UNIVERSITY
OF OSLO

Master's thesis

Quantum Information, Twirling and Representation Theory

Jakob Lange

Mathematics
30 ECTS credits

Department of Mathematics
Faculty of Mathematics and Natural Sciences

Spring 2023

Jakob Lange

Quantum Information, Twirling and Representation Theory

Supervisor:
Sergey Neshveyev

Abstract

In this master thesis, we describe the general theory of unitary 2-designs, and construct the Clifford design. In the case of qubits, we additionally obtain an effective way of sampling operators from a unitary 2-design and show that in this case, the Clifford design is actually a unitary 3-design.

As a main result we show that any unitary 2-design, which is a group (in $\mathrm{PU}(\mathcal{H})$) and contains a nontrivial, normal abelian subgroup (in $\mathrm{PU}(\mathcal{H})$), is a Clifford design.

We also show how one can construct *asymptotic* unitary 2-designs that are optimal according to an earlier conjecture. Finally we show how one can construct sets of unitaries such that twirling a noisy channel by these, will transform the noise to a Pauli-channel.

Contents

List of Tables

Acknowledgements

I want to start by thanking my advisor Sergey Neshveyev for giving me an interesting problem to work on. He has been great to work with and has always patiently answered my questions, whether I asked him in person or over email. Studying representation theory has been a fun challenge and has helped me learn a lot in an area where I did not have much experience.

I enjoy Sergey's way of using various mathematical structures to clarify proofs, this is something I can learn a lot from. I also had a lot of fun during our meetings as he has great humour and many fun stories.

Secondly I want to thank Alexander Mueller Hermes for his difficult, but very interesting course on 'Quantum Information Theory' in spring 2022. Here he first mentioned that studying representation theory could be interesting in that context.

I also want to give a special thanks to my grandparents, Vagn and Birthe Lundsgaard Hansen, for helping me out with feedback on my thesis before it was in final form. This was a huge help.

I want to thank my beautiful partner in life Hanna for her company through the years. I hope for many more.

I want to thank all my fellow students, especially the ones I hung out with in NHA's 1101. We had some good times and I always appreciated the funny rants. Special thanks to Alexander Gjelsvik Ravnanger for always providing valuable feedback, and listening to me trying to explain various things I was confused about.

Lastly, I would like to thank all the professors whose classes I attended during my studies.

Introduction

This thesis delves into the concept of twirling in quantum information theory, specifically in relation to unitary t-designs. Twirling is a technique used to transform quantum channels into channels with more desirable properties, and has a wide range of applications including quantum cryptography ([Cha05]), error correction ([CB19]), and fidelity estimation ([Dan05]).

The focus of the thesis is on unitary t-designs, which are collections of unitary matrices that approximate the full group of unitary matrices in a certain way. The inherent symmetries in this approximation allows for representation theory to give a good description of the structure of unitary t-designs.

After a brief overview of the necessary mathematical preliminaries, we follow [GAE07] in a general description of the properties of unitary 2-designs. We also show that the Clifford bound holds for all designs coming from representations of groups.

Chapter 3 presents original research about the structure of unitary 2-designs from projective representations. We start out building intuition on the requirements for being a unitary 2-design from a particular representation. Following [GAE07], we construct the Clifford design, which is a standard design found in the literature.

We then investigate the relationship between unitary 2-designs and groups containing nontrivial normal abelian subgroups. Our main result shows that if a unitary 2-design is based on a projective representation of a group G containing a nontrivial, normal abelian subgroup K, then this design is equivalent to a Clifford design.

The result is new, and restricts the structure of non-Clifford designs from projective representations of groups, as it implies that such groups cannot contain nontrivial, normal solvable subgroups.

Going on, we follow [GAE07] in the construction of asymptotic unitary 2-designs and [Can+20] in the construction of a qubit design based on the projective linear group. We also show that for qubits, the Clifford design is actually a unitary 3-design.

In the final chapter, the thesis explores an application of twirling in fidelity estimation and shows how sets of unitaries can be obtained to convert noisy quantum channels to Pauli channels.

Chapter 1

Background

Before getting to the main part of the thesis, we need to cover some material that the reader might not be familiar with. We will assume that the reader is familiar with basics of functional analysis but not necessarily quantum mechanics / information theory or representation theory. If the reader is familiar with these topics this chapter can safely be skipped. We will have a quick section on notation which can be useful to read.

1.1 Notation

We will generally assume that $\mathcal{H}$ is a finite dimensional Hilbert space over $\mathbb{C}$ with $d = \dim(\mathcal{H})$. $B(\mathcal{H})$ and $\mathcal{U}(\mathcal{H})$ are the bounded and unitary operators on $\mathcal{H}$. $\mathcal{U}(d)$ the unitary operators on $\mathbb{C}^d$. G will usually be a finite group. The n-fold tensor product of $\mathbb{C}^d$ is denoted by $(\mathbb{C}^d)^{\otimes n}$. Similarly if $X \in \mathcal{H}$, $X^{\otimes n}$ denotes the n-fold tensor product of X. Qubits are unit vectors of $\mathbb{C}^2$ and the n-qubit space is $(\mathbb{C}^2)^{\otimes n}$. We will use *bra-ket* notation as this is common in quantum information theory. Using this we write $|v\rangle$ for $v \in \mathcal{H}$ and $\langle w|$ for $w^* \in \mathcal{H}^*$. We have $w^*(v) = \langle w|v\rangle$, and $|v\rangle\!\langle w| \in B(\mathcal{H})$ is the map $|u\rangle \mapsto \langle w|u\rangle\,|v\rangle$.

1.2 Bases and traces in different spaces

We will work a lot in the spaces $\mathcal{H}, B(\mathcal{H})$ and $B(B(\mathcal{H}))$. This section will give a brief overview of useful relations between these spaces. We have the *operator-vector correspondence*:

$$B(\mathcal{H}) \simeq \mathcal{H} \otimes \overline{\mathcal{H}}$$

via

$$|v\rangle\!\langle w| \mapsto |v\rangle \otimes |\overline{w}\rangle\,. \tag{1.1}$$

$B(\mathcal{H})$ is equipped with the *Hilbert-Schmidt* inner product

$$\langle X\,, Y\rangle_{B(\mathcal{H})} = \mathrm{Tr}\Big(XY^\dagger\Big)$$

turning $B(\mathcal{H})$ into a Hilbert space. For V, X, $W \in B(\mathcal{H})$ we set

$$V \cdot W^\dagger := (X \mapsto VXW).$$

The operator-vector correspondence above then extends to $B(B(\mathcal{H}))$,

$$B(B(\mathcal{H})) \simeq B(\mathcal{H}) \otimes \overline{B(\mathcal{H})}$$

via

$$V \cdot W \mapsto V \otimes \overline{W}. \tag{1.2}$$

For $\phi \in B(B(\mathcal{H}))$ we have

$$\operatorname{Tr}(\phi) := \sum_{i=1}^{\dim(\mathcal{H})^2} \langle \phi(e_i), e_i \rangle$$

where $\{e_i\}$ is an orthonormal basis with respect to $\langle \cdot, \cdot \rangle_{B(\mathcal{H})}$. This extends the inner product to $B(B(\mathcal{H}))$.

The inner products on $B(\mathcal{H})$ and $B(B(\mathcal{H}))$ can be used to decompose operators using the *Gram-Schmidt* procedure. We will usually skip the subscript and just write $\langle \cdot, \cdot \rangle$ since the context should make it clear which is being used.

1.3 Quantum mechanics/Information

A brief description of the necessary prerequisites is given here, more information can be found in [Wat18].

A quantum mechanical system is described by a Hilbert space ($\mathcal{H}$) usually referred to as a *state space*. The basic elements of interest are called *states*. States are described in one of two ways: either as unit vectors $|v\rangle \in \mathcal{H}$ or as *density operators* $\rho \in B(\mathcal{H})$. *Density operators* are just positive operators with trace 1. Unit vectors give rise to density operators in a natural way: $|v\rangle \mapsto |v\rangle\langle v|$. These states are called *pure states*. If a density operator ρ is not on this form, ρ is called a *mixed state*.

Given to systems $\mathcal{H}_A$ and $\mathcal{H}_B$ we can consider their *product space* $\mathcal{H}_A \otimes \mathcal{H}_B$. Let ρ_{AB} be a state on $\mathcal{H}_A \otimes \mathcal{H}_B$. If $\rho_{AB} = \rho_A \otimes \rho_B$ for some $\rho_A \in \mathcal{H}_A$, respectively $\rho_B \in \mathcal{H}_B$, ρ_{AB} is called a *product state*. If ρ_{AB} is a convex linear combination of product states, ρ_{AB} is called a *separable state*. If ρ_{AB} is not of this form, ρ_{AB} is an *entangled state*. Viewing states as unit vectors, we say a state is entangled if it does not have the form $|\psi\rangle \otimes |\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ for states $|\psi\rangle \in \mathcal{H}_A$, respectively $|\phi\rangle \in \mathcal{H}_B$.

Example 1.3.1 (Entangled states)
Let $\mathcal{H} = \mathbb{C}^d$ and $\{|i\rangle\}_{i=0}^{d-1}$ be an orthonormal basis for $\mathcal{H}$ (usually called *the computational basis for* $\mathcal{H}$). Then

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \left(\sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle \right),$$

and

$$|\Omega\rangle\langle\Omega| = \frac{1}{d} \sum_{i,j=0}^{d} |i\rangle\langle j| \otimes |i\rangle\langle j|,$$

are examples of entangled states. These are in fact *maximally entangled.* To understand what this means we need to develop the notion of *partial trace.*

Given systems $\mathcal{H}_A$, $\mathcal{H}_B$ and $\rho_{AB} \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$, the linear map $\operatorname{Tr}_B = \operatorname{id}_A \otimes \operatorname{Tr}$ is called the *partial trace on system B*. Similarly $\operatorname{Tr}_A = \operatorname{Tr} \otimes \operatorname{id}_B$ is the *partial trace on system A*. With $|\Omega\rangle\langle\Omega|$ as in Example 1.3.1, we see that both $\operatorname{Tr}_A(|\Omega\rangle\langle\Omega|)$ and $\operatorname{Tr}_B(|\Omega\rangle\langle\Omega|)$ equals $\frac{1}{d} I_d$. This characterises being *maximally entangled.*

Definition 1.3.2 (Maximally entangled state)
Given systems $\mathcal{H}_A, \mathcal{H}_B$ of dimensions d_A, d_B respectively and a *pure state* $|\psi\rangle\langle\psi| \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ we say that $|\psi\rangle\langle\psi|$ is *maximally entangled* if $\mathrm{Tr}_B(|\psi\rangle\langle\psi|) = \frac{1}{d_A} I_A$ and $\mathrm{Tr}_A(|\psi\rangle\langle\psi|) = \frac{1}{d_B} I_B$.

Maximally entangled states are related to unitary operators from $\mathcal{H}_B$ to $\mathcal{H}_A$ via an isomorphism similar to that in Equation (1.1). If $|\psi_{AB}\rangle\langle\psi_{AB}| \in B(\mathcal{H}_A \otimes \mathcal{H}_B)$ is maximally entangled, then there exists orthonormal bases $\{|v_i\rangle\}_{i=1}^d$ and $\{|w_i\rangle\}_{i=1}^d$ of $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively such that

$$|\psi_{AB}\rangle = \sum_{i=1}^{d} \lambda_i |v_i\rangle \otimes |w_i\rangle ,$$

where $|\lambda_i| = 1/\sqrt{d}$. It is then clear that

$$U_\psi = \sqrt{d} \sum_{i=1}^{d} \lambda_i |v_i\rangle\langle w_i| \tag{1.3}$$

belongs to $\mathcal{U}(\mathcal{H}_B, \mathcal{H}_A)$. On the other hand if $U \in \mathcal{U}(\mathcal{H}_B, \mathcal{H}_A)$ then U is an isometry and diagonal with respect so some orthogonormal bases of $\mathcal{H}_A, \mathcal{H}_b$. Hence the reverse map gives a vector corresponding to a maximally entangled state.

Recall that for finite dimensional Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ a linear map $T : B(\mathcal{H}_A) \mapsto B(\mathcal{H}_B)$ is called *completely positive* if for all $\mathcal{H}_C$, the map $\mathrm{id}_C \otimes T$ is positive. Now we describe how states are mapped between different spaces via *quantum channels*.

Definition 1.3.3 (Quantum channel)
Given Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, a *quantum channel* $T : B(\mathcal{H}_A) \mapsto B(\mathcal{H}_B)$ is a completely positive, trace preserving map.

A useful relation between $B(B(\mathcal{H}_A), B(\mathcal{H}_B))$ and $B(\mathcal{H}_A) \otimes B(\mathcal{H}_B)$ describing when maps are completely positive is the *Choi Jamiolkovski isomorphism*. Making use of the maximally entangled state $|\Omega\rangle\langle\Omega|$ in Example 1.3.1, the *Choi-matrix* of an operator $T : B(\mathcal{H}_A) \mapsto B(\mathcal{H}_B)$ is defined as

$$C_T := (\mathrm{id}_A \otimes T)(d_A |\Omega\rangle\langle\Omega|).$$

We see that this is an isomorphism since $T(|i\rangle\langle j|) = (\langle i| \otimes I_B) C_T (|j\rangle \otimes I_B)$. It is well known that C_T is positive if and only if T is completely positive.

1.3.1 Stabiliser measurement

Although the thesis does not deal directly with error correction, some constructions are closely related to the topic. To understand the relation, one needs to know what a *stabiliser measurement* is.

Let $U \in \mathcal{U}(\mathcal{H})$ with eigenvalues ± 1. For $|\psi\rangle \in \mathcal{H}$ we can write

$$|\psi\rangle = a |\psi_+\rangle + b |\psi_-\rangle ,$$

where $U |\psi_\pm\rangle = \pm |\psi_\pm\rangle$. We can use the $+1$ eigenspace of U for computing and the -1 space for detecting errors.

Let

$$H := \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \in B(\mathbb{C}^2),$$

and

$$CU := I \otimes |0\rangle\langle 0| + U \otimes |1\rangle\langle 1| \in B(\mathcal{H} \otimes \mathbb{C}^2).$$

We can attach an *ancillary* qubit $|0\rangle$ to our original state $|\psi\rangle$ and perform the operation

$$(I \otimes H)CU(I \otimes H)\,|\psi\rangle \otimes |0\rangle = a\,|\psi_+\rangle \otimes |0\rangle + b\,|\psi_-\rangle \otimes |1\rangle\,.$$

Measuring the second system ($\mathbb{C}^2$) in the computational basis collapses our state to either $|\psi_+\rangle$ or $|\psi_-\rangle$. If we measure $|0\rangle$ we do nothing and if we measure $|1\rangle$ we can perform error correction to get back to the $+1$ eigenspace of U. A thorough description of quantum error correction can be found in [Got97].

1.4 Representation theory

This section contains the basics of representation theory. All proofs can be found in [Eti+11].

A representation of a group G on a Hilbert space $\mathcal{H}$ is a homomorphism $\pi : G \mapsto B(H)$. A representation is called irreducible if the only invariant subspaces of $\mathcal{H}$ under $\pi(G)$ are $\{0\}$ and $\mathcal{H}$. If π_1, π_2 are representations of G on $\mathcal{H}_1, \mathcal{H}_2$ respectively, then $T \in B(\mathcal{H}_1, \mathcal{H}_2)$ is called an *intertwiner* if $\pi_2(g)T = T\pi_1(g)$ for all $g \in G$. *Schur's lemma* is a useful result stating that if $\mathcal{H}_2$ is irreducible then T is surjective and that if $\mathcal{H}_1$ is irreducible then T is injective.

A finite dimensional representation $\mathcal{H}$ is called *completely reducible* if $\mathcal{H} = \bigoplus_{j=1}^{k} \mathrm{n}_j\mathcal{H}_j$ where $\mathcal{H}_j$ are distinct irreducible representations of $\mathcal{H}$ and $\mathrm{n}_j\mathcal{H}_j = \bigoplus_{i=1}^{n_j} \mathcal{H}_j$.

Schur's lemma implies that if $\mathcal{H}$ is a completely reducible representation of G then the space of *intertwiners* is isomorphic to $\bigoplus_{j=1}^{k} \mathrm{Mat}_{n_j}(\mathbb{C})$. In particular, if all $n_j = 1$, any intertwiner is a linear combination of projections onto the irreducible subspaces of $\mathcal{H}$. Furthermore we have

$$\pi = \bigoplus_{j=1}^{k} n_j\pi_j, \qquad \pi_j = \pi|_{\mathcal{H}_j}. \tag{1.4}$$

Two representations $\mathcal{H}$, $\mathcal{H}'$ of a group G are *equivalent* if there is an isomorphism $T : \mathcal{H} \to \mathcal{H}'$ that is an intertwiner of G. Picking representatives $\mathcal{H}_i$ from the equivalence classes of irreducible representations of G we have the formula for the order of G,

$$|G| = \sum_i \dim(\mathcal{H}_i)^2. \tag{1.5}$$

The *character* $\mathcal{X}_\pi : G \to \mathbb{C}$ of a representation π is defined as

$$\mathcal{X}_\pi(g) := \mathrm{Tr}(\pi(g)).$$

From Equation (1.4) we have $\mathcal{X}_\pi = \bigoplus_j n_j\mathcal{X}_{\pi_j}$.

For representations π and ρ of a finite group G we have an inner product given by

$$\langle \mathcal{X}_\pi\,, \mathcal{X}_\rho\rangle := \frac{1}{|G|}\sum_{g\in G} \mathcal{X}_\pi(g)\overline{\mathcal{X}_\rho(g)}.$$

One checks that the characters $\mathcal{X}_{\pi_j}$ form an orthonormal basis for a Hilbert space. From the above discussion it then follows that

$$\langle \mathcal{X}_{\pi}, \mathcal{X}_{\pi} \rangle = \sum_{j=1}^{k} n_j^2. \tag{1.6}$$

Another important result which will be used is *Frobenius divisibility*. This result says that the dimension of an irreducible representation divides the order of G.

We will work with *unitary* and *projective* representations of groups as well. A *unitary* representation π is just a representation such that the operators $\pi(g)$ are unitary. It is well known, that any representation of a finite group is equivalent to a unitary representation. A *projective* representation of a group is a representation π such that

$$\pi(g)\pi(h) = c(g,h)\pi(gh)$$

where $c(g,h) \in \mathbb{C}$.

Chapter 2

Unitary t-designs

In this chapter we will introduce unitary t-designs and discuss various properties of these. Overall this section outlines the results in [GAE07] section 2, but rearranges the material and expands on a few results. Specifically we make an observation which shows that the *Clifford bound* holds for group designs. We start out by defining what a unitary t-design is, and then use representation theory to show some general results about designs from groups. We then restrict to the case $t = 2$ and after this prove some properties that hold for all designs, not only designs from groups.

Definition 2.0.1 (Unitary t-design)
A unitary t-design for d dimensions is a finite set $\mathcal{D} = \{U_j\}_{j=1}^{k} \subset \mathcal{U}(d)$ such that for any polynomial $p(U)$ of degree at most t in the elements of $U, U^\dagger$ we have the following equality:

$$\frac{1}{|\mathcal{D}|} \sum_{U \in \mathcal{D}} p(U) = \int_{U(d)} p(U) dU, \tag{2.1}$$

where dU denotes the Haar measure over the unitary group.

Defining $T_{U,t}(X) := \int_{U(d)} U^{\otimes t} \rho(U^\dagger)^{\otimes t}$ and $T_{\mathcal{D},t}(X) := \frac{1}{|\mathcal{D}|} \sum_{U \in \mathcal{D}} U^{\otimes t} \rho(U^\dagger)^{\otimes t}$ we see that the above definition is equivalent to

$$T_{\mathcal{D},t}(X) = T_{U,t}(X)$$

for all $X \in B(\mathcal{H})$.

2.1 Unitary designs and representation theory

We start out connecting unitary t-designs arising from groups to their irreducible subspaces and thus their characters. We then restrict ourselves to the case $t = 2$ and make some more generalisations here. We show how this can be used to search through databases and find designs for different t and dimensions d. If the reader is not familiar with representation theory the basics are covered in Section 1.4.

Given a finite group G and a representation $\pi(g) = U_g$, we can construct a design $\mathcal{D}_\pi = \{U_g\}_{g \in G}$. Consider then the representation $\rho(U) := U^{\otimes t}$, of the unitary group on $\mathcal{H} = (\mathbb{C}^d)^{\otimes t}$. Because of the unitary invariance of the Haar measure, $T_{U,t}(X)$ commutes with $\rho(U')$ for all $U' \in \mathcal{U}(\mathcal{H})$. If $\mathcal{D}_\pi$ is a unitary t-design this implies that for all $X \in B(\mathcal{H})$, $T_{\mathcal{D},t}(X)$ is an *intertwiner* of ρ. Thus $\mathcal{D}_\pi$ is a unitary t-design if and only if the representation $\pi_t(g) := \pi(g)^{\otimes t}$ decomposes into the same irreducible subspaces as ρ.

Schur-Weyl duality is an important result from representation theory that tells us exactly how $(\mathbb{C}^d)^{\otimes n}$ decomposes into irreducible subspaces with respect to ρ and a certain representation of the symmetric group S_t on $(\mathbb{C}^d)^{\otimes t}$. Given $\tau \in S_t$, it is not difficult to see that $\tau \mapsto \sigma_\tau$ defined by

$$\sigma_\tau(\bigotimes_{j=1}^{t} v_j) := \bigotimes_{j=1}^{t} v_{\sigma^{-1}(j)} \tag{2.2}$$

is a representation of S_t. *Schur-Weyl duality* then tells us that

$$(\mathbb{C}^d)^{\otimes t} = \bigoplus_\lambda V_\lambda \otimes W_\lambda$$

where V_λ, W_λ are irreducible subspaces under ρ and σ respectively. λ runs over the *Young tableaux* with no more than d rows, indexing the irreducible representations of S_t (for this thesis it is not important to know what these are). This implies in particular that the intertwiners of ρ are the operators σ_τ and vice versa. Also note that we get

$$(\mathbb{C}^d)^{\otimes t} = \bigoplus_\lambda \dim(W_\lambda) V_\lambda. \tag{2.3}$$

This leads to the following proposition:

Proposition 2.1.1 (t-designs and irreducible subspaces)
Let π be a representation of G on $\mathcal{H}$. Let $\pi_t(g) := \pi(g)^{\otimes t}$. Assume $t \leq \dim(\mathcal{H})$, then the following are equivalent:

1. *$\mathcal{D}_\pi$ is a t-design.*
2. *$\langle \mathcal{X}_{\pi_t}, \mathcal{X}_{\pi_t} \rangle = t!$.*
3. *$T_{\mathcal{D}_\pi,t}(X) \in span\{\sigma_\tau \mid \tau \in S_t\}$ for all $X \in B(\mathcal{H})$.*

Proof. The equivalence of 1 and 2 follows by Schur-Weyl duality since

$$\langle \mathcal{X}_{\pi_t}, \mathcal{X}_{\pi_t} \rangle = \sum_\lambda \dim(W_\lambda)^2 = |S_t| = t!, \tag{2.4}$$

using equations (1.6), (2.3), (1.5) and the fact that the spaces W_λ are representative of the irreducible representations of S_t.

The equivalence with 3 follows again from Schur-Weyl duality as the operators σ_τ are the intertwiners of ρ. ■

Remark 2.1.2. The previous proposition gives a useful way of finding group designs by searching through character tables. Further checking that $T_{\mathcal{D},t}(X)$ is in span $\{\sigma_\tau \mid \tau \in S_t\}$ is an 'easy' way of checking that $\mathcal{D}$ is a t-design. Point 3 in fact holds for any unitary 2-design, not just the ones from groups.

Corollary 2.1.3
Let π be a representation of G on $\mathcal{H}$. If $\mathcal{D}_\pi$ is a unitary t-design for some $t \in \mathbb{N}$, then π is irreducible.

Remark 2.1.4. If $\mathcal{D}_\pi$ is a t-design from a projective representation of a group, then *Schur's lemma* and the previous corollary tells us that the centraliser $Z(\mathcal{D}_\pi)$ of $\mathcal{D}_\pi$ is $\mathbb{C}I$. Picking representatives of $\mathcal{D}_\pi/Z(\mathcal{D}_\pi)$ is still a unitary 2-design, and thus we can in general assume that the representation is faithfull (in $\mathrm{PU}(\mathcal{H})$).

2.1.1 Searching through character tables

As mentioned, Proposition 2.1.1 gives a way of finding t-designs by searching through character tables. This can be done in a programmatic way using the GAP-system, which is also done in [GAE07]. Below is a list of 2-designs that were found in this way (although there are many more). For each dimension where a design was found we list the smallest found design.

Table 2.1: Designs for various dimensions of Hilbert spaces found using the GAP-system. *size* is the size of the group. *name* is the name of the group in the 'CTblLib'-package. *rep nr* is the number of the irreducible character in the character table.

dim	size	name	rep nr
2	24	2.L2(3)	5
3	168	L3(2)	2
4	3840	4_2.2^4:A5	17
5	3000	5^1+2.2A4	9
6	15120	6.A7	31
7	115248	7^(1+2).Sp(2,7)	19
8	80640	4_1.L3(4)	19
9	77760	3.ONM6	19
10	190080	2.M12	16
11	13685760	U5(2)	3
12	2690072985600	6.Suz	153
13	4585351680	S6(3)	2
14	87360	Sz(8).3	4
18	150698880	3.J3	22
21	27590492160	3.U6(2)	47
26	17971200	2F4(2)'	2
28	291852288000	2.Ru	37
41	65784756654489600	S8(3)	2
43	227787103272960	U7(2)	3
45	10200960	M23	3
342	1382446517760	3.ON	31
1333	86775571046077562880	J4	2

The method used to find the designs is as follows. First one obtains a list of all groups with character tables. Since characters must be irreducible we loop through the irreducible characters. Using that

$$\mathcal{X}_\pi \mathcal{X}_\pi = \mathcal{X}_{\pi\otimes\pi} = \mathcal{X}_{\pi_2},$$

we then check Equation (2.4). For $t = 2$ one does not need to consider the dimension of $\mathcal{H}$ when writing the code. However, for $t = 3$ it is well known that the symmetric subspace $\mathrm{Sym}^3(\mathbb{C}^2)$ is irreducible under ρ and one can then check that

$$(\mathbb{C}^2)^{\otimes 3} \simeq \mathrm{Sym}^3(\mathbb{C}^2) \oplus 2\mathbb{C}^2.$$

For a 3-qubit design arising from π we therefore have

$$\langle \mathcal{X}_{\pi_3}, \mathcal{X}_{\pi_3} \rangle = 5 \neq 3!$$

and thus the dimension needs to be considered for $t > 2$.

The author has written some code that shows how the table can be produced [Lan]. How the code is used is explained in the corresponding README.md file.

2.1.2 Unitary 2-designs arising from groups

We now restrict ourselves to the special case $t = 2$. First, for $X \in B(\mathcal{H})$, define $\mathrm{Ad}_X \in B(B(\mathcal{H}))$ by $\mathrm{Ad}_X(Y) := XYX^\dagger$. We then see that $\mathcal{D}$ being a unitary 2-design is equivalent to

$$\frac{1}{|\mathcal{D}|} \sum_{U \in \mathcal{D}} \mathrm{Ad}_{U^\dagger} \circ \phi \circ \mathrm{Ad}_U = \int_{\mathcal{U}(\mathcal{H})} \mathrm{Ad}_{U^\dagger} \circ \phi \circ \mathrm{Ad}_U dU \qquad \text{for all } \phi \in B(B(\mathcal{H})).$$

Following this we set

$$\widetilde{\phi}_{\mathcal{D}} := \frac{1}{|\mathcal{D}|} \sum_{U \in \mathcal{D}} \mathrm{Ad}_{U^\dagger} \circ \phi \circ \mathrm{Ad}_U, \tag{2.5}$$

and define $\widetilde{\phi}_{\mathcal{U}(\mathcal{H})}$ correspondingly.

It is not difficult to see that $U \mapsto \mathrm{Ad}_U$ is a representation of $\mathcal{U}(\mathcal{H})$ on $B(\mathcal{H})$, and it is well known that the irreducible subspaces of this representation are $\mathbb{C}I$ and

$$B(\mathcal{H})_0 := \{X \in B(\mathcal{H}) \mid \mathrm{Tr}(X) = 0\}.$$

Denoting by $\mathrm{Tr}(\cdot)$ the map, $X \mapsto \mathrm{Tr}(X)$, one can check that the operators

$$P_I := \frac{1}{d}\mathrm{Tr}(\cdot) \quad \text{and} \quad P_0 := \mathrm{id} - \frac{1}{d}\mathrm{Tr}(\cdot)$$

project onto the spaces $\mathbb{C}I$, $B(\mathcal{H})_0$ respectively. Observe that given a representation π, $\mathrm{Ad}_\pi(g) := \mathrm{Ad}_{\pi(g)}$ defines a representation on $B(\mathcal{H})$. We expand a theorem from [GAE07] which describes properties of 2-designs.

Theorem 2.1.5 (Group 2-designs)
Let G be a finite group and π a unitary representation of G on $\mathbb{C}^d$. Then the following are equivalent:

1. *$\mathcal{D}_\pi$ is a 2-design.*
2. *The irreducible subspaces of π_2 are the symmetric and asymmetric subspaces of $(\mathbb{C}^2)^{\otimes 2}$. The irreducible subspaces of Ad_π are $\mathbb{C}I$ and $B(\mathcal{H})_0$.*
3. *$T_{\mathcal{D},2}(X) \in span\left\{I, \sigma_{(12)}\right\}$ for all $X \in B(\mathcal{H})$. $\widetilde{\phi}_{\mathcal{D}} \in span\left\{\frac{1}{d}\mathrm{Tr}(\cdot), id\right\}$ for all $\phi \in B(B(\mathcal{H}))$.*
4. *$\langle \mathcal{X}_{\pi_2}, \mathcal{X}_{\pi_2} \rangle = \langle \mathcal{X}_{Ad_\pi}, \mathcal{X}_{Ad_\pi} \rangle = 2$.*
5. *The characters*

$$\mathcal{X}_S(g) := \frac{\mathcal{X}_\pi(g)^2 + \mathcal{X}_\pi(g^2)}{2}$$

$$\mathcal{X}_A(g) := \frac{\mathcal{X}_\pi(g)^2 - \mathcal{X}_\pi(g^2)}{2}$$

are irreducible.

The above equivalences then implies:

6. *π is irreducible.*
7. *$|\mathcal{D}_\pi|$ is divisible by d, $\frac{1}{2}d(d \pm 1)$ and $d^2 - 1$.*
8. *$|\mathcal{D}_\pi| \geq d^4 - d^2$.*
9. *For $d > 2$ π is not self-conjugate.*

Proof. The equivalence of 1, 2, 3 and 4 should be clear from the preceding discussion. 4 is equivalent to 5 since

$$\mathcal{X}_S + \mathcal{X}_A = \mathcal{X}_\pi^2 = \mathcal{X}_{\pi_2}.$$

6: This is Corollary 2.1.3.
7: We recall that the dimension of an irreducible subspace divides the order of a group. Since $\mathcal{H}$ is irreducible under π, d is a divisor. The dimensions of the symmetric and antisymmetric subspaces are $\frac{1}{2}d(d \pm 1)$ respectively so these must be divisors. Lastly $\dim(B(\mathcal{H})_0) = d^2 - 1$.
8: First we have that $|\mathcal{D}_\pi| \geq \dim(\mathbb{C}I)^2 + \dim(B(\mathcal{H})_0)^2 = 1 + (d^2-1)^2 = d^4 - 2d^2 + 2$. The smallest number that satisfies this bound and is divisible by $d^2 - 1$ is $d^4 - d^2$.
9: Observe that if π is irreducible and self-conjugate then

$$1 = \langle \mathcal{X}_\pi \,, \mathcal{X}_\pi \rangle = \frac{1}{|G|} \sum_{g \in G} \operatorname{Tr}(\pi(g))^2 = \langle \mathcal{X}_{\pi_2} \,, 1_G \rangle,$$

where 1_G is the trivial representation. Thus 1_G is a 1-dimensional irreducible subspace of π_2 but the dimensions of both the symmetric and antisymmetric subspaces are larger than 1 for $d > 2$. ■

Remark 2.1.6. If π is a projective representation, all statements in the theorem except 7 still hold. Note however that Ad_π is still a true representation in this case, so one could replace 7 by $|\mathcal{D}_\pi|$ is divisible by $d^2 - 1$.

Remark 2.1.7. Point 3 in the theorem is true for all unitary 2-designs, not just the ones based on groups.

In [GAE07] they pose the following conjecture:

Conjecture 2.1.8 (The Clifford bound)

$$d^4 - d^2$$

is a lower bound for the cardinality of any unitary 2-design.

Theorem 2.1.5 and Remark 2.1.6 show that this is in particular true for all designs based on *projective representations* of groups. The proof was based on using the representation Ad_π, instead of π_2 which is used in [GAE07]. The result might be known since the Ad_π representation is used in many other papers such as [Dan05], which introduced the term unitary t-design.

2.2 General unitary 2-designs

In this section we stray away from group-designs and answer some properties that hold for all unitary 2-designs. We prove a general lower bound on the size of a unitary 2-design. We then introduce a concept that relates the result of the characters found in the previous section, to the traces of matrices in any design. Even though we do not base these designs on groups, representation theory is fundamental to the proofs, due to the symmetries arising from twirling over the Haar measure.

2.2.1 A lower bound

We want to show that a lower bound on any unitary 2-design in dimension d is d^4-2d^2+2. We start with the following lemma.

Lemma 2.2.1
Under the representation $U \otimes V \mapsto Ad_{U\otimes V}$ of $\mathcal{U}(\mathcal{H}) \otimes \mathcal{U}(\mathcal{H})$, the Hilbert space $B(\mathcal{H} \otimes \mathcal{H})$ decomposes into irreducible subspaces in the following way:

$$B(\mathcal{H} \otimes \mathcal{H}) = (\mathbb{C}I \otimes \mathbb{C}I) \oplus (\mathbb{C}I \otimes B(\mathcal{H})_0) \oplus (B(\mathcal{H})_0 \otimes \mathbb{C}I) \oplus (B(\mathcal{H})_0 \otimes B(\mathcal{H})_0).$$

Proof. This follows from the fact that tensor products of irreducible representations are irreducible. ■

Before showing the lower bound from [GAE07], recall that for a d-dimensional Hilbert space we have the state $|\Omega\rangle$ defined by

$$|\Omega\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle \,.$$

Theorem 2.2.2
A lower bound on the size of a unitary 2-design in dimension d is

$$d^4 - 2d^2 + 2.$$

Proof. Let $\mathcal{H} = \mathbb{C}^d$ and for $U \in \mathcal{U}(\mathcal{H})$ set $|v_U\rangle := (I \otimes U)\,|\Omega\rangle$. Let $\mathcal{D}$ be a collection of unitaries and define $\phi \in B(B(\mathcal{H} \otimes \mathcal{H}))$ by

$$\phi(A) := \frac{1}{\mathcal{D}} \sum_{U \in \mathcal{D}} \langle v_U|A|v_U\rangle\, |v_U\rangle\!\langle v_U| \,.$$

Recalling the definition of a unitary 2-design one sees that $\mathcal{D}$ is a unitary 2-design if and only if

$$\phi(A) = \int_{\mathcal{U}(\mathcal{H})} \langle v_U|A|v_U\rangle\, |v_U\rangle\!\langle v_U| \,\mathrm{d}U.$$

Clearly $|\mathcal{D}| \geq \mathrm{rank}(\phi)$ and thus we compute $\mathrm{rank}(\phi)$ to get a lower bound on $\mathcal{D}$. One can check that

$$|v_U\rangle = (I \otimes U)\,|\Omega\rangle = (U^T \otimes I)\,|\Omega\rangle \,,$$

which implies that ϕ is an intertwiner of the representation $U \otimes V \mapsto \mathrm{Ad}_{U\otimes V}$. ϕ therefore projects onto the irreducible subspaces of this representation which are given in Lemma 2.2.1. By irreducibility, the intersection of each of these 4 subspaces with $\ker(\phi)$ is either trivial or the whole subspace. Clearly $\mathbb{C}I \otimes \mathbb{C}I$ has trivial intersection with $\ker(\phi)$. Then note that

$$\langle v_U|(X\otimes Y)|v_U\rangle = \langle\Omega|\,(X\otimes U^\dagger Y U)\,|\Omega\rangle = \mathrm{Tr}\Big(XU^\dagger Y^\dagger U\Big), \tag{2.6}$$

which shows that

$$(\mathbb{C}I \otimes B(\mathcal{H})_0) \oplus (B(\mathcal{H})_0 \otimes \mathbb{C}I) \subset \ker(\phi).$$

Now let V be any unitary s.t $\mathrm{Tr}(V) = 0$. Using (2.6) again we have

$$\mathrm{Tr}\Big(\phi(V\otimes V)(V\otimes V)^\dagger\Big) = \int_{\mathcal{U}(\mathcal{H})} |\langle v_U|V\otimes V|v_U\rangle|^2\,\mathrm{d}U > 0,$$

and thus the intersection of $B(\mathcal{H})_0 \otimes B(\mathcal{H})_0$ with $\ker(\phi)$ is trivial. This implies that $\mathrm{rank}(\phi) = d^4 - 2d^2 + 2$, and hence this is a lower bound for $|\mathcal{D}|$ as discussed. ■

2.2.2 Frame potential

In this short section we follow [GAE07] and define the *frame potential.* This gives an easy way of checking whether a collection of matrices is a unitary 2-design. First observe that for a character $\mathcal{X}_\pi$ of a representation of G we have:

$$\langle \mathcal{X}_{\pi_2}, \mathcal{X}_{\pi_2}\rangle = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Tr}(\pi(g))|^4 = \frac{1}{|G|^2}\sum_{g',g\in G}\Big|\mathrm{Tr}\Big(\pi(g')^\dagger\pi(g)\Big)\Big|^4.$$

Defining the *frame potential* of a design $\mathcal{P}(\mathcal{D})$ as

$$\mathcal{P}(\mathcal{D}) := \frac{1}{|\mathcal{D}|^2}\sum_{U_k,U_{k'}\in\mathcal{D}}|\mathrm{Tr}(U_k U_{k'})|^4,$$

it becomes clear that for a group design $\mathcal{P}(\mathcal{D}) = 2$.

Is this true in general? As shown in [GAE07], the answer is yes and the following theorem is proved.

Theorem 2.2.3
Let $\mathcal{D}$ be a finite collection of unitaries, $C_U, C_\mathcal{D}$ the Choi-matrices *of $T_{U,2}, T_{\mathcal{D},2}$. Then*

$$\mathcal{P}(\mathcal{D}) = 2 - \|C_U - C_\mathcal{D}\|_2^2. \tag{2.7}$$

In particular, $\mathcal{D}$ is a unitary 2-design if and only if $\mathcal{P}(\mathcal{D}) = 2$ which is also the smallest possible value for the frame potential of any finite collection of unitaries.

Proof. We compute $\|C_U - C_\mathcal{D}\|_2^2$:

$$\|\Delta\|_2^2 = \mathrm{Tr}\Big(C_U C_U^\dagger - C_U C_\mathcal{D}^\dagger - C_\mathcal{D}^\dagger + C_\mathcal{D} C_\mathcal{D}^\dagger\Big).$$

First we check that

$$\begin{aligned}\mathrm{Tr}\Big(C_\mathcal{D} C_\mathcal{D}^\dagger\Big) &= \frac{1}{|\mathcal{D}|^2}\sum_{i,j=1}^{d}\sum_{U,V\in\mathcal{D}}\mathrm{Tr}\Big(V^{\dagger\otimes 2}U^{\otimes 2}\,|i\rangle\langle j|\,U^{\dagger\otimes 2}V^{\otimes 2}\,|j\rangle\langle i|\Big)\\ &= \frac{1}{|\mathcal{D}|^2}\sum_{U,V\in\mathcal{D}}\Big|\mathrm{Tr}\Big(V^{\dagger\otimes 2}U^{\otimes 2}\Big)\Big|^2 = \mathcal{P}(\mathcal{D}).\end{aligned}$$

Letting P_s, P_a denote the projections on the symmetric and antisymmetric subspaces of $\mathbb{C}^d \otimes \mathbb{C}^d$, *Schur-Weyl duality* gives that

$$T_{U,2} = \frac{\langle \cdot\,, P_s \rangle}{\mathrm{Tr}(P_s)} + \frac{\langle \cdot\,, P_a \rangle}{\mathrm{Tr}(P_a)}.$$

Then

$$C_U = \frac{P_s \otimes P_s}{\mathrm{Tr}(P_s)} + \frac{P_a \otimes P_a}{\mathrm{Tr}(P_a)}$$

and hence $\mathrm{Tr}\Big(C_U C_U^\dagger\Big) = 2$.

Since P_s and P_a are intertwiners of $U \otimes U$ we have that

$$\mathrm{Tr}\Big(C_U C_{\mathcal{D}}^\dagger\Big) =$$
$$\frac{1}{\mathcal{D}} \mathrm{Tr}\left(\sum_{U \in \mathcal{D}} \sum_{i,j=1}^{d} \left(P_s \left|i\right\rangle\!\left\langle j\right| \otimes \frac{U^{\otimes 2} P_s \left|i\right\rangle\!\left\langle j\right| U^{\dagger\otimes 2}}{\mathrm{Tr}(P_s)} + P_a \left|i\right\rangle\!\left\langle j\right| \otimes \frac{U^{\otimes 2} P_a \left|i\right\rangle\!\left\langle j\right| U^{\dagger\otimes 2}}{\mathrm{Tr}(P_a)} \right)\right)$$
$$= \frac{1}{\mathcal{D}} \sum_{U \in \mathcal{D}} \left(\frac{\mathrm{Tr}(P_s)^2}{\mathrm{Tr}(P_s)} + \frac{\mathrm{Tr}(P_a)^2}{\mathrm{Tr}(P_a)} \right) = 2 = \mathrm{Tr}\Big(C_{\mathcal{D}} C_U^\dagger\Big).$$

From this we get

$$\mathcal{P}(\mathcal{D}) = 2 - \left\| C_U - C_{\mathcal{D}}^\dagger \right\|_2^2,$$

completing the proof. ∎

Remark 2.2.4. Since 2 is the minimal value this allows for numerical searches via optimising the frame potential.

Chapter 3

Designs from normal abelian subgroups

In this chapter we go through unitary 2-designs arising from nontrivial, normal abelian subgroups. We start out with a simple example to build some intuition. After the building of intuition we construct the *Clifford design* following [GAE07]. The intuition from the first part makes it clear exactly why this is a unitary 2-design. Finally we show that all unitary 2-designs containing normal abelian subgroups are in fact similar to the Clifford design. This result gives some new bounds on the order of group-designs for non-prime-power dimensional Hilbert spaces.

3.1 Building intuition from $\hat{A} \times A$

Throughout the chapter we let G be a finite group. A and K will both denote finite abelian groups. In general, the identity of these groups will be denoted by e. Recall that a *character* on A is a homomorphism $\mathcal{X} : A \to \mathbb{T}$, and let $\hat{A}$ be the group of *characters* on A. The identity of $\hat{A}$ is denoted by $\mathcal{X}_e$ and is the *trivial* character mapping all elements of A to $1 \in \mathbb{T}$.

Assume $\hat{A} \times A$ is a nontrivial, normal subgroup of G. A comes with a natural embedding $A \to G$ by $a \mapsto (\mathcal{X}_e, a)$. Similarly, $\hat{A}$ has a natural embedding $\hat{A} \to G$ by $\mathcal{X}_a \mapsto (\mathcal{X}_a, e)$. We will often identify elements by their images in G.

Set $\mathcal{H} := \ell^2(A)$ with an orthonormal basis $\{\delta_a \,|\, a \in A\}$. Assume that $\pi : G \mapsto B(\mathcal{H})$ is a projective unitary representation of G such that

$$\begin{aligned} \pi(a)\delta_b &= \delta_{a+b} \quad \text{for all } a, b \in A, \\ \pi(\mathcal{X}_a)\delta_b &= \mathcal{X}_a(b)\delta_b \quad \text{for } \mathcal{X}_a \in \hat{A},\, b \in A. \end{aligned}$$

If we assume G is a 2-design what can we then say about G?

It turns out that G is a unitary 2-design if and only if G acts transitively on $(\hat{A} \times A) \setminus \{(\mathcal{X}_e, e)\}$ via conjugation.

We can assume that

$$\pi|_{\hat{A}\times A}(\mathcal{X}_a, b) = \pi(\mathcal{X}_a)\pi(b).$$

We will drop the restriction label hoping that it will be clear from the context. We have

$$\pi(\mathcal{X}_x, y)\pi(\mathcal{X}_a, b)\delta_c = \mathcal{X}_a(b + c)\mathcal{X}_x(y + b + c)\delta_{y+b+c},$$

which implies that

$$\pi(\mathcal{X}_x, y)\pi(\mathcal{X}_a, b) = \mathcal{X}_x(b)\overline{\mathcal{X}_a(y)}\,\pi(\mathcal{X}_a, b)\pi(\mathcal{X}_x, y),$$

giving the commutator relation

$$\zeta(\pi(\mathcal{X}_x, y), \pi(\mathcal{X}_a, b)) = \mathcal{X}_x(b)\overline{\mathcal{X}_a(y)}. \tag{3.1}$$

We will use the following definition.

Definition 3.1.1 (Symplectic bicharacter)
Let K be a finite abelian group. A function

$$\zeta : K \times K \to \mathbb{T}$$

is a *bicharacter* if ζ is multiplicative in both arguments. ζ is *symplectic* if it is both *skew-symmetric* ($\zeta(k, k) = 1$ for all $k \in K$) and *nondegenerate* (both $\zeta(k, \cdot)$ and $\zeta(\cdot, k)$ are nontrivial characters for all $k \in K \setminus \{e\}$).

Setting $\zeta((\mathcal{X}_x, y), (\mathcal{X}_a, b)) := \zeta((\pi(\mathcal{X}_x, y), \pi(\mathcal{X}_a, b))$, this becomes a symplectic bicharacter on $\hat{A} \times A$. We also see that if $(\mathcal{X}_a, b) \neq (\mathcal{X}_e, e)$, then $\mathrm{Tr}(\pi(\mathcal{X}_a, b)) = 0$ which implies that $\pi(\hat{A} \times A)$ is an orthogonal basis for $B(\mathcal{H})$. This leads to the following definition.

Definition 3.1.2 (Weyl-type basis)
Let K be a finite abelian group. A *Weyl-type basis* for $B(\mathcal{H})$, is an orthogonal basis of the form $\{\pi(k)\}_{k\in K}$ for a projective representation $\pi : K \to B(\mathcal{H})$, such that for all $a, b \in K$, the *bicharater* ζ defined by

$$\pi(a)\pi(b) = \zeta(a, b)\pi(b)\pi(a)$$

is *symplectic.*

Recall from (2.5) that for $\phi \in B(B(\mathcal{H}))$ we set

$$\widetilde{\phi}_G = \frac{1}{|G|}\sum_{g\in G} \mathrm{Ad}_{\pi(g)} \circ \phi \circ \mathrm{Ad}_{\pi(g)^\dagger}.$$

We need the following lemma which describes a symmetry in Weyl-type bases.

Lemma 3.1.3
Assume $\pi(K)$ is a Weyl-type basis with symplectic bicharacter ζ, and that for some $a, b \in K$ we have a map $\phi \in B(B(\mathcal{H}))$ defined by

$$\phi(X) = \pi(a)X\pi(b)^\dagger.$$

Then we have

$$\widetilde{\phi}_K(X) = \delta_{a,b}\pi(a)X\pi(a)^\dagger.$$

Proof. Identifying ϕ via the isomorphism from Equation (1.2),

$$B(B(\mathcal{H})) \simeq B(\mathcal{H}) \otimes \overline{B(\mathcal{H})},$$
$$(X \mapsto \pi(a)X\pi(b)^\dagger) \mapsto \pi(a) \otimes \overline{\pi(b)},$$

$\widetilde{\phi}_K$ becomes

$$\frac{1}{|K|}\sum_{k\in K} \mathrm{Ad}_{\pi(k)}(\pi(a)) \otimes \overline{\mathrm{Ad}_{\pi(k)}(\pi(b))} = \frac{1}{|K|}\sum_{k\in K} \zeta(k,a)\pi(a) \otimes \overline{\zeta(k,b)\pi(b)}$$
$$= \frac{1}{|K|}\sum_{k\in K} \zeta(k,ab^{-1})\pi(a) \otimes \overline{\pi(b)} = \delta_{a,b}\pi(a) \otimes \overline{\pi(a)},$$

using that $\zeta(\cdot, ab^{-1})$ is a nontrivial character on K when $a \neq b$. Using the isomorphism in reverse direction completes the proof. ■

Recall from Theorem 2.1.5, that $\pi(G)$ being a unitary 2-design is equivalent to

$$\widetilde{\phi}_G \in \operatorname{span}\left\{\mathrm{id}, \mathrm{Tr}(\cdot)\frac{I}{d}\right\}. \tag{3.2}$$

We are now ready to prove the following.

Proposition 3.1.4 (Designs from Weyl-type bases)
Let K be a nontrivial, normal abelian subgroup of G. Assume π is a projective unitary representation of G, such that $\pi(K)$ is a Weyl-type basis. Then $\pi(G)$ is a unitary 2-design if and only if G acts transitively on $K \setminus \{e\}$ via conjugation.

Proof. We need to check Equation (3.2) for all $\phi \in B(B(\mathcal{H}))$. We can identify a basis for $B(B(\mathcal{H}))$ with elements $\pi(a) \otimes \overline{\pi(b)}$. Observe that twirling by G is the same as twirling by K and then by representatives of G/K. Using Lemma 3.1.3 we can therefore restrict ourselves to check twirling of the elements $\pi(a) \otimes \overline{\pi(a)}$.

Clever use of the *Choi-Krauss* isomorphism shows that for any orthogonal basis of unitaries $\mathcal{B}$ we have

$$\mathrm{Tr}(\cdot)\frac{I}{d} = \frac{1}{d^2}\sum_{U\in\mathcal{B}} \mathrm{Ad}_U \mapsto \frac{1}{d^2}\sum_{U\in\mathcal{B}} U \otimes \overline{U}. \tag{3.3}$$

Thus in particular this holds for the basis $\pi(K)$. Since K is normal in G, twirling an element $\pi(a) \otimes \overline{\pi(a)}$ by G we get

$$\sum_{g\in G} \mathrm{Ad}_{\pi(g)}(\pi(a)) \otimes \overline{\mathrm{Ad}_{\pi(g)}(\pi(a))} = \frac{|G|}{|[a]|}\sum_{a'\in[a]} \pi(a') \otimes \overline{\pi(a')}, \tag{3.4}$$

where $[a]$ is the conjugacy class of a. Using (3.3) it becomes clear that G is a unitary 2-design if and only if G acts transitively on $K \setminus \{e\}$ via conjugation. ■

Corollary 3.1.5
Given G, $\hat{A} \times A$ and π as described in the beginning of this section, $\pi(G)$ is a unitary 2-design if and only if G acts transitively on $(\hat{A}\times A)\setminus\{(\mathcal{X}_e, e)\}$ via conjugation. Furthermore

$$A \simeq \bigoplus_{i=1}^{n} \mathbb{Z}_p$$

for some prime p and $n \in \mathbb{N}$

Proof. For the first part we observe that $\pi(\hat{A} \times A)$ is a Weyl-type basis. For the second part transitivity of the action of G gives that all nontrivial elements of $\hat{A} \times A$ must have the same order. ∎

3.2 The Clifford design

The construction of the Clifford design in this section is almost the same as the representation of $\hat{A} \times A$ in the previous section. In this section we are, however, a bit more specific as to how the characters are constructed. This simplifies the construction of asymptotic designs satisfying the Clifford bound in Section 4.3. The construction follows that of [GAE07].

Let p be an odd prime, $d = p^j$ a prime power and $\mathbb{F}_d$ the field containing d elements. We can get a field extension $\mathbb{F}_{d^m}$ as an m-dimensional vector space over $\mathbb{F}_d$. For an element $a \in \mathbb{F}_{d^m}$ we have the *trace* defined by

$$\mathrm{Tr}_{\mathbb{F}_{d^m}/\mathbb{F}_d}(a) := \sum_{k=0}^{m-1} a^{d^k} \tag{3.5}$$

which takes values in $\mathbb{F}_d$ since a^{d^k} are the *Galois conjugates* of a in $\mathbb{F}_{d^m}$. The trace is $\mathbb{F}_d$-linear, and we get a nondegenerate $\mathbb{F}_d$-bilinear form

$$\langle a\,, b\rangle_{\mathbb{F}_{d^m}/\mathbb{F}_d} = \mathrm{Tr}_{\mathbb{F}_{d^m}/\mathbb{F}_d}(ab). \tag{3.6}$$

We can define a character (with respect to the additive structure) on $\mathbb{F}_d$ by

$$\mathcal{X}_d(a) := \exp\left(i\frac{2\pi}{p}\,\mathrm{Tr}_{\mathbb{F}_d/\mathbb{F}_p}(a)\right).$$

For this section we will set $V := \mathbb{F}_d^{2n}$ for some $n \in \mathbb{N}$. For $v \in V$ we will sometimes write

$$v = \begin{pmatrix} a \\ b \end{pmatrix} \qquad a, b \in \mathbb{F}_d^n.$$

With this notation, we can equip V with the *symplectic* bilinear form defined by

$$\left[\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a' \\ b' \end{pmatrix}\right] = \begin{pmatrix} a^T & b^T \end{pmatrix} \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \begin{pmatrix} a' \\ b' \end{pmatrix} = \sum_{j=1}^{n} (a_j b'_j - a'_j b_j). \tag{3.7}$$

From this we get a symplectic bicharacter ζ on V,

$$\zeta\left(\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a' \\ b' \end{pmatrix}\right) := \mathcal{X}_p\left(\left[\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a' \\ b' \end{pmatrix}\right]\right). \tag{3.8}$$

A matrix S is called *symplectic* if it satisfies

$$S^T \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} S = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}.$$

We denote the group of $2n \times 2n$ symplectic matrices over $\mathbb{F}_d$ by $\mathrm{Sp}(\mathbb{F}_d, n)$.

By checking Equation (3.7) and (3.8) one sees that the symplectic matrices are the automorphisms of V which preserve ζ.

Now consider $\mathcal{H} = \mathbb{C}^d$ with a basis $\{|j\rangle \mid j \in \mathbb{F}_d\}$, and define the operators

$$z_d(a)\,|b\rangle := \mathcal{X}_d(ab)\,|b\rangle \quad \text{and} \quad x_d(a)\,|b\rangle := |a+b\rangle\,.$$

This gives us the *Weyl operators*

$$w_d(a,b) := \mathcal{X}_d(-2^{-1}ab)z_d(a)x_d(a). \tag{3.9}$$

This makes sense on a 1-particle system and we can extend it to an n-particle system ($w_{d,n} \in B(\mathcal{H}^{\otimes n})$) via

$$w_{d,n}(a,b) := \bigotimes_{j=1}^{n} w_d(a_j, b_j) \quad a, b \in \mathbb{F}_d^n.$$

We will denote the set of these operators by $\mathcal{W}_{d,n}$. We get the relations

$$\begin{aligned} w_{d,n}(a,b)w_{d,n}(a',b') &= \zeta((a,b),(a',b'))w_{d,n}(a',b')w_{d,n}(a,b) \\ &= \mathcal{X}_d\left(2^{-1}\left[\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} a' \\ b' \end{pmatrix}\right]\right) w_{d,n}((a+a'),(b+b')) \end{aligned} \tag{3.10}$$

We observe that $w_{d,n}$ is really a projective representation of $\mathbb{F}_d^{2n}$, similar to the representation π of $\hat{A} \times A$ from Section 3.1. Since $\mathcal{W}_{d,n}$ is a Weyl-type basis, Proposition 3.1.4 tells us that the normaliser of $\mathcal{W}_{d,n}$ in $\mathrm{PU}(\mathcal{H}^{\otimes n})$ is a unitary 2-design. This is called the *Clifford group* and hence the name *Clifford design.* We will denote the *Clifford group* by $\mathcal{C}_{d,n}$.

Denoting by $\mathrm{Aut}(\mathcal{W}_{d,n}, \zeta)$ the automorphisms of $\mathcal{W}_{d,n}$ preserving ζ, we shall in the next section show that $\mathcal{C}_{d,n}/\mathcal{W}_{d,n} \simeq \mathrm{Aut}(\mathcal{W}_{d,n}, \zeta)$. Since the automorphisms are just the *symplectic matrices*, this tells us that $\mathcal{C}_{d,n}/\mathcal{W}_{d,n} \simeq \mathrm{Sp}(\mathbb{F}_d, n)$.

Based on this construction we define a *Clifford-type* design as follows.

Definition 3.2.1 (Clifford-type design)
A unitary 2-design is of *Clifford-type* if it is similar to the construction above. In other words, a design of Clifford-type is based on a faithful projective representation of $\mathbb{Z}_p^{2n}$, providing the symplectic bicharacter (3.7), and a subgroup of $\mathrm{Sp}(\mathbb{F}_p, n)$ acting transitively on $\mathbb{Z}_p^{2n} \setminus \{0\}$.

Remark 3.2.2. The coefficient $\mathcal{X}_d(-2^{-1}ab)$ for the Weyl-operators is chosen so that we get Equation (3.10). This gives us that $w_{d,n}(a,b)$ and $w_{d,n}(a',b')$ commute if and only if $w_{d,n}(a,b)w_{d,n}(a',b') = w_{d,n}(a+a', b+b')$. This makes the construction of stabiliser states in Section 4.1 a bit easier. Without this coefficient the commutator relation is still the same and everything continues to make sense for $p = 2$ so that the Clifford group is a unitary 2-design in this case as well. In fact, we shall in Section 4.5 show that in this case, the Clifford group is a unitary 3-design.

3.2.1 Reducing the size of the Clifford design

Picking $\tilde{d} = p^k$ and $\tilde{n}$ such that $\tilde{d}^{\tilde{n}} = d^n$ we see that the previous construction gives a family of unitary 2-designs in dimension d^n. One can show that if $\tilde{n} < n$ then

$$|\mathrm{Sp}(\mathbb{F}_{\tilde{d}}, \tilde{n})| < |\mathrm{Sp}(\mathbb{F}_d, n)| \quad \text{but} \quad \left|\mathcal{W}_{\tilde{d},\tilde{n}}\right| = |\mathcal{W}_{d,n}|.$$

Since the size of the twirling set is $|\mathrm{Sp}(\mathbb{F}_d, n)||\mathcal{W}_{d,n}|$ it follows that we reduce the size by going from $(\mathbb{C}^d)^{\otimes n}$ to $\mathbb{C}^{d^n}$. In [GAE07] they give the sizes

$$|\mathrm{Sp}(\mathbb{F}_p, n)| = O(p^{2n^2+n}),$$
$$|\mathrm{Sp}(\mathbb{F}_{p^n}, 1)| = p^n(p^{2n} - 1) = O(p^{3n}),$$

which shows that this is an exponential reduction in size from worst to best case. However, these examples still do not meet the Clifford bound.

It is not difficult to see that the subgroup of $\mathrm{Sp}(\mathbb{F}_2, 1)$

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}$$

acts transitively on $\mathbb{F}_2^2 \setminus \{0\}$ thereby providing a unitary 2-design of order 12 in 2 dimensions satisfying the Clifford bound.

In [Cha05] it is shown that subgroups satisfying the Clifford bound can also be found in dimensions $3, 5, 7$ and 11. In the same paper it is also shown that for $n > 1$ such subgroups of $\mathrm{Sp}(\mathbb{F}_{p^n}, 1)$ cannot be found.

To reduce the size one can look for subgroups of $\mathrm{Sp}(\mathbb{F}_p, n)$ smaller than $\mathrm{Sp}(\mathbb{F}_{p^n}, 1)$ that acts transitively on nonzero elements. It is not known whether such subgroups exist in general, but in [GAE07] they list the generators for such a subgroup of $\mathrm{Sp}(\mathbb{F}_3, 2)$ of order 160. Since $|\mathrm{Sp}(\mathbb{F}_9, 1)| = 720$ this is a good reduction.

3.3 Group 2-designs containing normal abelian subgroups

In this section, we generalise the results of the previous section to prove that if G is a unitary 2-design and G contains a normal nontrivial abelian subgroup, then G is a *Clifford-type design.*

We begin by recalling the definition of a 2-cocycle belonging to $\mathsf{Z}^2(K, \mathbb{T})$.

Definition 3.3.1 (2-cocycle $c \in \mathsf{Z}^2(K, \mathbb{T})$)
A 2-cocycle is a function $c : K \times K \to \mathbb{T}$ satisfying

$$c(gh, k)c(g, h) = c(g, hk)c(h, k) \quad \text{for all } g, h, k \in K. \tag{3.11}$$

We have the following proposition, adapted from [Kar80], connecting symplectic bicharacters to the second cohomology group $\mathsf{H}^2(K, \mathbb{T})$.

Proposition 3.3.2 (Yamazaki (1964a))
For $c \in \mathsf{Z}^2(K, \mathbb{T})$, define the skew-symmetric bicharacter ζ_c by

$$\zeta_c(g, h) := c(g, h)\overline{c(h, g)}.$$

The corresponding map, $[c] \mapsto \zeta_c$, defines an isomorphism between $\mathsf{H}^2(K, \mathbb{T})$ and the group of skew-symmetric bicharacters.

We now show how faithful irreducible projective representations are connected to symplectic bicharacters.

Theorem 3.3.3
There is a 1-1 correspondence between the set of faithful irreducible projective representations $\pi : K \to \mathrm{PU}(\mathcal{H})$ and the set of symplectic bicharacters on K.

Proof. We start by showing that each symplectic bicharacter ζ gives a faithful irreducible projective representation π. By Proposition 3.3.2, there exist $c \in \mathsf{Z}^2(K, \mathbb{T})$ such that $\zeta(a,b) = c(a,b)\overline{c(b,h)}$. This gives us the *twisted group algebra* $\mathbb{C}_a K$ with the multiplicative structure

$$a \cdot_c b = c(a,b)ab.$$

We can assume that $c(a,1) = c(1,a) = 1$ for all $a \in K$. Setting $a^* = a^{-1}$, $\mathbb{C}_c K$ becomes a finite dimensional, simple C^*-algebra and therefore $\mathbb{C}_c K \simeq B(\mathcal{H})$ for some finite dimensional Hilbert space. By the nondegeneracy of ζ, $\mathbb{C}_c K$ has trivial center and thus the representation $\pi : K \to \mathbb{C}_c K = B(H)$ is irreducible.

For the other direction assume that $\pi : K \to \mathrm{PU}(\mathcal{H})$ is a faithful irreducible projective representation and let $c \in \mathsf{Z}^2(K, \mathbb{T})$ be the 2-cocycle induced by π. Observe that

$$\pi(b)\pi(a) = \overline{c(b,a)}\pi(ab) = c(a,b)\overline{c(b,a)}\pi(a)\pi(b) = \zeta(a,b)\pi(a)\pi(b) \tag{3.12}$$

which gives us a skew-symmetric bicharacter ζ. We show that ζ is nondegenerate and thus symplectic by showing that $\mathbb{C}_c K \simeq B(\mathcal{H})$. For $\mathcal{X} \in \hat{K}$ let

$$B(\mathcal{H})_{\mathcal{X}} := \left\{ T \in B(\mathcal{H}) \,|\, \mathrm{Ad}_{\pi(a)}(T) = \mathcal{X}(a)T \text{ for all } a \in K \right\}.$$

By complete reducibility of the representation Ad_π (or just by writing the projections) we have

$$B(\mathcal{H}) = \bigoplus_{\mathcal{X} \in \hat{K}} B(\mathcal{H})_{\mathcal{X}}.$$

Note that by irreducibility of π we have $B(\mathcal{H})_{\mathcal{X}_e} = \mathbb{C}I$.

We now show that each nontrivial subspace $B(\mathcal{H})_{\mathcal{X}}$ is 1-dimensional. Suppose $0 \neq T \in B(\mathcal{H})_{\mathcal{X}}$, then $T^* \in B(\mathcal{H})_{\overline{\mathcal{X}}}$, so that TT^* and T^*T belongs to $B(\mathcal{H})_e = \mathbb{C}I$. Further, if $S \in B(\mathcal{H})_{\mathcal{X}}$ then $T^*S \in B(\mathcal{H})_{\mathcal{X}_e}$ implies that $S = \lambda T$, $\lambda \in \mathbb{C}$ which again implies that $B(\mathcal{H})_{\mathcal{X}}$ is 1-dimensional.

Let

$$\Gamma := \left\{ \mathcal{X} \in \hat{K} \,|\, B(\mathcal{H})_{\mathcal{X}} \neq 0 \right\}.$$

For $\mathcal{X} \in \Gamma$ we can write $B(\mathcal{H})_{\mathcal{X}} = \mathbb{C}T_{\mathcal{X}}$ for some $T_{\mathcal{X}} \in B(\mathcal{H})$. Since $T^*_{\mathcal{X}} \in B(\mathcal{H})_{\overline{\mathcal{X}}}$ and $T_{\mathcal{X}_1}T_{\mathcal{X}_2} \in B(\mathcal{H})_{\mathcal{X}_1\mathcal{X}_2}$, we have that Γ is a subgroup of $\hat{K}$. Assuming that $\Gamma \neq \hat{K}$ we get that $\hat{\Gamma}$ is a proper subgroup of K, and thus the set

$$\Gamma^\perp = \{a \in K \,|\, \mathcal{X}(a) = 1 \text{ for all } \mathcal{X} \in \Gamma\}$$

is a nontrivial subgroup of K. This implies that for all $a \in \Gamma^\perp$, we have $\pi(a) = kI$, $k \in \mathbb{C}$, contradicting faithfulness of π. Thus $\left|\hat{K}\right| = |K| = \dim(B(\mathcal{H}))$. Since π is irreducible, $\pi(K)$ is a basis of $B(\mathcal{H})$, and thus $\mathbb{C}_c K \simeq B(\mathcal{H})$ via $a \mapsto \pi(a)$. This implies that the center of $\mathbb{C}_c K$ is trivial, which by Equation (3.12) shows that ζ is nondegenerate and hence symplectic, thereby completing the proof. ■

Remark 3.3.4. From Equation (3.12) one sees that in the above proof we can identify $\mathcal{X}_a$ with $\zeta(a,\cdot)$ so that $B(\mathcal{H})_{\mathcal{X}_a} = \mathbb{C}\pi(a)$. Furthermore the spaces $\mathbb{C}\pi(a)$ are orthogonal and thus $\pi(K)$ becomes a Weyl-type basis. If K is normal in G, Proposition 3.1.4 tells us that $\pi(G)$ is a unitary 2-design if and only if G acts transitively on $K \setminus \{e\}$. We therefore want to establish a relation between the normaliser and the group of automorphisms of K.

Let ζ be a symplectic bicharacter on K, and let π be the unique, irreducible representation corresponding to ζ. Let

$$C := N_{\mathrm{PU}(\mathcal{H})}(K)$$

be the normaliser of $\pi(K)$ in $\mathrm{PU}(\mathcal{H})$. Then we have the following result.

Proposition 3.3.5
Let $\mathrm{Aut}(K,\zeta)$ *be the group of automorphisms of* K *preserving* ζ. *Then*

$$C/K \simeq \mathrm{Aut}(K,\zeta),$$

or in other words, the sequence

$$1 \longrightarrow K \xrightarrow{\pi} C \xrightarrow{Ad} \mathrm{Aut}(K,\zeta) \longrightarrow 1$$

is exact.

Proof. For this proof we will identify K with $\pi(K)$ and write a instead of $\pi(a)$.

We first show that $\mathrm{Ad} : C \to \mathrm{Aut}(K,\zeta)$ is well defined. Let $g \in C$, clearly $\mathrm{Ad}_g \in \mathrm{Aut}(K)$. From Equation (3.12) we have that $ba = \zeta(a,b)ab$. We get

$$\mathrm{Ad}_g(b)\mathrm{Ad}_g(a) = \mathrm{Ad}_g(ba) = \zeta(a,b)\,\mathrm{Ad}_g(a)\mathrm{Ad}_g(b)$$

and

$$\mathrm{Ad}_g(b)\mathrm{Ad}_g(a) = \zeta(\mathrm{Ad}_g(a),\mathrm{Ad}_g(b))\,\mathrm{Ad}_g(a)\mathrm{Ad}_g(b)$$

which implies that

$$\zeta(a,b) = \zeta(\mathrm{Ad}_g(a),\mathrm{Ad}_g(b)).$$

Hence $\mathrm{Ad}_g \in \mathrm{Aut}(K,\zeta)$. Next we show the map is surjective. Let $c \in \mathsf{Z}^2(K,\mathbb{T})$ such that $\zeta(a,b) = c(a,b)\overline{c(b,a)}$. Let $\alpha \in \mathrm{Aut}(K,\zeta)$ and set $c_\alpha(a,b) := c(\alpha(a),\alpha(b))$. We have

$$\zeta(a,b) = c_\alpha(a,b)\overline{c_\alpha(b,a)},$$

and thus by Proposition 3.3.2, $[c] = [c_\alpha]$ in $\mathsf{H}^2(K,\mathbb{T})$. This implies that there exists $f : K \to \mathbb{T}$ such that

$$c_\alpha(a,b) = f(a)f(b)\overline{f(ab)}c(a,b).$$

We then define $\theta : \mathbb{C}_c K \to \mathbb{C}_c K$ by

$$\theta(a) := \overline{f(a)}\alpha(a).$$

One checks that $\theta \in \mathrm{Aut}(\mathbb{C}_c K)$ and since $\mathbb{C}_c K \simeq B(\mathcal{H})$, θ therefore corresponds to an automorphism of $B(\mathcal{H})$. Thus $\theta = \mathrm{Ad}_g$ for some $g \in \mathrm{PU}(\mathcal{H})$.

Finally we show that $\ker(\mathrm{Ad}) = K$. Assuming g is in the kernel we have that $gag^{-1} = f(a)$ for some $f : K \to \mathbb{T}$. This implies the equations:

$$gabg^{-1} = f(ab)ab,$$
$$gag^{-1}gbg^{-1} = f(a)f(b)ab,$$

and thus $f \in \hat{K}$. Then $f = \zeta(\cdot,h)$ for some $h \in K$, and thus $g = \lambda h$ for some $\lambda \in \mathbb{T}$. ■

We can now describe unitary 2-designs G from $\mathrm{PU}(\mathcal{H})$, containing normal nontrivial abelian subgroups.

Proposition 3.3.6
Let G be a subgroup of $\mathrm{PU}(\mathcal{H})$, and let K be a nontrivial normal abelian subgroup of G. Then G is a unitary 2-design if and only if the following two conditions are satisfied:

1. *K is irreducible.*
2. *If ζ is the corresponding bicharacter, then $G/K \subset \mathrm{Aut}(K, \zeta)$ and G acts transitively on $K \setminus \{I\}$.*

Proof. The regular representation of G is clearly faithful. Since K is normal in G, the set

$$B(\mathcal{H})^{\mathrm{Ad}_K} := \{X \in B(\mathcal{H}) \,|\, \mathrm{Ad}_a(X) = X \text{ for all } a \in K\},$$

is Ad_G-invariant and contains the identity. If G is a unitary 2-design, $B(\mathcal{H})^{\mathrm{Ad}_K}$ is either $\mathbb{C}I$ or $B(\mathcal{H})$. Since K is nontrivial we have that $B(\mathcal{H})^{\mathrm{Ad}_K} = \mathbb{C}I$. Hence by Theorem 3.3.3, K corresponds to a symplectic bicharacter ζ. From Remark 3.3.4 we then see that G acts transitively on $K \setminus \{I\}$, and from Proposition 3.3.5 we get that $G/K \subset C/K \simeq \mathrm{Aut}(K, \zeta)$. If on the other hand the two conditions are satisfied, it should be clear from Remark 3.3.4 and Proposition 3.1.4 that G is a unitary 2-design. ■

Corollary 3.3.7
If $K \subset G \subset \mathrm{PU}(\mathcal{H})$ as above and G is a unitary 2-design, then G is a Clifford-type *design on $\ell^2(\mathbb{Z}_p^{2n})$ for some prime p and integer $n \geq 1$.*

Proof. K can be identified with a faithful projective representation of $\mathbb{Z}_p^{2n}$ for some prime p and integer $n \geq 1$. One can then show that every symplectic bicharacter of $\mathbb{Z}_p^{2n}$ is the standard one (3.7) up to an automorphism of $\mathbb{Z}_p^n$. This completes the proof. ■

Remark 3.3.8. If K is an abelian group with symplectic bicharacter $\hat{\zeta}$, then by [Kar80] theorem 1.8, K decomposes as a direct product of groups of the form $\mathbb{Z}_{p^m} \times \mathbb{Z}_{p^m}$ with the standard symplectic bicharacter. In particular $(K, \hat{\zeta})$ is always of the form $(\hat{A} \times A, \zeta)$ where

$$\zeta((\mathcal{X}_x, a), (\mathcal{X}_y, b)) = \mathcal{X}_x(b)\overline{\mathcal{X}_y(a)}$$

from Section 3.1.

3.4 Sylow restrictions on non-Clifford designs

Corollary 3.3.7 tells that if a group G is a unitary 2-design, but not a *Clifford-type* design, then it cannot contain a nontrivial, normal abelian subgroup. In particular, if $\dim(\mathcal{H})$ is not a prime power this is always the case.

Recall that a group G is *solvable* if there exists a sequence of groups $\{H_i\}_{i=1}^n$, such that $G = H_1$, $H_n = \{e\}$, H_{i+1} is normal in H_i and H_i/H_{i+1} is abelian. If G is solvable, picking H_{i+1} as the *commutator subgroup* of H_i, gives such a sequence where each H_i is normal in G and thus non-Clifford designs cannot contain nontrivial, normal solvable subgroups. The *Feit-Thompson* theorem which says that all groups of odd order are solvable then tells us that non-Clifford designs cannot contain nontrivial normal subgroups of odd order.

Assume that $|G| = p^k m$ for $k \geq 1$ and a prime p such that $\gcd(p, m) = 1$. A *Sylow p-subgroup* is a subgroup $H \subset G$ such that $|H| = p^k$. Let N_p denote the number of Sylow p-subgroups of G. *Sylow´s 3rd theorem* says that there is at least one Sylow p-subgroup, that all Sylow p-subgroups are conjugate, that N_p divides m and that $N_p \equiv 1 \pmod{p}$. If $N_p = 1$ this means that the Sylow p-subgroup is normal in G and thus non-Clifford designs cannot have $N_p = 1$ for any prime.

We summarise the above discussion in the following corollary.

Corollary 3.4.1 (Solvable subgroup restriction on non-Clifford designs)
Assume G is a unitary 2-design but not a Clifford-type design. Then G cannot contain a nontrivial, normal solvable subgroup (and hence not a nontrivial normal subgroup of odd order). In particular, the order of G is given by its prime factorisation

$$|G| = \prod_{i=1}^{n} p_i^{k_i},$$

and hence the number of Sylow p_i-groups is greater than 1 for each p_i. This is true for all group designs of non prime-power dimension.

We want to investigate whether this significantly restricts which orders of groups can give unitary 2-designs. The following, is a simple algorithm that determines some cases where $N_p = 1$ for a prime p in the prime factorisation of $|G|$.

Algorithm to determine if $N_p = 1$ for some prime p

1. Write $|G|$ in its prime factorisation $|G| = p_1^{k_1} \dots p_n^{k_n}$.
2. For each p_i in the factorisation do the following:
   (a) Let $m = \prod_{j \neq i} p_j^{k_j}$.
   (b) If $m < p_i$ then $N_{p_i} = 1$ and we can stop the loop.
   (c) We know $N_{p_i} = 1 + kp_i$ for some $k \in \mathbb{N}$. Therefore if $m > p_i$ we can set $k = 1$ and start the following inner loop:
      i. If $1 + kp_i > m$ then $N_{p_i} = 1$ and we can stop the loop.
      ii. If $1 + kp_i$ divides m then we could have $N_{p_i} = 1 + kp_i$ so we stop the inner loop and cannot exclude the group.
      iii. Add 1 to k.
   (d) If the inner loop in the previous step tells us that $N_{p_i} = 1$ we can exclude the group and stop the outer loop, otherwise we continue with p_{i+1}.

The GitHub repository linked at [Lan], has a simple python implementation of the above algorithm, as explained in the corresponding README.md file (note that this algorithm is not optimised).

To see whether the restrictions are significant, we exclude possible group orders smaller than orders of designs already known. As mentioned in Section 3.2.1, we know that for dimensions 2, 3, 5, 7 and 11, there is an optimal design so there is no need to check exclusions here. Further, we know that for prime powers $d = p^k$ there is a design of order $d^5 - d^3$. This gives an upper bound for designs in these dimensions.

For other dimensions there is no general known design, but one can choose the smallest known design (if any) as an upper bound, or just a large number if no design is known. Table 3.1 below shows how many orders can be excluded for different dimensions.

Table 3.1: Table showing exclusions based on restrictions from Sylow theorems. Left column is the dimension. *CB* is the Clifford bound (lower bound) for a group design. *UB* is the upper bound for the search. For prime-power dimensions this is chosen as $d^5 - d^3$. For other dimensions the values are taken from Table 2.1 and for dim = 15 just a large number. *# groups* is the number of orders between CB and UB divisible by $\dim^2 - 1$. *# exclusions* is the number of groups excluded based on the previous algorithm.

dim	LB	UB	# groups	# exclusions	% excluded
4	240	960	48	26	54.17
6	1260	15120	396	268	67.68
8	4032	32256	448	282	62.95
9	6480	12960	81	37	45.68
10	9900	190080	1820	1315	72.25
12	20592	9999991	69786	62294	89.26
13	28392	369096	2028	1205	59.42
14	38220	87360	252	158	62.70
15	50400	1000000	4239	2853	67.30
16	65280	1044480	3840	2805	73.05

The restrictions seem significant and could be used for better search of non-Clifford designs. However it also seems that the restrictions are so strong that group designs might not be the best option in this case.

It would be interesting to further investigate the structure on non-Clifford group designs. Can they be direct products of groups? The groups $6.A7$ and $Sz(8).3$ from Table 2.1 could be interesting to study as examples. $6.A7$ is *sextuple cover* of A_7 and seems to have a structure that is well understood. $Sz(8).3$ is related to the *Suzuki groups* and gives the design of order 87360 in dimension 14. This is in particular interesting as the order is smaller than the Clifford design in dimension 13.

Chapter 4

Other constructions

In this Chapter we follow [GAE07] in a construction of *asymptotic 2-designs* satisfying the Clifford bound. Continuing, we follow [Can+20] and obtain a unitary design based on a connection between a classical code and the *projective special linear group*. For the first construction, *stabiliser groups* and *states* are important.

4.1 Stabiliser groups and states

We will continue in this section with $d = p^m$ being the power of a prime. Let $\mathcal{H} = \mathbb{C}^d$, $V = \mathbb{F}_d^2$ and $w = w_d$ as in Equation (3.9). Further recall the symplectic bilinear form $[\cdot, \cdot]$ defined by Equation (3.7). We do the constructions as in [GAE07]. Let M be a subspace of V such that $[a, b] = 0$ for all $a, b \in M$. Recall from Equation (3.10) that two operators, $w(m)$ and $w(m')$ commute, if and only if $w(m)w(m') = w(m + m')$. From this we see that $w(M)$ is a group.

Define the operator

$$\rho_M := \frac{1}{|M|} \sum_{m \in M} w(m).$$

It is clear that $\rho_M w(m) = w(m)\rho_M = \rho_M$. Further

$$\rho_M \rho_M = \frac{1}{|M|^2} \sum_{m,m' \in M} w(m)w(m') = \frac{1}{|M|} \sum_{m \in M} w(m) = \rho_M, \tag{4.1}$$

which shows that ρ_M projects onto the $+1$ common eigenspace of the operators $w(M)$. This justifies calling $w(M)$ a *stabiliser group*. The dimension of the eigenspace is found by taking the trace of ρ_M. Since $w(0)$ is the only operator with nonzero trace we get

$$\mathrm{Tr}(\rho_M) = \frac{1}{|M|} \sum_{m \in M} \mathrm{Tr}(w(m)) = \frac{d}{|M|}. \tag{4.2}$$

Stabiliser groups are important in error correction and the dimension, of the $+1$ eigenspace tells us how many errors we can correct. Choosing a character $\mathcal{X}$ on M, we see in a similar way that

$$\rho_{M,\mathcal{X}} = \frac{1}{|M|} \sum_{m \in M} \mathcal{X}(m)w(m)$$

is a projection on a $\frac{d}{|M|}$ dimensional subspace of $\mathcal{H}$. Here the eigenvalues of $w(m)$ are $\overline{\mathcal{X}(m)}$ as opposed to 1. When $d = |M|$ we see from (4.2), that $\rho_{M,\mathcal{X}}$ is a pure state called a *stabiliser state*.

Remark 4.1.1. For $p = 2$ the characters takes values in ± 1. Assuming that the $+1$ eigenspace of M is used for computing, one can perform *stabiliser measurements* (Section 1.3.1) to determine if an error has occurred. One can then either continue computing in the resulting subspace or apply error correction to get back to the $+1$ eigenspace of M.

4.2 Mutually unbiased bases

Following [GAE07], we now introduce the concept of *mutually unbiased bases*, which we will use to construct *asymptotic designs*.

Definition 4.2.1 (Mutually unbiased bases (MUBs))
A collection of orthonormal bases $\{\mathcal{B}_i\}_{i\in I}$ for a d-dimensional Hilbert space is said to be *mutually unbiased* if for all $i \neq j \in I$, $w \in \mathcal{B}_i$ respectively $v \in \mathcal{B}_j$, we have $|\langle w|v\rangle| = d^{-1/2}$.

4.2.1 Basic construction

Let $V = \mathbb{F}_d^2$ be as in the previous section. Let

$$v_a = \begin{pmatrix} a \\ 1 \end{pmatrix}, \quad M_a = \{\lambda v_a \,|\, \lambda \in \mathbb{F}_d\}.$$

Since the symplectic form $[\cdot\,,\cdot]$ (Equation (3.7)) is antisymmetric and bilinear it is clear that $[\lambda v_a\,,\lambda' v_a] = 0$ for all $\lambda, \lambda' \in \mathbb{F}_d$. Since $|M_a| = d$, calculations similar to that in the previous section tells us that we get a collection of *stabiliser states* defined by

$$|\psi_b^a\rangle\langle\psi_b^a| := \frac{1}{d}\sum_{\lambda\in\mathbb{F}_d} \mathcal{X}_d(\lambda b) w(\lambda v_a), \quad b \in \mathbb{F}_d.$$

Letting $\mathcal{B}_a := \{|\psi_b^a\rangle \,|\, b \in \mathbb{F}_d\}$, we claim that this is a collection of MUBs. Since $\mathrm{Tr}(|\psi_b^a\rangle\langle\psi_b^a|) = 1$, they have norm 1. We check they are orthogonal:

$$|\langle\psi_b^a|\psi_{b'}^a\rangle|^2 = \mathrm{Tr}(|\psi_b^a\rangle\langle\psi_b^a|\,|\psi_{b'}^a\rangle\langle\psi_{b'}^a|) = \frac{1}{d^2}\sum_{\lambda,\lambda'\in\mathbb{F}_d} \mathcal{X}_d(\lambda b)\mathcal{X}_d(\lambda' b')\,\mathrm{Tr}(w((\lambda+\lambda')v_a))$$
$$= \frac{1}{d}\sum_{\lambda\in\mathbb{F}_d} \mathcal{X}_d(\lambda(b-b')) = \delta_{b,b'}.$$

Checking that the bases are unbiased we observe that for $a \neq a'$, $\mathrm{Tr}(w(\lambda v_a + \lambda' v_{a'}))$ equals 0 unless $\lambda = \lambda' = 0$. Similar calculations to the ones above then show that

$$\left|\left\langle\psi_{b'}^{a'}\middle|\psi_b^a\right\rangle\right|^2 = \frac{1}{d}\mathcal{X}_d(0)^2 = \frac{1}{d},$$

and thus the $\{\mathcal{B}_a\}$ are mutually unbiased. Letting $M_\infty := \left\{(\lambda,0)^T \,|\lambda \in \mathbb{F}_d\right\}$ and employing the same reasoning as above we get a final basis that is mutually unbiased to all bases $\mathcal{B}_a$. The final collection $\{\mathcal{B}_a\}_{a\in\mathbb{F}_d} \cup M_\infty$ is thus a set of $d+1$ MUBs.

To get the *asymptotic* designs we use a collection of unbiased maximally entangled states on $(\mathbb{C}^d)^{\otimes 2}$ which we use to find unitaries for our design. To get this collection of maximally entangled states, we use the MUB construction on $(\mathbb{C}^d)^{\otimes 2}$, and show that some number of the obtained stabiliser states are maximally entangled. To do this, we need to quickly discuss how $\mathcal{W}_{d^n,1}$ and $\mathcal{W}_{d,n}$ are related.

4.2.2 Factoring Weyl operators

Let $B = \mathbb{F}_d$ and $F = \mathbb{F}_{d^m}$ be a field extension of B with basis $\{e_i\}_{i=1}^m$. Since the B-bilinear form from (3.6),

$$\langle a\,, b\rangle_{F/B} = \mathrm{Tr}_{F/B}(ab)$$

is nondegenerate, there is a *dual basis* $\{e^i\}_{i=1}^m$ such that $\langle e^j\,, e_i\rangle_{F/B} = \delta_{i,j}$. Following [GAE07] we let $\{a^i\}_{i=1}^m$, $\{a_i\}_{i=1}^m$ denote the expansion coefficients of a w.r.t the bases $\{e_i\}_{i=1}^m$ and $\{e^i\}_{i=1}^m$, that is,

$$a = \sum_{i=1}^m a^i e_i = \sum_{i=1}^m a_i e^i.$$

We get the following lemma:

Lemma 4.2.2 (Factoring Weyl operators)
Under the isomorphism $\mathcal{H}^{d^n} \overset{\Psi}{\simeq} \mathcal{H}^{d^{\otimes n}}$:

$$|a\rangle = \left|a^1 e_1 + ... + a^n e_n\right\rangle \overset{\Psi}{\mapsto} \left|a^1\right\rangle \otimes \cdots \otimes |a^n\rangle\,,$$

the Weyl operators in $\mathcal{W}_{d^n,1}$ factor as

$$w_{d^n}(a,b) \mapsto w_d(a_1, b^1) \otimes \cdots \otimes w_d(a_n, b^n).$$

Proof. First we check:

$$x_{d^n}(a)\,|b\rangle = |a+b\rangle = \left|\left(\sum_{j=1}^n (a^j + b^j)e_j\right)\right\rangle \overset{\Psi}{\mapsto} \bigotimes_{j=1}^n x_d(a^j)\left|b^j\right\rangle.$$

Secondly it is well known that $\mathrm{Tr}_{\mathbb{F}_{d^n}/\mathbb{F}_p} = \mathrm{Tr}_{\mathbb{F}_d/\mathbb{F}_p} \circ \mathrm{Tr}_{\mathbb{F}_{d^n}/\mathbb{F}_d}$. Hence we get

$$\begin{aligned}\mathcal{X}_{d^n}(ab) = \exp\left(i\frac{2\pi}{p}\,\mathrm{Tr}_{\mathbb{F}_d/\mathbb{F}_p} \circ \mathrm{Tr}_{\mathbb{F}_{d^n}/\mathbb{F}_d}(ab)\right) &= \mathcal{X}_d\left(\mathrm{Tr}_{\mathbb{F}_{d^n}/\mathbb{F}_d}(ab)\right) \\ &= \mathcal{X}_d\left(\sum_{j,k=1}^n a_j b^k\ \mathrm{Tr}_{\mathbb{F}_{d^n}/\mathbb{F}_d}(e^j e_k)\right) = \prod_{j=1}^n \mathcal{X}_d\left(a_j b^j\right),\end{aligned}$$

which implies that

$$z_{d^n}(a)\,|b\rangle = \mathcal{X}_{d^n}(ab)\,|b\rangle = \prod_{j=1}^n \mathcal{X}_d(a_j b^j)\left|\sum_{j=1}^n (b^j e_j)\right\rangle \overset{\Psi}{\mapsto} \bigotimes_{j=1}^n \mathcal{X}_d(a_j b^j)\left|b^j\right\rangle = \bigotimes_{j=1}^n z_d(a_j)\left|b^j\right\rangle.$$

Finally

$$w_{d^n}(a,b) = \mathcal{X}_{d^n}(-2^{-1}ab)z_{d^n}(a)x_{d^n}(b)$$
$$\overset{\Psi}{\longmapsto} \bigotimes_{j=1}^{n} \mathcal{X}_{d^n}(-2^{-1}a_j b^j)z_d(a_j)x_d(b^j) = \bigotimes_{j=1}^{n} w_d(a_j, b^j),$$

thereby completing the proof. ■

We can now prove the following theorem from [GAE07].

Theorem 4.2.3 (Mutually unbiased bases for $\mathbb{C}^d \otimes \mathbb{C}^d$)
Let $d = p^m$ be the power of a prime. Then for $\mathbb{C}^d \otimes \mathbb{C}^d$ there exists d^2+1 MUBs, d^2-d of which are maximally entangled and $d+1$ which are products of pure states.

Proof. The construction of the *stabiliser states* $\{|\psi_b^a\rangle\langle\psi_b^a|\}_{a,b\in\mathbb{F}_{d^2}}$ along with M_∞ from Section 4.2.1 gives a collection of d^2+1 MUBs. Assume further that bases $\{e_1, e_2\}, \{e^1, e^2\}$ of $\mathbb{F}_{d^2}$ over $\mathbb{F}_d$ has been chosen s.t $\langle e_i, e^j\rangle_{\mathbb{F}_{d^2}/\mathbb{F}_d} = \delta_{ij}$. We have

$$|\psi_b^a\rangle\langle\psi_b^a| = \frac{1}{d^2}\sum_{\lambda\in\mathbb{F}_{d^2}} \mathcal{X}_{d^2}(\lambda b)w_{d^2}(\lambda v_a)$$
$$= \frac{1}{d^2}\sum_{\lambda\in\mathbb{F}_{d^2}} \mathcal{X}_{d^2}(\lambda b)w_d((\lambda a)_1, \lambda^1)\otimes w_d((\lambda a)_2, \lambda^2). \quad (4.3)$$

Let $N_a := \{\lambda v_a \,|\, (\lambda a)_2 = \lambda^2 = 0\}$ and trace out the second tensor factor to get information of the state. We get

$$\mathrm{Tr}_2(|\psi_b^a\rangle\langle\psi_b^a|) = \frac{1}{d}\sum_{\lambda v_a\in N_a} \mathcal{X}_{d^2}(\lambda b)w_d((\lambda a)_1, \lambda^1). \quad (4.4)$$

Since N_a is an $\mathbb{F}_d$ vector space we have that $|N_a| = d^n$. It is clear that $n \leq 2$ since $N_a \subset M_a$. If $n = 0$, $N_a = \{0\}$ which implies $\lambda = 0$ so that Equation (4.4) becomes

$$\frac{1}{d}\mathcal{X}_{d^2}(0)w_d(0) = \frac{1}{d}I_d$$

showing that $|\psi_b^a\rangle\langle\psi_b^a|$ is maximally entangled. If $n = 1$ then N_a is the $\mathbb{F}_d$-linear span of some vector $\lambda' v_a$ and (4.4) becomes

$$d^{-1}\sum_{c\in\mathbb{F}_d} \mathcal{X}_{d^2}(c(\lambda' b))w_d(c((\lambda' v_a)_1, (\lambda')^1)).$$

By calculations as in (4.1), this is a pure state, which implies that $|\psi_b^a\rangle\langle\psi_b^a|$ is a product of pure states. For $n = 2$ we have $(\lambda a)_2 = \lambda^2 = 0$ for all λ so Equation (4.3) becomes

$$\rho \otimes \frac{1}{d}I_d$$

for some state ρ, but then $|\psi_b^a\rangle\langle\psi_b^a|$ is not pure so this cannot happen.

By the reasoning above it is clear that $M_\infty = \mathrm{span}(1, 0)$, gives rise to a product state. We show now that there are exactly d vectors v_a such that $|N_a| = d$. From the definition of N_a we see that

$$\lambda v_a \in N_a \iff (\lambda = \lambda^1 e_1 \quad \text{and} \quad \lambda a = (\lambda a)_1 e^1 = b e^1,\, b \in \mathbb{F}_d).$$

Assuming that $|N_a| = d$ we see that λ^1 takes on all values in $\mathbb{F}_d$. From the above we also see that $a = (e_1)^{-1}b$ for some $b \in \mathbb{F}_d$. On the other hand if

$$a = (e_1)^{-1}b,$$

then $|N_a| = d$ by letting λ^1 run through $\mathbb{F}_d$. Hence there are exactly d vectors v_a such that $|N_a| = d$. This gives $d+1$ product states, finishing the proof. ∎

4.3 Asymptotic 2-designs

We are now prepared to construct *asymptotic 2-designs*. Recall from Theorem 2.2.3, that $\mathcal{P}(\mathcal{D}) = 2$ is equivalent to $\mathcal{D}$ being a unitary 2-design. First we state the definition of such designs from [GAE07].

Definition 4.3.1 (Asymptotic 2-designs)
Let $\mathcal{I} \subseteq \mathbb{N}$ be an index set. A family of sets of unitaries $\mathcal{D}_d$, $d \in \mathcal{I}$ is an *asymptotic 2-design* if the unitaries in $\mathcal{D}_d$ are d-dimensional and

$$\lim_{d\to\infty} \mathcal{P}(\mathcal{D}_d) = 2.$$

We prove the existence of such a design as in [GAE07]. It is, in fact, a corollary of Theorem 4.2.3.

Corollary 4.3.2 (Existence of asymptotic designs)
Let $\mathcal{I}$ be the set of prime-power integers. Then there exists an asymptotic 2-design $\mathcal{D}_d$, $d \in \mathcal{I}$ satisfying the Clifford bound and thus these are conjecturely optimal.

Proof. For $d \in \mathcal{I}$ we use Theorem 4.2.3 to get $d^2(d^2-d)$ maximally entangled states $\{|\psi_b^a\rangle\langle\psi_b^a|\}$. Using Equation (1.3) these maximally entangled states give us unitaries for our design $\mathcal{D}_d$. Recalling that the substitution between matrices and vectors (Equation (1.3)) adds a factor of $\dim(H)^2$ we compute the frame potential of $\mathcal{D}_d$.

$$\begin{aligned}\mathcal{P}(\mathcal{D}_d) = \frac{1}{|\mathcal{D}_d|^2} \sum_{U,U'\in\mathcal{D}} \left|\operatorname{Tr}\left(U'U^\dagger\right)\right|^4 &= \frac{d^4}{|\mathcal{D}_d|^2} \sum_{a,b,a',b'} \left|\left\langle \psi_b^a \middle| \psi_{b'}^{a'} \right\rangle\right|^4 \\ &= \frac{d^4}{|\mathcal{D}_d|}\left(1 + \frac{|\mathcal{D}_d| - d^2}{d^4}\right) = \frac{2d^4 - d^3 - d^2}{d^4 - d^3} \xrightarrow[d\to\infty]{} 2.\end{aligned}$$

∎

It is not really clear what this type of convergence means, and as [GAE07] writes, the question whether a design is 'almost as good' as twirling with respect to the Haar measure, depends on the application. Consider 2 quantum channels ψ, ϕ and let C_ψ, C_ϕ be their respective Choi matrices. Then we have the metric $d_{\text{pro}}(\psi,\phi) := d^{-1}\operatorname{Tr}(|C_\psi - C_\phi|)$. The following proposition tells us that asymptotic designs converge with respect to this metric. Before we state it, recall that $T_{\mathcal{D}}$ (respectively T_U) are the channels induced by twirling an operator by $\mathcal{D}$ (respectively $\mathcal{U}(\mathcal{H})$).

Proposition 4.3.3 (Convergence of asymptotic 2-designs)
Let $\mathcal{D}_d$ be an asymptotic 2-design, then $d_{pro}(T_U, T_{\mathcal{D}_d}) \xrightarrow[d\to\infty]{} 0$.

The proof in [GAE07] seems to be missing a square root where they use the Cauchy-Schwarz inequality. We provide a slightly different proof.

Proof. Let C_U and $C_{\mathcal{D}_d}$ be the Choi-matrices $T_U, T_{\mathcal{D}_d}$. Using Theorem 2.2.3 we see that

$$\mathcal{P}(\mathcal{D}_d) \xrightarrow[d\to\infty]{} 2 \iff \|C_U - C_{\mathcal{D}_d}\|_2^2 \xrightarrow[d\to\infty]{} 0.$$

This implies that the eigenvalues (s_i) of $|C_U - C_{\mathcal{D}_d}|$ go to zero. We get that

$$d_{\text{pro}}(T_U, T_{\mathcal{D}_d}) = \frac{1}{d}\,\text{Tr}(|C_U - C_{\mathcal{D}_d}|) = \frac{1}{d}\sum_{i=1}^{d} s_i \le \sup_{1\le i\le d} s_i \xrightarrow[d\to\infty]{} 0.$$

■

4.4 Kerdock designs

In this section we will follow the ideas of [Can+20] and construct a Clifford-design which allows for random sampling and where the implementation of the unitary operators as quantum circuits is understood. The construction is based on the *Kerdock set*, which we will now define.

4.4.1 The Kerdock set

The finite field $F = \mathbb{F}_{2^n}$, can be obtained by adjoining a root θ to an irreducible polynomial, $p(x)$ over $\mathbb{F}_2$, of degree $n-1$. We will sometimes represent elements of $\mathbb{F}_{2^n}$ as row vectors in $\mathbb{F}_2^n$ via $a = \sum_{k=0}^{n-1} a_k\theta^k \mapsto (a_0, \dots, a_{n-1}) \in \mathbb{F}_2^n$.

We will shift back and forth between these representations, hoping it is clear from the context which one is being used. In general, this means that when we do multiplication by other elements, we see them as elements of $\mathbb{F}_{2^n}$, but when doing multiplication by matrices in $\mathbb{F}_2^{n\times n}$, we view them as elements of $\mathbb{F}_2^n$.

If

$$p(x) = \sum_{k=0}^{n-1} p_k x^k,$$

we can represent multiplication by θ via the matrix

$$A_\theta := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ p_0 & p_1 & \cdots & p_{n-1} \end{pmatrix}$$

such that $a\theta = aA_\theta$. In this way we can represent multiplication by any $z \in \mathbb{F}_{2^n}$ as A_z.

Recall from Equation (3.5) and (3.6) the bilinear form $\langle a\,, b\rangle_{\mathbb{F}_{2^n}} = \text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ab)$. Since the form is bilinear and nondegenerate, it can be represented by an invertible matrix W. That is, W is defined by the equation

$$\text{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(ab) = aWb^T. \tag{4.5}$$

We will use the following set to obtain a unitary 2-design.

Definition 4.4.1 (The Kerdock set)
For an integer n, let $z \in \mathbb{F}_{2^n}$ and define the matrix $P_z \in \mathbb{F}_2^{n\times n}$ by

$$P_z := A_z W \tag{4.6}$$

where W is the matrix defined by (4.5).

The *Kerdock set* $P_K(n)$ is defined as

$$P_K(n) := \{P_z \mid z \in \mathbb{F}_{2^n}\}.$$

The following lemma describes some properties of the Kerdock set.

Lemma 4.4.2
$P_K(n)$ is an n-dimensional vector space over $\mathbb{F}_2$ consisting of symmetric matrices. The nonzero matrices are invertible.

Proof. From finite field arithmetic we have that $A_{z_1} + A_{z_2} = A_{z_1+z_2}$ which implies that $P_{z_1} + P_{z_2} = P_{z_1+z_2}$ and hence $P_K(n)$ is a vector space. It should be clear that it is n-dimensional. To see that the matrices are symmetric, first note by (4.5) that $W_{ij} = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(\theta^i\theta^j) = W_{ji}$. Then observe that for all $x, y \in \mathbb{F}_{2^n}$ we have

$$xP_zy^T = xA_zWy^T = \mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(xzy) = xW(A_zy)^T = xP_z^Ty.$$

Finally, assume that $0 \neq z \in \mathbb{F}_{2^n}$. Since W is invertible, (4.6) implies that $xP_z = 0$ if and only if $xA_z = 0$ which in turn implies that $x = 0$, proving that nonzero matrices are invertible. ∎

4.4.2 The Kerdock set and the Weyl operators

In this section we explain how the Kerdock set is used to partition the Weyl operators in a way that later gives a unitary 2-design.

Weyl operators for p=2

We start out quickly defining the Weyl operators for $p = 2$ in a way that is convenient for our purpose. It is analogous to Section 3.2, and can be skipped. What is important to know is that the Weyl operators are defined in a way such that they are self-adjoint and such that sets of commuting operators generate groups.

Let

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \text{and} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

For $a, b \in \mathbb{F}_2$ set

$$w_2(a,b) := i^{ab}\, Z^a X^b.$$

For $a, b \in \mathbb{F}_2^n$ we can extend this via

$$w_{2,n} := \bigotimes_{k=1}^{n} w_2(a_k, b_k).$$

The Weyl operators in $B(\mathbb{C}^{2^{\otimes n}})$ are usually called *Pauli operators*, but we will keep referring to them as Weyl operators to keep language consistent throughout the text. Further we will write

$$w(a,b) := w_{2,n}(a,b), \quad a,b \in \mathbb{F}_2^n$$

in this section to save on notation.

For $a,b \in \mathbb{F}_2^n$ we can consider (a,b) as a row vector in $\mathbb{F}_2^{2n}$. Recall from Equation (3.7) that we have a symplectic bilinear form $[\cdot,\cdot]$ on $\mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n}$ defined by

$$[(a,b),(c,d)] = (a,b)\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}(c,d)^T.$$

Using this, we get the *symplectic bicharacter* $\zeta : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \mapsto \{\pm 1\}$ by

$$\zeta((a,b),(c,d)) = (-1)^{[(a,b),(c,d)]}, \tag{4.7}$$

from which we see that

$$w(a,b)w(c,d) = \zeta((a,b),(c,d))\, w(c,d)w(a,b) = \zeta((a,b),(c,d))\, w((a+c),(b+d)). \tag{4.8}$$

Groups of Weyl operators from the Kerdock set

Observe that the Weyl operators are self-adjoint and that each operator is its own inverse. Equation (4.8) then implies that a set of k distinct, commuting Weyl operators generate a group of order 2^k. Let $P_z \in P_K(n)$ and consider the matrix $(\, P_z \,|\, I_n \,) \in \mathbb{F}_2^{n \times 2n}$. Each row of $(\, P_z \,|\, I_n \,)$ defines a Weyl operator, and using that

$$(\, P_z \,|\, I_n \,)\begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}(\, P_z \,|\, I_n \,)^T = P_z + P_z = 0$$

we see that the Weyl operators defined by the rows of $(\, P_z \,|\, I_n \,)$ generate a group.

Recalling that $P_K(n)$ is a vector space and that the nonzero matrices are invertible, the above discussion implies that the set $\{(\, P_z \,|\, I_n \,) \mid P_z \in P_K(n)\}$ corresponds to a collection of 2^n groups, each of order 2^n, all intersecting trivially. Adding to this the Weyl operators generated by the matrix $(\, I_n \,|\, 0 \,)$, we see that that these $2^n + 1$ groups partition all Weyl operators.

We summarise the above discussion in the lemma below.

Lemma 4.4.3
The matrices $(\, P_z \,|\, I_n \,)$, $P_z \in P_K(n)$ and $(\, I_n \,|\, 0 \,)$ give a collection of $2^n + 1$ groups of order 2^n with trivial intersection. Each nontrivial Weyl operator belongs to exactly one of these groups.

Remark 4.4.4. [Can+20] goes on to show that the Kerdock set also defines a set of MUBs. They use this result to simplify the calculation of the *weight-distribution* of the *Kerdock code* (a classical code used for error correction), giving an interesting connection between classical codes and quantum information.

4.4.3 Sampling from a unitary 2-design

In this section we use the Kerdock set to establish a relation between the *projective special linear group* and the *symplectic matrices.* The design is the same as the one obtained from $\mathrm{Sp}(\mathbb{F}_{2^n}, 1)$ in Section 3.2.1 but allows for effective random sampling of operators.

First recall that the *projective line* $\mathbb{F}_{2^n} \cup \{\infty\}$ can be identified with the set of points $\{(z,1) \mid z \in \mathbb{F}_{2^n}\} \cup \{(1,0)\}$. In this way we can identify the matrices $\{(\, P_z \mid I_n \,) \mid z \in \mathbb{F}_{2^n}\} \cup \{(\, I_n \mid 0 \,)\}$ with the *projective line.*

The projective special linear group $(\mathrm{PSL}(2, 2^n))$ can be identified with the group of transformations

$$f(z) = \frac{az+b}{cz+d} \quad a, b, c, d \in \mathbb{F}_{2^n}\,,\; ad + bc = 1, \tag{4.9}$$

acting on the *projective line.*

We want to obtain these transformations as symplectic matrices. To do this we will use the matrices in Table 4.1. In [Can+20] they mention that there is a standard way of transforming these to quantum circuits.

Table 4.1: Symplectic matrices used for obtaining the transformations in Equation (4.9).

Symplectic matrices		
$\Omega = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$	$L_Q = \begin{pmatrix} (Q^{-1})^T & 0 \\ 0 & Q \end{pmatrix}$	$T_P = \begin{pmatrix} I_n & 0 \\ P & I_n \end{pmatrix}$, $P = P^T$

Before the next lemma recall that the matrix A_z corresponds to multiplication by z in $\mathbb{F}_{2^n}$. Since squaring is an automorphism of $\mathbb{F}_{2^n}$ the matrix $A_{z^{1/2}}$ is well defined. Recall further from (4.5) that W is defined by $\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_2}(xy) = xWy^T$ and from (4.6) that $P_z = A_z W$.

Proposition 4.4.5
The Weyl operators and the group of transformations (4.9) acting on the matrices $\{(\, P_z \mid I_n \,) \mid P_z \in P_K(n)\} \cup \{(\, I_n \mid 0 \,)\}$ *from Lemma 4.4.3 is a unitary 2-design. Further we obtain a method of sampling these elements by picking* $a, b, c \in \mathbb{F}_{2^n}$ *and build circuits corresponding to the operators*

$$T_{P_a} L_{A_b} \Omega L_{W^{-1}} T_{P_c}$$

from Table 4.1.

Proof. That we obtain a unitary 2-design is in some way already known since $\mathrm{PSL}(2, 2^n) \simeq \mathrm{Sp}(\mathbb{F}_{2^n}, 1)$. We provide a slightly different proof.

We need to show that the transformations are transitive on the nontrivial Weyl operators. First recall from Lemma 4.4.3 that the matrices $\{(\, P_z \mid I_n \,) \mid z \in \mathbb{F}_{2^n}\} \cup \{(\, I_n \mid 0 \,)\}$ partition all Weyl operators . The transformation $z \mapsto zx$ is obtained by the matrix $L_{A_{x^{-1/2}}}$ and it is not difficult to see that $(0, a) L_{A_{a^{-1}b}} = (0, b)$ and thus the operators L_{A_x} act transitively on nontrivial elements of the group generated by $(\, 0 \mid I_n \,)$.

Using the transformations $z \mapsto z + x$ and $z \mapsto 1/z$ which are obtained from the matrices T_{P_x} and $\Omega L_{W^{-1}}$ respectively, one can map $(\, 0 \mid I_n \,)$ to the remaining matrices. Hence the transformations act transitively on the nontrivial Weyl operators, implying that we get a unitary 2-design.

In the computations below we will abuse the "="-sign and extend the meaning to matrices that are row-equivalent.

To obtain the sampling elements observe that we need to realise the transformation

$$(\,P_z \,|\, I_n\,)\begin{pmatrix}(A_a)^T & W^{-1}A_c\\ P_b & A_d\end{pmatrix} = (\,P_{az+b}\,|\,A_{cz+d}\,) = \left(\,P_{\frac{az+b}{cz+d}}\,|\,I_n\,\right).$$

We then observe that

$$\begin{pmatrix}I_n & 0\\ P_y & I_n\end{pmatrix}\begin{pmatrix}(A_x)^T & 0\\ 0 & A_{x^{-1}}\end{pmatrix}\begin{pmatrix}0 & W^{-1}\\ W & 0\end{pmatrix}\begin{pmatrix}I_n & 0\\ P_kW & I_n\end{pmatrix} = \begin{pmatrix}A_{xk} & W^{-1}A_x\\ P_{xyk+x^{-1}} & A_{xy}\end{pmatrix}.$$

Picking $x = c$, $y = d/c$, $k = a/c$, and $b = xyk + x^{-1}$ and noticing that the 4 matrices correspond to

$$T_{P_{d/c}}L_{A_{c^{-1}}}\Omega L_{W^{-1}}T_{P_{a/c}},$$

completes the proof. ■

[Can+20] contains a discussion concerning the sizes of the circuits required to implement the operators. It would also be interesting to investigate how random sampling from the unitary design approximates the full unitary 2-design.

[Can+20] further discuss how one can implement *logical unitary 2-designs*. By this they mean a unitary 2-design on a subspace that is protected by an error correcting code.

4.5 A unitary 3-design

We follow the ideas from [Can+20] and show that the Clifford group on qubits is a unitary 3-design. To do this we need the following lemma.

Lemma 4.5.1
Let $(w(a,b), w(a',b'))$ and $(w(c,d), w(c',d'))$ be pairs of commuting operators all different from the identity operator. Then there exists a symplectic matrix S, such that $(a,b)S = (c,d)$ and $(a',b')S = (c',d')$. In other words, the Clifford group acts transitively on pairs of nontrivial, commuting Weyl operators. Similarly, the Clifford group acts transitively on pairs of anticommuting Weyl operators.

Proof. Recall that $w(a,b)$ and $w(c,d)$ commute if using the symplectic bilinear form (3.7) we have that $[(a,b),(c,d)] = 0$. Denoting by $\{e_i\}_{i=1}^{2n}$ the standard basis vectors of $\mathbb{F}_2^{2n}$ it suffices to show that for any pair $(a,b),(c,d)$ such that $[(a,b),(c,d)] = 0$ there exists a symplectic matrix S such that $e_1S = (a,b)$ and $e_2S = (c,d)$. Picking the first two rows of S to be (a,b) and (c,d) and filling in the remaining rows to get a symplectic matrix one sees that there are many such matrices. The same argument works for anticommuting operators. ■

Theorem 4.5.2
The Clifford group is a unitary 3-design on qubits.

The proof is omitted in [Can+20], we provide a possible argument. A similar argument is used in [Web16], another argument is found in [Zhu17].

The proof takes up a bit of space, so before giving it, we discuss a few natural questions related to the result:

1. Is the Clifford design a unitary 3-design for other prime power dimensions?
2. Can we find subgroups of the Clifford group that are unitary 3-designs?
3. Is the Clifford group a t-design for any $t > 3$?

The answer to (1) and (3) is shown to be negative in both [Web16] and [Zhu17]. [Zhu17] goes on to show that except from dimension 4, the answer to (2) is negative as well. It is also interesting how both papers use different methods to reach their result. [Web16] uses the same approach as we use, namely decomposing intertwiners as Weyl operators, while [Zhu17] calculates the norm of the characters as in Proposition 2.1.1. In [Zhu+16] they show that the four-fold tensor product of the Clifford group affords only one more irreducible subspace than the four-fold tensor product of the unitary group. They describe the decomposition of this extra subspace in detail, and show that it is in fact a *stabiliser code*, which is an interesting result.

Proof of Theorem 4.5.2. Let $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ and recall the representation of S_3, $\tau \mapsto \sigma_\tau$ on $\mathcal{H}^{\otimes 3}$ defined by

$$\sigma_\tau(v_1 \otimes v_2 \otimes v_3) = v_{\tau^{-1}(1)} \otimes v_{\tau^{-1}(2)} \otimes v_{\tau^{-1}(3)}.$$

By Proposition 2.1.1, we need to show that twirling $X \in B(\mathcal{H}^{\otimes 3})$ by representatives of the Clifford group ($\mathcal{C}_{2,n}$) we have

$$\frac{1}{|\mathcal{C}_{2,n}|} \sum_{U \in \mathcal{C}_{2,n}} U^{\otimes 3} X (U^\dagger)^{\otimes 3} \in \operatorname{span}\left\{I, \sigma_{(12)}, \sigma_{(13)}, \sigma_{(23)}, \sigma_{(123)}, \sigma_{(132)}\right\}.$$

Throughout the proof we mostly write the Weyl operators as w_j instead of $w(a,b)$, except when writing $w(a,b)$ is used for explicit calculation. Recall further that Weyl operators on $B(\mathcal{H})$ are denoted by $\mathcal{W}_{2,n}$ and that they are self-adjoint.

Letting $d = 2^n$, we now decompose the permutation operators with respect to the basis of Weyl operators.

$$\begin{aligned}
\langle w_1 \otimes w_2 \otimes w_3 \,, \sigma_{12} \rangle &= \frac{1}{d^3} \sum_{i,j,k}^{d} \langle i|\, w_1 \,|j\rangle\langle j|\, w_2 \,|i\rangle\langle k|\, w_3 \,|k\rangle \\
&= \frac{1}{d^3} \operatorname{Tr}(w_1 w_2) \operatorname{Tr}(w_3) = \frac{1}{d}\, \delta_{w_1,w_2}\, \delta_{w_3,I}.
\end{aligned}$$

We get a similar decomposition for $\sigma_{(13)}$ and $\sigma_{(23)}$. For $\sigma_{(123)}$ we get:

$$\begin{aligned}
\langle w_1 \otimes w_2 \otimes w_3 \,, \sigma_{123} \rangle &= \frac{1}{d^3} \sum_{i,j,k=1}^{d} \langle i|\, w_1 \,|j\rangle\langle j|\, w_2 \,|k\rangle\langle k|\, w_3 \,|i\rangle \\
&= \frac{1}{d^3} \operatorname{Tr}(w_1 w_2 w_3) = \frac{1}{d^2} \delta_{(w_2 w_1),w_3}.
\end{aligned}$$

By similar calculations, we get a similar expression for $\sigma_{(132)}$. We thus have the operators:

$$\sigma_{(12)} = \frac{1}{d} \sum_{w \in \mathcal{W}_{2,n}} w \otimes w \otimes I, \ \ \sigma_{(13)} = \frac{1}{d} \sum_{w \in \mathcal{W}_{2,n}} w \otimes I \otimes w, \ \ \sigma_{(23)} = \frac{1}{d} \sum_{w \in \mathcal{W}_{2,n}} I \otimes w \otimes w,$$
$$\sigma_{(123)} = \frac{1}{d^2} \sum_{w_1, w_2 \in \mathcal{W}_{2,n}} w_1 \otimes w_2 \otimes w_2 w_1, \quad \sigma_{(132)} = \frac{1}{d^2} \sum_{w_1, w_2 \in \mathcal{W}_{2,n}} w_1 \otimes w_2 \otimes w_1 w_2.$$

Recalling that Weyl operators either commute or anticommute we note that

$$\begin{aligned} \sigma_{(123)} + \sigma_{(132)} &= \frac{1}{d^2} \sum_{w_1, w_2 \in \mathcal{W}_{2,n}} w_1 \otimes w_2 \otimes (w_2 w_1 + w_1 w_2) \\ &= \frac{2}{d^2} \sum_{\substack{w_1, w_2 \in \mathcal{W}_{2,n} \\ w_1 w_2 = w_2 w_1}} w_1 \otimes w_2 \otimes w_1 w_2, \\ \sigma_{(123)} - \sigma_{(132)} &= \frac{2}{d^2} \sum_{\substack{w_1, w_2 \in \mathcal{W}_{2,n} \\ w_1 w_2 = -w_2 w_1}} w_1 \otimes w_2 \otimes w_2 w_1. \end{aligned}$$

We use the technique of first twirling a basis-element by the Weyl operators and then by representatives of the Clifford group. The identity is clearly unaltered so we will consider non-identity elements below. Twirling $w(a,b) \otimes w(c,d) \otimes w(e,f)$ by the Weyl operators we get

$$\begin{aligned} &\frac{1}{d^2} \sum_{w(n,m) \in \mathcal{W}_{2,n}} \mathrm{Ad}_{w(n,m)^{\otimes 3}} (w(a,b) \otimes w(c,d) \otimes w(e,f)) \\ &\qquad = \frac{1}{d^2} \sum_{w(n,m) \in \mathcal{W}_{2,n}} \zeta((n,m),(a+c+e, b+d+f)) w(a,b) \otimes w(c,d) \otimes w(e,f) \end{aligned}$$

which equals 0 if $w(a,b)w(c,d) \neq \pm w(e,f)$. This gives two cases to examine for the full Clifford twirl:

1. Two Weyl operators are equal and the third is the identity operator.
2. None of the three Weyl operators w_1, w_2 and w_3 is the identity.

In the first case, the transitive action of the Clifford group on the nontrivial Weyl operators implies that that if $w_i = w_j$ then the twirl of this operator belongs to $\mathrm{span}(\left\{I, \sigma_{(ij)}\right\})$.

For the second case, assume that $w_3 = w_1 w_2$ and $w_1 w_2 = -w_2 w_1$. The transitive action of the Clifford group on pairs of anticommuting Weyl operators (Lemma 4.5.1) implies that twirling $w_1 \otimes w_2 \otimes w_1 w_2$ by the Clifford group gives an operator proportional to

$$\sum_{\substack{w, w' \in \mathcal{W}_{2,n} \\ ww' = -w'w}} w \otimes w' \otimes ww' = \frac{d^2}{2} (\sigma_{(123)} - \sigma_{(132)}).$$

If w_1 and w_2 commute, we get an operator proportional to

$$\frac{d^2}{2} (\sigma_{(123)} + \sigma_{132}) + 2I - d(\sigma_{(12)} + \sigma_{(13)} + \sigma_{(23)})$$

using the identities listed above. This completes the proof. ∎

Chapter 5

Applications

In this chapter we will demonstrate how twirling can be used for error correction and fidelity estimation.

5.1 Average and entanglement fidelity estimation

In this section we briefly go through an application of fidelity estimation discussed in [Dan+09]. *Entanglement fidelity* is a measure of how well a quantum channel preserves entanglement and is defined in the following way:

Definition 5.1.1 (Entanglement fidelity)
Let $\phi : B(\mathcal{H}_A)$ be a quantum channel, $\rho \in B(\mathcal{H}_B \otimes \mathcal{H}_A)$ a maximally entangled state. The *entanglement fidelity* of ϕ, $F_{\mathrm{e}}(\phi)$ is defined as

$$F_{\mathrm{e}}(\phi) := \mathrm{Tr}\Big(\rho^\dagger (\mathrm{id} \otimes \phi)(\rho)\Big).$$

This is well defined since if ρ' is another maximally entangled state we have that $\rho' = \mathrm{Ad}_{I\otimes U}(\rho)$ for some $U \in \mathcal{U}(\mathcal{H}_A)$. One then checks that

$$\mathrm{Tr}\Big(\rho^\dagger (\mathrm{id} \otimes \phi)(\rho)\Big) = \mathrm{Tr}\Big(\rho'^\dagger (\mathrm{id} \otimes \phi)(\rho')\Big).$$

From this it is not difficult to see that if $\mathcal{D}$ is a collection of unitaries, then $F_e(\phi) = F_e(\widetilde{\phi}_{\mathcal{D}})$, i.e, entanglement fidelity is invariant under twirling by unitaries. Again letting $\widetilde{\phi}_{\mathcal{U}(\mathcal{H}_A)}$ be as in (2.5) we have that

$$\widetilde{\phi}_{\mathcal{U}(\mathcal{H}_A)} = p\,\mathrm{Tr}(\cdot)\frac{I}{d} + (1-p)\mathrm{id} \tag{5.1}$$

for some $p \in [0,1]$. Doing the calculations one then gets that

$$F_e(\phi) = \frac{p}{d^2} + (1-p). \tag{5.2}$$

Entanglement fidelity is related to the *average fidelity*, F_{avg}, of a channel defined by

$$F_{\mathrm{avg}}(\phi) := \int_{\mathcal{U}(\mathcal{H}_A)} \mathrm{Tr}\Big(U\,|0\rangle\langle 0|\,U^\dagger \phi(U\,|0\rangle\langle 0|\,U^\dagger)\Big)\,\mathrm{d}U = \langle 0|\,\widetilde{\phi}_{\mathcal{U}(\mathcal{H}_A)}(|0\rangle\langle 0|)\,|0\rangle\,. \tag{5.3}$$

It is clear that F_{avg} is invariant under twirling by unitaries. Combining this with (5.1) we get that $F_{\text{avg}}(\phi) = \frac{p}{d} + (1-p)$. Using (5.2) we then get

$$F_{\text{avg}} = \frac{dF_{\text{e}} + 1}{d+1}.$$

Implementing a unitary 2-design, for example as in Proposition 4.4.5, we would get a simple way of measuring both *average* and *entanglement fidelity* via the final equality in (5.3).

5.2 Twirling noisy channels

In this section we will discuss an application of twirling in quantum error correction outlined in [CB19]. We rephrase their exposition using that the commutator relation between the Weyl operators is a symplectic bicharacter which clarifies the ideas.

For circuits used in error correction, there is an error-threshold of the components below which errors can be made arbitrarily small by scaling the error correcting code. Obtaining the threshold can introduce noise and we will show how one can use twirling to convert this noise to channels of the form

$$\sum_{j=1}^{k} p_j w_{2,n}(a_j, b_j).$$

Such channels are called *Pauli-channels* and can be simulated effectively on classical computers as shown in [AG04]. Note that we will keep referring to the operators $\mathcal{W}_{2,n}$ as Weyl operators. From the calculations done in previous chapters, it is clear that twirling by the full set of Weyl operators will reduce any noise channel to a Pauli-channel. We demonstrate here a technique that reduces the size of the twirling set to be comparable to the *Weyl-basis* of the error.

Given an n-qubit system and a noise channel ϕ our goal is to construct a twirling set $\mathcal{D}$ such that the twirled channel of ϕ is a Pauli-channel i.e $\widetilde{\phi}_{\mathcal{D}} = \sum_{w \in \mathcal{W}_{2,n}} p_w \text{Ad}_w$. First we will introduce some requirements on the twirling set.

5.2.1 Requirements of twirling set

Since any channel ϕ can be decomposed as

$$\phi = \sum_{j=1}^{N} \text{Ad}_{M_j}, \quad \sum_{j=1}^{N} M_j^\dagger M_j = I,$$

it suffices to consider noise channels of the form $\phi = \text{Ad}_M$. Let V be the *Weyl-basis* for M, i.e

$$V := \{ v \in \mathcal{W}_{2,n} | \operatorname{Tr}(Mv) \neq 0 \}.$$

Then we have

$$M = \frac{1}{2^n} \sum_{v \in V} \operatorname{Tr}(Mv) v.$$

Recall that the commutator relation $w_1 w_2 = \zeta(w_1, w_2) w_2 w_1$ is a symplectic bicharacter defined by Equation (4.7). Twirling ϕ by a set $\mathcal{D}$ and using the isomorphism

$(X \mapsto AXB^\dagger) \mapsto A \otimes \overline{B}$ (Section 1.2), we get

$$\begin{aligned}\widetilde{\phi}_{\mathcal{D}} \mapsto \frac{1}{2^{2n}|\mathcal{D}|} \sum_{v,v' \in V} \mathrm{Tr}(Mv)\overline{\mathrm{Tr}(Mv')} \sum_{w \in \mathcal{D}} wvw \otimes \overline{wv'w} \\ = \frac{1}{2^{2n}|\mathcal{D}|} \sum_{v,v' \in V} \mathrm{Tr}(Mv)\overline{\mathrm{Tr}(Mv')} v \otimes \overline{v'} \sum_{w \in \mathcal{D}} \zeta(w, vv') \\ = \frac{1}{2^{2n}} \sum_{v \in V} |\mathrm{Tr}(Mv)|^2 v \otimes \overline{v} + \frac{1}{2^{2n}|\mathcal{D}|} \sum_{\substack{v,v' \in V \\ v \neq v'}} n\, \mathrm{Tr}(Mv)\overline{\mathrm{Tr}(Mv')} v \otimes \overline{v'} \sum_{w \in \mathcal{D}} \zeta(w, vv').\end{aligned}$$

This becomes a Pauli-channel if and only if the second term in the last channel is 0 i.e

$$\sum_{w \in \mathcal{D}} \zeta(w, vv') = 0 \quad \text{for all } v \neq v'. \tag{5.4}$$

This holds in particular if $\mathcal{D}$ is a group and $\zeta(\cdot, vv')$ defines a nontrivial character for $v \neq v'$. This is really the same as $\zeta(\cdot, v)$ defining a nontrivial character for all non-identity elements $v \in V$. We will now lay out a method for constructing such sets. The idea here is to get a basis for the noise and generate a group from this. The dual of this group is then such a set.

5.2.2 Construction of twirling set

We start this section out by a quick introduction of language following [CB19]. For the Weyl-operators, define the $*$-operation by: $w(a, b) * w(c, d) = w(a + b, c + d)$. This corresponds multiplication by the elements in $PU(\mathbb{C}^{2^{\otimes n}})$ and makes $\mathcal{W}_{2,n}$ into a group. In this section we will often write elements of $\mathcal{W}_{2,1}$ by their standard Pauli operators, i.e

$$w_2(0, 0) = I, \quad w_2(1, 0) = Z, \quad w_2(0, 1) = X, \quad w_2(1, 1) = Y.$$

The construction in [CB19] relies on the notion of a *commutator table* defined below.

Definition 5.2.1 (Commutator table)
For $Q, H \subset \mathcal{W}_{2,n}$ a commutator table of Q and H is defined to be:

	h_1	h_2	...
q_1	$\zeta(q_1, h_1)$	$\zeta(q_1, h_2)$	...
q_2	$\zeta(q_2, h_1)$	$\zeta(q_2, h_2)$	...
$\vdots$	$\vdots$	$\vdots$	$\ddots$

Since $\zeta(\cdot, v)$ and $\zeta(v, \cdot)$ are both homomorphisms under standard multiplication they are homomorphisms under the $*$-operation. This gives the following row- and column composition by element wise multiplication:

$$\text{row; } \zeta(a_i * a_j, b_k) = \zeta(a_i, b_k)\zeta(a_j, b_k),$$
$$\text{column; } \zeta(a_i, b_j * b_k) = \zeta(a_i, b_j)\zeta(a_i, b_k).$$

We will now use these ideas to create a twirling set in a simple case.

Example 5.2.2
Consider the 2-qubit Hilbert space $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$. For $A, B \in B(\mathbb{C}^2)$ we will denote $A \otimes B$ by AB through this example for ease of writing. Assume we have an error Ad_M where M is proportional to

$$XY + YZ + ZX.$$

The *Weyl-basis* for M is:

$$V = \{XY, YZ, ZX\}.$$

We see that $XY * YZ = ZX$. If we can find elements $A, A' \in B(\mathcal{H})$ such that $\zeta(A, XY) = \zeta(A', YZ) = -1$ and $\zeta(A', XY) = \zeta(A, YZ) = 1$, then taking our twirling set $\mathcal{D}$ as the group generated by A, A' should work. We can pick the operators IZ and XI to generate the group $\mathcal{D} := \{II, IZ, XI, XZ\}$. Table 5.1 is a commutator table for $\mathcal{D}, V$ and we see that $\zeta(\cdot, A)$ indeed defines a nontrivial character for all $A \in V$.

Table 5.1: Commutator table for our twirling set $\mathcal{D}$ and the Pauli-basis V of M

	XY	YZ	ZX
IZ	-1	1	-1
XI	1	-1	-1
XZ	-1	-1	1
II	1	1	1

In the table we have added an extra horizontal and vertical line. These indicate that the table could be generated by row and column operations from the "inner table". The size of $\mathcal{W}_{2,2}$ is 16, but the size of our group is 4 and thus we have a quadratic reduction.

Note that it is important that for the generating elements A of $\mathcal{D}$ we have $\zeta(A, XY) \neq \zeta(A, YZ)$. This is illustrated by picking generating elements $\{ZI, IX\}$ to get $G = \{II, ZI, IX, ZX\}$, see Table 5.2.

Table 5.2: Commutator relations in the group G and the Pauli-basis V of M

	XY	YZ	ZX
ZI	-1	-1	1
IX	-1	-1	1
ZX	1	1	1
II	1	1	1

Here the both XY and YZ defines nontrivial characters on G but ZX does not and hence Equation (5.4) is not satisfied.

We will now go through a systematic way of constructing the twirling sets based on [CB19], where they first introduce a *generator table* which is really the "inner table" in Example 5.2.2 above.

Definition 5.2.3 (Generator table)
A generator table for $Q, H \in \mathcal{W}_{2,n}$ is a commutator table with values

$$\zeta(q_j, h_k) = 1 - 2\delta_{jk}.$$

The rows and columns of such a table are independent in the sense that they cannot be obtained from each other under row- and column composition. Composing row elements generates a group and columns become nontrivial characters for this group. Since the $*$-operation is commutative and every nontrivial element has order 2, the above discussion of course works for the abelian groups $\mathbb{Z}_2^n$. This table can be used to construct a twirling set as described below.

Steps to construct twirling set $\mathcal{D}$ (from [CB19])

1. Decompose M to its Pauli basis V.

2. Find the sets:
   $\widetilde{V}$: A smallest set such that elements of $V \setminus \widetilde{V}$ are compositions of elements in $\widetilde{V}$.
   $\widetilde{V}_s$: The elements in $\widetilde{V}$ used to generate elements in $V \setminus \widetilde{V}$.

3. Find smallest integer N satisfying the equations

$$N \geq \log_2(|V|),$$
$$N \geq \left|\widetilde{V}_s\right|.$$

4. Let $H = \mathbb{Z}_2^N$ and $\tilde{H}$ be a generating set of H. The previous step ensures that we can construct a map from V into H which gives a commutator table.

5. Map elements V to H using the following steps:
   a) Define an injective map from $\widetilde{V}_s$ to a subset of elements in $\tilde{H}$.
   b) Map $V \setminus \widetilde{V}$ to elements in $H \setminus \tilde{H}$ by following composition relations in the previous map.
   c) Map elements in $\widetilde{V} \setminus \widetilde{V}_s$ to any subset of remaining elements in H.
   a)-c) tell how V is mapped to H.

6. Create a generator table $\zeta(q_i, h_j)$ of size N. From column compositions we can get a commutator table where we can identify the values $h \in H$, with the column as elements $v \in V$.

7. Find elements $w_i \in \mathcal{W}_{2,n}$ such that $\zeta(w_i, v_j) = \zeta(q_i, h_j)$ and let $\tilde{\mathcal{D}} := \{w_1, ..., w_N\}$.

8. One can then twirl by $\mathcal{D} := \langle\tilde{\mathcal{D}}\rangle$ or by all sets $\{I, w\}$, $w \in \mathcal{D}$.

Note that there can be many generating sets $\tilde{\mathcal{D}}$.

Remark 5.2.4. The algorithm suggested can be extended to non-qubit spaces. Given an error M one identifies the Weyl-basis V for M. Then one generates a group in PU($\mathcal{H}$) from V. The *dual* of this group then gives a twirling set satisfying Equation (5.4).

In their paper [CB19] ask how given two errors, M, N one can construct a twirling set for MN. Labeling the Weyl-bases for M, N by V_M, V_N respectively, we generate the group $G := \langle V_M \cup V_N\rangle$. Pick $\mathcal{D}$ to be a twirling set obtained from finding a generating set of G and constructing a generator table as explained. If E is an error which is a polynomial in M and N we then have that $\widetilde{E}_{\mathcal{D}}$ is a Pauli-channel.

5.2.3 Twirling and stabiliser measurement

We follow [CB19], and show that if we have a subspace $\mathcal{H}_L \subset \mathcal{H}$ defined by a *stabiliser group* (Section 4.1), then for any stabiliser s of $\mathcal{H}_L$, twirling by $\{I, s\}$ and performing stabiliser measurements (Section 1.3.1) of s are equivalent. Assume again we have some noise M with Pauli basis V. We can write

$$M = M_+ + M_-,$$

where M_+, (respectively M_-), are sums of elements in V that commutes, (respectively anticommutes), with s. Twirling Ad_M by $\{I, s\}$ we get

$$\widetilde{\mathrm{Ad}}_{M\{I,s\}} = \frac{1}{2}\left(\mathrm{Ad}_M + \mathrm{Ad}_{sMs}\right) = \frac{1}{2}\left(\mathrm{Ad}_{(M_+ + M_-)} + \mathrm{Ad}_{(M_+ - M_-)}\right) = \mathrm{Ad}_{M_+} + \mathrm{Ad}_{M_-}.$$

For an s-stabiliser measurement first recall that the operators

$$\frac{1+s}{2} \quad \text{and} \quad \frac{1-s}{2}$$

project onto the ± 1-eigenspaces of s. Then observe that

$$\begin{aligned} sM &= \frac{1+s}{2}(M_+ + M_-) - \frac{1-s}{2}(M_+ + M_-) \\ &= \left(M_+\frac{1+s}{2} - M_-\frac{1-s}{2}\right) - \left(M_+\frac{1-s}{2} - M_-\frac{1+s}{2}\right) = M_+ s + M_- s. \end{aligned}$$

Thus for $|\psi\rangle \in \mathcal{H}_L$, $M_+|\psi\rangle$ and $M_-|\psi\rangle$ are the projections of $M|\psi\rangle$ onto the ± 1-eigenspaces of s. If we then perform a stabiliser measurement on $|\psi\rangle\langle\psi|$ and ignore the result, we end up with

$$M_+ |\psi\rangle\langle\psi| M_+ + M_- |\psi\rangle\langle\psi| M_- = \widetilde{\mathrm{Ad}}_{M\{I,s\}}(|\psi\rangle\langle\psi|).$$

Thus the stabiliser measurement and the twirling are equivalent in the logical subspace $\mathcal{H}_L$.

Conclusion

We have explored the theory of unitary t-designs and some of their applications in quantum information.

Our focus has been on unitary 2-designs, with a construction of the Clifford design and techniques for making it smaller as main points. Additionally, we have shown that for qubits, the Clifford design is actually a 3-design, and we obtained an effective way of sampling from a unitary 2-design in this case. It would be interesting to see if this method of sampling extends beyond the qubit case.

We have also shown that unitary 2-designs containing nontrivial, normal abelian subgroups are equivalent to Clifford designs, which is a new result. As a corollary, if G is a group (in $\mathrm{PU}(\mathcal{H})$) but not a Clifford-type design, we cannot have $N_p = 1$ for any Sylow p-subgroup of G. It seems that this is a significant restriction to which orders can be non-Clifford designs.

It would be interesting to further investigate how significant a restriction this is. For example, one could investigate whether non-Clifford designs can be a product of groups.

Finally, we have briefly covered an application of unitary 2-designs in fidelity estimation, and discussed how twirling can be used to transform noise channels to Pauli channels.

References

[AG04] Aaronson, S. and Gottesman, D. 'Improved simulation of stabilizer circuits'. In: *Phys. Rev. A* 70 (5 Nov. 2004), p. 052328. DOI: 10.1103/PhysRevA.70.052328.

[Can+20] Can, T. et al. 'Kerdock Codes Determine Unitary 2-Designs'. In: *IEEE Transactions on Information Theory* 66.10 (Oct. 2020), pp. 6104–6120. DOI: 10.1109/tit.2020.3015683.

[CB19] Cai, Z. and Benjamin, S. C. 'Constructing Smaller Pauli Twirling Sets for Arbitrary Error Channels'. In: *Scientific Reports* 9.1 (2019), p. 11281. DOI: 10.1038/s41598-019-46722-7.

[Cha05] Chau, H. 'Unconditionally Secure Key Distribution in Higher Dimensions by Depolarization'. In: *IEEE Transactions on Information Theory* 51.4 (Apr. 2005), pp. 1451–1468. DOI: 10.1109/tit.2005.844076.

[Dan+09] Dankert, C. et al. 'Exact and approximate unitary 2-designs and their application to fidelity estimation'. In: *Phys. Rev. A* 80 (1 July 2009), p. 012304. DOI: 10.1103/PhysRevA.80.012304.

[Dan05] Dankert, C. *Efficient Simulation of Random Quantum States and Operators*. 2005. arXiv: quant-ph/0512217 [quant-ph].

[Eti+11] Etingof, P. et al. *Introduction to representation theory*. 2011. arXiv: 0901.0827 [math.RT].

[GAE07] Gross, D., Audenaert, K. and Eisert, J. 'Evenly distributed unitaries: On the structure of unitary designs'. In: *Journal of Mathematical Physics* 48 (Oct. 2007), p. 052104. DOI: 10.1063/1.2716992.

[Got97] Gottesman, D. *Stabilizer Codes and Quantum Error Correction*. 1997. arXiv: quant-ph/9705052 [quant-ph].

[Kar80] 'Chapter 8 Projective Representations of Abelian Groups'. In: *Group Representations*. Ed. by Karpilovsky, G. Vol. 180. North-Holland Mathematics Studies. North-Holland, 1980, pp. 357–389. DOI: https://doi.org/10.1016/S0304-0208(09)70080-5.

[Lan] Lange, J. https://github.com/Kortelange/master_thesis.

[Wat18] Watrous, J. *The theory of quantum information*. eng. Cambridge, 2018.

[Web16] Webb, Z. *The Clifford group forms a unitary 3-design*. 2016. arXiv: 1510.02769 [quant-ph].

[Zhu+16] Zhu, H. et al. *The Clifford group fails gracefully to be a unitary 4-design*. 2016. arXiv: 1609.08172 [quant-ph].

[Zhu17] Zhu, H. 'Multiqubit Clifford groups are unitary 3-designs'. In: *Physical Review A* 96.6 (Dec. 2017). DOI: 10.1103/physreva.96.062336.