1)$ and $\Pi_2 : G \rightarrow \text{U}(d_2)$ be two representations of the group G . A matrix $A \in \mathbb{C}^{d_1 \times d_2}$ is called an *intertwiner* or *G -homomorphism* if it has the following property for all group elements g :

$$\Pi_1(g)A = A\Pi_2(g). \quad (107)$$

There is a powerful lemma that gives the exact form of all such matrices in the case of irreducible representations:

Lemma 3 (Schur's lemma). *Given two irreducible representations $\Pi_1 : G \rightarrow \text{U}(d_1)$ and $\Pi_2 : G \rightarrow \text{U}(d_2)$ of the group G , all the possible intertwiners between them are:*

1. 0 if the two irreps are not equivalent,
2. $c\mathbb{1}$ for some $c \in \mathbb{C}$ if they are equivalent.

One way to construct new representations from existing ones is by taking the tensor product of two representations:

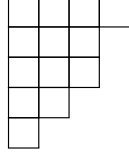
$$\begin{aligned} \Pi_1 \otimes \Pi_2 : G &\rightarrow \text{U}(d_1) \otimes \text{U}(d_2), \\ g &\mapsto \Pi_1(g) \otimes \Pi_2(g). \end{aligned} \quad (108)$$

These representations are usually not irreducible even if Π_1 and Π_2 were irreps. The decomposition of such representations into irreps is governed by so-called fusion rules, which are connected to the group structure.

Let us continue our discussion with the representation theory of the unitary group $\text{U}(d)$:

Proposition 10. *Every irreducible representation of the unitary group $\text{U}(d)$ that appears in the irrep decomposition of the t -fold tensor product of the defining representation can be labeled by a Young diagram of t boxes with at most d rows. These are known as tensor irreducible representations (tensor irreps).*

A Young diagram of t boxes and k rows is a collection of t boxes arranged in rows and columns that are left-justified such that the number of boxes in each row is non-increasing. For example, the following a Young diagram of 13 boxes in 5 rows:


(109)

It turns out that the label of the trivial representation is a Young diagram with zero boxes, whereas the label of the defining representation is a Young diagram with one box.

The fusion rules of the unitary group are governed by the following theorem:

Theorem 4. *Let Π_μ and Π_ν be tensor irreps of $U(d)$ labeled by Young diagrams μ and ν with at most d rows (their depth is at most d). Their tensor product decomposes as*

$$\Pi_\mu \otimes \Pi_\nu \cong \bigoplus_{\text{depth}(\lambda) \leq d} c_{\mu,\nu}^\lambda \Pi_\lambda, \quad (110)$$

where $c_{\mu,\nu}^\lambda$ are nonnegative integers called *Littlewood-Richardson coefficients*.

These coefficients are well-known in the literature or can be calculated using the Littlewood-Richardson rule. The two basic examples are the following:

$$\Pi_\square^{\otimes 2} \cong \Pi_\square \oplus \Pi_{\square\square}, \quad (111)$$

$$\Pi_\square^{\otimes 3} \cong \Pi_\square \oplus \Pi_{\square\square}^{\oplus 2} \oplus \Pi_{\square\square\square}. \quad (112)$$

The main topic of this article is unitary t -designs, that is, finite collection of unitaries that reproduce a t -fold average (or twirl) of the entire unitary group. The twirl operation, in general, means the following:

Definition 7. Let G be a compact group, and $\Pi : G \rightarrow U(d)$ be a unitary representation. Then, we define the twirl operation on a matrix $M \in \mathbb{C}^{d \times d}$:

$$\mathcal{T}(M) := \int_G \Pi(g) M \Pi(g)^\dagger dg, \quad (113)$$

where the integration is over the Haar measure of the compact group G .

For example in Eqs. (1) and (5), the twirling happens with the t -fold tensor product of the defining representation, that is, $U^{\otimes t}$.

A nice property of the twirl operation is that for any input matrix M the output $\mathcal{T}(M)$ is a matrix that commutes with every representant operator $\Pi(g)$, or, put differently, a special kind of intertwiner. In the cases of unitary t -designs, the output commutes with every unitary of the form $U^{\otimes t}$.

If the representation Π is irreducible, the output matrix is proportional to the identity due to Schur's lemma. The proportionality constant is $\text{Tr}(M)$. That is, we have a 1-design.

B.1 Recap of character theory

For a given finite group G , the representation theory is well explicable: There are exactly as many inequivalent irreps of G as the number of conjugacy classes in G . Based on this notion, any representation of G can be described by the multiplicities of the specific irreps.

Usually, it is hard to compute the irreducible decomposition of a specific representation of G , to handle this problem, character theory is used. The character can be defined for any representation of a group in the following way. In the following, we shall use Π and ρ , respectively, to differentiate between representations of the unitary group $U(d)$ and the finite group G .

Definition 8. The *character* of a representation ρ , denoted by χ_ρ , is defined as:

$$\chi_\rho(g) := \text{Tr}(\rho(g)), \quad g \in G. \quad (114)$$

The character χ_ρ is a *class function* on G , because it is constant in each conjugacy class due to the cyclicity of the operator trace. A character χ_ρ is *irreducible* if the representation ρ is irreducible.

Characters encode significant information about the representations of any group (even infinite) and are useful in distinguishing inequivalent representations or checking the irreducibility of a representation. The irreducible characters of a finite group G form a *character table* which encodes useful information about G in a compact form. The character table consists of n rows and n columns where n is the number of conjugacy classes of G . Each row corresponds to an irreducible character and each column to a conjugacy class. The elements are the values of a specific irreducible character on a specific conjugacy class. The character table also carries orthogonality properties.

The *inner product* of two class functions α, β of G is defined as

$$\langle \alpha, \beta \rangle := \frac{1}{|G|} \sum_{g \in G} \alpha(g) \overline{\beta(g)}. \quad (115)$$

Proposition 11 (Orthogonality relation 1.). *For any finite group G and its irreducible characters χ_i, χ_j the following holds:*

$$\langle \chi_i, \chi_j \rangle = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j. \end{cases} \quad (116)$$

In our research, we investigate finite subgroups of the unitary group, with particular focus on their behavior under tensor powers. Given any finite group G and a unitary representation ρ , the image of ρ can be thought of as a subgroup of $U(d)$. Therefore, in the following, we shall consider G a subgroup of $U(d)$ by ρ . Given the unitary group $U(d)$, we consider the t -fold tensor power of its defining representation, and analyze how its irreducible components decompose when restricted to a finite subgroup $G < U(d)$. For each irreducible component appearing in the tensor power representation (which are labeled by Young diagrams), we study the restriction to G and determine its decomposition into irreps of G . To compute this decomposition, we utilize the character table of G as well as its power map, which encodes how the powers of conjugacy classes map to other conjugacy classes. These tools allow us to determine precisely how a given representation of the full unitary group decomposes into irreducible components upon restriction to the finite subgroup.

Let G be a finite group with a representation ρ in d dimensions and γ be a Young diagram with t boxes in at most d rows. The irreducible decomposition of the representation ρ_γ of G which is the restriction of Π_γ to $\rho(G)$ can be calculated by taking the inner product of its character $\chi_\gamma(\cdot) = \text{Tr}(\rho_\gamma(\cdot))$ with each irreducible character χ_j . The inner product $\langle \chi_\gamma, \chi_j \rangle$ gives the multiplicity of the representation corresponding to χ_j in the

irreducible decomposition of ρ_γ . The character χ_γ can be calculated as

$$\chi_\gamma(g) = \frac{1}{t!} \sum_{\pi \in S_t} \gamma(\pi) \prod_{k=1}^t \chi_\rho(g^k)^{a_k(\pi)}, \quad (117)$$

where $\gamma(\pi)$ is the character of the irrep indexed by the Young diagram γ of the t -degree symmetric group S_t evaluated at permutation π and $a_k(\pi)$ is the number of cycles of length k in π . This result is derived from Theorem 2.7.9 in Ref. [44]. Using this equation, characters can be calculated using the GAP system for any specific group G and the irreducibility of the representation ρ_γ can be calculated. Thus, the conditions of Theorem 1 can be checked and compatible groups $G_1, \dots, G_\ell$ can be found.

References

- [1] Christoph Dankert. “Efficient Simulation of Random Quantum States and Operators” (2005). [arXiv:quant-ph/0512217](#).
- [2] Christoph Dankert, Richard Cleve, Joseph Emerson, and Etera Livine. “Exact and approximate unitary 2-designs and their application to fidelity estimation”. *Phys. Rev. A* **80** (2009).
- [3] A J Scott. “Optimizing quantum process tomography with unitary 2-designs”. *J. Phys. A* **41**, 055308 (2008).
- [4] Aidan Roy and A. J. Scott. “Unitary designs and codes”. *Des. Codes Cryptogr.* **53**, 13–31 (2009).
- [5] D. Gross, F. Krahmer, and R. Kueng. “A Partial Derandomization of PhaseLift Using Spherical Designs”. *J. Fourier Anal. Appl.* **21**, 229–266 (2014).
- [6] Joonwoo Bae, Beatrix C Hiesmayr, and Daniel McNulty. “Linking entanglement detection and state tomography via quantum 2-designs”. *New J. Phys.* **21**, 013012 (2019).
- [7] Daniel A Roberts and Beni Yoshida. “Chaos and complexity by design”. *J. High Energy Phys.* **2017**, 1–64 (2017).
- [8] Lorenzo Leone, Salvatore FE Oliviero, You Zhou, and Alioscia Hama. “Quantum chaos is quantum”. *Quantum* **5**, 453 (2021).
- [9] Joel J Wallman and Steven T Flammia. “Randomized benchmarking with confidence”. *New J. Phys.* **16**, 103032 (2014).
- [10] Mahnaz Jafarzadeh, Ya-Dong Wu, Yuval R Sanders, and Barry C Sanders. “Randomized benchmarking for qudit Clifford gates”. *New J. Phys.* **22**, 063014 (2020).
- [11] Hsin-Yuan Huang, Richard Kueng, and John Preskill. “Predicting many properties of a quantum system from very few measurements”. *Nat. Phys.* **16**, 1050–1057 (2020).
- [12] Senrui Chen, Wenjun Yu, Pei Zeng, and Steven T Flammia. “Robust shadow estimation”. *PRX Quantum* **2**, 030348 (2021).
- [13] Mirko Arienzo, Markus Heinrich, Ingo Roth, and Martin Kliesch. “Closed-form analytic expressions for shadow estimation with brickwork circuits”. *Quantum Inf. Comput.* **23**, 961–993 (2023).
- [14] Jonas Helsen and Michael Walter. “Thrifty Shadow Estimation: Reusing Quantum Circuits and Bounding Tails”. *Phys. Rev. Lett.* **131** (2023).
- [15] D. Gross, K. Audenaert, and J. Eisert. “Evenly distributed unitaries: On the structure of unitary designs”. *J. Math. Phys.* **48**, 052104 (2007).
- [16] Maxwell West, Diego García-Martín, N. L. Diaz, M. Cerezo, and Martin Larocca. “No-go theorems for sublinear-depth group designs” (2025). [arXiv:2506.16005](#).
- [17] Lorenzo Grevink, Jonas Haferkamp, Markus Heinrich, Jonas Helsen, Marcel Hinsche, Thomas Schuster, and Zoltán Zimborás. “Will it glue? on short-depth designs beyond the unitary group” (2025). [arXiv:2506.23925](#).
- [18] Hoi Fung Chau. “Unconditionally secure key distribution in higher dimensions by depolarization”. *IEEE Trans. Inf. Theory* **51**, 1451–1468 (2005).
- [19] Markus Heinrich, Martin Kliesch, and Ingo Roth. “Randomized benchmarking with random quantum circuits” (2023). [arXiv:2212.06181](#).
- [20] Zak Webb. “The Clifford group forms a unitary 3-design”. *Quantum Inf. Comput.* **16**, 1379–1400 (2015).
- [21] Huangjun Zhu. “Multiqubit Clifford groups are unitary 3-designs”. *Phys. Rev. A* **96**, 062336 (2017).

- [22] Richard Kueng and David Gross. “Qubit stabilizer states are complex projective 3-designs” (2015). [arXiv:1510.02767](#).
- [23] Eiichi Bannai, Gabriel Navarro, Noelia Rizo, and Pham Huu Tiep. “Unitary t -groups”. *J. Math. Soc. Jpn.* **72**, 909 – 921 (2020).
- [24] Matthew A Graydon, Joshua Skanes-Norman, and Joel J Wallman. “Clifford groups are not always 2-designs” (2021). [arXiv:2108.04200](#).
- [25] Fernando G. S. L. Brandão, Aram W. Harrow, and Michał Horodecki. “Local Random Quantum Circuits are Approximate Polynomial-Designs”. *Commun. Math. Phys.* **346**, 397–434 (2016).
- [26] Michał Oszmaniec, Adam Sawicki, and Michał Horodecki. “Epsilon-Nets, Unitary Designs, and Random Quantum Circuits”. *IEEE Trans. Inf. Theory* **68**, 989–1015 (2022).
- [27] Jonas Haferkamp. “Random quantum circuits are approximate unitary t -designs in depth $O\left(nt^{5+o(1)}\right)$ ”. *Quantum* **6**, 795 (2022).
- [28] P.D Seymour and Thomas Zaslavsky. “Averaging sets: A generalization of mean values and spherical designs”. *Adv. Math.* **52**, 213–240 (1984).
- [29] Ingemar Bengtsson and Karol Życzkowski. “Geometry of Quantum States: An Introduction to Quantum Entanglement”. *Cambridge University Press*. Cambridge, UK (2017). 2 edition.
- [30] Eiichi Bannai, Yoshifumi Nakata, Takayuki Okuda, and Da Zhao. “Explicit construction of exact unitary designs”. *Adv. Math.* **405**, 108457 (2022).
- [31] W. Fulton and J. Harris. “Representation Theory: A First Course”. *Graduate Texts in Mathematics*. Springer New York. Springer New York, NY (1991).
- [32] Ágoston Kaposi, Zoltán Kolarovszki, Adrian Solymos, Tamás Kozsik, and Zoltán Zimborás. “Constructing Generalized Unitary Group Designs”. *Pages 233–245*. Springer. (2023).
- [33] “GAP – Groups, Algorithms, and Programming, Version 4.14.0”. <https://www.gap-system.org>(2024).
- [34] David Amaro-Alcalá, Barry C Sanders, and Hubert de Guise. “Randomised benchmarking for universal qudit gates”. *New J. Phys.* **26**, 073052 (2024).
- [35] Giulio Chiribella, Giacomo Mauro D’Ariano, and Martin Roetteler. “Identification of a reversible quantum gate: assessing the resources”. *New J. Phys.* **15**, 103019 (2013).
- [36] Fernando GSL Brandao, Aram W Harrow, and Michał Horodecki. “Local random quantum circuits are approximate polynomial-designs”. *Comm. Math. Phys.* **346**, 397–434 (2016).
- [37] Thomas Schuster, Jonas Haferkamp, and Hsin-Yuan Huang. “Random unitaries in extremely low depth”. *Science* **389**, 92–96 (2025).
- [38] Adrian Solymos, Dávid Jakab, and Zoltán Zimborás. “Extendibility of Brauer states” (2024). [arXiv:2411.04597](#).
- [39] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman. “Real Randomized Benchmarking”. *Quantum* **2**, 85 (2018).
- [40] Bruce C Berndt, Ronald J Evans, and Kenneth S Williams. “Gauss and Jacobi sums”. *Wiley*. (1998).
- [41] Aleksandr A. Kirillov. “Elements of the Theory of Representation”. *Springer*. (1976).
- [42] Roe Goodman and Nolan R. Wallach. “Symmetry, Representations, and Invariants”. *Springer*. (2009).
- [43] Matthias Christandl. “The Structure of Bipartite Quantum States - Insights from Group Theory and Cryptography”. PhD thesis. University of Cambridge. (2006). [arXiv:quant-ph/0604183](#).

- [44] K. Lux and H. Pahlings. “Representations of Groups: A Computational Approach”. [Cambridge Stud. Adv. Math.](#) Cambridge University Press. Cambridge, UK (2010).