Quantum Designs

Foundations of a
non-commutative Design Theory

by

Gerhard Zauner
Zieglergasse 45/13, 1070 Vienna, Austria
Email: mail@gerhardzauner.at

Translation of the Thesis

"Quantendesigns, Grundzüge einer nichtkommutativen Designtheorie"

which was submitted in fulfillment of the requirements for the
academic Degree of Doctor of Natural Sciences
at the University of Vienna

Vienna 1999

I would like to thank Prof. Dr. Neumaier for supervising this thesis, and for many stimulating discussions. I am also grateful to Dr. Göttfert for his efforts in refereeing this work.

Preface to the English translation (11 years after)

This Ph.D. thesis - written in German language - was accepted at the University of Vienna in 1999. Prof. Arnold Neumaier afterwards kindly made it available on his homepage[1].

To my suprise it was discovered there a few years later and several dozens of articles cited it since. This English translation shall help to make it easier accessible.

Quantum Designs are sets of orthogonal projection matrices in finite dimensional Hilbert Spaces (I used the letter b for the dimension throughout this paper, to emphasize a parallel to classical (combinatorial) design theory, explained in chapter 1.2), with certain features (described in greater detail in chapter 1.1):

A fundamental differentiation is whether the quantum design is *regular*, which means if all projections (subspaces projected on) have same dimension r, and furthermore the special case $r = 1$ (this means that the subspaces are spanned by single (unit) vectors).

Two classes of (complex) quantum designs with $r = 1$ got much attention in the literature in the last years (just as they play a central role in my thesis):

- *MUBs (Mutually Unbiased Bases)* are called in my thesis regular and *affine quantum designs* with $r = 1$.

  The maximum number of MUBs is $b + 1$. Sets of $b + 1$ MUBs when b is a prime were first found by I.D.Ivanovic (1981, 1997)[2]. W.K.Wootters and B.D.Fields established (1989)[3] the term *"mutually unbiased"* and gave solutions of $b + 1$ MUBs whenever b is a power of a prime.

  Not aware of these papers this concept was independently rediscovered and generalized to irregular designs (independent observables, see chapter 1.3) already in my master thesis (1991) and later summarized and embedded in a more general context in this doctoral thesis again.

  Also (already in my master thesis and here) maximal solutions were given for the general case of regular affine quantum designs with $r \geq 1$ consisting of $r(b^2 - 1)/(b - r)$ so called *complete orthogonal classes* whenever b is a powers of a prime (chapter 3.2).

  As well already in my master thesis and here for $b = 6$ an infinite family of MUB-triples was constructed and it was (probably the first time) conjectured that 4 MUBs don't exist in this dimension (chapter 3.3).

[1] http://www.mat.univie.ac.at/ neum/ms/zauner.pdf

[2] Ivanovic, I D.: Geometrical description of quantal state determination, *J.Phys.A: Math.Gen* **14** (1981), 3241–3245, Unbiased projector base over $\mathbb{C}^3$, *Phys. Letters* **228** (1997)

[3] Wootters, W.K. and Fields, B.D.: Optimal State-Determination by Mutually Unbiased Measurements, *Annals of Physics* **191** (1989), 363–381.

- *SIC POVMs (Symmetric Informationally Complete Positive Operator Valued Measures)* are called in my thesis regular *quantum designs with degree 1*, $r = 1$ and b^2 elements.

  The assigned vectors span b^2 equiangular lines. Equiangular lines were first investigated by J.J.Seidel et.al. (1966, 1973, ...)[4], mainly for the real case. S.G.Hoggar (1982)[5] analyzed the complex case and gave solutions (of b^2 vectors) for $b = 2, 3$ and 8.

  In this thesis further maximal analytic and numerical solutions weren given (see chapter 3.4) and it was (probably the first time) conjectured that such solutions in the complex case exist in any dimension b (generated by the Weyl-Heisenberg group and with a certain additional symmetry of order 3).

  J.M.Renes, R.Blume-Kohout, A.J.Scott and C.M.Caves (2003)[6] independently (not aware of this thesis) analyzed the same structures in 2003, gave further numerical solutions and coined the term SIC-POVM, which is standard in literature since.

I would like to thank Dr. Rania Wazir for doing most of the translation of this thesis to English.

Gerhard Zauner, Vienna, 2010-07-16

[4] see e.g. references [52, 55] in the thesis

[5] see reference [43] in the thesis

[6] Renes, J., Blume-Kohout, R., Scott, A.J. and Caves, C.M.: Symetric Informationally Complete Quantum Measurements, *Journal of Mathematical Physics* **45**(6) (2004), 2171–2180, Preprint quant-ph/0310075.

Contents

Preface

This thesis initiated with a series of investigations into the probabilistic structures that lie at the foundation of quantum theory. During the course of this research, new relations to combinatorial design theory were discovered. Just as quantum mechanics is a non-commutative generalization of classical mechanics, the theory which will be proposed here can be considered a non-commutative generalization of classical, combinatorial design theory. Besides we will also generalize concepts from the theory of spherical designs.

Let V be a finite-dimensional complex (or real) vector space with an inner product. In this paper, we will consider sets of subspaces of V (in analogy with classical design theory, which studies sets of subsets of a given finite set). We will also briefly discuss infinite-dimensional Hilbert spaces in section 1.3.

Every linear subspace of V has an associated linear map $\mathbf{P}$, which projects all vectors in V orthogonally onto the subspace. We will assume throughout this paper, that an ordered orthonormal basis for V is given. We will talk about matrices rather than linear maps; that is, the main object of this paper are sets of orthogonal projection matrices $\mathbf{P}$. It is well-known that such matrices have the following two properties (see [39] and [57]): Orthogonal projections are *idempotent*, i.e. $\mathbf{P}^2 = \mathbf{P}$; furthermore, they are *self-adjoint*, i.e. $\mathbf{P} = \mathbf{P}^*$, where $\mathbf{P}^*$ is the adjoint (i.e. transposed and complex conjugated) matrix of $\mathbf{P}$. Conversely, one can show that every idempotent and self-adjoint matrix corresponds to an orthogonal projection. The trace of the orthogonal projection (i.e. the sum of the diagonal entries of the matrix written w.r.t. any arbitrary orthonormal basis for V) equals the *dimension* r of the associated linear subspace.

Quantum designs are sets of orthogonal projection matrices with additional properties, which will be defined in greater detail in the first section. Their interpretations from the points of view of three well-known theories will be explored in the remaining sections of the first part of this article. The special case of mutually commuting projection matrices renders the definitions and structures of classical, combinatorial design theory. Next, we will give a brief introduction to probability theory, which forms the basis for quantum theory, and we will show that the elements of the generalized design theory in complex vector spaces developed in this paper have a natural interpretation using this formalism. Finally, we introduce the concept of spherical t-designs and its various generalizations, which are closely connected with quantum designs.

In the second part of the paper, we develop some elements of the general theory further. We derive several bounds, construct a duality operation, and investigate automorphism groups. These results are then applied to two classes of quantum designs which generalize the most well-known classical combinatorial designs: *balanced incomplete block designs* and *affine designs*.

In the third part of the paper, several basic constructions for the abovementioned classes of quantum designs are discussed. In particular, we construct infinitely-many 2-designs over complex projective spaces. The methods we will apply are closely related to quantum theoretical formalisms in infinite-dimensional Hilbert spaces.

Finally, we list some open questions and suggestions for further investigations in the epilogue.

The following notation will be used throughout this paper:

- $\mathrm{tr}(\mathbf{A})$ denotes the trace of the matrix $\mathbf{A}$.
- $\mathbf{A} \otimes \mathbf{B}$ is the *Kronecker (or tensor) product* of the two matrices $\mathbf{A}$ and $\mathbf{B}$. The t-fold tensor product of the matrix $\mathbf{A}$ with itself is denoted by

$$\otimes^t \mathbf{A} = \underbrace{\mathbf{A} \otimes \cdots \otimes \mathbf{A}}_{t}.$$

- The group of all unitary (orthogonal) $b \times b$ matrices is denoted $U(b)$ (respectively $O(b)$). $S(b)$ is the group of all $b \times b$ permutation matrices, and consists of $b!$ elements.
- The set of all complex (or real) orthogonal projection matrices with a given trace r can be identified with the so-called complex (resp. real) Grassmannian (manifold) of the r-dimensional subspaces of $\mathbb{C}^b$ (resp. $\mathbb{R}^b$). We denote it by $G_r(\mathbb{C}^b)$ (resp. $G_r(\mathbb{R}^b)$).
- We denote by $\mathbb{J}_r^b$ the set of all diagonal projection matrices with a given trace r.

1 Basics

1.1 Definitions

Definition 1.1. A *quantum design* is a set $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ $(v \geq 2)$ of complex (or real) orthogonal $b \times b$ projection matrices.

- $\mathbf{D}$ is said to be *regular* if there exists an $r \in \mathbb{N}$ such that

$$\mathrm{tr}(\mathbf{P}_i) = r \qquad \text{for all } 1 \leq i \leq v. \tag{1.1}$$

- $\mathbf{D}$ is called *coherent* if there exists a $k \in \mathbb{R}$ such that

$$\mathbf{P}_1 + \cdots + \mathbf{P}_v = k\mathbf{I}, \tag{1.2}$$

  where $\mathbf{I}$ is the identity matrix.

- Let G be an arbitrary group of unitary $b \times b$ matrices. Then $\mathbf{D}$ is *t-coherent with respect to the group G* if the following relation holds for all matrices $\mathbf{U} \in G$:

$$\sum_{i=1}^{v} \otimes^t \mathbf{P}_i = \sum_{i=1}^{v} \otimes^t (\mathbf{U}\mathbf{P}_i\mathbf{U}^{-1}). \tag{1.3}$$

- A quantum design $\mathbf{D}$ that is s-coherent with respect to G for all $s \leq t$ is called a *quantum t-design w.r.t. G*. The *strength t w.r.t. G* is the maximal value of t such that $\mathbf{D}$ is a quantum t-design w.r.t. G.

- The cardinality of the set

$$\Lambda = \{\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j) : \ 1 \leq i \neq j \leq v\} = \{\lambda_1, \ldots, \lambda_s\}. \tag{1.4}$$

  is called the *degree s* of $\mathbf{D}$. In particular, $\mathbf{D}$ has degree 1 if and only if there exists a $\lambda \in \mathbb{R}$ such that

$$\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j) = \lambda \qquad \text{for all } 1 \leq i \neq j \leq v. \tag{1.5}$$

- A subset of $\mathbf{D}$ is an *orthogonal class* if the corresponding projections are mutually orthogonal. If the sum of all its projection matrices adds up to the identity matrix, then an orthogonal class is said to be *complete*. A quantum design is called *resolvable* if it can be written as the disjoint union of complete orthogonal classes.

- A degree 2 (i.e. $\Lambda = \{0, \lambda \neq 0\}$) resolvable quantum design will be called an *affine quantum design*.

All of these properties are preserved under base change by a matrix $U \in G$. In general, the indices of the projection matrices are not relevant - when instead the order is important, we will speak of an *ordered quantum design*.

Definition 1.2. Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ and $\mathbf{D}' = \{\mathbf{P}'_1, \ldots, \mathbf{P}'_v\}$ be two quantum designs. They are said to be *equivalent* or *isomorphic* if there is a $b \times b$ matrix $\mathbf{U} \in U(b)$ and a permutation π of $\{1, \ldots, v\}$ such that

$$\mathbf{P}'_i = \mathbf{U}\mathbf{P}_{\pi(i)}\mathbf{U}^{-1} \qquad \text{for all } 1 \leq i \leq v.$$

It is also possible that $\mathbf{U}$ equals $\mathbf{I}$, i.e. only permutation takes place.

If a quantum design is coherent, then $\sum_{i=1}^{v} \mathbf{P}_i = k\mathbf{I}$ commutes with every matrix, i.e. the quantum design is 1-coherent w.r.t. every group G. The converse also holds.

Proposition 1.3. *Let G be any irreducible group (that is, there is no subspace invariant w.r.t. all group elements). A quantum design is coherent exactly when it is* 1*-coherent w.r.t. G.*

Proof. We have already showed one direction. To prove the other direction, suppose that $\sum_{i=1}^{v} \mathbf{P}_i = \mathbf{U}\left(\sum_{i=1}^{v} \mathbf{P}_i\right)\mathbf{U}^{-1}$ for all $\mathbf{U} \in G$. Then we can apply the well-known *Lemma of Schur* (see e.g. [21, Lemma 27.3]), and it follows that $\sum_{i=1}^{v} \mathbf{P}_i = k\mathbf{I}$. □

In particular, it follows that quantum designs are 1-coherent w.r.t. the orthogonal, unitary, or permutative groups if and only if the quantum design is coherent. However, for $t \geq 2$ these three definitions no longer coincide.

Proposition 1.4. *Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a coherent quantum design with $\operatorname{tr}(\mathbf{P}_i) = r_i$, $1 \leq i \leq v$. Then the following equation holds:*

$$\sum_{i=1}^{v} r_i = bk. \tag{1.6a}$$

This shows that k must be an element of $\mathbb{Q}$. If in addition $\mathbf{D}$ is regular, then it follows that

$$vr = bk. \tag{1.6b}$$

Proof. Apply the trace function to equation (1.2). □

It becomes immediately clear that every resolvable quantum design, and hence every affine quantum design, is coherent. In this context, the integer k denotes the number of orthogonal classes. We will derive other properties in the next chapter, and proceed here with some more definitions.

Definition 1.5. Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be an arbitrary quantum design, and set

$$\overline{\mathbf{P}}_i = \mathbf{I} - \mathbf{P}_i \qquad \text{for all } 1 \leq i \leq v.$$

Then $\overline{\mathbf{D}} = \left\{\overline{\mathbf{P}}_1, \ldots, \overline{\mathbf{P}}_v\right\}$ is said to be the *complementary* design to $\mathbf{D}$.

The complementary design $\overline{\mathbf{D}}$ has the same parameters v and b as $\mathbf{D}$. The following properties are easily checked: $\overline{\mathbf{D}}$ is regular if and only if $\mathbf{D}$ is regular, and the following relation holds: $\overline{r} = b - r$. $\overline{\mathbf{D}}$ is coherent if and only if $\mathbf{D}$ is coherent, and the following relation holds: $\overline{k} = v - k$. In the case of regular quantum designs, $\overline{\mathbf{D}}$ has the same degree s as $\mathbf{D}$, with $\overline{\lambda_i} = b - 2r + \lambda_i$ for $1 \leq i \leq s$. Furthermore, $\overline{\overline{\mathbf{D}}} = \mathbf{D}$.

Theorem 1.6. $\mathbf{D}$ *is a quantum t-design with respect to an arbitrary group $G \subseteq U(b)$ exactly when its complementary design $\overline{\mathbf{D}}$ is.*

Proof. Let $\mathbf{U} \in G$ and $s \leq t$.

$$\sum_{i=1}^{v} \otimes^s(\mathbf{U}(\mathbf{I} - \mathbf{P}_i)\mathbf{U}^{-1}) = \sum_{i=1}^{v} \otimes^s(\mathbf{I} - \mathbf{U}\mathbf{P}_i\mathbf{U}^{-1})$$

can be written as the sum of 2^s terms such that each term, via a unitary $b^s \times b^s$ matrix (that permutes tensor products and commutes with all matrices of them form $\otimes^s\mathbf{U}$), is equivalent to

$$\sum_{i=1}^{v} \left(\otimes^{(s-j)}\mathbf{I}\right) \otimes \left(\otimes^j(\mathbf{U}\mathbf{P}_i\mathbf{U}^{-1})\right) = \sum_{i=1}^{v} \left(\otimes^{(s-j)}\mathbf{I}\right) \otimes \left(\otimes^j\mathbf{P}_i\right)$$

for some $0 \leq j \leq s$ by using the j-coherence for $j \leq s$. The s-coherence of $\overline{\mathbf{D}}$ for all $s \leq t$ follows. Since $\overline{\overline{\mathbf{D}}} = \mathbf{D}$, this proves the theorem. $\square$

Clearly the *union* $\mathbf{D} \cup \mathbf{D}' = \{\mathbf{P}_1, \ldots, \mathbf{P}_v, \mathbf{P}'_1, \ldots, \mathbf{P}'_{v'}\}$ of two quantum designs $\mathbf{D}$ and $\mathbf{D}'$ is regular and/or t-coherent (resp. a quantum t-designs) w.r.t. G, if both quantum designs are such.

Definition 1.7. Let $\mathbf{D}_1 = \{\mathbf{P}_{11}, \ldots, \mathbf{P}_{1v}\}$ and $\mathbf{D}_2 = \{\mathbf{P}_{21}, \ldots, \mathbf{P}_{2v}\}$ be two quantum designs consisting of v orthogonal projections each, and let

$$\mathbf{P}_i = \mathbf{P}_{1i} \oplus \mathbf{P}_{2i} = \begin{pmatrix} \mathbf{P}_{1i} & 0 \\ 0 & \mathbf{P}_{2i} \end{pmatrix} \qquad \text{for all } 1 \leq i \leq v. \tag{1.7}$$

Then $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ is called the *sum* of $\mathbf{D}_1$ and $\mathbf{D}_2$.

The sum is coherent, with parameter k, if and only if all its summands are coherent and have the same parameter k. The sum of two regular quantum designs is itself regular. The sum of two degree 1 quantum designs also has degree 1.

The same way we can construct the *product* of two quantum designs $\mathbf{D}_1$ and $\mathbf{D}_2$ using the Kronecker (or tensor) product $\mathbf{P}_i = \mathbf{P}_{1i} \otimes \mathbf{P}_{2i}$.

Definition 1.8. A quantum design $\mathbf{D}$ is *reducible* if it is unitarily equivalent to the sum of two non-vanishing quantum designs $\mathbf{D}_1$ and $\mathbf{D}_2$. Otherwise, it is called *irreducible.*

$\mathbf{D}$ is reducible if and only if there exists a non-trivial subspace $\mathbf{T}$ of the vector space $\mathbb{C}^b$ which remains invariant under all projections $\mathbf{P}_i$, $1 \leq i \leq v$. Since the projection matrices are self-adjoint, the orthogonal complement to $\mathbf{T}$ is then also invariant, and this is equivalent to the existence of a transformation that puts all matrices into the form (1.7) (with orthogonal projections of size $\dim(\mathbf{T}) \neq 0$ and $\operatorname{codim}(\mathbf{T}) \neq 0$).

Definition 1.9. A quantum design $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ is called *commutative* if the projections $\mathbf{P}_i$, $1 \leq i \leq v$, commute pairwise.

If $\mathbf{D}$ is commutative, then, since projection matrices are self-adjoint, there must exist a unitary matrix $\mathbf{U}$ such that $\mathbf{U}^{-1}\mathbf{P}_i\mathbf{U}$ is diagonal for all $1 \leq i \leq v$ (see [57]). This means that $\mathbf{D}$ is unitarily equivalent to a quantum design consisting solely of diagonal matrices - so to speak a "totally reducible" quantum design. The diagonal entries can only be 1 or 0, because orthogonal projections are idempotent.

1.2 Classical Design Theory

The concept of a finite *incidence structure* is the most fundamental construct in classical combinatorial design theory. An incidence structure is an ordered triple $(V, \mathbf{B}, I)$, where $V = \{p_1, \ldots, p_b\}$ and $\mathbf{B} = \{B_1, \ldots, B_v\}$ are sets containing b respectively v elements, and $I \subseteq V \times \mathbf{B}$ is a binary relation.

The elements of $\mathbf{B}$, called blocks, can also be seen as subsets of V via the correspondence $p_i \in B_j \Leftrightarrow (p_i, B_j) \in I$.

The associated *incidence matrix* $\mathbf{M} = (m_{ij})_{1\leq i\leq b, 1\leq j\leq v}$ is the $b \times v$ matrix defined by

$$m_{ij} = \begin{cases} 1 & \text{if } p_i \in B_j, \\ 0 & \text{else.} \end{cases}$$

Permuting the columns and/or rows of the incidence matrix produces *isomorphic* or *equivalent* incidence structures.

The *dual incidence structure* $(\mathbf{B}, V, I^*)$ can be obtained from $(V, \mathbf{B}, I)$ by swapping the roles of blocks and points, such that $(B_j, p_i) \in I^*$ if and only if $(p_i, B_j) \in I$. The incidence matrix associated to the dual structure is then the transpose of $\mathbf{M}$.

Theorem 1.10. *A unique - up to equivalence - incidence structure $(V, \mathbf{B}, I)$ can be associated to every commutative quantum design $\mathbf{D}$, and vice versa. The correspondence can be achieved as follows. Let all orthogonal projections be diagonalized simultaneously, and use the diagonals to construct the columns of the incidence matrix. In other words, the incidence matrix $\mathbf{M} = (m_{ij})_{1\leq i\leq b, 1\leq j\leq v}$ corresponds to the projections*

$$\mathbf{P}_j = \operatorname{diag}(m_{1j}, \ldots, m_{bj}) \qquad \text{for all } 1 \leq j \leq v. \tag{1.8}$$

Then we have:

(i) $\operatorname{tr}(\mathbf{P}_j) = r_j$, $1 \leq j \leq v$, *corresponds to the number of ones in the j-th column of $\mathbf{M}$, i.e. the cardinality of the block B_j. In particular, $\mathbf{D}$ is regular if and only if all blocks are of the same size.*

(ii) Let $k_i, 1 \leq i \leq b$, be the i-th diagonal entry of $\mathbf{P}_1 + \cdots + \mathbf{P}_v$. Then k_i corresponds to the number of ones in the i-th row of $\mathbf{M}$; that is, k_i corresponds to the number of blocks that contain p_i. In particular, $\mathbf{D}$ is coherent if and only if the points in V are each contained in the same number of blocks.

(iii) $\operatorname{tr}(\mathbf{P}_i\mathbf{P}_j) = \lambda_{ij}$, $1 \leq i \neq j \leq b$, *corresponds to the number of places at which there are ones both in the i-th and the j-th column of $\mathbf{M}$, i.e. to the cardinality of the intersection of the blocks B_i and B_j.*

If, on the other hand, we associate the rows of an incidence matrix (rather than the columns) to the diagonal projection matrices (or equivalently, if we transpose the incidence matrix obtained according to the association described above), we obtain a correspondence with the dual incidence structures. Clearly, the duals of the above properties hold for this "dual association"; that is, $\mathrm{tr}(\mathbf{P}_j)$ *corresponds to the number of blocks that contain* p_j*, the i-th diagonal entry of* $\mathbf{P}_1 + \cdots + \mathbf{P}_v$ *corresponds to the cardinality of the block* B_i*, and* $\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j)$ *corresponds to the number of blocks that contain both* p_i *and* p_j*.*

Proof. To prove the uniqueness of the association: If all orthogonal projections $\mathbf{D}$ are diagonalized simultaneously, then the only remaining permissible equivalence operations are: permutation π of the indices, which corresponds to a permutation of the columns of the associated incidence matrix, and unitary similarity-preserving transformations by $b \times b$ permutation matrices $\mathbf{U}$, which corresponds to a permutation of the rows of the incidence matrix.

All other properties are easily checked. □

Example 1.11. The incidence matrix

$$\mathbf{M} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

corresponds to the unique *projective plane* of order 2. It is associated with a commutative quantum design that is regular - with $r = 3$, coherent - with $k = 3$, and has degree 1 and $\lambda = 1$. The same also holds for the dual association.

Balanced incomplete block designs, BIBD for short (see for example [20], [76], and [34]), are the most well-known constructs in classical design theory. They are incidence structures with the following properties: every block contains exactly k elements, every element is contained in exactly r blocks, and every two distinct elements are both contained in exactly λ blocks. Via the dual association, the BIBD's correspond to commutative, regular, and coherent quantum designs of degree 1. Alternative terms for these classical designs are $S_\lambda(2, k, v) -$ *designs* (see [13]), as well as $2 - (v, k, \lambda) -$ *designs* (see [47]). Projective planes are special cases of *symmetric* BIBD's ($b = v$).

It is worth noting that the parameters (v, b, r, k, λ) in Theorem 1.10 (in this paper) were selected in such a way, that according to the dual association they correspond precisely to their usage in classical design theory.

According to the association described in Theorem 1.10, the complete orthogonal classes of a commutative quantum design correspond to the so-called *parallel classes* of blocks in classical design theory, which completely decompose the point set. The concept of resolvability agrees precisely with that of the classical definition (see [13, Definition I.5.4]).

Via the association given in Theorem 1.10, commutative, regular, affine quantum designs (the regularity condition is not a severe constraint, as will become clear in section 2.3) correspond to so-called (g, k, λ)-*nets*, resp. *affine 1-designs* (see [20, II.4.1]) in classical design theory. This is equivalent to the definition of the so-called *orthogonal arrays* of strength 2 (see [20] or [13]). The special case $\lambda = 1$ agrees with the classical definition of mutually orthogonal latin squares, resp. affine planes (see especially [26]). According to the dual association, commutative, affine quantum designs correspond precisely to so-called *transversal designs* $\mathrm{TD}_\lambda(k, g)$.

An incidence structure is said to be a t-wise balanced design if every subset of V with t-elements is contained in a constant number of exactly λ blocks. A t-wise balanced design in which every block contains exactly r elements is called a *t-design* (resp. $t-(v, k, \lambda)$-design or $S_\lambda(2, k, v)$-design). Every t-design is also an s-design for all $s \leq t$, and the inequality $t \leq r < b$ holds. (see [13, I. Theorem 3.2)] or [20, IV.49]).

Theorem 1.12. *Let* $\mathbf{D}$ *be a quantum design consisting only of diagonal projection matrices. Then according to the association described in Theorem 1.10, its* t*-coherence w.r.t. the permutation group* $S(b)$ *corresponds exactly to* $\mathbf{D}$ *being* s*-wise balanced for all* $s \leq t$*. Combinatorial* t*-designs correspond exactly to regular, diagonal quantum* t*-designs w.r.t.* $S(b)$*.*

Proof. Let $\mathbf{Q}_j$, $1 \leq j \leq b$, be the $b \times b$ diagonal matrices with 1 in the j-th diagonal place, and 0 everywhere else. The b^t matrices $\mathbf{Q}_{j_1} \otimes \mathbf{Q}_{j_2} \otimes \cdots \otimes \mathbf{Q}_{j_t}$, with $1 \leq j_i \leq b$, are a basis for the space of all diagonal $b^t \times b^t$ matrices.

Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a diagonal quantum design. The diagonal matrix $\otimes^t \mathbf{P}_i$ has 1 as the coefficient of $\mathbf{Q}_{j_1} \otimes \cdots \otimes \mathbf{Q}_{j_t}$ if and only if $\mathbf{P}_i$ has 1 at all diagonal places $j_1, j_2, \ldots, j_t$ - according to the association given in Theorem 1.10, this occurs if and only if the points $p_{j_1}, \ldots, p_{j_t}$ are all contained in the i-th block - and 0 everywhere else. Thus, the coefficient of $\mathbf{Q}_{j_1} \otimes \cdots \otimes \mathbf{Q}_{j_t}$ for the matrix $\sum_{i=1}^{v} \otimes^t \mathbf{P}_i$ is precisely the number of blocks that contain all t points $p_{j_1}, \ldots, p_{j_t}$ simultaneously. It follows therefore that the associated classical design is s-wise balanced for all $s \leq t$ if and only if the coefficients of $\mathbf{Q}_{j_1} \otimes \cdots \otimes \mathbf{Q}_{j_t}$ are equal for all possible indices $j_1, j_2, \ldots, j_t$ with s distinct values. $\mathbf{Q}_{j_1} \otimes \cdots \otimes \mathbf{Q}_{j_t}$ with s distinct indices can be mapped onto just such matrices using similarity transformations with arbitrary $b \times b$ permutation matrices $\mathbf{S}$:

$$\mathbf{A} \to (\otimes^t \mathbf{S})\mathbf{A}(\otimes^t \mathbf{S}^{-1}).$$

In particular, any set of s indices can be mapped onto any other such set by using an appropriate permutation matrix. It follows that $\sum_{i=1}^{v} \otimes^t \mathbf{P}_i$ remains invariant under all such mappings (i.e. $\mathbf{D}$ is t-coherent w.r.t. $S(b)$) if and only if the associated classical design is s-wise balanced for all $s \leq t$. $\square$

The association described here is the standard association, and not, as with the BIBD's (resp. $S_\lambda(t, k, v)$-designs with $t = 2$), the dual version given in Theorem 1.10. Thus, all parameters given here are dual to their usage in classical design theory. This has the following background.

Whereas in classical design theory the *Duality Principle* holds - i.e. for every definition and theorem, there is a dual statement - this symmetry no longer holds for non-commutative quantum designs. The transition to non-commutativity causes a *breaking of symmetry*. It is sometimes still possible to generalize both dual definitions, but they then have completely different properties.

Thus e.g., although it is possible to generalize the property of being t-wise balanced in accordance with the dual association (see Section 1.3), it turns out this definition is not very useful.

There are many more definitions of classical designs (see [4], [13], [20] and [76]). Using the concept of an *association scheme* (see for example [20] or [29]), it is possible to define so-called *partially balanced incomplete block designs* (PBIBD) as generalizations of transversal designs. Assume we have an association scheme with s classes on a set of v projection matrices, then the PBIBD correspond, via the dual association, to regular, coherent, degree s quantum designs, that have the following property: with the set Λ consisting of s elements, for each pair of i-associated projections $\mathbf{P}_l, \mathbf{P}_j$, the equality $\mathrm{tr}(\mathbf{P}_l\mathbf{P}_j) = \lambda_i \in \Lambda$ holds. We will not study these structures any further here.

1.3 Quantum-theoretic Interpretation

Classical physics, probability theory, and design theory as well are based on Boolean logic - i.e. a structure that is described by subsets of a given set. Quantum theory, on the other hand, is based on orthocomplementary, quasi-modular lattices, which are built up from closed linear subspaces of separable, complex Hilbert spaces (see [58]). Every such subspace can be associated uniquely with an orthogonal projection, which projects onto it. They correspond to the events (or properties) of the quantum-mechanical system. Thereby mutually orthogonal subspaces, resp. projections, correspond to mutually exclusive events. We will now briefly sketch the *quantum probability theory* (see [12] and [32]) which can be built upon this.

Probability measures are described by so-called density operators - positive semi-definite, self-adjoint operators that are normalized w.r.t. their trace (see GLEASON's Theorem in [19]). The probability $\mu_D(\mathbf{P})$ of a projection $\mathbf{P}$ is defined by

$$\mu_D(\mathbf{P}) = \mathrm{tr}(\mathbf{PD}).$$

Random variables correspond to self-adjoint operators $\mathbf{A}$ that are called *observables* in quantum mechanics. Let χ_B be the characteristic function of a Borel set $B \in \mathbb{R}$; hence $\chi_B(\mathbf{A})$ is a spectral projection of $\mathbf{A}$. Then the probability of measuring a value for $\mathbf{A}$ out of the set B is given by

$$\mu_D(\chi_B(\mathbf{A})) = \mathrm{tr}(\mathbf{D}\chi_B(\mathbf{A})).$$

The *conditional probability* of the projection $\mathbf{P}_2$ given $\mathbf{P}_1$ is

$$\mu_D(\mathbf{P}_2 \mid \mathbf{P}_1) = \frac{\mathrm{tr}(\mathbf{P}_2\mathbf{P}_1\mathbf{D}\mathbf{P}_1)}{\mathrm{tr}(\mathbf{P}_1\mathbf{D})}.$$

See [12, Ch. 26] and [32, Th. 5.26]. This formula is equivalent to describing changes of the state by the measuring process according to LÜDERS(see [56] and [16]). In analogy with the classical theory, it is also possible to define the *joint probability* $\mu_D(\mathbf{P}_2 \sqcap \mathbf{P}_1)$ of measuring first $\mathbf{P}_1$ and then $\mathbf{P}_2$ via

$$\mu_D(\mathbf{P}_2 \sqcap \mathbf{P}_1) = \mu_D(\mathbf{P}_2 \mid \mathbf{P}_1)\mu_D(\mathbf{P}_1) = \mathrm{tr}(\mathbf{P}_2\mathbf{P}_1\mathbf{D}\mathbf{P}_1).$$

The conditional and joint probabilities in quantum theory - in contrast with classical probability theory - generally depend on the order of the events. The following definition for the *independence* of two projections is analogous to that in classical probability theory, but in the quantum case we must require additionally independence from the order of the events, i.e.

$$\mu_D(\mathbf{P}_2 \sqcap \mathbf{P}_1) = \mu_D(\mathbf{P}_1 \sqcap \mathbf{P}_2) = \mu_D(\mathbf{P}_1)\mu_D(\mathbf{P}_2).$$

We will now restrict our attention to finite-dimensional, complex Hilbert spaces (i.e. to $\mathbb{C}^b$). Furthermore, we define as density operator $\mathbf{D} = \frac{1}{b}\mathbf{I}$, which corresponds to a "uniformly distributed" probability $\mu(\mathbf{P}) = \frac{1}{b}\operatorname{tr}(\mathbf{P})$. In this case, the joint probability $\mu(\mathbf{P}_2 \sqcap \mathbf{P}_1) = \frac{1}{b}\operatorname{tr}(\mathbf{P}_1\mathbf{P}_2)$ does not depend on the order, and two projections are independent w.r.t. μ whenever $\operatorname{tr}(\mathbf{P}_1\mathbf{P}_2) = \frac{1}{b}\operatorname{tr}(\mathbf{P}_1)\operatorname{tr}(\mathbf{P}_2)$ holds.

The v projection matrices $\{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ of a quantum design can be thought of as v events in this quantum mechanical system. Their probabilities $\mu(\mathbf{P}_i) = \frac{1}{b}\operatorname{tr}(\mathbf{P}_i)$ are equal if and only if the quantum design is regular. The joint probabilities $\mu(\mathbf{P}_i \sqcap \mathbf{P}_j) = \frac{1}{b}\operatorname{tr}(\mathbf{P}_i\mathbf{P}_j)$ for all $1 \leq i \neq j \leq v$ are constant if and only if the quantum design has degree 1. In general, the degree s indicates the number of distinct joint probabilities.

Definition 1.13. The spectral decomposition

$$\mathbf{A}_i = \sum_{l=1}^{g_i} a_{il}\mathbf{P}_{il}$$

of k self-adjoint matrices $\mathbf{A}_i$, $1 \leq i \leq k$, defines k complete orthogonal classes (i.e. a resolution) on the quantum design, which is built up from all the projections. We call the orthogonal classes, resp. obervables, $\mathbf{A}_i$ *mutually independent* (w.r.t. $\frac{1}{b}\mathbf{I}$), if any pair of projections from distinct orthogonal classes is independent, i.e. if

$$\operatorname{tr}(\mathbf{P}_{il}\mathbf{P}_{jm}) = \frac{1}{b}\operatorname{tr}(\mathbf{P}_{il})\operatorname{tr}(\mathbf{P}_{jm}) \tag{1.9}$$

holds for all $1 \leq i \neq j \leq k$ and $1 \leq l \leq g_i$, $1 \leq m \leq g_j$.

If we require in addition that the quantum design constructed from the projections is regular, then we get a regular affine quantum design of degree 2, with $\Lambda = \{0, r^2/b\}$. We will show in Section 2.3 that all affine quantum designs have mutually independent orthogonal classes.

Up until now, only special cases thereof have been treated in the quantum mechanics literature.[7] SCHWINGER [68] described the equation (1.9) for one-dimensional projections as *maximum degree of incompatibility* (also see ACCARDI [1]).

PARTHASARATHY [65] considered so-called *spin observables* $\mathbf{X}_i$, $1 \leq i \leq k$ with only two eigenvalues (± 1). He required that the density operator $\mathbf{D}$ satisfy $\operatorname{tr}(\mathbf{X}_i\mathbf{D}) = 0$ and $\operatorname{tr}(\mathbf{X}_i\mathbf{X}_j\mathbf{D}) = c_{ij}$, with $\mathbf{C} = (c_{ij})$ a positive-definite matrix. The special case $\mathbf{D} = \frac{1}{b}\mathbf{I}$, $\mathbf{C} = \mathbf{I}$ conforms to the formulation of the problem above. As a special case of our theory, we will show in Section 2.3 that $k \leq n^2 - 1$ holds in this case (see also [65, Exercise 5.8 (4)]). We will also present the classical structures (associated, via Theorem 1.10, for commutative observables) on which Parthasarathy pointed by the example of the Hadamard matrix [65, Page 16].

We now briefly sketch another definition, which however has not yet proven to be very fruitful. Iteration of the quantum mechanical measurement process

[7] Remark (2010): As mentioned already in the preface, I was not aware of papers of I.D.Ivanovic, W.K.Wootters and B.D.Fields about MUBs when writing my thesis.

yields

$$\mu_d(\mathbf{P}_{i_t} \sqcap \cdots \sqcap \mathbf{P}_{i_1}) = \mathrm{tr}(\mathbf{P}_{i_t}\mathbf{P}_{i_{(t-1)}} \cdots \mathbf{P}_{i_1}\mathbf{D}\mathbf{P}_{i_1} \cdots \mathbf{P}_{i_{(t-1)}}\mathbf{P}_{i_t})$$

for the probability of measuring $\mathbf{P}_{i_1}, \mathbf{P}_{i_2}, \ldots, \mathbf{P}_{i_t}$ one after the other (see [72, Equation 5.15]). Let us now examine quantum designs for which the joint probability of t distinct, random projections w.r.t. $\frac{1}{b}\mathbf{I}$ is constant (and independent of the order). Consider the classical combinatorial designs corresponding to these quantum designs via the dual association described in Theorem 1.10. Then the joint probability of the t projections is proportional to the number of blocks in the classical design that contain all t points $p_{i_1}, p_{i_2}, \ldots, p_{i_t}$ - i.e. via the dual association in the commutative case, the constant probability corresponds precisely to the classical definition of t-balanced designs.

If the projections are all one-dimensional, then it is easy to see that the joint probability for t projections is independent of the order, and in the case of quantum designs of degree 1 this joint probability is constant and equal to λ^t/b; that is, any $t \geq 2$ projections of a regular, degree 1 quantum design with $r = 1$ always have constant joint probability. This does not hold in general (e.g. for $r \geq 2$ or in the commutative case). We will not investigate these quantum designs for $t > 2$ any deeper here.

Let X be a locally-compact set with Borel measure dx, and for all $x \in X$, let ψ_x be a normalized vector from a separable complex Hilbert space. There are various definitions on the basis of which the vectors ψ_x, $x \in X$, are called *coherent states* (see [22], [50] and [80]). What all definitions have in common is that

$$\int_X \mathbf{P}_x \, dx = \mathbf{I} \tag{1.10}$$

holds with $\mathbf{P}_x$ being the orthogonal projections onto the one-dimensional subspace spanned by ψ_x. Let $\mathbb{C}^b$ be the Hilbert space, $X = \{1, 2, \ldots, v\}$, and dx be the point measure that assigns weight $\frac{1}{k}$ to each $1 \leq i \leq v$. Then the equation (1.10) agrees exactly with the definition of coherence of the regular quantum design $\{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$. The generalizations to multi-dimensional projections are called *vector-coherent states* in quantum theory.

A widespread approach to the theory of coherent states goes via group theory (see [80]). Let G be a Lie Group, $\mathbf{U}(g)$ be an irreducible, unitary representation of G over a Hilbert space, and let ψ_0 be a normalized (initial-) vector. Let H be the subgroup of G that, up to an arbitrary phase factor, leaves ψ_0 invariant, and for every $x \in G' \cong G/H$ choose a coset representative $g(x) \in G$. The coherent states are defined by

$$\psi_x = \mathbf{U}(g(x))\psi_0.$$

If one defines an appropriate normalized *Haar measure* dx on G', then, using Schur's Lemma, equation (1.10) follows immediately from the irreducibility of the representation $\mathbf{U}$ (see [80]). We will encounter analogous connections for quantum designs when investigating their *automorphism groups* in Section 2.5.

Incidentally, coherence can also be given a probability-theoretic motivation. In Section 1.4 we will show that a regular quantum design is coherent if and only if the average (over the design's projections) of the probabilities $\mu_D(\mathbf{P})$ w.r.t. an arbitrary density matrix $\mathbf{D}$ is equal to the average over all projections with the same trace.

As we will show in the next two examples, not just the definitions of quantum design, but significant construction approaches as well have their counterpart in quantum theory. The so-called *Weyl operators*, and the by these generated so-called *Heisenberg group* play a central role thereby (see [74]).

As technical prerequisite for our first example, we note that the following relation holds for arbitrary projections $\mathbf{P}_1$ and $\mathbf{P}_2$ in infinite-dimensional Hilbert spaces: $\operatorname{tr}(\mathbf{P}_1\mathbf{P}_2\mathbf{P}_1) = \operatorname{tr}(\mathbf{P}_2\mathbf{P}_1\mathbf{P}_2)$. (The expression $\operatorname{tr}(\mathbf{P}_1\mathbf{P}_2)$ is generally not defined, except in the case where either $\mathbf{P}_1$ or $\mathbf{P}_2$ is in the so-called trace class [67]). While the identity operator $\mathbf{I}$ in infinite-dimensional vector spaces is not a density operator - because it cannot be normalized - it is nonetheless possible to define something like independence with respect to it.

Let $\mathbf{A}$ and $\mathbf{B}$ be two self-adjoint operators over a separable Hilbert space with spectrum $\sigma(\mathbf{A})$ and $\sigma(\mathbf{B})$, respectively. We will say that they are independent (w.r.t. $\mathbf{I}$), if there are borel measures μ_A on $\sigma(\mathbf{A})$ and μ_B on $\sigma(\mathbf{B})$ such that, for any two compact subset $E \in \sigma(\mathbf{A})$ and $F \in \sigma(\mathbf{B})$, the following relation holds:

$$\operatorname{tr}(\chi_E(\mathbf{A})\chi_F(\mathbf{B})\chi_E(\mathbf{A})) = \mu_A(E)\mu_B(F). \tag{1.11}$$

If the Hilbert space is finite-dimensional, then this definition coincides with the definition of independence w.r.t. $\frac{1}{b}\mathbf{I}$. Let $\mathbf{A} = \sum_{i=1}^{g} a_i\mathbf{P}_i$ and $\mathbf{B} = \sum_{j=1}^{h} b_j\mathbf{Q}_j$. From (1.11), it follows that $\operatorname{tr}(\mathbf{P}_i\mathbf{Q}_j)\operatorname{tr}(\mathbf{P}_l\mathbf{Q}_m) = \operatorname{tr}(\mathbf{P}_i\mathbf{Q}_m)\operatorname{tr}(\mathbf{P}_l\mathbf{Q}_j)$, and through summation over l and m one obtains $\operatorname{tr}(\mathbf{P}_i\mathbf{Q}_j) = \frac{1}{b}\operatorname{tr}(\mathbf{P}_i)\operatorname{tr}(\mathbf{Q}_j)$. Vice versa, the measures $\mu_A(a_i) = \frac{1}{\sqrt{b}}\operatorname{tr}(\mathbf{P}_i)$ and $\mu_B(b_j) = \frac{1}{\sqrt{b}}\operatorname{tr}(\mathbf{Q}_j)$ are appropriate Borel measures according to the above definition.

The position operator $\mathbf{X}$ and the impulse operator $\mathbf{P}$ are each defined on a dense subset of $\mathcal{L}^2(\mathbb{R})$ via the equations

$$(\mathbf{X}f)(x) = xf(x) \quad \text{and} \quad (\mathbf{P}f)(x) = -i\frac{d}{dx}f(x).$$

It is easy to see (see also [3]) that using the Lebesgue-Borel measure λ on $\mathbb{R}$, one gets $\operatorname{tr}(\chi_E(\mathbf{X})\chi_F(\mathbf{P})\chi_E(\mathbf{X})) = \frac{1}{2\pi}\lambda(E)\lambda(F)$, i.e. $\mathbf{X}$ and $\mathbf{P}$ are independent (even though they are linked via the canonical commutation relation and through Heisenberg's uncertainty principle). Determining the probability theoretic background for the independence of the position and impulse operators was the main motivation behind the author's master thesis [79] and thus also indirectly for the present work.

Now let $\mathbf{A}_\alpha = \cos(\alpha)\mathbf{X} - \sin(\alpha)\mathbf{P}$, with $\alpha \in [0, \pi)$. Then $\mathbf{A}_\alpha$ and $\mathbf{A}_\beta$, for $\alpha \neq \beta$, are also mutually independent (because they are unitarily equivalent to $c\mathbf{X}$ and $d\mathbf{P}$ with $c, d \neq 0$, see [78]). This means that the $\mathbf{A}_\alpha$, with $\alpha \in [0, \pi)$, make up an infinite set of mutually independent operators.

Using $\mathbf{U}_\alpha(t) = e^{i\mathbf{A}_\alpha t}$ with $t \in \mathbb{R}$, we can now assign a one-parameter strongly continuous group of unitary operators to each $\mathbf{A}_\alpha$. Vice versa, the infinitesimal generators $\mathbf{A}_\alpha$ are uniquely determined - up to a constant factor - by these groups. Letting $c = t\sin(\alpha)$ and $d = t\cos(\alpha)$ we get

$$\mathbf{U}_\alpha(t) = \mathbf{W}(c, d) = e^{-icd/2} e^{-ic\mathbf{P}} e^{-id\mathbf{X}}. \tag{1.12}$$

These operators are precisely the Weyl operators mentioned above, and with $c, d \in \mathbb{R} \to \mathbf{W}(c, d)$ make up the unique unitary, irreducible, projective representation of the additive group $\mathbb{R} \times \mathbb{R}$, resp. $\mathbb{C}$ (see Thirring [74, Page 76]). Thus, using polar coordinates, they can be decomposed into one-parameter unitary groups that each determine one of infinitely-many mutually independent operators.

In Section 3.2 we will apply a similar technique to finite-dimensional *Weyl matrices* in order to construct maximal affine quantum designs.

Our second example deals with classical coherent states, also known as *states of minimal uncertainty*, in the Hilbert space $\mathcal{L}^2(\mathbb{R})$. These were historically the origin of the concept of coherence, and have many applications in quantum theory. The initial vector ψ_0 is the ground state of the harmonic oscillator (vacuum state), which is also the eigenvector of the infinite-dimensional *Fourier Transformation.* The projections $\mathbf{P}_x$, $x \in \mathbb{C}$ arise by applying the Weyl operators, and the following relation holds for their joint or *transition probabilites* (see [80, Equation 2.20]):

$$\lambda_{xy} = \mathrm{tr}(\mathbf{P}_x \mathbf{P}_y) = e^{-|x-y|^2} \qquad \text{for all } x, y \in \mathbb{C}.$$

This means for classical coherent states $\mathrm{tr}(\mathbf{P}_x \mathbf{P}_y)$ only depends on $|x - y|$. (They obey a kind of "infinite metric association scheme").

Analogously with the above technique for classical coherent states, in Section 3.4 we will apply the finite-dimensional Weyl matrices to construct maximal, regular, coherent quantum designs of degree 1. The initial vector will be the eigenvector of a matrix constructed with the help of a Fourier matrix (and very similar to it).

These two examples also show that it is possible to generalize parts of quantum design theory to infinite-dimensional Hilbert spaces. However, this line of investigation will not be pursued any further here.

1.4 Spherical t-Designs

We will first need to investigate the concept of t-coherence closer, and this in turn requires some more technical preparation.

A set X of (complex) $b \times b$ matrices is a *G-space* with respect to a group $G \subseteq U(b)$ if the following holds: for all $\mathbf{P} \in X$ and $\mathbf{U} \in G$, we have $\mathbf{UPU}^{-1} \in X$ as well. If in addition for every $\mathbf{P}, \mathbf{Q} \in X$ there is a $\mathbf{U} \in G$ such that $\mathbf{UPU}^{-1} = \mathbf{Q}$, then we say that G acts *transitively* on X, and X is called a *homogeneous* G-space (see [14, I.4], [49, I.2.2]).

The sets of all complex (resp. real) orthogonal projection matrices with a given trace r and w.r.t. the group $G = U(b)$ (resp. $O(b)$) are examples of homogeneous G-spaces. These spaces can also be identified with $G_r(\mathbb{C}^b)$ (resp. $G_r(\mathbb{R}^b)$), the so-called *complex (resp. real) Grassmannian (manifold)* of the r-dimensional subspaces of $\mathbb{C}^b$ (resp. $\mathbb{R}^b$). Analogously, the sets of all diagonal projection matrices with a given trace r and w.r.t. the group $G = S(b)$ also form homogeneous G-spaces.

Let $\mathbf{P}_0$ be any given point in X. The set of all elements in G that fix $\mathbf{P}_0$ make up a subgroup H of G, and

$$\pi : \mathbf{U} \to \mathbf{UP}_0\mathbf{U}^{-1}$$

is the projection of G onto the homogeneous G-space (or quotient manifold) $X \cong G/H$. This also means that G together with any given element of a homogeneous G-space X completely determines (generates) that space. Let $\mathbf{P}_0$ be a projection with trace r and $G = U(b)$, then it necessarily follows that $X = G_r(\mathbb{C}^b)$. In this case, the subgroup H is equivalent to $U(r) \times U(b-r)$. Analogously, we find that for $G = O(b)$ holds $H \sim O(r) \times O(b-r)$.

On every group $G \subseteq U(b)$ there is defined a unique normalized and left-invariant integral - the so-called *Haar integral*; and since $G \subseteq U(b)$ is compact, this integral is also right-invariant (see [14, I, Theorem 5.12]). For any continuous function $f : X \to \mathbb{C}$, it is possible to define a unique, normalized integral on X that is invariant w.r.t. G using the projection π, by setting

$$\int_X f(\mathbf{P})dp = \int_G f(\mathbf{UP}_0\mathbf{U}^{-1})du. \tag{1.13}$$

(See [49, Section II.9]). In the example of the homogeneous G-space generated by the diagonal projection matrices w.r.t. $S(b)$, the integral becomes a discrete sum.

Definition 1.14. Let $\mathbf{P}_0$ be a given element of a homogeneous G-space X. For arbitrary $t \geq 1$, we refer to the tensor

$$\mathbf{K}_t(X) = \int_X \otimes^t \mathbf{P} dp = \int_G \otimes^t \mathbf{UP}_0\mathbf{U}^{-1} du$$

as the *t-coherence tensor with respect to the G-space X*.

If $\mathbf{P}_0$ is a projection with trace r, then, since the integral is normalized, it follows that for all homogeneous G-spaces $\mathrm{tr}(\mathbf{K}_t(X)) = r^t$. In particular, for $t = 1$ and irreducible groups G we get $\mathbf{K}_1(X) = \frac{r}{b}\mathbf{I}$.

Theorem 1.15. *Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a quantum design, let $G \subseteq U(b)$, and let X_i, $1 \le i \le v$, be the G-spaces generated by the $\mathbf{P}_i$. Then $\mathbf{D}$ is t-coherent w.r.t. G if and only if*

$$\sum_{i=1}^{v} \otimes^t \mathbf{P}_i = \sum_{i=1}^{v} \mathbf{K}_t(X_i). \tag{1.14}$$

If $\mathbf{D}$ is also regular, and $X_i = X$ for all $1 \le i \le v$, then it follows that

$$\frac{1}{v}\sum_{i=1}^{v} \otimes^t \mathbf{P}_i = \mathbf{K}_t(X). \tag{1.15}$$

Proof. Let $\mathbf{D}$ be t-coherent w.r.t. G. We just need to integrate the equation (1.3) over the group G, and we immediately obtain the equation (1.14).

If, on the other hand, this equation is satisfied by a quantum design, then since $\mathbf{K}_t(X_i) = \otimes^t \mathbf{U}(\mathbf{K}_t(X_i)) \otimes^t \mathbf{U}^{-1}$ for all $\mathbf{U} \in G$, t-coherence w.r.t. G immediately follows. □

The polynomial space $\mathrm{Pol}(X, t)$ is defined as the restriction of the set of complex polynomials in b^2 variables (interpreted as coordinates in the space of complex $b \times b$ matrices) of degree less than or equal to t to the set (manifold) X. Let $\mathbf{C}$ be any $b^t \times b^t$ matrix with $t \ge 1$, and $\mathbf{P} \in X$. The *homogeneous polynomials* of degree t in $\mathrm{Pol}(X, t)$, which we call $\mathrm{Hom}(X, t)$, are precisely all $f(\mathbf{P}) = \mathrm{tr}\left((\otimes^t \mathbf{P})\mathbf{C}\right)$ that do not vanish on X. The matrix entries of $\otimes^t \mathbf{P}$ that do not vanish on X are the monomials of degree t.

Theorem 1.16. *Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a quantum design, and $G \subseteq U(b)$. In addition let X_i, $1 \le i \le v$ be the G-spaces generated by the $\mathbf{P}_i$, and set $X = \bigcup_{i=1}^{v} X_i$. $\mathbf{D}$ is t-coherent w.r.t. G if and only if the following relation holds for all homogeneous polynomials $f(\mathbf{P}) \in \mathrm{Hom}(X, t)$:*

$$\sum_{i=1}^{v} f(\mathbf{P}_i) = \sum_{i=1}^{v} \int_{X_i} f(\mathbf{P}) dp. \tag{1.16}$$

If $\mathbf{D}$ is also regular, and $X_i = X$ for all $1 \le i \le v$, then we have

$$\frac{1}{v}\sum_{i=1}^{v} f(\mathbf{P}_i) = \int_{X} f(\mathbf{P}) dp. \tag{1.17}$$

This means that the average of every degree t homogeneous polynomial over all elements of the design is equal to the average over the entire homogeneous G-space X. The design is a quantum t-design if and only if this holds for all polynomials $f(\mathbf{P}) \in \mathrm{Pol}(X, t)$.

Proof. To prove the theorem, we just need to multiply the equations from Theorem 1.15 by an arbitrary complex $b^t \times b^t$ matrix, and then take the trace. The converse holds for every monomial, i.e. for all entries of $\otimes^t \mathbf{P}$. □

We now consider the special case of quantum designs with $r = 1$.

The vectors of the complex (resp. real) unit sphere Ω in a b-dimensional vector space V are mapped onto orthogonal projections, i.e. elements of the Grassmannian $G_1(\mathbb{C}^b)$ (resp. $G_1(\mathbb{R}^b)$), via

$$\mathbf{e} = (e_i)_{1\le i\le b} \;\mapsto\; \mathbf{P_e} = (e_i\bar{e}_j)_{1\le i,j\le b}. \tag{1.18}$$

This implies that quantum designs with $r = 1$ can also be described using normalized vectors - as so-called *spherical designs*. However, these vectors are not uniquely determined by the equation (1.18), because normalized vectors that only differ by a complex phase (resp. a real phase ± 1) - and thus span the same subspace - correspond to the same projection $\mathbf{P}$. A subset Y of the unit sphere is called *antipodal* if for every vector $\mathbf{e} \in Y$ also $-\mathbf{e} \in Y$. Quantum designs with $r = 1$ can therefore also be described by the antipodal spherical designs of $2v$ vectors. Real quantum designs with $r = 1$ correspond to unique, antipodal spherical designs.

It follows immediately from $\mathbf{P_e}\,\mathbf{x} = \langle \mathbf{x}|\mathbf{e}\rangle\,\mathbf{e}$ for all $\mathbf{x} \in V$ that

$$\operatorname{tr}(\mathbf{P_e P_f}) = |\langle \mathbf{e}|\mathbf{f}\rangle|^2 \qquad \text{for all } \mathbf{e}, \mathbf{f} \in V. \tag{1.19}$$

In a real vector space, the absolute value of the inner product of two normalized vectors equals the *cosine* of the angle between them. This implies that in real vector spaces, regular degree 1 quantum designs with $r = 1$ correspond to *systems of equiangular lines.* These were first studied in [55] and [52].

Later, Delsarte, Goethals and Seidel [24] extended the investigation to include complex vector spaces and angle sets containing s elements (with $s \ge 2$). Vector spaces over the quaternions were studied in [41]. In the case of real vector spaces, the phase of the inner product was sometimes taken into consideration to determine the degree (see for example [25]).

A survey of well-known systems of equiangular lines in both real and complex vector spaces can be found in [43]. By constructing complementary designs for $b \ge 2$ and summing such designs, one immediately obtains examples of degree 1 quantum designs with $r \ge 2$.

Complete orthogonal classes correspond to orthonormal bases. Although degree 2 spherical designs, and in particular those with $\Lambda = \{0, \lambda\}$, have been treated in the literature, affine designs - that is, the decomposition of these designs into orthonormal bases - has never been explicitly investigated. Nonetheless, solutions have been found implicitly, and they will be described in Section 3.3.

Let $\mathbf{e}_j = (e_{ij})_{1\le i\le b}$ for $1 \le j \le v$ be normalized vectors, and let $\mathbf{E}$ be the $b \times v$ matrix that is obtained by writing the v vectors $\mathbf{e}_j$, $1 \le j \le v$ as columns, i.e. $\mathbf{E} = (e_{ij})_{1\le i\le b, 1\le j\le v}$. It then immediately follows that

$$\sum_{j=1}^{v} \mathbf{P_{e_j}} = \mathbf{EE}^*.$$

This shows that coherence is equivalent to $\mathbf{EE}^* = k\mathbf{I}$. Seidel in [69] described systems of vectors with this property as *eutactic*. Such systems had been previously studied by HADWIGER, who called them *normed coordinate stars* (see [33]), and even earlier had been investigated by POHLKE and SCHLÄFLI).

DELSARTE, GOETHALS and SEIDEL in [25] defined so-called (real) *spherical t-designs* in connection with results about systems of equiangular lines. A finite subset Y of the real unit sphere is said to have *index s* if the sum over the points of Y of the values of every homogeneous, harmonic polynomial of degree s is zero. It is called spherical t-design if has all indices less than or equal to t. Y has index s if and only if for every degree s homogeneous polynomial f, the sum over the points of Y of its values, divided by the number of points in Y, is equal to the integral of the polynomial over the unit sphere, i.e.

$$\frac{1}{|Y|}\sum_{y\in Y} f(y) = \int_{\Omega} f(y)d\omega(y).$$

In order to show that Y is a t-design, it suffices to prove this for $s = t$ (which then implies it also for $s-2, s-4, \ldots$) and for $s = t-1$ (and hence $s-3, s-5, \ldots$ follow) (see [30, Theorem 4.4]).

Via the map (1.18), the space of homogeneous polynomials of degree t over the Grassmannian $G_1(\mathbb{C}^b)$ is isomorphic to the space of polynomials over the complex unit sphere $\Omega(\mathbb{C}^b)$ that are homogeneous of degree t in the variables x_i and $\bar{x}_j$. Analogously, the space of degree t homogeneous polynomials over $G_1(\mathbb{R}^b)$ is isomorphic to the space of polynomials over $\Omega(\mathbb{R}^b)$ that are homogeneous of degree $2t$ (see also GODSIL [29, Chapter 14, Example 15]). For these polynomials, the integral over the Grassmannian is identical to the (normalized Haar) integral over the corresponding unit sphere.

From Theorem 1.16, it follows that a real spherical design has index $2t$ (and hence also all even indices less than $2t$) if and only if the corresponding regular quantum design is t-coherent with respect to $O(b)$ (and is thus a quantum t-design w.r.t. $O(b)$). In particular, index 2 is equivalent to coherence. The odd indices do not correspond to any properties of quantum designs, because they depend on the phases of the vectors. However, since antipodal spherical designs always have all odd indices, it is also possible to associate regular quantum t-design w.r.t. $O(b)$ and with $r = 1$ to antipodal spherical $(2t + 1)$-designs (with $2v$ vectors).

See [31] for a survey of well-known examples of spherical t-designs, and [36] for spherical 4-designs in particular. Via the complementary designs, we thus obtain our first examples of quantum t-designs with $r \geq 2$.

In the articles [63] and [71], it was shown that Y has index t if and only if the following equation holds:

$$\frac{1}{|Y|}\sum_{y\in Y} \otimes^t y = \mathbf{D} \qquad \text{with} \qquad \mathbf{D} = \int_{\Omega} \otimes^t y \, d\omega(y). \tag{1.20}$$

The tensors $\mathbf{D}$ to the index $2t$ are equivalent to the t-coherence tensors w.r.t. the real Grassmannian with $r = 1$ (for odd indices one has $\mathbf{D} = \mathbf{0}$). The relation to orthogonal invariance, as we applied it in the definition of t-coherence, was also noticed very early (see [30]), and was investigated in great detail in [64].

In [62], Neumaier generalized the concept of t-designs to so-called *Delsarte spaces*. He showed that besides the real unit sphere, also the projective spaces over the real and complex numbers, resp. the quaternions and the Cayley numbers (i.e. the symmetric spaces of rank 1), could be used, in conjunction with the metric defined by $d(\mathbf{PQ}) = \sqrt{1 - \mathrm{tr}(\mathbf{PQ})}$, to construct Delsarte spaces. In a series of articles (see [43], [44], [10], [45] and [46]), Hoggar investigated t-designs for these spaces. Such t-designs correspond to regular quantum designs with $r = 1$ w.r.t. $O(b)$ (resp. $U(b)$) in the real (resp. complex) case - i.e. over the real (resp. complex) Grassmannian $G_1(\mathbb{R}^b)$ (resp. $G_1(\mathbb{C}^b)$). In [43] many examples are given, and hence via the complementary designs we also get examples of quantum t-designs with $r \geq 2$ over the complex numbers.

Godsil's t-designs over so-called *polynomial spaces* are a further generalization that encompass both the concept of spherical t-designs as well as the concept of t-designs over projective spaces [29].

A polynomial space consists of a set Ω, a real-valued *separating function* ρ defined on Ω, and an inner product on the set $\mathrm{Pol}(\Omega)$ of polynomials over Ω.

Let $G \subseteq U(b)$, and let X_j, $1 \leq j \leq s$ be distinct, homogeneous G-spaces of $b \times b$ projection matrices (under similarity transformations from G). Let n_j for $1 \leq j \leq s$ be any natural numbers, set $w = n_1 + \cdots + n_s$, and let

$$\Omega = \bigcup_{j=1}^{s} X_j, \tag{1.21a}$$

$$\rho(\mathbf{P}, \mathbf{Q}) = \mathrm{tr}(\mathbf{PQ}) \quad \text{for all } \mathbf{P}, \mathbf{Q} \in \Omega, \tag{1.21b}$$

$$\langle f(\mathbf{P}) | g(\mathbf{P}) \rangle = \sum_{j=1}^{s} \frac{n_j}{w} \int_{X_j} f(\mathbf{P}) g(\mathbf{P}) dp \quad \text{for all } f(\mathbf{P}), g(\mathbf{P}) \in \mathrm{Pol}(\Omega), \tag{1.21c}$$

with the unique, normalized integral over the X_j, $1 \leq j \leq s$, defined by G. In this manner a polynomial space can be constructed in accordance with the definition in [29, Chapter 14.2]. The definition of degree for finite subsets of Ω based on this is in perfect agreement with our definition for quantum designs. t-designs over polynomial spaces are finite subsets $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ of Ω that satisfy

$$\langle 1 | f(\mathbf{P}) \rangle = \frac{1}{v} \sum_{i=1}^{v} f(\mathbf{P}_i) \quad \text{for all } f(\mathbf{P}) \in \mathrm{Pol}(\Omega).$$

According to Equation (1.16), this agrees with the definition of quantum t-designs $\mathbf{D}$ under the following condition: if m_j is the number of projections $\mathbf{P}_i \in X_j$, then $\frac{m_j}{v} = \frac{n_j}{w}$ for all $1 \leq j \leq s$. This condition is trivially satisfied if the design is regular, and all the X_i are the same (i.e. $s = 1$).

In [29], this construction is illustrated primarily using spherical designs and *Johnson Schemata* - which correspond to classical designs and are included as a commutative special case in our concept. It is only shortly mentioned in an example [29, Chapter 14.3 (i)] that the real Grassmannians together with the trace function form polynomial spaces.

Thus, fundamental concepts of this theory are valid also for quantum designs (see Section 2.1). In particular, so-called *Q-polynomial spaces* (which are equivalent to Delsarte spaces) were studied in [29], and a series of conclusions were drawn for such spaces. In Section 2.4 we will prove one of these results for degree 1 (and $t = 2$) over arbitrary Grassmannian manifolds. However, the generalization to arbitrary homogeneous G-spaces (and $s > 1$, resp. $t > 2$) is not the subject of this paper.

A subset $\mathbf{D}$ of a polynomial space is called *imprimitive* in [29, chapter 16.5], if there is a non-trivial partition of $\mathbf{D}$ such that $\mathbf{P}_i$ and $\mathbf{P}_j$ lie in the same *parallel class* if and only if $\rho(\mathbf{P}_i, \mathbf{P}_j) = \mathrm{tr}(\mathbf{P}_i\mathbf{P}_j) \in \Lambda' \subset \Lambda$. Resolvable quantum designs are imprimitive, with $\Lambda' = \{0\}$; however, in this case we must also require that the parallel (resp. orthogonal) classes are complete.

There are also two attempts in the literature to find appropriate generalizations in the direction of $r > 2$, resp. non-regularity.

Multi-spherical or Euclidean t-designs (see [63], [70], [71]) are a generalization of subsets of the unit sphere to arbitrary sets of vectors Y in $\mathbb{R}^b$. They can also be conceived of as subsets of several concentric spheres. Since the normalized integral of $\otimes^t y$ over the sphere with radius r is exactly $r^t\mathbf{D}$, the requirement for index t is stated as: $\sum_{y\in Y} \otimes^t y = \sum_{y\in Y} \|y\|^t\mathbf{D}$. Non-regular quantum designs can also be interpreted as designs on several spheres of radius r_i, $1 \leq i \leq v$, in the b^2-dimensional vector space of all $b \times b$ matrices. However, since in any case the computation of the coherence tensors only requires integration over (distinct) submanifolds (resp. subsets) of these spheres, it follows that the tensors are not proportional for varying r (and fixed b, t). Thus, the definition of t-coherence for non-regular quantum designs differs from that given above.

The definition of spherical designs is based on finite subsets of the unit sphere in real (or complex, etc) vector spaces. Early attempts ([53] and [40]) were made to generalize the theory from such vector (or linear) systems to systems of subspaces (planes). However, in these works the generalizations were restricted to so-called mutually *isoclinic* subspaces. In a real vector space, this condition means that the two vector (sub-) spaces must have the same dimension, and that the angle between any vector in one of the subspaces and its orthogonal projection onto another subspace must remain constant. Let $\mathbf{P}$ and $\mathbf{Q}$ be projections onto two equi-dimensional subspaces of $\mathbb{R}^n$. Then they are isoclinic if and only if there exists a parameter $\gamma \in \mathbb{R}$ such that

$$\mathbf{PQP} = \gamma\mathbf{P}. \tag{1.22}$$

(From this it follows that also $\mathbf{QPQ} = \gamma\mathbf{Q}$), see [53], Theorem 2.3). This definition can easily be extended to complex vector spaces (see [40]).

Assuming $\mathbf{P}$ and $\mathbf{Q}$ commute, then it follows that $\gamma\mathbf{P} = \mathbf{PQP} = \mathbf{QP}^2 = \mathbf{Q}^2\mathbf{P} = \mathbf{QPQ} = \gamma\mathbf{Q}$. Therefore either $\gamma = 0$ and $\mathbf{P}$ is orthogonal to $\mathbf{Q}$, or $\gamma = 1$ and $\mathbf{P} = \mathbf{Q}$. Commutative, mutually isoclinic designs are hence trivial.

One can now show that non-commutative projections that satisfy Equation (1.22) must be equi-dimensional. This means that the corresponding quantum design must be regular (whereas this was stated as a requirement in the articles [53] and [40]). This in turn implies $\mathrm{tr}(\mathbf{PQ}) = \mathrm{tr}(\gamma\mathbf{P}) = \gamma r$ and the following simple relation.

Proposition 1.17. *The orthogonal projections associated to the equi-isoclinic subspaces (that is mutually isoclinic subspaces with constant parameter $\gamma \neq 0$) form a regular degree* 1 *quantum design with $\lambda = \gamma r$.*

In Section 2.4 we will show that the main results of [53] and [40] actually hold for degree 1 quantum designs in general, without the considerable constraint that the subspaces be isoclinic.

In some papers the following relation between real spherical designs and classical designs was established (see for example [25], [71] and [45]). Vectors in a v-dimensional vector space, with coordinates $x_i \in \{0, 1\}$ and $\sum_{i=1}^{v} x_i^2 = k$ (i.e. lying on the sphere of radius k), were identified with the columns of an incidence matrix. The associated classical designs have constant block size k. In this manner, classical t-designs can be associated to spherical t-designs. Designs with non-constant block size correspond to multi-spherical designs.

This embedding is very similar to the one described in Theorem 1.10, which however embeds both spherical and classical designs in a more comprehensive theory. Furthermore, the characterization of classical designs via commutativity is, in contrast with the above embedding, independent of the representation (it remains preserved under equivalence transformations).

1.5 Comparison

The following table presents a comparison between the concepts of classical design theory and those of spherical designs with quantum design theory and its quantum theoretic interpretation.

Classical Designs	Spherical Designs	Quantum Designs	Quantum Theory
block B	normalized vector	projection matrix $\mathbf{P}$	event
cardinality of the block B	1	$\mathrm{tr}(\mathbf{P})$	$\sim$ likelihood of the event
constant block size	always satisfied	regular	equally probable events
constant number of blocks through each point	eutactic, index 2	coherent	coherent states
t-balanced, t-design	index $2t$, antipodal $(2t+1)$- design	t-coherent, quantum t-design	extension of the coherence
cardinality of the intersection of B_i and B_j	angle, inner product	$\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j)$	$\sim$ joint probability
constant intersection of two blocks	equiangular, degree 1	degree 1	constant joint probability
s values for the intersection of two blocks	degree s	degree s	s joint probabilities
resolvable	disjoint union of orthonormal bases	resolvable	$\sim$ sets of observables
affine 1-design, net, orthogonal array	disjoint union of orthonormal bases of degree 2	affine, regular quantum design	$\sim$ mutually independent observables

2 Properties

2.1 Bounds

Let X be a set of $b \times b$ matrices with constant trace r. Let $\mathbf{C} = \mathbf{I} \otimes \mathbf{C}'$, where $\mathbf{I}$ is the $b \times b$ identity matrix, and $\mathbf{C}'$ is a $b^{(t-1)} \times b^{(t-1)}$ matrix. Then it follows that

$$\operatorname{tr}\left((\mathbf{I} \otimes \mathbf{C}')(\otimes^t \mathbf{P})\right) = r \operatorname{tr}\left(\mathbf{C}'(\otimes^{(t-1)} \mathbf{P})\right) \in \operatorname{Hom}(X, t).$$

This implies that $\operatorname{Hom}(X, t-1) \subset \operatorname{Hom}(X, t)$ for homogeneous polynomials over X, and by induction we obtain $\operatorname{Hom}(X, t) = \operatorname{Pol}(X, t)$.

Proposition 2.1. *Suppose the quantum design $\mathbf{D}$ is regular and t-coherent w.r.t. a group G. It then follows that $\mathbf{D}$ is a quantum t-designs w.r.t. G.*

Proof. In the case of regular quantum designs, the G-space $X = \bigcup_{i=1}^{v} X_i$, where the X_i, $1 \leq i \leq v$, are the homogeneous G-spaces generated by the $\mathbf{P}_i$, has constant trace. The result follows from $\operatorname{Hom}(X, t) = \operatorname{Pol}(X, t)$ and Theorem 1.16. □

However attention is required, because even for regular quantum designs the G-space $X = \bigcup_{i=1}^{v} X_i$, where the X_i, $1 \leq i \leq v$, are the homogeneous G-spaces generated by the $\mathbf{P}_i$, is not necessarily itself homogeneous.

For regular quantum designs, there exists a homogeneous G-space X w.r.t. a group G if and only if G also acts transitively on $\mathbf{D}$. This can be easily seen, as on the one hand, G must act transitively on a subset of the G-space and vice versa, if this is the case, then $X_i = X$ for all $1 \leq i \leq v$ immediately follows.

Theorem 2.2 (Absolute Bounds)**.** *Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a degree s quantum design with $\operatorname{tr}(\mathbf{P}_i) = r_i \notin \Lambda$ for all $1 \leq i \leq v$. Furthermore, let X be any set of $b \times b$ matrices with $\mathbf{D} \subseteq X$. Then the following inequality holds:*

$$v \leq \dim(\operatorname{Pol}(X, s)). \tag{2.1}$$

Proof. Let $\Lambda = \{\lambda_1, \ldots, \lambda_s\}$. The polynomials

$$f_i(\mathbf{P}) = \prod_{l=1}^{s} \left(\operatorname{tr}\left(\mathbf{P}\mathbf{P}_i\right) - \lambda_l\right), \qquad 1 \leq i \leq v,$$

are contained in $\operatorname{Pol}(X, s)$, and the following holds on $\mathbf{D} \subseteq X$

$$f_i(\mathbf{P}_j) = \begin{cases} 0 & \text{for all } 1 \leq i \neq j \leq v, \\ \prod_{l=1}^{s}(r_i - \lambda_l) \neq 0 & \text{for all } 1 \leq i = j \leq v. \end{cases}$$

Thus, these polynomials are linearly independent, and it follows that their number v is bounded by $\dim(\operatorname{Pol}(X, s))$. □

In the case $r = 1$, the idea for the proof can be traced to KOORNWINDER [51]. It also holds particular for polynomial spaces (see [29, Theorem 14.4.1]). It is, however, not assumed that X be the union of G-spaces (we also don't need any integrals over X), and thus the theorem also holds for non-polynomial spaces (and sets X).

The condition $\mathrm{tr}(\mathbf{P}_i) = r_i \notin \Lambda$ for all $1 \leq i \leq v$ also permits a mild generalization (see [29, Theorem 14.4.1]).

If X is the real Grassmannian with $r = 1$, then $\mathrm{Pol}(G_1(\mathbb{R}^b), s)$ is equivalent to the space of homogeneous degree $2s$ polynomials defined over the unit sphere. It is a well-known fact that in this case, $\dim(\mathrm{Pol}(G_1(\mathbb{R}^b), s)) = \binom{b+2s-1}{b-1}$ holds. If X is the complex Grassmannian with $r = 1$, then $\mathrm{Pol}(G_1(\mathbb{C}^b), s)$ is equivalent to the space of polynomials over the unit sphere that are homogeneous of degree s in the variables x_i, and homogeneous of degree s in the variables $\bar{x}_j$ and one gets: $\dim(\mathrm{Pol}(G_1(\mathbb{C}^b), s)) = \binom{b+s-1}{b-1}^2$ (see [24]). Similar bounds were deduced in [25] by taking into consideration the phases of the inner products of vectors.

If $\mathbf{D}$ is regular, then in Theorem 2.2 we can also choose X to be a set with constant trace, thus obtaining $v \leq \dim(\mathrm{Hom}(X, t))$. In Section 2.4 we will show that for $s = 1$, this also holds for non-regular designs, and so in that case, Theorem 2.2 does not give the best-possible bounds.

Theorem 2.3. *Let the quantum design $\mathbf{D} = \{\mathbf{P}_1, \dots, \mathbf{P}_v\}$ be $2e$-coherent w.r.t. $G \subseteq U(b)$. Let X_i, $1 \leq i \leq v$, be the G-spaces generated by the $\mathbf{P}_i$, and set $X = \bigcup_{i=1}^{v} X_i$. Then we have*

$$v \geq \dim(\mathrm{Hom}(X, e)). \tag{2.2}$$

If $\mathbf{D}$ is a quantum $2e$-design w.r.t. G (e.g. regular), then

$$v \geq \dim(\mathrm{Pol}(X, e)). \tag{2.3}$$

Proof. Let $h_1, \dots, h_n$ be an orthonormal basis for $\mathrm{Hom}(X, e)$ with respect to the inner product given by

$$\langle h_l | h_m \rangle = \frac{1}{v} \sum_{i=1}^{v} \int_{X_i} h_l(\mathbf{P}) h_m(\mathbf{P}) dp,$$

i.e. $\langle h_l | h_m \rangle = \delta_{lm}$, $1 \leq l, m \leq n$. (Such a basis can always be found by using Gram-Schmidt orthogonalization). The products $h_l h_m$ are homogeneous of degree $2e$. Since the quantum design is $2e$-coherent w.r.t. G, Equation (1.16) implies

$$\sum_{i=1}^{v} h_l(\mathbf{P}_i) h_m(\mathbf{P}_i) = \delta_{lm} \quad \text{for all } 1 \leq l, m \leq n.$$

Therefore the polynomials are mutually orthogonal on $\mathbf{D}$, and hence are linearly independent. It follows that $n = \dim(\mathrm{Hom}(X, e))$ is bounded by $v = |\mathbf{D}|$.

The same considerations are valid using orthonormal bases of $\mathrm{Pol}(X, e)$ for quantum t-designs. $\square$

Those quantum designs for which (2.2) becomes equality are said to be *tight*.

Our proof proceeded along the lines of [29, Theorem 14.5.1], but the statement was generalized from quantum t-designs to t-coherence (for non-regular designs). For $r = 1$, these bounds agree exactly with the lower bounds for t-designs over projective spaces (see [10]). By considering the phases of vectors in [25], sharper bounds were deduced for real, spherical designs (see also [6] and [7]).

If $\mathbf{D}$ is a quantum $(2e+1)$-design, then it is also a quantum $2e$-design, and inequality (2.3) holds again. However, in general this bound is not the best possible. For example, for (1-) coherent quantum designs it yields $v \geq 1$. We will show though that for regular, coherent designs for example, we have the stronger inequality $v \geq b/r$.

We will need the following lemma before proceeding with some further (special) bounds.

Lemma 2.4. *Let $G \subseteq U(b)$, and let $\mathbf{K}_t(X_1)$ and $\mathbf{K}_t(X_2)$ be the two coherence tensors w.r.t. the homogeneous G-spaces X_1 and X_2. If $\mathbf{P}_1$ is any matrix in X_1, then*

$$\operatorname{tr}\left(\mathbf{K}_t(X_1)\mathbf{K}_t(X_2)\right) = \operatorname{tr}\left(\left(\otimes^t \mathbf{P}_1\right)\mathbf{K}_t(X_2)\right).$$

Proof. Let $\mathbf{P}_1 \in X_1$ and $\mathbf{P}_2 \in X_2$. We will use the fact that the trace function, as well as every coherence tensor w.r.t. a G-space, is invariant under similarity transformations with $U \in G \subseteq U(b)$.

$$\begin{aligned}
\operatorname{tr}\left(\mathbf{K}_t(X_1)\mathbf{K}_t(X_2)\right) &= \operatorname{tr}\left(\int_G \otimes^t(\mathbf{U}\mathbf{P}_1\mathbf{U}^{-1})du \int_G \otimes^t(\mathbf{V}\mathbf{P}_2\mathbf{V}^{-1})dv\right) \\
&= \int_G \int_G \operatorname{tr}\left(\otimes^t(\mathbf{U}\mathbf{P}_1\mathbf{U}^{-1}\mathbf{V}\mathbf{P}_2\mathbf{V}^{-1})\right) dv\, du \\
&= \operatorname{tr}\left(\int_G \otimes^t \mathbf{P}_1\mathbf{U}^{-1}\left(\int_G \otimes^t(\mathbf{V}\mathbf{P}_2\mathbf{V}^{-1})dv\right)\mathbf{U}du\right) \\
&= \operatorname{tr}\left(\left(\otimes^t\mathbf{P}_1\right)\mathbf{K}_t(X_2)\right).
\end{aligned}$$

□

Theorem 2.5 (Generalized Sidelnikov Inequality)**.** *Let X_i be homogeneous G-spaces w.r.t. $G \subseteq U(b)$ for all $1 \leq i \leq v$, and let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a quantum design with $\mathbf{P}_i \in X_i$. Then for all $t \in \mathbb{N}$, we have*

$$\sum_{i=1}^{v}\sum_{j=1}^{v}\left(\operatorname{tr}\left(\mathbf{P}_i\mathbf{P}_j\right)\right)^t \geq \sum_{i=1}^{v}\sum_{j=1}^{v}\operatorname{tr}\left(\mathbf{K}_t(X_i)\mathbf{K}_t(X_j)\right).$$

For regular quantum designs with $X_i = X$ for all $1 \leq i \leq v$, it follows that

$$\frac{1}{v^2}\sum_{i=1}^{v}\sum_{j=1}^{v}\left(\operatorname{tr}\left(\mathbf{P}_i\mathbf{P}_j\right)\right)^t \geq \operatorname{tr}\left(\left(\mathbf{K}_t(X)\right)^2\right). \tag{2.4}$$

$\mathbf{D}$ *is t-coherent w.r.t. G if and only if equality holds.*

Proof. Since $\mathbf{P} = \mathbf{P}^*$, it follows that $\mathbf{K}_t(X) = \mathbf{K}_t(X)^*$ as well, and thus the tensor

$$\mathbf{C} = \sum_{i=1}^{v} \otimes^t \mathbf{P}_i - \sum_{i=1}^{v} \mathbf{K}_t(X_i)$$

is self-adjoint. By applying Lemma 2.4, we conclude that

$$\mathrm{tr}(\mathbf{C}\mathbf{C}) = \sum_{i=1}^{v}\sum_{j=1}^{v} (\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j))^t - \sum_{i=1}^{v}\sum_{j=1}^{v} \mathrm{tr}\left(\mathbf{K}_t(X_i)\mathbf{K}_t(X_j)\right), \geq 0,$$

as desired. In the case of equaltiy, we have $\mathbf{C} = \mathbf{0}$, i.e. t-coherence w.r.t. G. $\square$

We will now briefly investigate the Grassmannians and the sets of diagonal $b \times b$ matrices with given trace r, which we denote by $\mathbb{J}_r^b$.

Via the association (1.18) integrals over the Grassmannians $X = G_1(\mathbb{C}^b)$, resp. $X = G_1(\mathbb{R}^b)$ of rank 1, are equivalent to the integral over the complex, resp. real, unit sphere Ω (see [43]) and it follows with an arbitrary (w.l.o.g. real) projection $\mathbf{P}_{\mathbf{e}}$ onto the one-dimensional subspace spanned by by a vector $\mathbf{e}$ in Ω with the help of Lemma 2.4 that

$$\mathrm{tr}\left((\mathbf{K}_t(X))^2\right) = \int_\Omega |\langle \mathbf{e}|\mathbf{y}\rangle|^{2t}\, d\omega(y) = \begin{cases} \frac{\Gamma(\frac{b}{2})}{\sqrt{\pi}\Gamma(\frac{b-1}{2})} \int_0^1 z^{t-\frac{1}{2}}(1-z)^{\frac{b-3}{2}} dz & \text{for } \mathbb{R}, \\ (b-1)\int_0^1 z^t (1-z)^{b-2} dz & \text{for } \mathbb{C}, \end{cases}$$

holds, where Γ denotes the gamma funtion. This immediately implies the following lemma.

Lemma 2.6.

$$\mathrm{tr}\left((\mathbf{K}_t(X))^2\right) = \begin{cases} \dfrac{1 \cdot 3 \cdot 5 \cdots (2t-1)}{b(b+2)\cdots(b+2t-2)} & \textit{for } X = G_1(\mathbb{R}^b), \\ \dfrac{t!}{b(b+1)\cdots(b+t-1)} & \textit{for } X = G_1(\mathbb{C}^b). \end{cases} \tag{2.5}$$

It is clear that for $X = \mathbb{J}_1^b$, $\mathrm{tr}(\mathbf{K}_t(X))^2 = \frac{1}{b}$ holds for all t.

The inequality (2.4), which in the real case is associated to the above formula, corresponds to the well-known *(*Sidelnikov Inequality) for spherical designs (see [30], [31], [63] and [71]).

For G-spaces X w.r.t. irreducible groups G we deduce immediately that

$$\mathrm{tr}\left((\mathbf{K}_1(X))^2\right) = \mathrm{tr}\left(\left(\frac{r}{b}\mathbf{I}\right)^2\right) = \frac{r^2}{b}.$$

We will also need the following explicit formulas for later.

Lemma 2.7.

$$\operatorname{tr}\left((\mathbf{K}_2(X))^2\right) = \begin{cases} \dfrac{r^2((b+1)r^2+2b-4r)}{b(b-1)(b+2)} & \textit{for } X = G_r(\mathbb{R}^b), \\ \dfrac{r^2(br^2+b-2r)}{b(b-1)(b+1)} & \textit{for } X = G_r(\mathbb{C}^b), \\ \dfrac{r^2(r^2+b-2r)}{b(b-1)} & \textit{for } X = \mathbb{J}_r^b. \end{cases} \tag{2.6}$$

Proof. Let $\mathbf{P}_j$, $1 \leq j \leq b$ be the diagonal $b \times b$ matrices with 1 in the j-th diagonal place and 0 everywhere else, and set $\mathbf{P} = \sum_{j=1}^r \mathbf{P}_j$.

For $X = G_r(\mathbb{R}^b), G_r(\mathbb{C}^b)$, and $\mathbb{J}_r^b$, we have $\mathbf{P} \in X$, and furthermore

$$\operatorname{tr}\left((\mathbf{K}_2(X))^2\right) = \sum_{i=1}^r \sum_{j=1}^r \sum_{l=1}^r \sum_{m=1}^r \operatorname{tr} \int_G \mathbf{P}_i \mathbf{U} \mathbf{P}_l \mathbf{U}^{-1} \otimes \mathbf{P}_j \mathbf{U} \mathbf{P}_m \mathbf{U}^{-1} du. \tag{2.7}$$

We use the following two facts: the trace is unitarily invariant; and for any $1 \leq i \neq j \leq r$ and $1 \leq l \neq m \leq r$, there exists a permutation matrix $\mathbf{S} \in S(b) \subset O(b) \subset U(b)$ that transforms the pair $\mathbf{P}_l, \mathbf{P}_m$ into the pair $\mathbf{P}_i, \mathbf{P}_j$ via a similarity transformation, and obtain

$$\operatorname{tr}\left((\mathbf{K}_2(X))^2\right) = r^2 x + 2r^2(r-1)y + r^2(r-1)^2 z.$$

Here x is the value of those terms of the sum (2.7) with $1 \leq i = j \leq r, 1 \leq l = m \leq r$, furthermore y is the value of those terms with either $1 \leq i \neq j \leq r, 1 \leq l = m \leq r$ or $1 \leq i = j \leq r, 1 \leq l \neq m \leq r$, and z is the value of those terms with $1 \leq i \neq j \leq r, 1 \leq l \neq m \leq r$. Furthermore, we have

$bx + b(b-1)y = \operatorname{tr} \int_G \left(\sum_{i=1}^b \mathbf{P}_i \mathbf{U} \mathbf{P}_l \mathbf{U}^{-1}\right) \otimes \left(\sum_{j=1}^b \mathbf{P}_j \mathbf{U} \mathbf{P}_l \mathbf{U}^{-1}\right) du = 1,$

$by + b(b-1)z = \operatorname{tr} \int_G \left(\sum_{i=1}^b \mathbf{P}_i \mathbf{U} \mathbf{P}_l \mathbf{U}^{-1}\right) \otimes \left(\sum_{j=1}^b \mathbf{P}_j \mathbf{U} \mathbf{P}_m \mathbf{U}^{-1}\right) du = 1.$

Now $x = \operatorname{tr}(\mathbf{K}_2(X'))^2$, where X' is the homogeneous G-space generated by one of the projections $\mathbf{P}_i$ with trace 1. We thus obtain the parameter x from the equations (2.5) for $t = 2$, resp. $x = \frac{1}{b}$ for $\mathbb{J}_r^b$, and so the equations (2.6) can be solved recursively. □

Analogous formulas can also be deduced for $t > 2$, but they quickly become very complicated.

In the next sections, we will especially investigate affine and degree 1 quantum designs more thoroughly, and in the process we will encounter applications of the inequalities derived here.

2.2 Coherent Duality

Just as with spherical designs, we will now give a general description of quantum designs using sets of vectors. Although these sets of vectors are not uniquely determined, they give rise to a unique operation on coherent quantum designs.

If $\{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$ is an orthonormal system in $\mathbb{C}^b$, then the orthogonal projection $\mathbf{P}$ onto the subspace of $\mathbb{C}^b$ that they span is given by $\mathbf{P}\,\mathbf{x} = \sum_{i=1}^{r} \langle \mathbf{x}|\mathbf{e}_i\rangle\, \mathbf{e}_i$ for all $\mathbf{x} \in \mathbb{C}^b$. Let $\mathbf{E}$ be the $b \times r$ matrix obtaineded by writing the r vectors $\mathbf{e}_j = (e_{1j}, \ldots, e_{bj})^t$ as columns, i.e. $(\mathbf{E})_{ij} = e_{ij}$ for all $1 \le j \le r$ and $1 \le i \le b$. Then the following relations hold:

$$\mathbf{P} = \mathbf{E}\mathbf{E}^*, \tag{2.8a}$$

$$\mathbf{I}_r = \mathbf{E}^*\mathbf{E}. \tag{2.8b}$$

Every orthogonal projection can be expressed in this form. However, the $b \times r$ Matrix $\mathbf{E}$ is not uniquely determined by $\mathbf{P}$. One can choose another orthonormal basis for the r-dimensional subspace onto which $\mathbf{P}$ projects. For an arbitrary $b \times r$ matrix $\mathbf{E}'$, the equations (2.8), i.e. $\mathbf{P} = \mathbf{E}'\mathbf{E}'^*$ and $\mathbf{I}_r = \mathbf{E}'^*\mathbf{E}'$, hold if and only if $\mathbf{E}' = \mathbf{E}\mathbf{V}$ holds, where $\mathbf{V}$ is a unitary $r \times r$ matrix.

Definition 2.8. Let $r_1 + \cdots + r_v = s$, and let $\mathbf{E}_i$, $1 \le i \le v$, be complex, $b \times r_i$ matrices. The $b \times s$ matrix

$$\mathbf{E} = \begin{pmatrix} \mathbf{E}_1 & \cdots & \mathbf{E}_v \end{pmatrix}$$

shall be called *quantum design matrix* (*QD-matrix for short*) with partition $(r_1, \ldots, r_v)$, if the following holds true:

$$\mathbf{E}_i^*\mathbf{E}_i = \mathbf{I}_{r_i} \qquad \text{for all } 1 \le i \le v.$$

Let $\mathbf{P}_i = \mathbf{E}_i\mathbf{E}_i^*$ for all $1 \le i \le v$. Then $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ is the quantum design *associated to the QD-matrix.*

Two QD-matrices $\mathbf{E} = (\mathbf{E}_1 \ldots \mathbf{E}_v)$ and $\mathbf{E}' = (\mathbf{E}'_1 \ldots \mathbf{E}'_v)$ are said to be *equivalent* or *isomorphic*, if there exist unitary $r_i \times r_i$ matrices $\mathbf{V}_i$, $1 \le i \le v$, a permutation π of $\{1, \ldots, v\}$, and a matrix $\mathbf{U} \in U(b)$, such that the following holds:

$$\mathbf{E}'_i = \mathbf{U}\mathbf{E}_{\pi(i)}\mathbf{V}_i \qquad \text{for all } 1 \le i \le v. \tag{2.9}$$

The definition of equivalence was chosen so as to agree with equivalence for quantum designs, i.e. for equivalence classes, the association is uniquely invertible.

Lemma 2.9. *Suppose the quantum design* $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ *and the QD-matrix* $\mathbf{E} = (\mathbf{E}_1 \ldots \mathbf{E}_v)$ *are associated to each other. Then we have:*

(i) $\mathbf{D}$ *is coherent if and only if the rows of* $\mathbf{E}$ *all have the same norm and are mutually orthogonal - i.e. when the following holds true*

$$\mathbf{E}\mathbf{E}^* = k\mathbf{I}_b. \tag{2.10}$$

(ii) *For the Hilbert-Schmidt-Norm* ($\|\mathbf{A}\| = (\mathrm{tr}(\mathbf{A}^*\mathbf{A}))^{1/2}$),

$$\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j) = \|\mathbf{E}_i^*\mathbf{E}_j\|^2 \tag{2.11}$$

holds for all $1 \leq i, j \leq v$*. In particular,* $\mathbf{D}$ *is of degree* 1 *if and only if* $\|\mathbf{E}_i^*\mathbf{E}_j\|^2 = \lambda$ *for all* $1 \leq i \neq j \leq v$*.*

Proof. (i) $\sum_{i=1}^{v} \mathbf{P}_i = \sum_{i=1}^{v} \mathbf{E}_i\mathbf{E}_i^* = \mathbf{E}\mathbf{E}^*$.

(ii) $\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j) = \mathrm{tr}(\mathbf{E}_i\mathbf{E}_i^*\mathbf{E}_j\mathbf{E}_j^*) = \mathrm{tr}(\mathbf{E}_j^*\mathbf{E}_i\mathbf{E}_i^*\mathbf{E}_j) = \mathrm{tr}\left((\mathbf{E}_i^*\mathbf{E}_j)^*(\mathbf{E}_i^*\mathbf{E}_j)\right) = \|\mathbf{E}_i^*\mathbf{E}_j\|^2$ for all $1 \leq i, j \leq v$.

□

Therefore, since QD-matrices associated to a coherent quantum design have mutually orthogonal rows, it follows that $b \leq s$. Together with $s = kb$ (equation (1.6a)), this implies

$$k \geq 1$$

for arbitrary coherent designs. For regular, coherent quantum designs, we then get $v \geq b/r$. Furthermore, $k = 1$ holds if and only if the QD-matrix is square and unitary. We will now exclude this trivial special case.

Definition 2.10. Let the coherent quantum design $\mathbf{D}$ with $k > 1$ be associated to the $b \times s$ QD-matrix $\mathbf{E}$ (with $s > b$). An $(s - b) \times s$ QD-matrix $\mathbf{E}^\perp$ with the same partition (of s) is called *coherently dual* to $\mathbf{E}$ if its rows are orthogonal to each other and to the rows of $\mathbf{E}$. Analogously, the quantum design $\mathbf{D}^\perp$ associated to $\mathbf{E}^\perp$ is called coherently dual to $\mathbf{D}$.

Coherent duality has nothing to do with the concept of duality in classical design theory (transposition of the incidence matrix). Only a trivial special case can be applied to classical designs (see below). However, there is a relationship concept of duality used in the theory of error-correcting codes.

Theorem 2.11. *For every coherent quantum design* $\mathbf{D}$ *with* $k > 1$*, there is a coherently dual quantum design* $\mathbf{D}^\perp$ *which is unique up to unitary equivalence.* $\mathbf{D}^{\perp\perp}$ *is unitarily equivalent to* $\mathbf{D}$*. The following relations hold:*

$$v^\perp = v, \qquad b^\perp = b(k-1),$$

$$k^\perp = \frac{k}{k-1}, \qquad r_i^\perp = r_i \quad \textit{for all } 1 \leq i \leq v,$$

$$\mathrm{tr}(\mathbf{P}_i^\perp\mathbf{P}_j^\perp) = \frac{1}{(k-1)^2}\,\mathrm{tr}(\mathbf{P}_i\mathbf{P}_j) \qquad \textit{for all } 1 \leq i \neq j \leq v.$$

In particular, $\mathbf{D}^\perp$ *has the same degree as* $\mathbf{D}$*, and is regular if and only if* $\mathbf{D}$ *is.*

Proof. Let $\mathbf{E} = (\mathbf{E}_1 \dots \mathbf{E}_v)$ be the QD-matrix associated to $\mathbf{D}$.

We will first prove, by construction, the existence of a coherently dual QD-matrix: Let $\widetilde{\mathbf{E}} = \frac{1}{\sqrt{k}}\mathbf{E} = (\widetilde{\mathbf{E}}_1 \dots \widetilde{\mathbf{E}}_v)$. The coherence of $\mathbf{D}$ together with equation (2.10) implies $\widetilde{\mathbf{E}}\widetilde{\mathbf{E}}^* = \mathbf{I}_b$. Thus, the rows of $\widetilde{\mathbf{E}}$ form an orthonormal system in $\mathbb{C}^s$, which can always be completed to an orthonormal basis with the addition of $(s-b)$ row vectors (for example using the Gram-Schmidt process). Now let $\widetilde{\mathbf{E}}^{\perp} = (\widetilde{\mathbf{E}}_1^{\perp} \ldots \widetilde{\mathbf{E}}_v^{\perp})$ be an $(s-b) \times s$ matrix that consists of the $(s-b)$ additional row vectors, and that is partitioned in the same way as $\widetilde{\mathbf{E}}$. Let

$$\mathbf{G} = \begin{pmatrix} \widetilde{\mathbf{E}}_1 & \ldots & \widetilde{\mathbf{E}}_v \\ \widetilde{\mathbf{E}}_1^{\perp} & \ldots & \widetilde{\mathbf{E}}_v^{\perp} \end{pmatrix}.$$

$\mathbf{G}$ is a unitary $s \times s$ matrix. It follows from the equality $\mathbf{G}\mathbf{G}^* = \mathbf{I}_s$ that $\mathbf{G}^*\mathbf{G} = \mathbf{I}_s$, i.e.

$$\widetilde{\mathbf{E}}_i^* \widetilde{\mathbf{E}}_j + \widetilde{\mathbf{E}}_i^{\perp *} \widetilde{\mathbf{E}}_j^{\perp} = \begin{cases} \mathbf{I}_{r_i} & \text{for all } 1 \leq i = j \leq v, \\ \mathbf{0} & \text{for all } 1 \leq i \neq j \leq v. \end{cases} \tag{2.12}$$

Now let $\mathbf{E}^{\perp} = \sqrt{\frac{k}{k-1}} \widetilde{\mathbf{E}}^{\perp} = (\mathbf{E}_1^{\perp} \ldots \mathbf{E}_v^{\perp})$. Then the equations $\widetilde{\mathbf{E}}_i^* \widetilde{\mathbf{E}}_i = \frac{1}{k} \mathbf{E}_i^* \mathbf{E}_i = \frac{1}{k} \mathbf{I}_{r_i}$ immediately imply that

$$\mathbf{E}_i^{\perp *} \mathbf{E}_i^{\perp} = \mathbf{I}_{r_i} \qquad \text{for all } 1 \leq i \leq v.$$

This means $\mathbf{E}^{\perp}$ is a QD-matrix, and by construction it is coherently dual to $\mathbf{E}$.

To prove uniqueness: As we can see from the above construction, all $\mathbf{U}^{\perp}\mathbf{E}^{\perp}$, where $\mathbf{U}^{\perp}$ is any unitary $(s-b) \times (s-b)$ matrix, are coherently dual to $\mathbf{E}$ and consequently also to all $\mathbf{U}\mathbf{E}$ where $\mathbf{U}$ is any unitary $b \times b$ matrix. However, these are all equivalence operations, and all further equivalence operations are in 1-1 correspondence to each other: Let $\mathbf{E}_i' = \mathbf{E}_{\pi(i)} \mathbf{V}_i$, with a permutation π and unitary $r_i \times r_i$ matrices for all $1 \leq i \leq v$. Then the $(\mathbf{E}_i^{\perp})' = \mathbf{E}_{\pi(i)}^{\perp} \mathbf{V}_i$ form a coherently dual QD-matrix, and vice versa.

About the parameters: $v^{\perp} = v$ and $r_i^{\perp} = r_i$ for all $1 \leq i \leq v$ are trivial. $b^{\perp} = s - b = kb - b = b(k-1)$. By definition, we also have $\widetilde{\mathbf{E}}^{\perp} \widetilde{\mathbf{E}}^{\perp *} = \mathbf{I}_{s-b}$; this implies $\mathbf{E}^{\perp} \mathbf{E}^{\perp *} = \frac{k}{k-1} \mathbf{I}_{s-b}$, and hence $k^{\perp} = \frac{k}{k-1}$. Finally, from the equations (2.12) and (2.11) follows, for all $1 \leq i \neq j \leq v$

$$\begin{aligned} \mathbf{E}_i^* \mathbf{E}_j &= -(k-1) \mathbf{E}_i^{\perp *} \mathbf{E}_j^{\perp}, \\ \|\mathbf{E}_i^* \mathbf{E}_j\|^2 &= (k-1)^2 \|\mathbf{E}_i^{\perp *} \mathbf{E}_j^{\perp}\|^2, \\ \operatorname{tr}(\mathbf{P}_i \mathbf{P}_j) &= (k-1)^2 \operatorname{tr}(\mathbf{P}_i^{\perp} \mathbf{P}_j^{\perp}). \end{aligned}$$

□

If the quantum design is real, then the coherently dual design can also be constructed over the reals, and is unique up to orthogonal equivalences.

If, for $t \geq 2$, a quantum design is t-coherent w.r.t. a group G, then the coherently dual quantum design is not necessarily also t-coherent w.r.t. G. Consider for example the spherical 4-design constructed from a regular pentagon in $\mathbb{R}^2$ (see [25]). It corresponds to a quantum 2-design w.r.t. $O(b)$, but it is easy to check that the coherently dual design is not 2-coherent w.r.t. $O(b)$. (The parameters $v = 5$ and $b = 3$ also violate the inequality $v \geq b(b+3)/2$ for spherical 4-designs, see [25], resp. [36]).

Hadwiger [33] showed that coordinate stars are precisely the orthogonal projections of an orthonormal basis for $\mathbb{R}^s$ $(s \geq b)$ onto a b-dimensional subspace (Pohlke's normal stars). From our proof it follows more generally that coherent quantum designs (up to a normalization factor) are precisely the orthogonal projections of an orthogonal decomposition of $\mathbb{C}^s$ (or $\mathbb{R}^s$) onto a b-dimensional subspace.

Proposition 2.12. *Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a coherent quantum design in $\mathbb{C}^b$, with $k \neq 1$ and $\operatorname{tr}(\mathbf{P}_i) = r_i$ for all $1 \leq i \leq v$. Then we have*

$$v \geq \frac{1}{r}(b + \max(r_1, \ldots, r_v)).$$

For regular quantum designs, this means that $v \geq 1 + \frac{b}{r}$.

Proof. There exists a coherently dual quantum design $\mathbf{D}^\perp$, and its parameters trivially satisfy the inequality $b^\perp \geq \max(r_1^\perp, \ldots, r_v^\perp)$. Thus, we have $b(k-1) \geq \max(r_1, \ldots, r_v)$, and together with $k = \frac{vr}{b}$ the desired inequalities follow. $\square$

This implies, for example, that there does not exist a coherent quantum design with $v = 3$, $b = 5$, $r = 2$ (even though $k = \frac{vr}{b} = \frac{6}{5} > 1$). We will soon see that there are (very many) quantum designs for which the inequalty here is actually an equality.

Lemma 2.13. *Every regular, coherent, degree 1 quantum design with $r = 1$ and $\lambda \neq 0$ is irreducible.*

Proof. Suppose $\mathbf{P}_i = \mathbf{P}_{1i} \oplus \mathbf{P}_{2i}$ for all $1 \leq i \leq v$. It follows from $1 = \operatorname{tr}(\mathbf{P}_i) = \operatorname{tr}(\mathbf{P}_{1i}) + \operatorname{tr}(\mathbf{P}_{2i})$ that either $\mathbf{P}_{1i} = 0$ and $\mathbf{P}_{2i} \neq 0$, or $\mathbf{P}_{1i} \neq 0$ and $\mathbf{P}_{2i} = 0$ holds for all $1 \leq i \leq v$. Coherence implies that there is at least one $\mathbf{P}_{1i} \neq 0$ (i.e. $\mathbf{P}_{2i} = 0$) and at least one $\mathbf{P}_{2j} \neq 0$ (i.e. $\mathbf{P}_{1j} = 0$). Therefore $\operatorname{tr}(\mathbf{P}_i\mathbf{P}_j) = \operatorname{tr}(\mathbf{P}_{1i}\mathbf{P}_{1j}) + \operatorname{tr}(\mathbf{P}_{2i}\mathbf{P}_{2j}) = 0$, in contradiction with $\lambda \neq 0$. $\square$

Examples 2.14. For each parameter $b^\perp = r^\perp \in \mathbb{N}$ and $v^\perp \geq 2$, there exist unique and trivial quantum designs $\mathbf{D}^\perp = \left\{\mathbf{P}_1^\perp = \mathbf{I}_{r^\perp}, \ldots, \mathbf{P}_v^\perp = \mathbf{I}_{r^\perp}\right\}$. The $\mathbf{D}^\perp$ each have degree 1, with $\lambda^\perp = r^\perp$.

Thus there exist unique - up to (unitary) equivalence - coherently dual quantum designs $\mathbf{D} = \mathbf{D}^{\perp\perp}$ with the parameters $r = r^\perp \in \mathbb{N}$ and $v = v^\perp \geq 2$, as well as

$$b = r(v-1), \quad k = \frac{v}{v-1} \quad \text{and} \quad \lambda = \frac{r}{(v-1)^2}.$$

$\mathbf{D}$ perfectly satisfies the inequality $v \geq 1 + b/r$ from Proposition 2.12. In the case $r = 1$, Lemma 2.13 implies that $\mathbf{D}$ is irreducible. The r-fold sum of identical copies of $\mathbf{D}$ provides the unique solution for the parameters $r \geq 2$.

The solutions for the parameter $r = 1$ can already be found in [25, Example 5.15], and can also be constucted as the corner vectors of a regular simplex in $\mathbb{R}^b$. In this case their sum is 0, and they even form (tight) spherical 2-designs.

If we were to take the complementary design of the solutions constructed above, take their coherent duals in turn, and then again the complementary design of those, and so on and so forth, then in general we would obtain infinitely-many other regular, coherent, degree 1 quantum designs. It follows that all those quantum designs are also unique solutions for their parameters, just like the initial solutions were.

The application of coherent duality to classical (commutative) designs only delivers such solutions in the trivial special case $k = 2$. For $k > 2$, it follows that $1 < k^{\perp} < 2$, and the coherently dual quantum design can no longer be classical (commutative).

If the quantum design $\mathbf{D}$ is regular and has degree s, then the coherently dual quantum design $\mathbf{D}^{\perp}$ is also regular, of degree s. This implies that under certain conditions, it is possible to construct coherently dual versions of the absolute limits given in Theorem 2.2. We will give an example of this in the next section.

2.3 Affine Quantum Designs

Proposition 2.15. *Let* $\mathbf{D}$ *be an affine quantum design, and let* $\{\mathbf{P}_{i1}, \ldots, \mathbf{P}_{ig_i}\}$, $1 \le i \le k$ *be its orthogonal classes. Then for any two projections from distinct orthogonal classes* $\mathbf{P}_{il}$ *and* $\mathbf{P}_{jm}$, $1 \le i \ne j \le k$, $1 \le l \le g_i$, $1 \le m \le g_j$, *we have*

$$\lambda = \operatorname{tr}(\mathbf{P}_{il}\mathbf{P}_{jm}) = \frac{1}{b} \operatorname{tr}(\mathbf{P}_{il}) \operatorname{tr}(\mathbf{P}_{jm}). \tag{2.13}$$

If the quantum design has $k = 2$ *orthogonal classes, then the dimensions of the projections within each orthogonal class are constant. If the quantum design has more than two orthogonal classes, then it must actually be regular.*

Proof. Since the orthogonal classes are complete, we have $\sum_{l=1}^{g_i} \mathbf{P}_{il} = \mathbf{I}$ for all $1 \le i \le k$. After multiplication by an arbitrary $\mathbf{P}_{jm}$ from the j-th orthogonal class, $j \ne i$, and subsequent application of the trace, we obtain $\lambda g_i = \operatorname{tr}(\mathbf{P}_{jm})$ for all $1 \le m \le g_j$. This implies that $\operatorname{tr}(\mathbf{P}_{jm}) = r_j$ is constant in each orthogonal class, and together with the equality $g_i = b/r_i$, this implies $\lambda = r_i r_j / b$, which is equation (2.13).

Now let $k \ge 3$, and pick any $1 \le i \ne j \le k$. Then there exists an $s \ne i, j$ s.t. $1 \le s \le k$. From the above equation, we get $\lambda g_i = r_s = \lambda g_j$, i.e. $g_i = g_j$, and this implies that $r_i = b/g_i$ is the same for all orthogonal classes. □

For affine designs with $k \ge 3$ orthogonal classes of order g, there are only 3 independent parameters, for example v, b, and r. The other parameters are then given by

$$g = \frac{b}{r}, \quad k = \frac{v}{g} \quad \text{and} \quad \lambda = \frac{r^2}{b}.$$

In the special case of commutative projections, Proposition 2.15 agrees with the statement of [13, Proposition I.7.3] for transversal designs, and accordingly for the dual orthogonal arrays (or affine 1-designs, or nets, see [20, II.2]). However, in [13] parameters may only take values in the natural numbers, whereas in our case, $\lambda \in \mathbb{Q}$ is also permissible.

Corollary 2.16. *If* $\mathbf{D}$ *is an affine quantum design, then the orthogonal classes are mutually independent. Conversely, a resolvable quantum design* $\mathbf{D}$ *with mutually independent orthogonal classes is an affine quantum design if and only if it is either regular, or* $k = 2$ *and the dimensions of the projections within each orthogonal class are constant.*

Let us briefly consider the case of spherical designs, i.e. $r = 1$. It then follows that $g = b$ and $\lambda = \frac{1}{b}$. Every projection matrix of the orthogonal class of an affine design with $r = 1$ has an associated orthonormal basis. Furthermore, for any two vectors $\mathbf{e}$, $\mathbf{f}$ from distinct orthonormal bases, we always have $|\langle \mathbf{e} | \mathbf{f} \rangle|^2 = 1/b$. In casual terms, we can say that each two orthonormal bases are maximally twisted w.r.t. each other.

We will now discuss the associated QD-matrices.

Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a resolvable quantum design, and $\mathbf{E} = (\mathbf{E}_1 \cdots \mathbf{E}_v)$ be an associated QD-matrix (i.e. $\mathbf{P}_i = \mathbf{E}_i\mathbf{E}_i^*$ and $\mathbf{E}_i^*\mathbf{E}_i = \mathbf{I}_{r_i}$ for all $1 \leq i \leq v$). Let $\widehat{\mathbf{E}}_i = (\mathbf{E}_{i1} \ldots \mathbf{E}_{ig_i})$ for all $1 \leq i \leq k$ be those submatrices of $\mathbf{E}$ that are associated to the i-th orthogonal class $\{\mathbf{P}_{i1}, \ldots, \mathbf{P}_{ig_i}\}$ of $\mathbf{D}$. Then the following holds:

$$\widehat{\mathbf{E}_i}\widehat{\mathbf{E}_i^*} = \sum_{l=1}^{g_i} \mathbf{E}_{il}\mathbf{E}_{il}^* = \sum_{l=1}^{g_i} \mathbf{P}_{il} = \mathbf{I}.$$

Therefore, $\widehat{\mathbf{E}}_i$ is a quadratic and unitary matrix, for all $1 \leq i \leq k$. The equivalence relations (2.9) imply that $\widehat{\mathbf{E}}_1 = \mathbf{I}$ can always be achieved, and hence

$$\widehat{\mathbf{E}}_i^{-1}\widehat{\mathbf{E}}_j = \begin{pmatrix} \mathbf{E}_{i1}^*\mathbf{E}_{j1} & \mathbf{E}_{i1}^*\mathbf{E}_{j2} & \ldots & \mathbf{E}_{i1}^*\mathbf{E}_{jg_j} \\ \mathbf{E}_{i2}^*\mathbf{E}_{j1} & \mathbf{E}_{i2}^*\mathbf{E}_{j2} & \ldots & \mathbf{E}_{i2}^*\mathbf{E}_{jg_j} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{E}_{ig_i}^*\mathbf{E}_{j1} & \mathbf{E}_{ig_i}^*\mathbf{E}_{j2} & \ldots & \mathbf{E}_{ig_i}^*\mathbf{E}_{jg_j} \end{pmatrix}$$

is also quadratic and unitary for all $1 \leq i \neq j \leq k$. Let $\mathrm{tr}(\mathbf{P}_{il}) = r_{il}$ for all $1 \leq i \leq k$, $1 \leq l \leq g_i$. Lemma 2.9 implies that $\mathbf{D}$ has mutually independent orthogonal classes if and only if the following holds for the $r_{il} \times r_{jm}$ submatrices $\mathbf{E}_{il}^*\mathbf{E}_{jm}$:

$$\|\mathbf{E}_{il}^*\mathbf{E}_{jm}\|^2 = \frac{r_{il}r_{jm}}{b}. \tag{2.14}$$

When $\mathbf{D}$ is regular, then these submatrices are quadratic, and the Hilbert-Schmidt norm is constant over them. The case $r = 1$ corresponds to well-known classes of matrices.

- If $r = 1$ and the quantum design is real, then the matrices $\sqrt{b}\widehat{\mathbf{E}}_i^{-1}\widehat{\mathbf{E}}_j$ are *Hadamard matrices* (see [2] and [75]). Such matrices can only exist for $b = 2$ or $b = 4t$, $t \in \mathbb{N}$, and their existence is conjectured for all such b. Consequently, two (or more) mutually independent orthogonal bases can only exist for these dimensions.

- In general for $r = 1$, $\sqrt{b}\widehat{\mathbf{E}}_i^{-1}\widehat{\mathbf{E}}_j$ has entries with absolute value 1, and is proportional to a unitary matrix. Such *generalized Hadamard matrices* over the complex numbers were investigated in [18], especially the case with n-th roots of untiy as entries. Examples for all $b \in \mathbb{N}$ can be obtained via the *Fourier matrices* $\mathbf{F}$ (see [5]) by taking $\sqrt{b}\mathbf{F}$. Consequently, in complex space there are two independent orthonormal bases in every dimension.

To conclude, all unitary block matrices whose $r_{il} \times r_{jm}$ submatrices have a Hilbert-Schmidt norm as in Equation (2.14) shall be called *generalized Block-Hadamard matrices.*

Example 2.17. Let $x, y, z \in [0, 2\pi)$,

$$\mathbf{E}_1(x) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & e^{ix} & -e^{ix} \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -e^{ix} & e^{ix} \end{pmatrix}, \quad \mathbf{E}_2(yz) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ e^{iy} & -e^{iy} & e^{iz} & -e^{iz} \\ 1 & 1 & -1 & -1 \\ -e^{iy} & e^{iy} & e^{iz} & -e^{iz} \end{pmatrix}.$$

Setting $w = y - x$, we get

$$\mathbf{E}_1(x)^{-1}\mathbf{E}_2(yz) = \frac{1}{2}\begin{pmatrix} 1 & 1 & e^{iz} & -e^{iz} \\ 1 & 1 & -e^{iz} & e^{iz} \\ e^{iw} & -e^{iw} & 1 & 1 \\ -e^{iw} & e^{iw} & 1 & 1 \end{pmatrix}.$$

This means that the standard basis and the columns of $\mathbf{E}_1(x)$ and $\mathbf{E}_2(yz)$ form, for all $x, y, z \in [0, 2\pi)$, a regular, affine quantum design with $r = 1$ and with $k = 3$ orthogonal classes. Up to equivalence, those are all such designs in $\mathbb{C}^4$.

Theorem 2.18. *Let $\mathbf{D}$ be a resolvable quantum design with mutually independent orthogonal classes, and let g_i, $1 \leq i \leq k$, be the number of projection matrices in the i-th orthogonal class. Then the following holds:*

$$\sum_{i=1}^{k} g_i - k \leq b^2 - 1 \qquad \textit{for complex quantum designs,}$$

$$\sum_{i=1}^{k} g_i - k \leq \binom{b+1}{2} - 1 \qquad \textit{for real quantum designs,}$$

$$\sum_{i=1}^{k} g_i - k \leq b - 1 \qquad \textit{for commutative quantum designs.}$$

Proof. For every $1 \leq i \leq k$, let $\{\mathbf{P}_{i1}, \ldots, \mathbf{P}_{ig_i}\}$ be the i-th orthogonal class. The matrices of every orthogonal class are mutually orthogonal, and thus independent. They span a g_i-dimensional subspace of the vector space of all $b \times b$ matrices. Furthermore, let $\mathbf{Q}_{ij} = \mathbf{P}_{ij} - \frac{1}{b}\left(\operatorname{tr}(\mathbf{P}_{ij})\right)\mathbf{I}$. Then $\sum_{j=1}^{g_i} \mathbf{Q}_{ij} = \mathbf{0}$ holds, i.e. these matrices are linearly dependent, and they therefore each span a $(g_i - 1)$-dimensional subspace (orthogonal to $\mathbf{I}$). For two matrices $\mathbf{Q}_{ij}$, $\mathbf{Q}_{lm}$, $i \neq l$, from two distinct orthogonal classes it can easily be checked, that $\operatorname{tr}(\mathbf{Q}_{ij}\mathbf{Q}_{lm}) = 0$. It follows that the $(g_i - 1)$-dimensional subspaces are orthogonal. In total, the projection matrices of the design thus span a subspace of dimension $1 + \sum_{i=1}^{k}(g_i - 1)$. Complex projection matrices can at most span the entire b^2-dimensional vector space of the $b \times b$ matrices, while real projection matrices span at most the $\frac{1}{2}b(b+1)$-dimensional subspace of all real, symmetric matrices and the diagonal projection matrices span at most a b-dimensional subspace. The three inequalities immediately follow. □

Theorem 2.19. *Let* $\mathbf{D}$ *be a regular, affine quantum design with* k *orthogonal classes. Then we have*

$$k \le \frac{r(b^2-1)}{b-r} \qquad \textit{for complex quantum designs,}$$

$$k \le \frac{r(b^2+b-2)}{2(b-r)} \qquad \textit{for real quantum designs,}$$

$$k \le \frac{r(b-1)}{b-r} \qquad \textit{for commutative quantum designs.}$$

$\mathbf{D}$ *is a quantum* 2*-design w.r.t.* $U(b)$, $O(b)$, *or* $S(b)$, *if and only if equality holds in the respective case.*

Proof. These inequalities follow directly from Theorem 2.18, with $g = b/r$. However, they also correspond to the special bounds of Theorem 2.5 for $t = 2$ and $X = G_r(\mathbb{C}^b), G_r(\mathbb{R}^b)$, resp. $\mathbb{J}_r^b$. We know the multiplicity of the values from $\Lambda = \{0, \lambda = \frac{r^2}{b}\}$, and use $g = b/r$ and $v = kb/r$ to get

$$\frac{1}{v^2}\sum_{i=1}^{v}\sum_{j=1}^{v}(\mathrm{tr}\,(\mathbf{P}_i\mathbf{P}_j))^2 = \frac{1}{v}(r^2 + g(k-1)\lambda^2) = \frac{r^3}{kb^2}(b + rk - r).$$

If we substitute the values for $\mathrm{tr}\,(\mathbf{K}_2(X))^2$ obtained in equation (2.6) into the inequality (2.4), then we get the above three inequalities. According to Theorem 2.5 equality holds if and only if the quantum designs are 2-coherent w.r.t. the particular groups belonging to the respective G-spaces. The (1-)coherence of affine quantum designs is trivial. □

It is also possible to apply the inequality from Theorem 2.5 more generally to nonregular, resolvable quantum designs with mutually independent orthogonal classes. However, in this case one obtains very complicated formulas (not those of Theorem 2.18).

A quantum design will be called *maximal* if the corresponding inequality from Theorem 2.18 (resp. Theorem 2.19) is actually an equality. Example 2.17 with $x = y = z = 0$ is a maximal real, affine quantum design, hence a quantum 2-design w.r.t. $O(b)$.

Using $b = g^2\lambda$ for regular, commutative designs we obtain the equivalent inequality

$$k \le \frac{g^2\lambda - 1}{g-1}.$$

This inequality is known as the *Placket-Burman Inequality* (see for example [13, Theorem II.2.12]) for classical affine designs (and especially for mutually orthogonal Latin Squares with $\lambda = 1$), or as the *Bose-Bush Bound* (see [27, Theorem II.4.5]) for transversal designs. Another well-known classical result states that equality holds if and only if the the affine design is a 2-design (see [13, Theorem II.8.8]).

Frequency Squares were investigated in classical design theory as generalizations of orthogonal Latin Squares. Via the association in Theorem 1.10, they correspond to commutative, resolvable quantum designs with mutually independent orthogonal classes that are not necessarily regular (see [37], [28] and [27]). In the commutative case, Theorem 2.18 also generalizes the inequalities for Frequency Squares (eg. [27, Theorem 1.5]).

We note that in the proof of Theorem 2.19 via the special inequality, we never used the resolvability of the design, but only the multiplicity of the values from $\Lambda = \{0, \frac{r^2}{b}\}$. With the help of the Gegenbauer polynomials, the inequalities for $r = 1$ can even be deduced without knowledge of these multiplicities; that is, they can be derived for arbitrary degree 2 designs with $\Lambda = \{0, \frac{1}{b}\}$, (see [43, table 2], resp. [24, table I]). However, all known solutions in this case are resolvable (see Section 3.2).

We will now show three methods for taking quantum designs with mutually independent orthogonal classes and constructing new such quantum designs out of them.

Proposition 2.20. *Let* $\mathbf{D}$ *and* $\mathbf{D}'$ *be two resolvable quantum designs, each with* k *mutually independent orthogonal classes* $K_i = \{\mathbf{P}_{i1}, \ldots, \mathbf{P}_{ig_i}\}$, $1 \leq i \leq k$, *resp.* $L_i = \{\mathbf{Q}_{i1}, \ldots, \mathbf{Q}_{ih_i}\}$, $1 \leq i \leq k$. *Then the product orthogonal classes* $K_i \otimes L_i = \{\mathbf{P}_{ij} \otimes \mathbf{Q}_{il} \,:\, 1 \leq j \leq g_i, 1 \leq l \leq h_i\}$ *are also mutually independent for all* $1 \leq i \leq k$.

Proof. $K_i \otimes L_i$ are clearly orthogonal classed. Independence follows easily from $\mathrm{tr}\,(\mathbf{A} \otimes \mathbf{B}) = \mathrm{tr}\,(\mathbf{A})\,\mathrm{tr}\,(\mathbf{B})$. □

This construction is a generalization to the non-commutative case of the well-known *Mac Neish's theorem* for transversal designs (see for example [13, Theorem I.7.7], and also [26] for the applications e.g. to orthogonal Latin Squares).

Let $\{\mathbf{P}_1, \ldots, \mathbf{P}_g\}$ and $\{\mathbf{Q}_1, \ldots, \mathbf{Q}_h\}$ be two independent orthogonal classes. Let $I \subseteq \{1, \ldots, g\}$ and $J \subseteq \{1, \ldots, h\}$ be any two subsets of the respective index sets. Then it is immediately clear that the projections $\mathbf{P} = \sum_{i \in I} \mathbf{P}_i$ and $\mathbf{Q} = \sum_{j \in J} \mathbf{Q}_j$ are also independent. Note, however, that this is not generally true for independence w.r.t. $\mathbf{D} \neq \frac{1}{b}\mathbf{I}$. By summing projections within orthogonal classes, we can easily construct new resolvable quantum designs with independent orthogonal classes out of known ones. But there are other applications, that involve classical designs. Commutative, resolvable quantum designs with mutually independent orthogonal classes are associated to resolvable incidence structures, in such a way that for any two blocks B and C from distinct parallel classes, we have $|B \cap C| = \frac{1}{g}|B||C|$. The special case of regular designs corresponds to classical affine 1-designs.

Proposition 2.21. *Let* $\mathbf{D}$ *be a regular, resolvable quantum design with* k *mutually independent orthogonal classes* $\{\mathbf{P}_{i1}, \ldots, \mathbf{P}_{ig}\}$*,* $1 \leq i \leq k$*. Let* $\mathbf{D}'$ *be a classical design (an incidence structure) with* g *points (w.l.o.g.* $\{1, \ldots, g\}$*) and* s *parallel classes of blocks, that is associated with a commutative (and hence resolvable) quantum design with mutually independent orthogonal classes.*

We can now define ks *mutually independent orthogonal classes by associating to every block* B *in* $\mathbf{D}'$*, the projections* $\mathbf{P}_B^i = \sum_{j \in B} \mathbf{P}_{ij}$*,* $1 \leq i \leq k$*.*

Proof. The $\mathbf{P}_B^i$ associated to the blocks of a parallel class in $\mathbf{D}'$ form, for all $1 \leq i \leq k$, one orthogonal class each. By the above remark, independence holds for any $\mathbf{P}_B^i$ and $\mathbf{P}_C^j$ with $1 \leq i \neq j \leq k$ and for any two blocks B and C, i.e. for arbitrary sums from two distinct orthogonal classes of $\mathbf{D}$. Let B and C be blocks from two distinct parallel classes. Since $\operatorname{tr}(\mathbf{P}_B^i \mathbf{P}_C^i) = r|B \cap C| = \frac{r}{g}|B||C| = \frac{1}{rg} \operatorname{tr}(\mathbf{P}_B^i) \operatorname{tr}(\mathbf{P}_C^i)$, follows, that for a fixed i, $1 \leq i \leq k$ the s orthogonal classes are mutually independent too. $\square$

We will be using the Propositions 2.20 and 2.21 in Chapter 3.

The sub-division into orthogonal classes remains unchanged for the coherently dual design. However, except for $k = 2$, the coherently dual design no longer has complete orthogonal classes. If the quantum design has mutually independent orthogonal classes (in particular, when it is an affine design), then this property does not hold in general for the coherently dual design. However, if we embed the coherently dual design in a $b(k-1)^2 = b^\perp(k-1)$-dimensional space, then this property holds again, and according to the following lemma the orthogonal classes can even be completed.

Lemma 2.22. *By adjoining additional projection matrices, every quantum designs with mutually independent (but not complete) orthogonal classes can be extended to such a design with complete orthogonal classes - in other words, the quantum design can be resolved.*

Proof. Fix an i for $1 \leq i \leq k$, and let $\{\mathbf{P}_{i1}, \ldots, \mathbf{P}_{ig_i}\}$ be the i-th orthogonal class. Suppose $\sum_{r=1}^{g_i} \mathbf{P}_{ir} = \mathbf{I}$ does not hold yet. The the i-th orthogonal class can be completed with $\mathbf{Q}_i = \mathbf{I} - \sum_{r=1}^{g_i} \mathbf{P}_{ir}$, and - as can easily be seen - $\mathbf{Q}_i$ is mutually independent from all other groups. All other orthogonal classes can be extended similarly. $\square$

The following proposition is a possible generalization of the well-known construction of *projective planes* out of *affine planes* (see [66]).

Lemma 2.23. *Suppose there exists an affine quantum design* $\mathbf{D}$ *with* k *orthogonal classes of order* g*, and let* $s \in \mathbb{N}$*, with* $s\lambda = t \in \mathbb{N}$*.*

Let $\mathbf{I}_m$ *be the* $m \times m$ *identity matrices. For* $1 \leq j \leq k$*, we define the* $k \times k$ *projection matrices* $\mathbf{Q}_j = \operatorname{diag}(\delta_{1j}, \ldots, \delta_{kj})$*, where* δ_{ij} *is the Kronecker symbol; furthermore, if* $\mathbf{P}_i$ *is in the* j*-th orthogonal class, then set* $\mathbf{P}_i' = (\mathbf{P}_i \otimes \mathbf{I}_s) \oplus (\mathbf{Q}_j \otimes \mathbf{I}_t)$*.*

The projection matrices $\mathbf{P}_i'$ form a degree 1 quantum design $\mathbf{D}'$ with the parameters $v' = v$, $b' = bs + kt$ and $\lambda' = t$. $\mathbf{D}'$ is regular if and only if $\mathbf{D}$ is, with $r' = rs + t$, and is coherent if and only if $\mathbf{D}$ is and $k = g$ holds.

Let $\mathbf{D}''$ be the design after extension by the projection $\mathbf{0}_{bs} \oplus \mathbf{I}_{kt}$. $\mathbf{D}''$ also has degree 1, with $v'' = v + 1$, $b'' = bs + kt$ and $\lambda'' = t$. $\mathbf{D}''$ is regular if and only if $\mathbf{D}$ is, and $k = 1 + \frac{1}{\lambda}$ holds; it is coherent if and only if $\mathbf{D}$ is, and $k = g + 1$ holds.

Proof. The proof follows immediately by applying the identities $\operatorname{tr}(\mathbf{A} \oplus \mathbf{B}) = \operatorname{tr}(\mathbf{A}) + \operatorname{tr}(\mathbf{B})$ and $\operatorname{tr}(\mathbf{A} \otimes \mathbf{B}) = \operatorname{tr}(\mathbf{A}) \operatorname{tr}(\mathbf{B})$. □

2.4 Degree 1 Quantum Designs

The following results are mainly generalizations of results about classical designs, systems of equiangular lines and isoclinic subspaces; we will apply the methods of Sections 2.1 and 2.2.

Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a quantum design with $\Lambda = \{\lambda_k : 1 \le k \le s\}$. We will say that $\mathbf{D}$ is *regularly schematic* if the number $n_j(\lambda_k)$ of distinct i, $1 \le i \le v$ with $\operatorname{tr}(\mathbf{P}_i\mathbf{P}_j) = \lambda_k$ is independent of j (i.e. $n_j(\lambda_k) = n_k$). See [46] for the special case of this definition for spherical designs.

Lemma 2.24. *Let $\mathbf{D}$ be a degree s coherent quantum design that is regularly schematic. Then either $k = 1$, the design has degree 1 and $\lambda = 0$, or the design must also be regular, with $r = \frac{1}{k-1}\sum_{k=1}^{m} n_k\lambda_k$.*

Proof. If we multiply the equation $\mathbf{P}_1 + \cdots + \mathbf{P}_v = k\mathbf{I}$ by a fixed $\mathbf{P}_j$, $1 \le j \le v$, and then apply the trace function, we get

$$\sum_{k=1}^{s} n_k\lambda_k = \operatorname{tr}(\mathbf{P}_j)(k-1) \qquad \text{for all } 1 \le j \le v.$$

Either $k = 1$, and thus the left-hand side is 0, or we can divide by $(k-1)$. □

The special case $k = 1$ and $\lambda = 0$ corresponds to having mutually orthogonal projections (resp. sub-spaces), and is trivial.

Proposition 2.25. *Every degree 1 quantum design with $\lambda \neq 0$ is regular. Its parameters satisfy:*

$$vr = bk, \tag{2.15a}$$
$$r(k-1) = \lambda(v-1). \tag{2.15b}$$

Proof. A degree 1 quantum design is clearly regularly schematic, with $n_1 = v - 1$, so the second equation follows from Lemma 2.24. We already proved the first equation in the first section (Equation (1.6b)). □

This means that coherent quantum designs (with $\lambda \neq 0$) can only have 3 independent parameters. Furthermore, we see that we must have $\lambda \in \mathbb{Q}$. These are exactly the same equations that apply to BIBD's (which correspond to the commutative case via the dual association of Theorem 1.10). However, in that case the parameters can only take values in the natural numbers; here, $k, \lambda \in \mathbb{Q}$ is also permissible. The equation (2.15b) follows also from the following theorem.

Theorem 2.26 (Special Bound)**.** *If $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ is a degree 1 quantum design, then the following holds:*

$$\lambda \ge \frac{1}{v(v-1)}\left(\frac{1}{b}\left(\sum_{i=1}^{v} r_i\right)^2 - vr\right).$$

In particular, for regular quantum designs we have:

$$\lambda \geq \frac{r(vr - b)}{b(v-1)}. \tag{2.16}$$

D *is coherent if and only if equality holds in each of the equations above.*

Proof. Using theorem 2.5 with $t = 1$ and $\mathbf{K}_1(X) = \frac{r}{b}\mathbf{I}$ for the (complex) Grassmannians of trace r, we get

$$vr + v(v-1)\lambda = \sum_{i=1}^{v}\sum_{j=1}^{v} \operatorname{tr}(\mathbf{P}_i\mathbf{P}_j) \geq \frac{1}{b}\left(\sum_{i=1}^{v} r_i\right)^2,$$

where equality holds exactly in the case of coherence. □

In the case that $\lambda < \frac{r^2}{b}$, the inequality (2.16) is equivalent to

$$v \leq \frac{b(r-\lambda)}{r^2 - b\lambda}. \tag{2.17}$$

In real vector spaces, this "'special bound"' agrees with the bound in [55, Theorem 3.6] for $r = 1$. In [53, Theorem 3.6] it was derived for arbitrary r in the special case of equi-isoclinic subspaces. With the same restriction, the bound was proven for complex vector spaces in [40].

A regular and coherent quantum design is called *complete* if $k = v$. By equation (1.6b), we then also have $r = b$, i.e. $\mathbf{P}_i = \mathbf{I}$ for all $1 \leq i \leq v$. Otherwise ($r < b$, $k < v$), the design is said to be *incomplete*.

Proposition 2.27. *Let* **D** *be a degree* 1 *quantum design with parameters* λ *and* $\operatorname{tr}(\mathbf{P}_i) = r_i$, $1 \leq i \leq v$. *Then*

$$0 \leq \lambda \leq r_i \leq b \qquad \textit{for all } 1 \leq i \leq v.$$

If $r_i = \lambda$ *for some* $1 \leq i \leq v$, *then* **D** *is reducible, and decomposes into a complete quantum design and a quantum design with* $\lambda = 0$.

Proof. The matrices $\mathbf{P}_i\mathbf{P}_j\mathbf{P}_i$ and $\mathbf{P}_i(\mathbf{I} - \mathbf{P}_j)\mathbf{P}_i = \mathbf{P}_i - \mathbf{P}_i\mathbf{P}_j\mathbf{P}_i$ are positive semi-definite for all $1 \leq i, j \leq v$. This implies that $0 \leq \operatorname{tr}(\mathbf{P}_i\mathbf{P}_j) = \operatorname{tr}(\mathbf{P}_i\mathbf{P}_j\mathbf{P}_i) \leq \operatorname{tr}(\mathbf{P}_i)$.

Equality holds for a given $1 \leq i \leq v$ in the second inequality if and only if $\mathbf{P}_i = \mathbf{P}_i\mathbf{P}_j\mathbf{P}_i$ for all $1 \leq j \leq v$. Thus, all $\mathbf{P}_j$ project onto the subspace $\mathbf{T}$ of V that $\mathbf{P}_i$ projects onto, and so the design is complete over $\mathbf{T}$.

If we restrict to the orthogonal complement of $\mathbf{T}$, then $\mathbf{P}_i$ vanishes, and it is easy to see that all other projection must be orthogonal. □

Complete designs and designs with $\lambda = 0$ are trivial and not very interesting, so we let $\lambda < r_i$ for all $1 \leq i \leq v$ in what follows below (the equations (2.15) imply that for regular and coherent quantum designs, this is simply equivalent to the fact that the quantum designs are incomplete).

Theorem 2.28 (Absolute Bound)**.** *Let* $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ *be a quantum design of degree* 1*, that is non-trivial, i.e. with* $\mathrm{tr}(\mathbf{P}_i) = r_i > \lambda$ *for all* $1 \leq i \leq v$*. Then the* v *projection matrices* $\mathbf{P}_i$*,* $1 \leq i \leq v$ *are linearly independent, and the Generalized Fisher Inequality holds:*

$$
\begin{aligned}
&v \leq b^2 && \text{for complex quantum designs,}\\
&v \leq \binom{b+1}{2} && \text{for real quantum designs,}\\
&v \leq b && \text{for commutative quantum designs.}
\end{aligned}
$$

Proof. The entries of the *Gram Matrix* $\mathbf{G}$, which is defined as the inner product of the v projection matrices, are given by:

$$
(\mathbf{G})_{ij} = \mathrm{tr}\left(\mathbf{P}_i \mathbf{P}_j\right) = \begin{cases} \lambda & \text{for all } 1 \leq i \neq j \leq v, \\ r_i & \text{for all } 1 \leq i = j \leq v. \end{cases}
$$

Hence, this matrix can be written in the form $\mathbf{G} = \mathbf{N} + \lambda \mathbf{J}$, where $\mathbf{N} = \mathrm{diag}(n_1, \ldots, n_v)$, $n_i = r_i - \lambda > 0$ for all $1 \leq i \leq v$, and $\mathbf{J}$ is the $v \times v$ matrix consisting entirely of ones. Since it is the sum of the positive-definite matrix $\mathbf{N}$ and the positive-semidefinite matrix $\lambda\mathbf{J}$, $\mathbf{G}$ is itself positive-definite. This implies that $\mathrm{Det}(\mathbf{G}) \neq 0$, and so $\mathbf{G}$ is non-singular and the v projection matrices are linearly independent. The three inequalities follow. □

Those quantum designs for which the corresponding inequality in Theorem 2.28 is actually an equality are called *maximal*.

In the real case, the inequality restricted to $r = 1$ can already be found in [55] and [52]. In [53], the inequality was derived for the special case of equi-isoclinic subspaces with arbitrary r. The complex version can be found in [40]. In the commutative case, the inequality $v \leq b$ is known in classical design theory as *Fisher's Inequality* (see for example [13, Theorem II.2.6]).

For regular quantum designs, the absolute bounds are also consequences of Theorem 2.2, $v \leq \dim(\mathrm{Hom}(X, 1)) = \dim(X)$, where X is the vector space of the complex, resp. real, resp. diagonal matrices with trace r. However, for non-regular designs it is only possible to deduce $v \leq \dim(\mathrm{Pol}(X, 1)) = \dim(\mathrm{Hom}(X, 1)) + 1$ from Theorem 2.2, since in this case the constant polynomial $f(\mathbf{P}) \equiv c$ does not lie in $\mathrm{Hom}(X, 1)$.

Using Q-polynomiality, it is possible to show that for real and complex designs with $r = 1$, $\mathbf{D}$ is a tight 2-design if and only if the absolute bound for degree 1 is achieved (see [29, Theorem 16.1.3]). For non-regular quantum designs, one can at best expect (tight) 2-coherence, but not (1-)coherence as well, since then we would have $v \geq \dim(\mathrm{Pol}(X,1)) = \dim(X)+1$. It is not known whether such structures exist. For regular quantum designs the same relation as for $r=1$ also hold for arbitrary r.

Theorem 2.29. *Let* $\mathbf{D}$ *be a regular and complex, resp. real, resp. diagonal quantum design with degree* $=1$ *and* $r > \lambda$*. Then* $\mathbf{D}$ *is maximal if and only if it is a (tight) quantum* 2*-design w.r.t.* $U(b)$*, resp.* $O(b)$*, resp.* $S(b)$*.*

Proof. (i) We will first show that all maximal and regular $\mathbf{D}$ are coherent.

By Theorem 2.28, the complex, resp. real, resp. diagonal projection matrices of a maximal quantum design are linearly independent, and hence span the space of all complex, resp. real, resp. diagonal matrices. In all three cases it is thus possible to obtain the identity matrix as a linear combination of these projection matrices, i.e. there exist complex numbers $c_i, 1 \leq i \leq v$ such that

$$\sum_{i=1}^{v} c_i \mathbf{P}_i = \mathbf{I}.$$

Multiplying by $\mathbf{P}_j, 1 \leq j \leq v$ and applying the trace, we obtain v equations in the unknowns c_i. These, together with the $v \times v$ matrix $\mathbf{J}$, the vector $\mathbf{j}$, whose entries also all consist of ones, and the vector $\mathbf{c} = (c_1, \ldots, c_v)$, are equivalent to the matrix equation

$$((r-\lambda)\mathbf{I} + \lambda \mathbf{J})\,\mathbf{c} = r\mathbf{j}.$$

As the sum of a positive-definite matrix with a positive semi-definite matrix, the matrix $(r-\lambda)\mathbf{I}+\lambda\mathbf{J}$ is itself positive-definite, and hence non-singular. Therefore, this matrix equation has a unique solution, given by

$$c_i \equiv c = \frac{r}{r+\lambda(v-1)} \qquad \text{for all } 1 \leq i \leq v.$$

This implies coherence with $k = 1/c$.

(ii) The coherence of $\mathbf{D}$, together with Theorem 2.26, implies that $\lambda = \frac{r(vr-b)}{b(v-1)}$ and

$$\frac{1}{v^2}\sum_{i=1}^{v}\sum_{j=1}^{v} (\mathrm{tr}\,(\mathbf{P}_i\mathbf{P}_j))^2 = \frac{1}{v}(r^2 + (v-1)\lambda^2) = \frac{r^2(b^2+vr^2-2rb)}{b^2(v-1)}.$$

If we substitute the values of $\mathrm{tr}\,(\mathbf{K}_2(X))^2$ from the equations (2.6) into the inequality (2.4), then we obtain the three inequalities of Theorem 2.28. According to Theorem 2.5, the respective 2-coherence w.r.t. the appropriate G-space groups follows exactly when equality holds. $\square$

The special case of this theorem for commutative quantum designs corresponds to *Ryser's Theorems* for classical symmetric incidence structures (see for example [13, Theorem II.3.2 and II.3.5]).

Up to this point, all results have been generalizations of results on classical designs (in particular BIBD's), systems of equiangular lines, and equi-isoclinic subspaces. What now follows is a result that appears to be new even in the case $r = 1$.

Theorem 2.30 (Coherently Dual Absolute Bound). *Let* **D** *be a regular, coherent, degree* 1 *quantum design with* $v > 1 + b/r$ *(i.e.* $k \neq 1$ *and different from a solution to example* 2.14*). Then the following relation holds for complex quantum designs:*

$$v \geq \frac{b}{r} + \frac{1 + \sqrt{4br + 1}}{2r^2}. \tag{2.18}$$

For real quantum designs we have instead:

$$v \geq \frac{b}{r} + \frac{2 - r + \sqrt{r^2 + 4r(2b - 1) + 4}}{2r^2}. \tag{2.19}$$

Proof. From $k > 1 + r/b$ we get $r < b(k - 1)$, and therefore $r^{\perp} < b^{\perp}$ holds for the parameters of the coherently dual quantum design $\mathbf{D}^{\perp}$. Together with equations (2.15) this implies $k^{\perp} < v^{\perp}$ and $r^{\perp} > \lambda^{\perp}$, hence $\mathbf{D}^{\perp}$ satisfies the preconditions of Theorem 2.28.

The inequality $v^{\perp} \leq \left(b^{\perp}\right)^2$ holds for complex quantum designs. This means $v \leq b^2 \left(k - 1\right)^2$, and using the identity $b(k - 1) = vr - b$ we get $v \leq (vr - b)^2$. Solving for v, and taking into account that $v \geq 1 + b/r$, we obtain the inequality (2.18).

If **D** is real, then we can choose $\mathbf{D}^{\perp}$ to be real as well. In this case we have $v^{\perp} \leq b^{\perp}(b^{\perp} + 1)/2$, i.e. $2v \leq b^2 \left(k - 1\right)^2 + b \left(k - 1\right)$. This, together with the identity $b(k - 1) = vr - b$ implies $2v \leq (vr - b)^2 + (vr - b)$. Solving for v, and taking into account that $v \geq 1 + b/r$, we obtain the inequality (2.19). □

For example, let $v = 5$, $b = 3$, $r = 1$ and hence $k = \frac{5}{3}$ and $\lambda = \frac{1}{6}$. These parameters satisfy the inequality $v \geq 1 + b/r$ given in Proposition 2.12, but not the inequality (2.18). Therefore, no solution exists.

In [24, Example 5.7] it was erroneously claimed that also for the parameters $b = 4$, $v = 6$, and $\lambda = \frac{1}{9}$, the special bound (2.17) becomes actually an equality, and therefore the design shall be coherent. However, although there does indeed exist a degree 1 quantum design with such parameters (see [55]), it does not exactly satisfy the special bound, and is therefore not coherent. For that to be the case, it should have had the parameter $\lambda = \frac{1}{10}$. Such a solution cannot exist though, because it would contradict equation (2.18).

2.5 Automorphism Groups

Definition 2.31. An *automorphism* of the quantum design $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ is an equivalence mapping of $\mathbf{D}$ into itself. It is described by a couple $(\mathbf{U}, \pi)$ consisting of a matrix $\mathbf{U} \in U(b)$ and a permutation π of $\{1, \ldots, v\}$, such that the following holds:

$$\mathbf{P}_i = \mathbf{U}\mathbf{P}_{\pi(i)}\mathbf{U}^{-1} \qquad \text{for all } 1 \leq i \leq v.$$

Let $G \subseteq U(b)$. The set of all automorphisms $(\mathbf{U}, \pi)$ with $\mathbf{U} \in G$ of a quantum design $\mathbf{D}$ is a group, with composition as the group operation. This group is called the *full automorphism group w.r.t.* G of $\mathbf{D}$, and is denoted $\mathrm{Aut}_G(\mathbf{D})$.

We will now disregard permutations, and consider only the unitary matrices. The map

$$\varphi : (\mathbf{U}, \pi) \mapsto \mathbf{U}$$

defines a homomorphism from $\mathrm{Aut}_G(\mathbf{D})$ into the group of all unitary $b \times b$ matrices, i.e. it is a *(unitary) linear representation* of $\mathrm{Aut}_G(\mathbf{D})$. It is quite clear that the homomorphism φ is injective if and only if all the projections $\mathbf{P}_i \in \mathbf{D}$ are distinct from each other. We will assume this in what follows. In that case, φ has a unique inverse, and we say that $\mathbf{U}$ *generates* the automorphism $(\mathbf{U}, \pi)$.

Proposition 2.32. *Let* $\mathrm{Aut}_G(\mathbf{D})$ *be the automorphism group of the quantum design* $\mathbf{D}$ *w.r.t.* G*, where* G *is any group, and* H *the image of* φ*. Then* $\mathbf{D}$ *is quantum* t*-design w.r.t.* H *for all* $t \in \mathbb{N}$*. In particular, if* H *is irreducible, then* $\mathbf{D}$ *is coherent.*

Proof. The t-coherence is immediate if, for arbitrary $(\mathbf{U}, \pi) \in \mathrm{Aut}(\mathbf{D})$, we perform a similarity transformation on the equation $\sum_{i=1}^{v} \otimes^t \mathbf{P}_i = \sum_{i=1}^{v} \otimes^t \mathbf{P}_{\pi(i)}$ using $\mathbf{U}$. For irreducible G, coherence follows from Schur's Lemma. □

Naturally, we are generally more interested in larger groups when investigating t-coherence. However, the irreducibility of H gives us a nice criterion for coherence.

The map

$$\psi : (\mathbf{U}, \pi) \mapsto \pi$$

induces a homomorphism from $\mathrm{Aut}_G(\mathbf{D})$ into the *symmetric group* S_v (of all permutations on a set of v elements), that is, we get a *representation as permutation group*. The image of $\mathrm{Aut}_G(\mathbf{D})$ under the map $\psi : (\mathbf{U}, \pi) \mapsto \pi$ will be denoted $\mathrm{Aut}^*_G(\mathbf{D}) \subseteq S_v$.

In general, the homomorphism ψ is not injective. The kernel of ψ (with id denoting the identity permutation) is given by $\mathrm{Ker}(\psi) = \{(\mathbf{U}, \mathrm{id}) \in \mathrm{Aut}_G(\mathbf{D})\}$ and always contains the subgroups $G \cap N$, where

$$N = \{(\alpha\mathbf{I}, \mathrm{id}) : \ \alpha \in \mathbb{C}, |\alpha| = 1\}.$$

The kernel of ψ is always a *normal subgroup*, and the following relation holds:

$$\mathrm{Aut}^*_G(\mathbf{D}) \cong \frac{\mathrm{Aut}_G(\mathbf{D})}{\mathrm{Ker}(\psi)}.$$

We can now invert ψ, and associate to every permutation $\pi \in \mathrm{Aut}^*_G(\mathbf{D})$ a unique coset of $\mathrm{Ker}(\psi)$ in $\mathrm{Aut}_G(\mathbf{D})$, and in particular we can choose a coset representative $(\mathbf{U}(\pi), \pi) \in \mathrm{Aut}_G(\mathbf{D})$. Without loss of generality, we can set $\mathbf{U}(\mathrm{id}) = \mathbf{I}$. If we then apply φ, we obtain a map $\pi \mapsto \mathbf{U}(\pi)$ from $\mathrm{Aut}^*_G(\mathbf{D})$ into the set of unitary $b \times b$ matrices. This map is especially of interest when $\mathrm{Ker}(\psi) = G \cap N$, and there is a simple criterion for checking this.

Lemma 2.33. *Let* $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ *be a quantum design, and* ψ *the homomorphism from* $\mathrm{Aut}(\mathbf{D})$ *into the symmetric group. If* $\mathbf{D}$ *is irreducible, then* $\mathrm{Ker}(\psi) = G \cap N$.

Proof. Suppose the quantum design $\mathbf{D}$ is irreducible, and let $(\mathbf{U}, \mathrm{id}) \in \mathrm{Ker}(\psi)$, i.e.

$$\mathbf{P}_i = \mathbf{U}\mathbf{P}_i\mathbf{U}^{-1} \qquad \text{for all } 1 \leq i \leq v.$$

Let A be the algebra of complex $b \times b$ matrices generated by the projections $\mathbf{P}_i$, $1 \leq i \leq v$ (finite products and linear combinations). Then A is also irreducible, and the matrix $\mathbf{U}$ commutes with all matrices in A. Thus, we can apply Schur's Lemma and obtain $\mathbf{U} = \alpha\mathbf{I}$, where $\alpha \in \mathbb{C}$ and $|\alpha| = 1$, because $\mathbf{U}$ is unitary. □

If G is sufficiently large (for example $G = U(b)$ or $O(b)$), then even the converse of Lemma 2.33 holds. Suppose the quantum design $\mathbf{D}$ is reducible; in an appropriate basis of $\mathbb{C}^b$, set $\mathbf{P}_i = \mathbf{P}_{1i} \oplus \mathbf{P}_{2i}$ for all $1 \leq i \leq v$, with $c \times c$ projection matrices $\mathbf{P}_{1i}$ and $d \times d$ projection matrices $\mathbf{P}_{2i}$, and $c, d \neq 0$. Let $\mathbf{U}_\epsilon = \mathbf{I}_c \oplus \epsilon\mathbf{I}_d$, where $\epsilon \in \mathbb{C}, |\epsilon| = 1$. Then it immediately follows that $(\mathbf{U}, \mathrm{id}) \in \mathrm{Ker}(\psi)$, and if $\mathbf{U}_\epsilon \in G$ for some $\epsilon \neq 1$, then we have $\mathrm{Ker}(\psi) \neq N \cap G$.

In what follows, let $\mathrm{Ker}(\psi) = N \cap G$. The group $N \cap G$ lies in the *center* of $\mathrm{Aut}_G(\mathbf{D})$, and therefore $\mathrm{Aut}_G(\mathbf{D})$ is a so-called *central extension* of $\mathrm{Aut}^*_G(\mathbf{D})$ by $N \cap G$. We then have

$$(\mathbf{U}(\pi), \pi) \circ (\mathbf{U}(\sigma), \sigma) = (\alpha(\pi, \sigma)\mathbf{I}, \mathrm{id}) \circ (\mathbf{U}(\pi \circ \sigma), \pi \circ \sigma),$$

where $\alpha(\pi, \sigma) \in \mathbb{C}$, $|\alpha(\pi, \sigma)| = 1$. If we apply φ to this, we get

$$\mathbf{U}(\pi)\mathbf{U}(\sigma) = \alpha(\pi, \sigma)\mathbf{U}(\pi \circ \sigma).$$

This means that the map

$$\mathbf{U}: \ \pi \mapsto \mathbf{U}(\pi)$$

induces a so-called *projective representation (or Strahldarstellung)* (see [21, Chapter 51-53], as well as [48] for a more in-depth exposition) of $\mathrm{Aut}^*_G(\mathbf{D})$ in the space of unitary $b \times b$ matrices, with *factor set* $\{\alpha(\pi,\sigma): \ \pi,\sigma \in \mathrm{Aut}^*_G(\mathbf{D})\}$. In particular, if $G \subseteq O(b)$, then we obtain a projective representation over $\mathbb{R}$ (with factor set $\{\pm 1\}$).

This projective representation is unitary; it is irreducible if and only if the ordinary representation φ is irreducible, and is injective if and only if φ is - i.e. if and only if all projections $\mathbf{P}_i \in \mathbf{D}$ are distinct. Another projective representation $\mathbf{U}'$ is associated to the same quantum design $\mathbf{D}$ if and only if $\mathbf{U}$ and $\mathbf{U}'$ are projectively equivalent, i.e. $\mathbf{U}'(\pi) = \rho(\pi)\mathbf{U}(\pi)$, where $\rho(\pi) \in \mathbb{C}$, $|\rho(\pi)| = 1$ for all $\pi \in \mathrm{Aut}^*_G(\mathbf{D})$.

For irreducible quantum designs $\mathbf{D}$, the study of the automorphism group $\mathrm{Aut}_G(\mathbf{D})$ can thus be restricted to the investigation of the finite group $\mathrm{Aut}^*_G(\mathbf{D})$ and its associated projective representations $\mathbf{U}(\pi)$. For example, if $G = U(b)$, $\mathrm{Aut}_G(\mathbf{D})$ consists of all $(\alpha\mathbf{U}(\pi),\pi)$ with $\pi \in \mathrm{Aut}^*_G(\mathbf{D})$, $\alpha \in \mathbb{C}$, $|\alpha| = 1$.

In the case of reducible quantum designs, a little more group theory comes into play. In general, the automorphism group can no longer be uniquely reconstructed from the matrices $\mathbf{U}(\pi)$.

A permutation group G over a set with v elements $\{1,\ldots,v\}$ is called *transitive* if, for all $1 \le i \ne j \le v$, there exists a $\pi \in G$ such that $\pi(i) = j$.

Suppose the subgroup $G \subseteq \mathrm{Aut}^*_G(\mathbf{D})$ is transitive, and to every $\pi \in G$ we can associate a $(\mathbf{U}(\pi),\pi) \in \mathrm{Aut}_G(\mathbf{D})$ (i.e. in the case of irreducible quantum designs $\mathbf{D}$, the induced projective representation). Then in order to completely describe the quantum design $\mathbf{D}$, it suffices to know one of its projection matrices, i.e. it suffices to know $\mathbf{P}_1$. All other projection matrices then follow easily, using the relations

$$\mathbf{P}_{\pi(1)} = \mathbf{U}(\pi)^{-1}\mathbf{P}_1\mathbf{U}(\pi) \qquad \text{for all } \pi \in G.$$

In other words, the projective representation of G plus an *initial projection* $\mathbf{P}_1$ generates the whole design.

In particular, a so-called *regular* subgroup G suffices. (A permutation group is said to be *regular* if it is transitive, and all $\pi \in G$, $\pi \ne \mathrm{id}$, are *fixed-point free*). Regular permutation groups must be of order v (see [13, Chapter III.3]).

Following the terminology of classical design theory, we will call a regular subgroup G of $\mathrm{Aut}^*_G(\mathbf{D})$ a *generalized Singer group* of the quantum design $\mathbf{D}$ (see [13, Chapter VI] resp. [47, Section 2.4]).

Automorphism groups over polynomial spaces (i.e. over G-spaces using our terminology) were investigated in [29]. Via the appropriate correspondences, the results can be carried over to quantum designs using the equations (1.21).

There are also similar studies for spherical designs (see [30], [31], [8] and [9]), where for certain given groups, there are also investigations of designs generated from an initial vector. In these cases usually only ordinary representations are used.

For non-singular classical, quadratic incidence structures, it is known that under every automorphism, the number of fixed points is equal to the number of fixed blocks (see [13, I. Prop. 4.8 and II. Cor. 2.4], resp. [47, Lemma 1.43 and Cor. 1.44]). For diagonal quantum designs, this means that for all $(\mathbf{S}, \pi) \in \mathrm{Aut}_G(\mathbf{D})$, the number of fixed points of π satisfies the following equation: $f(\pi) = \mathrm{tr}(\mathbf{S})$. An analogous relation can be extended to complex quantum designs.

Theorem 2.34. *Let $\mathbf{D} = \{\mathbf{P}_1, \ldots, \mathbf{P}_v\}$ be a quantum design with $v = b^2$ linearly independent orthogonal $b \times b$ projection matrices. Let $(\mathbf{U}, \pi) \in \mathrm{Aut}_G(\mathbf{D})$ and let $f(\pi)$ be the number of fixed points of the permutation π. Then*

$$f(\pi) = |\mathrm{tr}\,(\mathbf{U})|^2 .$$

Proof. Let $(\mathbf{U}, \pi) \in \mathrm{Aut}_G(\mathbf{D})$. Then $\mathbf{P}_l = \mathbf{U}\mathbf{P}_{\pi(l)}\mathbf{U}^{-1}$, and so $\mathbf{P}_{\pi(l)} = \mathbf{U}^*\mathbf{P}_l\mathbf{U}$ for all $1 \leq l \leq v$. This means that together with $\mathbf{P}_l = (p_{ij}^{(l)})$ and $\mathbf{U} = (u_{ij})$, for all $1 \leq i, j \leq b$ and $1 \leq l \leq v$ we have

$$p_{ij}^{(\pi(l))} = \sum_{m=1}^{b}\sum_{n=1}^{b} \bar{u}_{mi} p_{mn}^{(l)} u_{nj}.$$

Let $\mathbf{A} = (a_{l,(ij)}) = (p_{ij}^{(l)})$ for $1 \leq i, j \leq b$ and $1 \leq l \leq v$ be the matrix consisting of the projections as rows - we assume that the indices (ij) run through the b^2 pairs of numbers $1 \leq i, j \leq b$ in lexicographic order $(11, 12, \ldots, 1b, 21, \ldots)$. Via left-multiplication by the $v \times v$ permutation matrix $\mathbf{Q}_\pi$, which permutes the row vectors of $\mathbf{A}$ according to π, we obtain

$$\mathbf{Q}_\pi \mathbf{A} = \mathbf{A}(\overline{\mathbf{U}} \otimes \mathbf{U}).$$

By assumption, $\mathbf{A}$ has v linearly independent rows and is thus invertible. Therefore we get

$$\mathbf{Q}_\pi = \mathbf{A}(\overline{\mathbf{U}} \otimes \mathbf{U})\mathbf{A}^{-1}$$

and together with $f(\pi) = \mathrm{tr}(\mathbf{Q}_\pi)$ this implies

$$f(\pi) = \mathrm{tr}(\mathbf{A}(\overline{\mathbf{U}} \otimes \mathbf{U})\mathbf{A}^{-1}) = \mathrm{tr}(\overline{\mathbf{U}} \otimes \mathbf{U}) = \mathrm{tr}(\overline{\mathbf{U}})\,\mathrm{tr}(\mathbf{U}) = |\mathrm{tr}(\mathbf{U})|^2 .$$

□

We also observe that every quantum design that satisfies the preconditions of Theorem 2.34 is irreducible. (Suppose that $\mathbf{D}$ is unitarily equivalent to the sum of two quantum designs with matrices of size $b_1 \neq 0$, $b_2 \neq 0$ and $b_1 + b_2 = b$. Then the linearly independent projection matrices could span a subspace of dimension at most $(b_1^2 + b_2^2)$). Thus, the projective representation $\mathbf{U}(\pi)$ of $\mathrm{Aut}_G^*(\mathbf{D})$ is defined. Theorem 2.34 implies $f(\pi) = |\mathrm{tr}\,(\mathbf{U}(\pi))|^2$ for all $\pi \in \mathrm{Aut}_G^*(\mathbf{D})$.

In particular, Theorem 2.34 holds for maximal, degree 1 complex quantum designs (see Theorem 2.28). If we want to construct such quantum designs using a regular subgroup G, then the group must have order b^2, and must also have a projective representation in $\mathbb{C}^b$ for which the following holds:

$$|\mathrm{tr}\,(\mathbf{U}(\pi))|^2 = 0 \qquad \text{for all } \pi \in G,\ \pi \neq \mathrm{id},$$

because all $\pi \in G$, $\pi \neq \mathrm{id}$, are fixed-point free. Therefore, the representation cannot be equivalent to an ordinary representation, because the character would not be orthogonal to the trivial character.

We will investigate special groups of this kind in the next section.

3 Constructions

3.1 Weyl Matrices and the Fourier Matrix

We now introduce several matrices and relations that we will be using repeatedly. Let two unitary $b \times b$ matrices be defined by

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & e^{2\pi i/b} & 0 & \dots & 0 \\ 0 & 0 & e^{4\pi i/b} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & e^{2(b-1)\pi i/b} \end{pmatrix}, \quad \mathbf{V} = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

The following relations hold:

$$\mathbf{U}^b = \mathbf{V}^b = \mathbf{I}, \tag{3.1a}$$

$$\mathbf{V}^c\mathbf{U}^d = e^{2\pi icd/b}\mathbf{U}^d\mathbf{V}^c \qquad \text{fr alle } c, d \in \mathbb{Z}. \tag{3.1b}$$

Let $\mathbb{Z}_b = \mathbb{Z}/b\mathbb{Z}$ be the additive (cyclic) residue group modulo b, and $(c, d) \in \mathbb{Z}_b^2$. The mapping $(c, d) \mapsto \mathbf{V}^c\mathbf{U}^d$ gives a unique, irreducible and faithful *projective representation* of the b^2-element, additive abelian group of the vector space $\mathbb{Z}_b^2$ by the so-called *Weyl matrices* $\mathbf{V}^c\mathbf{U}^d$ (see Weyl [77, Chapter 4] resp. [48, Theorem 7.1])). The b^3 matrices $e^{2\pi iq/b}\mathbf{V}^c\mathbf{U}^d$ with $q, c, d \in \mathbb{Z}_b$ form an ordinary, irreducible and faithful representation of the (non-abelian) *Heisenberg group* (see [5]).

Now let $\mathbf{c} = (c_1, \dots, c_m)$ and $\mathbf{d} = (d_1, \dots, d_m)$ be two m-tuples of elements $c_i, d_i \in \mathbb{Z}_b$, $1 \le i \le m$. Then the mapping

$$(\mathbf{c}, \mathbf{d}) \mapsto \mathbf{W}(\mathbf{c}, \mathbf{d}) = \mathbf{V}^{c_1}\mathbf{U}^{d_1} \otimes \dots \otimes \mathbf{V}^{c_m}\mathbf{U}^{d_m} \tag{3.2}$$

gives a projective representation of the n^{2m}-element, additive abelian group of the vector space $\mathbb{Z}_b^{2m}$. It then immediately follows that

$$\mathbf{W}(\mathbf{c}, \mathbf{d})\mathbf{W}(\mathbf{c}', \mathbf{d}') = e^{-2\pi i\left(c_1'd_1 + \dots + c_m'd_m\right)/b}\mathbf{W}(\mathbf{c} + \mathbf{c}', \mathbf{d} + \mathbf{d}'). \tag{3.3}$$

Since $\operatorname{tr}(\mathbf{W}(\mathbf{c}, \mathbf{d}))$ equals b for $\mathbf{c} = \mathbf{d} = (0, \dots, 0)$, but is otherwise equal to 0, we have

$$\operatorname{tr}(\mathbf{W}(\mathbf{c}, \mathbf{d})\mathbf{W}^*(\mathbf{c}', \mathbf{d}')) = \begin{cases} b & \text{if } \mathbf{c} = \mathbf{c}' \text{ and } \mathbf{d} = \mathbf{d}', \\ 0 & \text{else.} \end{cases} \tag{3.4}$$

These matrices are orthogonal, and form a basis for the b^{2m}-dimensional vector space of all complex $b^m \times b^m$ matrices (see [68] for the case $m = 1$).

The *Fourier matrix* (sometimes also called *discrete Fourier Transformation* or *Schur matrix*) is a $b \times b$ matrix $\mathbf{F} = (f_{rs})_{0 \le r,s \le b-1}$ with the entries $f_{rs} = \frac{1}{\sqrt{b}} e^{2\pi i rs/b}$, i.e.

$$\mathbf{F} = \frac{1}{\sqrt{b}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & e^{2\pi i/b} & e^{2\pi i 2/b} & \dots & e^{2\pi i(b-1)/b} \\ 1 & e^{2\pi i 2/b} & e^{2\pi i 4/b} & \dots & e^{2\pi i 2(b-1)/b} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{2\pi i(b-1)/b} & e^{2\pi i 2(b-1)/b} & \dots & e^{2\pi i(b-1)(b-1)/b} \end{pmatrix}. \tag{3.5}$$

$\mathbf{F}$ is unitary, and we have:

$$\mathbf{F}^2 = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \end{pmatrix}, \qquad \mathbf{F}^4 = \mathbf{I}, \tag{3.6}$$

$$\mathbf{F}^{-1}\mathbf{V}\mathbf{F} = \mathbf{U} \qquad \text{and} \qquad \mathbf{F}^{-1}\mathbf{U}\mathbf{F} = \mathbf{V}^{-1}. \tag{3.7}$$

This immediately implies

$$\otimes^m \mathbf{F}^{-1} \mathbf{W}(\mathbf{c}, \mathbf{d}) \otimes^m \mathbf{F} = e^{2\pi i(c_1 d_1 + \dots + c_m d_m)/b} \mathbf{W}(-\mathbf{d}, \mathbf{c}).$$

There are a lot of papers written about the Fourier matrix (see [5] for a survey).

These matrices are the finite-dimensional analogue of the Weyl operators and of the Fourier transformation in the Hilbert space $\mathcal{L}^2(\mathbb{R})$, which play a central role in quantum mechanics. They are vital both in the construction of maximal, complex, affine quantum designs, and in the construction of maximal, degree 1, complex quantum designs.

3.2 Maximal Affine Quantum Designs

For any prime power $q = p^m$, and any integer $n \geq 2$, there exists a maximal, classical, affine (resp. transversal) 2-design with the parameters $b = q^n$, $r = q^{n-1}$, $\lambda = q^{n-2}$, $g = q$, $k = \frac{q^n-1}{q-1}$, and $v = \frac{q(q^n-1)}{q-1}$ (see [13, I.7] resp. [20, VI.7.7] – but with dual parameters). These designs can be obtained, for example, using the n-dimensional vector space over a finite field $\mathbb{F}$ of order q as point-set, and the $(n-1)$-dimensional *hyperplanes* of $\mathbb{F}^n$ as blocks. The smallest case, with $n = 2$ - i.e. $\lambda = 1$, corresponds to the existence of $q-1$ mutually orthogonal $q \times q$ Latin Squares, resp. affine planes of order q, and can be constructed in $\mathbb{F}^2$.

Using a similar construction, we will now to obtain an analogous result for maximal, affine quantum designs over the complex numbers. For this, we will require the following concept from Finite Field Theory (see [54, Chapter 2.3]).

Let $\mathbb{F}$ be a finite field of order q^m containing a sub-field $\mathbb{K}$ of order q. We can interpret $\mathbb{F}$ as an m-dimensional vector space over $\mathbb{K}$. An ordered m-tuple $\{\alpha_1, \ldots, \alpha_m\}$ of elements $\alpha_i \in \mathbb{F}$ is said to be a basis of $\mathbb{F}$ over $\mathbb{K}$, if every element $\mathbf{a} \in \mathbb{F}$ can be uniquely written in the form $\mathbf{a} = a_1\alpha_1 + \cdots + a_m\alpha_m$, with $a_i \in \mathbb{K}$ for all $1 \leq i \leq m$. The *Trace* $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\mathbf{a})$ of an element $\mathbf{a} \in \mathbb{F}$ over $\mathbb{K}$ is defined as $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\mathbf{a}) = \mathbf{a} + \mathbf{a}^q + \cdots + \mathbf{a}^{q^{m-1}}$. If $\mathbb{K}$ is the prime field of $\mathbb{F}$, then $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\mathbf{a})$ is called the *absolute trace*, and is simply abbreviated as Tr. The trace is a linear mapping of $\mathbb{F}$ onto $\mathbb{K}$. Two bases $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_m\}$ of $\mathbb{F}$ over $\mathbb{K}$ are *dual* if

$$\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\alpha_i\beta_j) = \begin{cases} 1 & \text{for all } 1 \leq i = j \leq m, \\ 0 & \text{for all } 1 \leq i \neq j \leq m. \end{cases}$$

Every basis has a dual basis.

Theorem 3.1. *For any prime power $q = p^m$ and for any integer $n \geq 1$, there exists a maximal, affine quantum 2-design w.r.t $U(b)$ with the parameters $b = q^n$, $r = q^{n-1}$, $\lambda = q^{n-2}$, $g = q$, $k = \frac{q^{2n}-1}{q-1}$, and $v = \frac{q(q^{2n}-1)}{q-1}$.*

Proof. We will first construct solutions for $n = 1$, i.e. $r = 1$.

Let $(\mathbf{c}, \mathbf{d})$ be a point in $\mathbb{F}^2$. Let $\{\alpha_1, \ldots, \alpha_m\}$ and $\{\beta_1, \ldots, \beta_m\}$ be two dual bases of the finite field $\mathbb{F}$ of order p^m over its prime field, which we will identify with $\mathbb{Z}_p$. Set $\mathbf{c} = c_1\alpha_1 + \cdots + c_m\alpha_m$ and $\mathbf{d} = d_1\beta_1 + \cdots + c_m\beta_m$. Then the mapping $(\mathbf{c}, \mathbf{d}) \mapsto \mathbf{W}(\mathbf{c}, \mathbf{d}) = \mathbf{V}^{c_1}\mathbf{U}^{d_1} \otimes \cdots \otimes \mathbf{V}^{c_m}\mathbf{U}^{d_m}$, in accordance with equation (3.2), gives a projective representation of the additive group of $\mathbb{F}^2$.

$(\mathbf{c}, \mathbf{d})$ and $(\mathbf{c}', \mathbf{d}')$ lie in a one-dimensional subspace of $\mathbb{F}^2$ if and only if $\mathbf{c}'\mathbf{d} = \mathbf{c}\mathbf{d}'$. If we apply the absolute trace to this equation, then the duality of the bases gives:

$$c_1'd_1 + \cdots + c_m'd_m = c_1d_1' + \cdots + c_md_m'.$$

Together with equation (3.3), this implies that the q matrices $\mathbf{W}(\mathbf{c}, \mathbf{d})$ that belong to a one-dimensional subspace of $\mathbb{F}^2$ commute with each other. From equation (3.4) it further follows that they are linearly independent. Thus, if they are all simultaneously diagonalized, they then span the space of all diagonal $q \times q$ matrices. In particular, using linear combinations it is therefore possible to construct a unique complete orthogonal class out of q one-dimensional projections.

All subspaces of $\mathbb{F}^2$ have only the origin in common, to which we associate the $q \times q$ identity matrix $\mathbf{I}$. For every one-dimensional projection $\mathbf{P}$ the matrix $\mathbf{P} - \frac{1}{q}\mathbf{I}$ is orthogonal to $\mathbf{I}$, and is thus a linear combination of $q-1$ matrices $\mathbf{W}(\mathbf{c}, \mathbf{d}) \neq \frac{1}{q}\mathbf{I}$. If $\mathbf{P}$ and $\mathbf{Q}$ are associated to two distinct linear subspaces, then these sets of Weyl matrices are disjoint. This, together with the orthogonality relations (3.4), implies

$$\operatorname{tr}\left((\mathbf{P} - \frac{1}{q}\mathbf{I})(\mathbf{Q} - \frac{1}{q}\mathbf{I})\right) = \operatorname{tr}(\mathbf{PQ}) - \frac{1}{q} = 0.$$

Hence, the projections are mutually independent. The $q+1$ one-dimensional subspaces of $\mathbb{F}^2$ thus provide the $q+1$ mutually independent orthogonal classes.

Now let $n \geq 2$ be any integer, and $b = q^n$. Let $\mathbf{D}$ be the solution with $r = 1$, i.e. with $k = q^n + 1$ orthogonal classes, constructed above; let also $\mathbf{D}'$ be the classical, affine design for $b = q^n$, with $s = \frac{q^n - 1}{q-1}$ parallel classes. Thus, the hypotheses of Proposition 2.21 are satisfied, and we obtain a quantum design with $ks = \frac{q^{2n}-1}{q-1}$ orthogonal classes. The regularity, with $r = q^{n-1}$, comes from the classical design, and the other parameters are just as easily verified. $\square$

The construction for $n = 1$ can be generalized by taking the n-fold tensor product of $\mathbf{W}(\mathbf{c}, \mathbf{d})$, and by considering the correspondence to one-dimensional subspaces of $\mathbb{F}^{2n}$. In this manner it is also possible to construct solutions for $n > 1$ directly, and to show that they contain the classical designs as subsets.

Now let $r = 1$ and q be and *odd* prime power. Then we can also explicitly describe vector sets for these quantum designs. An *additive character* χ over a finite field $\mathbb{F}$ of order q is a homomorphism of the additive group of $\mathbb{F}$ into the multiplicative group of the complex numbers, with absolute value 1. A non-trivial character can be defined using the trace via $\chi_1(\mathbf{a}) = e^{2\pi i \operatorname{Tr}(\mathbf{a})/p}$. Let $\mathbf{x}_1, \ldots, \mathbf{x}_q$ be the elements of $\mathbb{F}$ in random order, and suppose that for all $\mathbf{a} \in \mathbb{F}$

$$\mathbf{X}_\mathbf{a} = \frac{1}{\sqrt{q}} \begin{pmatrix} \chi_1(\mathbf{a}\mathbf{x}_1^2 + \mathbf{x}_1\mathbf{x}_1) & \chi_1(\mathbf{a}\mathbf{x}_1^2 + \mathbf{x}_1\mathbf{x}_2) & \ldots & \chi_1(\mathbf{a}\mathbf{x}_1^2 + \mathbf{x}_1\mathbf{x}_q) \\ \chi_1(\mathbf{a}\mathbf{x}_2^2 + \mathbf{x}_2\mathbf{x}_1) & \chi_1(\mathbf{a}\mathbf{x}_2^2 + \mathbf{x}_2\mathbf{x}_2) & \ldots & \chi_1(\mathbf{a}\mathbf{x}_2^2 + \mathbf{x}_2\mathbf{x}_q) \\ \vdots & \vdots & \ddots & \vdots \\ \chi_1(\mathbf{a}\mathbf{x}_q^2 + \mathbf{x}_q\mathbf{x}_1) & \chi_1(\mathbf{a}\mathbf{x}_q^2 + \mathbf{x}_q\mathbf{x}_2) & \ldots & \chi_1(\mathbf{a}\mathbf{x}_q^2 + \mathbf{x}_q\mathbf{x}_q) \end{pmatrix}.$$

For odd q, the standard basis and the columns of the q matrices $\mathbf{X}_a$ form exactly $q+1$ mutually independent orthonormal bases. This can be directly verified by using the orthogonality relations of the characters, and the following formula for non-trivial characters χ over finite fields of prime order q (see [54, Theorem 5.33]).

$$\left|\sum_{\mathbf{y}\in\mathbb{F}} \chi(\mathbf{a}\mathbf{y}^2 + \mathbf{x}\mathbf{y})\right| = \sqrt{q} \qquad \text{for all } \mathbf{a}, \mathbf{x} \in \mathbb{F},\ \mathbf{a} \neq \mathbf{0}. \tag{3.8}$$

We will briefly sketch the correspondence with the contruction in Theorem 3.1, and thus indirectly prove the formula (3.8).

To every $\mathbf{x} \in \mathbb{F}$, we associate its coordinate vector $\{x_1, \ldots, x_m\}$ w.r.t. the basis $\{\alpha_1, \ldots, \alpha_m\}$, and thus also a standard basis vector $\mathbf{e}_\mathbf{x} = \mathbf{e}_{x_1} \otimes \cdots \otimes \mathbf{e}_{x_m}$ in the m-fold tensor product of $\mathbb{C}^p$. The action of the matrices $\mathbf{W}(\mathbf{c}, \mathbf{d})$ can then be described by $\mathbf{W}(\mathbf{c}, \mathbf{d})\mathbf{e}_\mathbf{x} = e^{2\pi i \mathrm{Tr}(dx)/b}\mathbf{e}_{\mathbf{x}-\mathbf{c}} = \chi_1(\mathbf{d}\mathbf{x})\mathbf{e}_{\mathbf{x}-\mathbf{c}}$. This means that the tensor products of the $\mathbf{U}$ act on the basis vectors like multiplication by an additive character, and the tensorproducts of the $\mathbf{V}$ act like shifts.

Using the representation $\mathbf{X}_\mathbf{a}\mathbf{e}_\mathbf{x} = \frac{1}{\sqrt{q}} \sum_{\mathbf{y}\in\mathbb{F}} \chi_1(\mathbf{a}\mathbf{y}^2 + \mathbf{x}\mathbf{y})\mathbf{e}_\mathbf{y}$, it is also possible to view the $\mathbf{X}_\mathbf{a}$ as matrices in this basis. It is then easy to check that

$$\mathbf{X}_\mathbf{a}^{-1}\mathbf{W}(\mathbf{c}, \mathbf{d})\mathbf{X}_\mathbf{a} = \chi_1(\mathbf{a}\mathbf{c}^2 + \mathbf{d}\mathbf{c})\mathbf{W}(-(\mathbf{d} + 2\mathbf{a}\mathbf{c}), \mathbf{c}).$$

The matrices $\mathbf{W}(\mathbf{0}, \mathbf{d})$ are diagonal. For odd q, all linear subspaces of $\mathbb{F}^2$ different from $(\mathbf{0}, \mathbf{d}), \mathbf{d} \in \mathbb{F}$ are described by $\mathbf{a} \in \mathbb{F}$ using the equations $\mathbf{d} = -2\mathbf{a}\mathbf{c}$. All matrices $\mathbf{W}(\mathbf{c}, \mathbf{d})$ belonging to such a subspace are thus simultaneously diagonalized by $\mathbf{X}_\mathbf{a}$. Therefore, the columns of these matrices are the common eigenvectors. This does not hold in the case of even q.

For all $\mathbf{c}, \mathbf{d} \in \mathbb{F}$, the matrices $\mathbf{W}(\mathbf{c}, \mathbf{d})$ generate automorphisms of the corresponding design. In order to obtain a transitive group, it is however necessary to adjoin other automorphisms, for example in the basis just mentioned, $\mathbf{F}_m\mathbf{e}_\mathbf{x} = \frac{1}{\sqrt{q}} \sum_{\mathbf{y}\in\mathbb{F}} \chi_1(\mathbf{x}\mathbf{y})\mathbf{e}_\mathbf{y}$ resp. $\mathbf{G}_\mathbf{a}\mathbf{e}_\mathbf{x} = \chi_1(\mathbf{a}\mathbf{x}^2)\mathbf{e}_\mathbf{x}$ for odd q. The matrix $\mathbf{F}_m$ corresponds precisely to the m-fold tensor product of the Fourier matrix $\otimes^m\mathbf{F}$, and $\mathbf{X}_\mathbf{a} = \mathbf{G}_\mathbf{a}\mathbf{F}_m$.

Only finitely many 2-designs in complex projective spaces (this corresponds to the case $r = 1$) are known in the literature (see [43]). Resolvability was never explicitly studied. However, implicitly some solutions were found among the 2-designs of degree 2, namely those with $b = 2, 3, 4$ (see [43, Example 2,16,17]), and $b = 9$ (see [24, Example 5.9] and [43, Example 19]). These solutions were constructed from strongly regular graphs [15]. All of these designs are special cases of the above construction.[8]

Much less is known in the real case. As we have shown, real, affine quantum designs with $r = 1$ can only exist with $b = 2$ or $b = 4t$, $t \in \mathbb{N}$, and correspond to Hadamard matrices. The same thus holds true for maximal, real, affine

[8]Remark (2010): The constructions for $r = 1$ in this chapter are equivalent to the one given by W.K.Wootters and B.D.Fields in their paper: Optimal State-Determination by Mutually Unbiased Measurements, *Annals of Physics* **191** (1989), 363–381. They were also already contained in my master thesis (1991) were I independently (re-)discovered them.

designs with $k = (b+2)/2$ orthogonal classes. For example for $b = 2$, the 4 vectors $(1,0)$, $(0,1)$, $(1,\pm1)$ form a maximal solution (see also [43, Example 1]). Example 2.17 with $x = y = z = 0$ provides a maximal, real, affine quantum design with $b = 4$.

We end this section with a brief remark on quantum mechanics.

The maximal affine quantum designs in Theorem 3.1 also provide examples for the so-called *Pauli Problem* about determining quantum states through measurement (see [73] for an overview, resp. [17]). A maximal, regular, affine quantum design with $r = 1$ has $q+1$ mutually independent orthogonal classes. Suppose we interpret q of these as spectral projections of the quantum-mechanical observables $\mathbf{A}_i$, $1 \leq i \leq q$, and the q one-dimensional projections of the remaining orthogonal class as *pure states*. The measurement of their likelihoods w.r.t. the spectral projections of the observables $\mathbf{A}_i$ produces in each case the same value: $\frac{1}{q}$. This means that the states cannot be differentiated by measuring the q observables. Hence, the number of not *information-complete* [17] observables $\mathbf{A}_i$ w.r.t. pure states, which are even non-degenerate (i.e. they only have one-dimensional spectral projections) can become arbitrarily large with the dimension q of the vector space. This, for example, contradicts a conjecture by MOROZ [59] in the finite-dimensional case as well. (In [78], counter-examples were constructed in the infinite-dimensional Hilbert space $\mathcal{L}^2(\mathbb{R})$).

3.3 More Affine Quantum Designs

Corollary 3.2. *Let $b = q_1^{s_1} \cdots q_n^{s_n}$, with mutually prime prime powers q_i, and $s_i \in \mathbb{N}$ for all $1 \leq i \leq n$. Then in $\mathbb{C}^b$ there exists a regular, affine quantum design with*

$$r = q_1^{(s_1-1)} \cdots q_n^{(s_n-1)} \qquad \text{and} \qquad k = \min\left(\frac{q_1^{2s_1}-1}{q_1-1}, \ldots, \frac{q_1^{2s_n}-1}{q_n-1}\right).$$

Proof. This result follows directly from Theorem 3.1 and Proposition 2.20. □

This theorem too has an analogue for commutative designs in classical design theory (see [13, Corollary 7.8]). Other construction methods from the theory of transversal designs can be similarly generalized.

It is well-known that in the case of $n \times n$ Latin Squares (i.e. for affine or transversal designs with $\lambda = 1$), the inequality $N(n) \leq n - 1$ for the number $N(n)$ of squares (i.e. the Placket-Burman Inequality) cannot always be satisfied. It is conjectured that equality can only be achieved if n is a prime power. The same appears to hold true for complex, affine quantum designs with $r = 1$. (Presumably, it is possible to prove a result similar to the Theorem of Bruck-Ryser-Chowla [13, II.4.8]).

The parallelism seems to extend even further. For example, already Euler had conjectured that there did not exist two orthogonal Latin Squares of order 6. This was proven by Tarry around 1900, and corresponds to the non-existence of a transversal, resp. affine, design with $b = 36$, $r = g = 6$, $\lambda = 1$ and $k = 4$. Presumably a complex, affine quantum design with $b = g = 6$, $r = 1$, $\lambda = \frac{1}{6}$, and $k = 4$ does not exist either.[9]

Before providing examples with $b = 6$ and $k = 3$, we will introduce a general construction method for even b and $k = 3$.

Circulant matrices are matrices where each row is identical to the previous row, but is shifted one place to the right. For every circulant matrix $\mathbf{A}$, there exists a diagonal matrix $\bar{\mathbf{A}}$ such that, together with the Fourier matrix $\mathbf{F}$, we have $\mathbf{A} = \mathbf{F}^{-1}\bar{\mathbf{A}}\mathbf{F}$ (see [22]). Let

$$\mathbf{T} = \begin{pmatrix} \mathbf{A}_{11} & \mathbf{A}_{12} \\ \mathbf{A}_{21} & \mathbf{A}_{22} \end{pmatrix}$$

be a $2m \times 2m$ matrix with $m \times m$ circulant sub-matrices $\mathbf{A}_{ij} = \mathbf{F}^{-1}\bar{\mathbf{A}}_{ij}\mathbf{F}$ and $\bar{\mathbf{A}}_{ij} = \mathrm{diag}(a_{ij}^1, \ldots, a_{ij}^m)$ for all $1 \leq i, j \leq 2$. If $\mathbf{T}$ is unitary, then the 2×2 matrices $\mathbf{S}_k = (a_{ij}^k)_{1 \leq i,j \leq 2}$ are also unitary for all $1 \leq k \leq m$. It is easy to show that for every unitary 2×2 matrix $\mathbf{S}_k$, there exist parameters $b_l^k \in [0, 2\pi)$, $1 \leq l \leq 4$ such that

$$\mathbf{S}^k = \frac{1}{2}\begin{pmatrix} (e^{ib_1^k} + e^{ib_2^k}) & e^{ib_4^k}(e^{ib_1^k} - e^{ib_2^k}) \\ e^{-ib_3^k}(e^{ib_1^k} - e^{ib_2^k}) & e^{-ib_3^k}e^{ib_4^k}(e^{ib_1^k} + e^{ib_2^k}) \end{pmatrix}.$$

[9] Remark (2010): This statement is equivalent to the conjecture, that no more than 3 MUBs exist in dimension 6.

Now let $\mathbf{U}_l = \operatorname{diag}(e^{ib_l^1}, \ldots, e^{ib_l^m})$, $1 \leq l \leq 4$. It then immediately follows that $\mathbf{T} = \mathbf{E}_1^{-1}\mathbf{E}_2$, with

$$\mathbf{E}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{F} & \mathbf{U}_3\mathbf{F} \\ \mathbf{F} & -\mathbf{U}_3\mathbf{F} \end{pmatrix} \quad \text{and} \quad \mathbf{E}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{U}_1\mathbf{F} & \mathbf{U}_1\mathbf{U}_4\mathbf{F} \\ \mathbf{U}_2\mathbf{F} & -\mathbf{U}_2\mathbf{U}_4\mathbf{F} \end{pmatrix}.$$

the matrices $\mathbf{E}_1$ and $\mathbf{E}_2$ are unitary, and their entries all have the same absolute value: $\frac{1}{\sqrt{2m}}$. This means, if $\mathbf{T}$ also has entries with constant absolute value, then the standard basis and the columns of $\mathbf{E}_1$ and $\mathbf{E}_2$ form an affine quantum design with $b = 2m$, $r = 1$, and $k = 3$. Example 2.17 is an application of this construction to the case $m = 2$.

Example 3.3. For all $x \in [0, 2\pi)$, let

$$\mathbf{T}(x) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & -e^{-ix} & e^{ix} & -1 & ie^{-ix} & ie^{ix} \\ e^{ix} & 1 & -e^{-ix} & ie^{ix} & -1 & ie^{-ix} \\ -e^{-ix} & e^{ix} & 1 & ie^{-ix} & ie^{ix} & -1 \\ 1 & ie^{-ix} & ie^{ix} & 1 & e^{-ix} & -e^{ix} \\ ie^{ix} & 1 & ie^{-ix} & -e^{ix} & 1 & e^{-ix} \\ ie^{-ix} & ie^{ix} & 1 & e^{-ix} & -e^{ix} & 1 \end{pmatrix}.$$

For all $x \in [0, 2\pi)$, the matrices $\mathbf{T}(x)$ are unitary, and have circulant 3×3 submatrices and entries with constant absolute value $\frac{1}{\sqrt{6}}$. Therefore, the standard basis and the columns of the associated matrices $\mathbf{E}_1(x)$ and $\mathbf{E}_2(x)$ form an affine quantum design with $b = 6$, $r = 1$ and $k = 3$. They contain as a special case the solutions that can be constructed from affine designs with $b = 2, 3$ and $k = 3$ using Proposition 3.2. Other affine designs with the same parameters are not known. It was not possible (even with the help of a computer search) to find more orthonormal bases, in order to extend the designs also to $k = 4$.[10]

[10] Remark (2010): P.Jaming, M.Matolcsi, P.Mora, F.Szöllösi and M.Weiner constructed in 2009 a further (inequivalent) family of MUB-triples, see: arXiv:0902.0882v2: An Infinite Family of MUB-Triplets in Dimension 6. Also these triplets could not be extended to $k = 4$. In Appendix B of this paper the construction given here was added.

3.4 Maximal Quantum Designs of Degree 1

Systems of equiangular lines that achieve the absolute bound (i.e. tight 2-designs of degree 1 over projective space) are known in the following cases:

In the real case there are solutions with $b = 2, 3, 7$ and 27 (see [55, 6.6]) and [52]). For $b = 4, 5, 6$ and other values of b, it is possible to prove that the absolute bound cannot be reached (see [52]).

In the complex case examples are known for $b = 2, 3$ and 8 (see [24, Example 6.4] and [43, Examples 5 and 8]).[11].

We will restrict ourselves to the complex case here, and will construct more (non-equivalent) examples with $b = 3$ and solutions for $b = 4$ and $b = 5$, as well as numerical solutions for $b = 6$ and 7. Using the complementary designs, we can also obtain maximal (tight) quantum 2-designs w.r.t. $U(b)$ for $r \geq 2$.

This motivates the conjecture that in the complex case, there exist solutions for all $b \in \mathbb{N}$. The special case of commutative designs corresponds to symmetric BIBD's (and in turn projective planes are a special case of these). For these classical designs, the Bruck-Ryser-Chowla Theorem rules out certain solutions. However, this behavior, unlike with affine designs, does not seem to carry over to the non-commutative case.

The automorphism groups of all these designs have regular subgroups that are generated by the Weyl matrices (with a view to the considerations at the end of Section 2.5 this is not surprising). The solutions for $2 \leq b \leq 7$ use the $b \times b$ Weyl matrices. In the solution for $b = 8$, the 3-fold tensor product of the 2×2 Weyl matrices generate a regular automorphism group (however, here it was not attempted to generate a solution using the 8×8 Weyl matrices). For $2 \leq b \leq 7$, there is in each case an automorphism of order 3 that can be generated by a matrix $\mathbf{Z}$ of order 3, because the designs are irreducible. Thus, for $b = 2, 4, 5, 7$ the automorphism group is complete ($\mathrm{Aut}^*(\mathbf{D})$ has $3b^2$-elements). Since in this case we have $3 \nmid b^2$, the automorphism generated by $\mathbf{Z}$ must necessarily have a fixed point in the permutation. For $3|b$, i.e. $b = 3, 6$, there are additional automorphisms. In this case, the automorphism associated to $\mathbf{Z}$ has 3 fixed points, and it therefore follows that in all cases, the eigenvector of $\mathbf{Z}$ can be selected as initial vector.

Let $\mathbf{Z} = (z_{rs})_{0 \leq r,s \leq b-1}$ be a $b \times b$ matrix, with entries defined by

$$z_{rs} = \frac{e^{i\pi(b-1)/12}}{\sqrt{b}} e^{\pi i(2rs+(b+1)s^2)/b}. \tag{3.9}$$

This matrix can be written as $\mathbf{Z} = e^{i\pi(b-1)/12}\mathbf{FG}$, where $\mathbf{F}$ is the Fourier matrix, and $\mathbf{G} = (g_{rs})_{0 \leq r,s \leq b-1}$ is a diagonal matrix with diagonal entries given

[11] Remark (2010): an overview of the current known solutions can be found in A.J.Scott and M.Grassl: SIC-POVMs: A new computer study, arXiv:0910.5784v2. There also the ideas and results of this chapter are summarized

by $g_{ss} = e^{\pi i(b+1)s^2/b}$, $0 \leq s \leq b-1$. The matrix $\mathbf{Z}$ has properties similar to those of the Fourier matrix; it is unitary, and satisfies the following relations:

$$\mathbf{Z}^3 = \mathbf{I}, \tag{3.10a}$$

$$\mathbf{Z}^{-1}\mathbf{V}\mathbf{Z} = \mathbf{U} \quad \text{and} \quad \mathbf{Z}^{-1}\mathbf{U}\mathbf{Z} = e^{\pi i(b-1)/b}\mathbf{V}^{-1}\mathbf{U}^{-1}. \tag{3.10b}$$

The possible eigenvalues of $\mathbf{Z}$ are precisely the cube roots of unity: 1, $\alpha = e^{i2\pi/3}$, and $\alpha^2 = e^{i4\pi/3}$. The following table shows the multiplicities of the eigenvalues as they depend on the order b:

b	1	$e^{i2\pi/3}$	$e^{i4\pi/3}$
$3m$	$m+1$	m	$m-1$
$3m+1$	$m+1$	m	m
$3m+2$	$m+1$	$m+1$	m

(3.11)

The equations (3.10b) are easily verified. They imply that $\mathbf{Z}^3$ commutes with all Weyl matrices and - since the Weyl matrices span the space of all $b \times b$ matrices - that $\mathbf{Z}^3 = \varepsilon\mathbf{I}$, with $|\varepsilon| = 1$. In order to show that $\varepsilon = 1$ and to prove table (3.11), we need to use some results about *Gauss sums.* This is similar like for the Fourier matrix (see [5]). We sketch the proof. If p and q be relatively prime integers, then

$$\frac{1}{\sqrt{q}}\sum_{r=0}^{q-1} e^{-i\pi r^2 p/q} = \frac{e^{-i\pi/4}}{\sqrt{p}}\sum_{r=0}^{p-1} e^{i\pi r^2 q/p}. \tag{3.12}$$

This equation can be derived from the transformation formula $f(t) = (\frac{\pi}{t})^{1/2} f(\frac{\pi^2}{t})$ for the *Theta function* $f(t) = \sum_{n=-\infty}^{\infty} e^{-n^2 t}$ (see [11, Chapter 6, equation (13)]). Using the relatively prime integers $q = b$ and $p = b-1$, and complete induction, we obtain

$$\frac{1}{\sqrt{b}}\sum_{r=0}^{b-1} e^{i\pi(b+1)r^2/b} = e^{-i\pi(b-1)/4}.$$

By comparing this equation with $\mathbf{Z}^2 = \varepsilon\mathbf{Z}^{-1} = \varepsilon\mathbf{Z}^*$ evaluated at the point $(0,0)$, we get $\varepsilon = 1$. Using the same equation with $b = 3m$ we immediately obtain $\mathrm{tr}(\mathbf{Z}) = e^{i\pi/6}\sqrt{3}$. In the cases $b = 3m+1$ or $b = 3m+2$, by applying equation (3.12) to the relatively prime integers $q = b$ and $p = b-3$, we see that $\mathrm{tr}(\mathbf{Z}_b) = \mathrm{tr}(\mathbf{Z}_{(b-3)})$ holds for the $b \times b$ matrices $\mathbf{Z}_b$. Using induction, and the fact that $\mathrm{tr}(\mathbf{Z}_1) = 1$, and $\mathrm{tr}(\mathbf{Z}_2) = \frac{e^{i\pi/12}}{\sqrt{2}}(1 + e^{i5\pi/2}) = e^{i\pi/3}$, it follows that

$$\mathrm{tr}(\mathbf{Z}) = \begin{cases} e^{i\pi/6}\sqrt{3} = 2 + e^{i2\pi/3} & \text{if } b \equiv 0 \pmod 3, \\ 1 & \text{if } b \equiv 1 \pmod 3, \\ e^{i\pi/3} = 1 + e^{i2\pi/3} & \text{if } b \equiv 2 \pmod 3. \end{cases}$$

Since $\mathbf{Z}^3 = \mathbf{I}$, it is clear that $\mathbf{Z}$ has exactly the cube roots of unity 1, $e^{i2\pi/3}$, and $e^{i4\pi/3}$ as possible eigenvalues; table (3.11) follows directly from this.

The group $W = \{e^{ix}\mathbf{V}^c\mathbf{U}^d\colon\ c,d \in \mathbb{Z}_b,\ x \in \mathbb{R}\}$ is obtained by multiplying the Weyl matrices by arbitrary phases. We now consider the group $\mathrm{Aut}(W)$ of (outer) automorphisms of W in $U(b)$[12] , i.e. the set of all unitary $b \times b$ matrices $\mathbf{A}$ such that there exist $x, y \in \mathbb{R}$ and $j,k,l,m \in \mathbb{Z}$ satisfying:

$$\mathbf{A}^{-1}\mathbf{V}\mathbf{A} = e^{ix}\mathbf{V}^j\mathbf{U}^k, \tag{3.13a}$$

$$\mathbf{A}^{-1}\mathbf{U}\mathbf{A} = e^{iy}\mathbf{V}^l\mathbf{U}^m. \tag{3.13b}$$

We observe that $W \subset \mathrm{Aut}(W)$. Using equations (3.7) resp. (3.10b), it follows that also $\mathbf{F}, \mathbf{Z} \in \mathrm{Aut}(W)$. There are other elements in $\mathrm{Aut}(W)$ (for example, the matrix $\mathbf{G}$ mentioned above). Suppose that the Weyl matrices generate a regular subgroup of the automorphism group of a quantum design $\mathbf{D}$; in other words, let

$$\mathbf{D} = \{\mathbf{V}^c\mathbf{U}^d\mathbf{P}_1\mathbf{U}^{-d}\mathbf{V}^{-c} : c,d \in \mathbb{Z}_b\} \tag{3.14}$$

where $\mathbf{P}_1$ is any $b \times b$ projection matrix. Every similarity transformation of $\mathbf{D}$ by a matrix $\mathbf{A} \in \mathrm{Aut}(W)$ yields a design of the form (3.14), with a new initial projection $\mathbf{P'} = \mathbf{A}^{-1}\mathbf{P}\mathbf{A}$. If $\mathbf{P}_1$ is a projection onto an eigenvector of $\mathbf{Z} \in \mathrm{Aut}(W)$, then $\mathbf{Z}$ must generate an automorphism. The design obtained after transformation by $\mathbf{A} \in \mathrm{Aut}(W)$ has an initial projection $\mathbf{P'}$ that projects onto the eigenvector of the matrix $\mathbf{Z'} = \mathbf{A}^{-1}\mathbf{Z}\mathbf{A}$, which is equivalent to $\mathbf{Z}$.

Example: $\mathbf{b = 2}$ (see also [24, Example 6.4]).

According to Table (3.11), $\mathbf{Z}$ has the two eigenvalues 1 and $\alpha = e^{i2\pi/3}$; the associated eigenvectors are

$$\psi_1 = \begin{pmatrix} Y \\ e^{i\pi/4}X \end{pmatrix}, \qquad \psi_\alpha = \begin{pmatrix} X \\ e^{i5\pi/4}Y \end{pmatrix},$$

with $X = \sqrt{\frac{1}{2}(1 - \frac{1}{\sqrt{3}})}$ and $Y = \sqrt{\frac{1}{2}(1 + \frac{1}{\sqrt{3}})}$. The QD-matrix $\mathbf{E}_2$ belonging to the quantum design $\mathbf{D}_2 = \{\mathbf{V}^c\mathbf{U}^d\psi_1 : c,d \in \mathbb{Z}_2\}$ is given by

$$\mathbf{E}_2 = \begin{pmatrix} Y & Y & e^{i\pi/4}X & -e^{i\pi/4}X \\ e^{i\pi/4}X & -e^{i\pi/4}X & Y & Y \end{pmatrix}.$$

With $X^2 - Y^2 = -\frac{1}{\sqrt{3}}$ and $\sqrt{2}XY = \frac{1}{\sqrt{3}}$ it follows immediately that $\mathbf{D}_2$ has degree 1. With a little bit of computation, it is possible to check that this design (up to equivalence) is the only degree 1 maximal quantum design in $\mathbb{C}^2$, and that $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{Z}$ generate the whole automorphism group. Similarly, the complementary quantum design with degree 1 is generated by ψ_α.

Example: $\mathbf{b = 3}$.

According to Table (3.11), $\mathbf{Z}$ has the eigenvalues 1 (twice) and $\alpha = e^{i2\pi/3}$ (once). The eigenvector belonging to the eigenvalue α does not provide a degree

[12] Remark (2010): This group is known in the literature as *Clifford group* or *Jacobi Group*, see e.g. D.M.Appleby: Properties of the extended Clifford group with applications to SIC-POVMs and MUBs, arXiv:0909.5233.

1 quantum design. Orthonormal eigenvectors belonging to the eigenvalue 1 are, for example:

$$\psi_{1a} = \frac{1}{\sqrt{6}} \begin{pmatrix} 2 \\ -\alpha^2 \\ -\alpha^2 \end{pmatrix}, \qquad \psi_{1b} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}.$$

In the $\mathbf{Z}$ eigenspace spanned by ψ_{1a} and ψ_{1b}, there is a one-parameter family of solutions. For any $x \in \mathbb{R}$, let

$$\psi_x = (\cos x)\psi_{1a} + (\alpha^2 \sin x)\psi_{1b}.$$

We will soon show that the quantum designs $\mathbf{D}_{3,x} = \{\mathbf{V}^c\mathbf{U}^d\psi_x : c, d \in \mathbb{Z}_3\}$ for all $x \in \mathbb{R}$ all have degree 1. The case $b = 3$ is special, because there exists a matrix $\mathbf{A} \in \mathrm{Aut}(W)$ that diagonalizes $\mathbf{Z}$, namely $\mathbf{A} = \mathbf{ZG}$, with $\mathbf{G} = \mathrm{diag}(1, \alpha^2, \alpha^2)$. The relation $\mathbf{AZA}^{-1} = \alpha\mathbf{G}$ holds. The transformed quantum designs $\mathbf{D}'_{3,x} = \mathbf{AD}_{3,x}$ are generated by $\psi'_x = \mathbf{A}\psi_x$, and it can be seen immediately that $\psi'_x = e^{i\pi/6}(0, e^{-ix}, e^{ix})^t$ holds. If we multiply ψ'_x by the complex phase $e^{i(x-\pi/6)}$, then setting $y = 2x$ we obtain the QD matrix

$$\mathbf{E}'_{3,y} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 0 & e^{iy} & e^{iy}\alpha & e^{iy}\alpha^2 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & e^{iy} & e^{iy}\alpha & e^{iy}\alpha^2 \\ e^{iy} & e^{iy}\alpha & e^{iy}\alpha^2 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

In this form, it is obvious that for all $y \in \mathbb{R}$, the quantum design $\mathbf{D}'_{3,y}$ has degree 1. By swapping columns, we see that we can assume that $y \in [0, \frac{2\pi}{3})$ (however, there are several such identifications).

The solution to $y = \pi$ can be found in [24, Example 6.4] and [43, Example 5]. It has a complete automorphism group with a 216-element permutation group $\mathrm{Aut}^*(\mathbf{D})$ that is generated by $\mathbf{U}$, $\mathbf{V}$, $\mathbf{G}$ and $\mathbf{Z}$. For $y = 0$, the whole automorphism group is generated by $\mathbf{U}$, $\mathbf{V}$, $\mathbf{G}$ and $\mathbf{F}^2$ (and $\mathrm{Aut}^*(\mathbf{D})$ has 54 elements); while for $y \not\approx 0, \pi$, the automorphism group is just generated by $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{G}$ (and $\mathrm{Aut}^*(\mathbf{D})$ has 27 elements).

Example: $\mathbf{b = 4}$.

According to Table (3.11), $\mathbf{Z}$ has the eigenvalues 1 (twice), α (once), and α^2 (once). The eigenvectors belonging to the eigenvalues α and α^2 do not generate a degree 1 quantum design. Let $\varrho = e^{i\pi/4}$. As can easily be verified, orthonormal eigenvectors belonging to the eigenvalue 1 are, for example:

$$\psi_{1a} = \frac{1}{\sqrt{6}} \begin{pmatrix} \varrho + 1 \\ i \\ \varrho - 1 \\ i \end{pmatrix}, \qquad \psi_{1b} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix}.$$

Now let $X = \frac{1}{2}\sqrt{3 - \frac{3}{\sqrt{5}}}$, $Y = \frac{1}{2}\sqrt{1 + \frac{3}{\sqrt{5}}}$, and

$$\psi_k = X\psi_{1a} + \varrho^k Y\psi_{1b} \qquad \text{for } k = 1, 3, 5, 7.$$

For all k=1,3,5,7, the quantum designs $\mathbf{D}_{4,k} = \{\mathbf{V}^c\mathbf{U}^d\psi_k : c,d \in \mathbb{Z}_4\}$ have degree 1. Using $\langle\psi_{1a}|\mathbf{U}\psi_{1a}\rangle = \frac{\sqrt{2}}{3}$, $\langle\psi_{1b}|\mathbf{U}\psi_{1b}\rangle = 0$, $\langle\psi_{1a}|\mathbf{U}\psi_{1b}\rangle = \frac{1}{\sqrt{3}}$ and $\langle\psi_{1b}|\mathbf{U}\psi_{1a}\rangle = -\frac{1}{\sqrt{3}}$, it immediately follows that

$$|\langle\psi_k|\mathbf{U}\psi_k\rangle|^2 = 2\left|\frac{X^2}{3} \pm i\frac{XY}{\sqrt{3}}\right|^2 = \frac{1}{5}.$$

Similarly, one can show that

$$\left|\langle\psi_k|\mathbf{U}^2\psi_k\rangle\right|^2 = \left|\frac{X^2}{3} - Y^2\right|^2 = \frac{1}{5},$$

$$\left|\langle\psi_k|\mathbf{V}\mathbf{U}^2\psi_k\rangle\right|^2 = 2\left|\frac{-iX^2}{3} \pm \frac{XY}{\sqrt{3}}\right|^2 = \frac{1}{5}.$$

The invariance of the inner product under similarity transformations by $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{Z}$ implies all other equations for degree 1. The matrices $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{Z}$ generate an automorphism group whose permutation group $\mathrm{Aut}^*(\mathbf{D})$ has 48 elements. With the aid of a computer, it was possible to show that this was indeed the whole automorphism group.

Example: b = 5.

According to Table (3.11), $\mathbf{Z}$ has the eigenvalues 1 (twice), α (twice) and α^2 (once). Let $\varepsilon = e^{i2\pi/5}$. Two orthonormal vectors associated to the eigenvalue 1 are, for example:

$$\psi_{1a} = \frac{e^{i\pi/10}}{2\sqrt{30}} \begin{pmatrix} 2\sqrt{2\left(5+\sqrt{5}\right)} \\ \left(\sqrt{5-2\sqrt{5}}+\sqrt{15}\right)\varepsilon \\ \left(\sqrt{5-2\sqrt{5}}-\sqrt{15}\right)\varepsilon^4 \\ \left(\sqrt{5-2\sqrt{5}}-\sqrt{15}\right)\varepsilon^4 \\ \left(\sqrt{5-2\sqrt{5}}+\sqrt{15}\right)\varepsilon \end{pmatrix},$$

$$\psi_{1b} = \frac{1}{2\sqrt{15}} \begin{pmatrix} 0 \\ \sqrt{15+\sqrt{15\left(5+2\sqrt{5}\right)}} \\ -\left(\sqrt{15-\sqrt{15\left(5+2\sqrt{5}\right)}}\right)\varepsilon^3 \\ \left(\sqrt{15-\sqrt{15\left(5+2\sqrt{5}\right)}}\right)\varepsilon^3 \\ -\sqrt{15+\sqrt{15\left(5+2\sqrt{5}\right)}} \end{pmatrix}.$$

Now let $X = \frac{1}{2}\sqrt{3-\sqrt{3}}$, $Y = \frac{1}{2}\sqrt{1+\sqrt{3}}$, and $\beta = \sqrt{\frac{1}{10}\left(5+\sqrt{5}\right)} + i\sqrt{\frac{1}{10}\left(5-\sqrt{5}\right)}$. We define the following four vectors

$$\psi_{(j,k)} = X\psi_{1a} + j\beta^k Y\psi_{1b} \qquad \text{mit } j,k = \pm 1.$$

The quantum designs $\mathbf{D}_{5,j,k} = \{\mathbf{V}^c\mathbf{U}^d\psi_{(j,k)} : c,d \in \mathbb{Z}_5\}$ have degree 1 for all $j,k = \pm 1$. The proof requires tedious computations that we will not reproduce here. We note that due to symmetries, it suffices for example to verify the four relations $\left|\langle\psi_{(j,k)}|\mathbf{V}^r\mathbf{U}^s\psi_{(j,k)}\rangle\right|^2 = \frac{1}{6}$ with $r = 0,-1$ and $s = 1,2$. Furthermore, it is enough to check the relations for only one of the four initial vectors, since the four solutions are equivalent. It is easy to check that, given $\mathbf{G} = \mathrm{diag}(1,\varepsilon^3,\varepsilon^2,\varepsilon^2,\varepsilon^3)$ ($\mathbf{G} \in \mathrm{Aut}(W)$), $\mathbf{G}^{-1}\bar{\psi}_{(1,1)} = -\varepsilon^2 X\psi_{1a} + \bar{\beta}Y\varepsilon^2\psi_{1b} = -\varepsilon^2\psi_{(-1,-1)}$ holds, and it is furthermore immediate that $\psi_{(-1,k)} = \mathbf{F}^2\psi_{(1,k)}$.

Additionally, as we will show now, there are exactly four (equivalent) eigenvectors in the 2-dimensional eigenspace of $\mathbf{Z}$ belonging to the eigenvalue α that produce quantum designs of degree 1. Let

$$\mathbf{T} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

We have $\mathbf{T}^{-1}\mathbf{V}\mathbf{T} = \mathbf{V}^2$, and $\mathbf{T}^{-1}\mathbf{U}\mathbf{T} = \mathbf{U}^3$. This implies that $\mathbf{T} \in \mathrm{Aut}(W)$ and hance also $\mathbf{TG}$. Furthermore, it is easy to show that $(\mathbf{TG})^{-1}\mathbf{Z}\mathbf{TG} = \alpha\mathbf{Z}^{-1}$. Assume now that ψ is an eigenvector of $\mathbf{Z}$ (and thus also of $\mathbf{Z}^{-1}$) belonging to the eigenvalue 1. From the above relations it follows that $\mathbf{Z}(\mathbf{TG}\psi) = \alpha(\mathbf{TG}\psi)$. This means that $\mathbf{TG}$ transforms the eigenvectors of $\mathbf{Z}$ associated to the eigenvalue 1 into eigenvectors belonging to the eigenvalue α (and vice versa). Since $\mathbf{TG} \in \mathrm{Aut}(W)$, this means that the four vectors $\mathbf{TG}\psi_{(j,k)}$, with $j,k = \pm 1$, also generate quantum designs of degree 1.

$\mathbf{U}$, $\mathbf{V}$ and $\mathbf{Z}$ generate an automorphism group with a 75-element permutation group $\mathrm{Aut}^*(\mathbf{D})$. Using a computer program it was possible to show that this is indeed the whole automorphism group.

Example: $\mathbf{b = 6}$.

The following numerical solution exists:

$$\psi = \begin{pmatrix} 0.618729 \\ 0.154397 + i \cdot 0.063793 \\ 0.319614 + i \cdot 0.373905 \\ 0.089576 + i \cdot 0.006425 \\ -0.242374 - i \cdot 0.073843 \\ 0.523986 + i \cdot 0.021978 \end{pmatrix}.$$

$\mathbf{U}\mathbf{V}^{-1}\bar{\psi}$ is an eigenvector of $\mathbf{Z}$ corresponding to the eigenvalue 1. $\mathbf{D}_6 = \{\psi_{c,d} = \mathbf{V}^c\mathbf{U}^d\psi : c,d \in \mathbb{Z}_6\}$ has degree 1, with a precision of $\left||\langle\psi_{c,d}|\psi_{e,f}\rangle|^2 - \frac{1}{7}\right| \leq 10^{-6}$ for all $(c,d) \neq (e,f)$.

By taking tensor products of, and applying an appropriate permutation to, $\mathbf{U}$, $\mathbf{V}$ and $\mathbf{Z}$ in $\mathbb{C}^2$, and $\mathbf{U}$, $\mathbf{V}$, $\mathbf{R}$ and $\mathbf{Z}$ in $\mathbb{C}^3$, it is possible to produce an outer automorphism group with 5184 elements that contains the matrix $\mathbf{Z}$.

Example: $\mathbf{b = 7}$.

The following numerical solution exists:

$$\psi = \begin{pmatrix} 0.196001 \\ -0.032164 + i \cdot 0.465343 \\ -0.618610 + i \cdot 0.010962 \\ 0.012587 + i \cdot 0.204539 \\ 0.177171 + i \cdot 0.243931 \\ -0.081634 - i \cdot 0.105666 \\ 0.346649 - i \cdot 0.300538 \end{pmatrix}.$$

ψ is an eigenvector of $\mathbf{Z}$ corresponding to the eigenvalue 1. $\mathbf{D}_7 = \{\psi_{c,d} = \mathbf{V}^c\mathbf{U}^d\psi : c, d \in \mathbb{Z}_7\}$ has degree 1, with a precision $\left| |\langle\psi_{c,d}|\psi_{e,f}\rangle|^2 - \frac{1}{8} \right| \leq 10^{-6}$ for all $(c,d) \neq (e,f)$.

The examples for $b = 2, 3, 4, 5, 6, 7$ make the following conjecture plausible. For all $b \geq 2$, there exist vectors in the $\left(\left[\frac{b}{3}\right] + 1\right)$-dimensional eigenspace belonging to the eigenvalue 1 of the $b \times b$ matrix $\mathbf{Z}$, such that it is possible to generate maximal degree 1 quantum designs starting from designs of the form (3.14). For $b = 3m + 2$ there exist also such vectors in the eigenspace of the same dimension, belonging to the eigenvalue α.[13] In contrast, the following solution adheres to a different construction rule.

Example: $\mathbf{b = 8}$.

In [41] and [42], Hoggar constructed 64 unit vectors in $\mathbb{H}^4$ (the 4-dimensional vector space over the Quaternions) with $\frac{1}{3}$ or $\frac{1}{9}$ as squares of their pairwise angles, i.e. with $\Lambda = \{\frac{1}{3}, \frac{1}{9}\}$. He also indicated that through complexification, 64 unit vectors in $\mathbb{C}^8$ with $\lambda = \frac{1}{9}$ arise. These can be constructed by using

$$\psi = \frac{1}{\sqrt{6}}(1 + i, 0, -1, 1, -i, -1, 0, 0)^t$$

as initial vector, and applying the 3-fold tensor product of the 2×2 Weyl matrices, i.e. the matrices $\mathbf{W}(\mathbf{c}, \mathbf{d})$ with $\mathbf{c}, \mathbf{d} \in \mathbb{Z}^3$ (as generators of a regular automorphism group).

[13]Remark (2010): In http://www.imaph.tu-bs.de/qi/problems/problems.html this conjecture is listed under Problem 23 in Quantum Information Theory.

3.5 More Quantum Designs of Degree 1

Via the dual association of Theorem 1.10, commutative, regular, and coherent degree 1 quantum designs (i.e. according to Theorem 2.26, regular quantum designs of degree 1 for which the special bound $\lambda \geq \frac{r(vr-b)}{b(v-1)}$ becomes an equality) correspond to *balanced incomplete block designs*. These designs are the focus of a large number of articles (see [20, Chapter I] for a survey). We assemble here some well-known results from the non-commutative case.

For $r = 1$, infinite families of solutions were already constructed for the special case $k = 2$ (i.e. $v = 2b$ and $\lambda = \frac{1}{2b-1}$).

By appealing to the Theory of Hadamard Matrices, the following constructions can be found for even b (see [24, Example 5.8] and [43, Example 14]). Let $\mathbf{H}$ be a skew-symmetric Hadamard matrix of order $n = 4m$, i.e. $\mathbf{H} = \mathbf{I} + \mathbf{A}$ with a skew-symmetric (Conference) matrix $\mathbf{A}$. Since $\mathbf{A}\mathbf{A}^T = (n-1)\mathbf{I}$ and $\mathrm{tr}(\mathbf{A}) = 0$, it follows that $\mathbf{A}$ has 2 eigenvalues $\pm i\sqrt{n-1}$, each with multiplicity $2m$. Let $\mathbf{G} = \mathbf{I} + \frac{i}{\sqrt{n-1}}\mathbf{A}$. The matrix $\mathbf{G}$ has rank $2m$, and it is easy to see that

$$\left(\frac{1}{\sqrt{2}}\mathbf{G}\right)\left(\frac{1}{\sqrt{2}}\mathbf{G}^*\right) = \mathbf{I} + \frac{i}{\sqrt{n-1}}\mathbf{A}.$$

This means that the $4m$ columns of $\frac{1}{\sqrt{2}}\mathbf{G}$ are normalized, and that the inner product of any pair of distinct column of $\frac{1}{\sqrt{2}}\mathbf{G}$ equals $\pm\frac{i}{\sqrt{n-1}}$. This implies that there exists a solution for $b = 2m$. It is conjectured that there exists a skew-symmetric Hadamard matrix for all $m \in \mathbb{N}$. This would provide a solution for all even b. It is quite easy to obtain explicit solutions for all $n = 2^k$. Paley's construction (see [13, Theorem I.9.11]) for prime powers $q \equiv 3 \pmod 4$, with $n = q + 1$, is also well-known. It gives solutions in for the case $b = (q + 1)/2$.

In the case of b odd, there is a construction for $b = (q+1)/2$, where q is any prime power $q \equiv 1 \pmod 4$. In this case solutions were even constructed in the reals, using symmetric C-matrices and Paley's construction - see [55, Theorem 6.3]. Solutions for other odd b are not known.

In $\mathbb{C}^b$, we can give solutions for (even, as well as odd) $b = (q + 1)/2$, where q is any odd prime power, by the following method.

Let χ be a non-trivial additive character of a finite field $\mathbb{F}$ of prime order q. Let $a_1, a_2, \ldots, a_q$ be the elements of $\mathbb{F}$. In $\mathbb{F}$ there are exactly $\frac{q-1}{2}$ non-zero squares - denote these by $b_1, b_2, \ldots, b_{\frac{q-1}{2}}$. Then the following $(\frac{q+1}{2}) \times (q + 1)$ matrix $\mathbf{E}$ is a QD-matrix, to which we can associate a regular, coherent, degree 1 quantum design, with $r = 1$, $v = q + 1$, $b = \frac{q+1}{2}$, $k = 2$ and $\lambda = \frac{1}{q}$.

$$\mathbf{E} = \begin{pmatrix} 1 & \frac{1}{\sqrt{q}} & \frac{1}{\sqrt{q}} & \cdots & \frac{1}{\sqrt{q}} \\ 0 & \sqrt{\frac{2}{q}}\chi(b_1 a_1) & \sqrt{\frac{2}{q}}\chi(b_1 a_2) & \cdots & \sqrt{\frac{2}{q}}\chi(b_1 a_q) \\ 0 & \sqrt{\frac{2}{q}}\chi(b_2 a_1) & \sqrt{\frac{2}{q}}\chi(b_2 a_2) & \cdots & \sqrt{\frac{2}{q}}\chi(b_2 a_q) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \sqrt{\frac{2}{q}}\chi(b_{\frac{q-1}{2}} a_1) & \sqrt{\frac{2}{q}}\chi(b_{\frac{q-1}{2}} a_2) & \cdots & \sqrt{\frac{2}{q}}\chi(b_{\frac{q-1}{2}} a_q) \end{pmatrix}. \tag{3.15}$$

It follows from $|\chi| = 1$ that every column of $\mathbf{E}$ is normalized. Coherence follows from the special inequality. The inner product of the first with the j-th column, where $2 \leq j \leq q+1$, is clearly $\frac{1}{\sqrt{q}}$. For the absolute value of the inner product of any two other columns, this follows from equation 3.8 for Gauss sums. It is quite obvious that these designs are coherently dual to themselves.

In [55] and [52], additional regular, coherent designs of degree 1 in $\mathbb{R}^b$, and for $k \neq 2$ too (see also [24, Example 5.7], e.g. for $b = 6$ and $v = 16$), were constructed using *regular two graphs* [15]. The solutions of Example 2.14 represent further examples, as do the maximal designs of Section 3.4.

The following table shows the possible parameters for regular, coherent, degree 1 quantum designs with $r = 1$, and their dependence on v and b. The value $\lambda = \frac{v-b}{b(v-1)}$ is inserted in the table. The inequalities for complex designs from Section 2.4 were taken into consideration. λ is written in bold for all those parameters for which we have just given solutions above ($k = 2$ for example corresponds to the entries with $v = 2b$).

b\v	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	0	$\mathbf{\frac{1}{4}}$	$\mathbf{\frac{1}{3}}$												
3		0	$\mathbf{\frac{1}{9}}$		$\mathbf{\frac{1}{5}}$	$\frac{2}{9}$	$\frac{5}{21}$	$\mathbf{\frac{1}{4}}$	← Absolute Bound						
4			0	$\mathbf{\frac{1}{16}}$		$\frac{1}{8}$	$\mathbf{\frac{1}{7}}$	$\frac{5}{32}$	$\frac{1}{6}$	$\frac{7}{40}$	$\frac{2}{11}$	$\frac{3}{16}$	$\frac{5}{26}$	$\frac{11}{56}$	$\mathbf{\frac{1}{5}}$
5				0	$\mathbf{\frac{1}{25}}$		$\frac{3}{35}$	$\frac{1}{10}$	$\mathbf{\frac{1}{9}}$	$\frac{3}{25}$	$\frac{7}{55}$	$\frac{2}{15}$	$\frac{9}{65}$	$\frac{1}{7}$	$\frac{11}{75}$
6					0	$\mathbf{\frac{1}{36}}$		$\mathbf{\frac{1}{16}}$	$\frac{2}{27}$	$\frac{1}{12}$	$\mathbf{\frac{1}{11}}$	$\frac{7}{72}$	$\frac{4}{39}$	$\frac{3}{28}$	$\mathbf{\frac{1}{9}}$
7						0	$\mathbf{\frac{1}{49}}$			$\frac{2}{35}$	$\frac{5}{77}$	$\frac{1}{14}$	$\mathbf{\frac{1}{13}}$	$\frac{4}{49}$	$\frac{3}{35}$
8							0	$\mathbf{\frac{1}{64}}$			$\frac{1}{22}$	$\frac{5}{96}$	$\frac{3}{52}$	$\frac{1}{16}$	$\mathbf{\frac{1}{15}}$

↖ orthonormal bases ↖ example 2.14 ↖ coherently dual absolute bound

Stronger upper (and coherently dual lower) bounds hold for real designs, and it is possible to show that there do not exist solutions for all permissible parameters within those bounds. For example, there are no solutions in the case $b = 4$ and $v > 6$ (see [52]). Using coherent duality, it follows that there are no real solutions for $b = 4$, aside from the one given in example 2.14. In the complex case, no such non-existence proofs are known. However, there are large gaps even among small values; finding other complex solutions therefore presents a great challenge. Due to coherent duality, it is possible to restrict the search to the case $k \leq 2$, i.e. $v \leq 2b$.

Complementary designs, r-fold sums, and coherently dual designs of degree 1 coherent designs all have degree 1 themselves. In this manner we obtain many solutions for $r \geq 2$.

Epilogue

A number of open problems and conjectures were mentioned in this paper. Below, we list some of them, together with suggestions for further investigations.

(i) Generalize other concepts from the theory of spherical designs, such as that of zonal orthogonal polynomials (see [29]). Use this to develop the theory of t-coherence, resp. of quantum t-designs over homogeneous G-spaces, further.

(ii) Extend the concepts of vector space and projections to the Quaternions and the Cayley numbers.

(iii) Generalize the non-existence proofs from classical design theory (such as the Bruck-Ryser-Chowla Theorem [13, II.4.8] for affine designs) and the non-existence proofs for tight t-designs with $r = 1$ (see [6], [7], [10]).

(iv) Show that there are no affine quantum designs for $b = 6$, $r = 1$ and $k = 4$.

(v) For all $b \in \mathbb{N}$, construct maximal, regular, degree 1 quantum designs (i.e. tight, regular quantum 2-designs) over the complex numbers (using the method from Section 3.4).

(vi) Construct other regular, coherent quantum designs of degree 1, especially for small parameter values. Are there other restrictions for complex quantum designs besides the bounds in Section 2.4?

(vii) As a generalization of *partially balanced incomplete block designs*, investigate and construct quantum designs with association schemes.

(viii) Interpret quantum-mechanical systems in finite-dimensional Hilbert spaces (e.g. spin observables) as sets of projection matrices (spectral projections, or states), and thus as quantum designs. Can certain systems be uniquely characterized as quantum designs (probabilistically)?

(ix) Develop further the concept for infinite-dimensional Hilbert spaces, and/or infinite (continuous) sets of orthogonal projections, as briefly sketched in Section 1.3.

References

[1] Accardi, L.: Some trends and problems in quantum probability, in: Accardi, L. et. al. (eds.), *Quantum Probability and Applications to the Quantum Theory of Irreversible Processes*, LNM. 1055, Springer, Berlin, Heidelberg, New York, 1984.

[2] Agaian, S.S.: *Hadamard Matrices and their Applications*, LNM. 1168, Springer, Berlin, Heidelberg, New York, 1985.

[3] Amrein, W.O. and Berthier, A.M.: On support properties of L^p-funktions and their Fourier transforms, *J. Funct. Anal.* **24** (1977), 258–267.

[4] Anderson, I.: *Combinatorial Designs: Construction Methods*, Ellis Horwood, Chichester, 1990.

[5] Auslander, L. and Tolimieri, R.: Is computing with the finite Fourier Transform pure or applied mathematics?, *Bull. Amer. Math. Soc. (N.S.)* **1** (1979), no. 6, 847–897.

[6] Bannai, E. and Damerell, R.M.: Tight spherical designs, I, *J. Math. Soc. Japan*, **31** (1979), 199–207.

[7] Bannai, E. and Damerell, R.M.: Tight spherical designs, II, *J. London Math. Soc. (2)*, **21** (1980), 13–30.

[8] Bannai, E.: Spherical t-designs which are orbits of finite groups, *J. Math. Soc. Japan* **36** (1984), 341–354.

[9] Bannai, E.: Spherical designs and group representation, *AMS Contemp. Math.* **34** (1984), 95–107.

[10] Bannai, E. and Hoggar, S.G.: On tight t-designs in compact symmetric spaces of rank one, *Proc. Japan Acad. Ser. A Math. Sci.* **61** (1985), 78–82.

[11] Bellman, R.: *Analytic Number Theory*, Benjamin/Cummings, Reading, MA, 1980.

[12] Beltrametti, E.G. and Cassinelli, G.: *The Logic of Quantum Mechanics*, Addison-Wesley, Reading, MA, 1981.

[13] Beth, Th., Jungnickel, D. and Lenz, H.: *Design Theory*, BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1985.

[14] Brcker Th. and tom Dieck, T.: *Representation of Compact Lie Groups*, Graduate Texts in Mathematics 98, Springer, New York, 1985.

[15] Brouwer, A.E., Cohen, A.M. and Neumaier, A.: *Distance-Regular Graphs*, Ergebnisse der Mathematik and ihrer Grenzgebiete, 3. Folge, Band 18, Springer, Berlin, 1989.

[16] Bub, J.: Conditional probabilities in non-Boolean possibility structures, in: Hooker, C.A. (ed.), *The Logico-Algebraic Approach to Quantum Mechanics II*, Reidel, Dodrecht, 1979.

[17] Busch, P. and Lahti, P.J.: The Determination of the Past and the Future of a Physical System in Quantum Mechanics, *Found. Phys.* **19** (1989), 633–678.

[18] Butson, A.T.: Generalized Hadamard Matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.

[19] Cohen, D.W.: *An Introduction to Hilbert Space and Quantum Logic*, Springer, New York, 1989.

[20] Colburn, C.J. and Dinitz, J.H.: *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, FL, 1996.

[21] Curtis, C.W. and Reiner, I.: *Representation Theory of Finite Groups and Associative Algebras*, John Wiley & Sons, New York, 1962.

[22] Davis, E.B.: *Quantum Theory of Open Systems*, Academic Press, London, 1976.

[23] Davis, Ph.J.: *Circulant Matrices*, John Wiley & Sons, New York, 1979.

[24] Delsarte, P. Goethals, J.M. and Seidel, J.J.: Bounds for systems of lines and Jacobi polynomials, *Philips Res. Rep.* **30** (1975), Bouwkamp volume, 91–105.

[25] Delsarte, P. Goethals, J.M. and Seidel, J.J.: Spherical Codes and Designs, *Geom. Dedicata* **6** (1977), 363–388.

[26] Dénes, J. and Keedwell, A.D.: *Latin Squares and their Application*, Academic Press, New York, 1974.

[27] Dénes, J. and Keedwell, A.D.: *Latin Squares: New Developements in the Theory and Applications*, North-Holland, Amsterdam, 1991.

[28] Federer, W.T. and Mandeli, J.P.: Orthogonal F-rectangles, orthogonal arrays and codes, *J. Comb. Theory Ser. A* **43** (1986), 149–164.

[29] Godsil, C.D.: *Algebraic Combinatorics*, Chapman & Hall, New York, London, 1993.

[30] Goethals, J.M. and Seidel, J.J.: Spherical designs, in: Ray Chaudhuri, D.K. (ed.), *Relations Between Combinatorics and Other Parts of Mathematics*, Proc. Symp. Pure Math. **34**, AMS, Providence, 1979, pp. 255–272.

[31] Goethals, J.M. and Seidel, J.J.: Cubatur formulae, polytopes and spherical designs, in: Davis, C. (ed.), *The Geometric Vein, Coxeter Festschrift*, Springer, Berlin, 1981, pp. 203–218.

[32] Gudder, S.P.: *Quantum Probability*, Academic Press, San Diego, 1988.

[33] Hadwiger, H.: Über ausgezeichnete Vektorsteren and reguläre Polytope, *Comment. Math. Helv.* **13** (1940), 90–107.

[34] Hall, M. Jr.: *Combinatorial Theory*, 2nd ed., John Wiley & Sons, New York, 1986.

[35] Halmos, P.R.: Two subspaces, *Trans. Amer. Math. Soc.* **144** (1969), 381–389.

[36] Hardin, R.H. and Sloane, N.J.A.: New spherical 4-designs, *Discrete Math.* **106/107** (1992), 255–264.

[37] Hedayat, A. and Seiden, E.: F-square and orthogonal F-squares designs: A generalization of Latin square and orthogonal Latin squares designs, *Ann. Math. Stat.* **41** (1970), 2035–2044.

[38] Helgason, S.: *Differential geometry and symmetric spaces*, Academic Press, New York, 1962.

[39] Hoffman, K. and Kunze, R.: *Linear Algebra*, 2nd ed., Prentice-Hall, Englewood Cliffs, N.J., 1971.

[40] Hoggar, S.G.: Quaternionic equi-isoclinic n-planes, *Ars Combin.* **2** (1976), 11–13.

[41] Hoggar, S.G.: Bounds for quaternionic line systems and reflection groups, *Math. Scand.* **43** (1978), 241–249.

[42] Hoggar, S.G.: Two quaternionic 4-polytopes, in: Davis, C. (ed.), *The Geometric Vein, Coxeter Festschrift*, Springer, Berlin (1981), 219–230.

[43] Hoggar, S.G.: t-Designs in Projective Spaces, *European J. Combin.* **3** (1982), 233–254.

[44] Hoggar, S.G.: Parameters of t-designs in $\mathbb{F}P^{d-1}$, *European J. Combin.* **5** (1984), 29–36.

[45] Hoggar, S.G.: t-designs in Delsarte spaces, in: Ray Chaudhuri, D.K. (ed.), *Coding Theory and Designs Theory*, Part II, IMA Vol. 21, Springer, Berlin (1990) 144–165.

[46] Hoggar, S.G.: t-Designs with General Angel Set, *European J. Combin.* **13** (1992), 257–271.

[47] Hughes, D.R. and Piper, F.C.: *Design Theory*, Cambridge University Press, Cambridge, 1985.

[48] Karpilovsky, G.: *Projective Representations of Finite Groups*, Marcel Dekker, New York, 1985.

[49] Kirillov, A.A.: *Elements of the Theory of Representations*, Springer, Berlin, Heidelberg, New York, 1976.

[50] Klauder, J.R. and Skagerstam, B.S.: *Coherent States*, World Scientific, Singapore, 1985.

[51] Koornwinder, T.H.: A Note on the Absolute Bound for Systems of Lines, *Nederl. Akad. Wetensch. Proc. Ser. A* **79** (= *Indag. Math.* **38**), (1976), 152–153.

[52] Lemmens, P.W.H. and Seidel, J.J.: Equiangular lines, *J. Algebra* **24** (1973), 494–512.

[53] Lemmens, P.W.H. and Seidel, J.J.: Equi-isoclinic subspaces of Euclidian spaces, *Nederl. Akad. Wetensch. Proc. Ser. A* **76** (= *Indag. Math.* **35**), (1973), 98–107.

[54] Lidl, R. and Niederreiter, H.: *Finite Fields - Encyclopedia of mathematics and its applications 20*, 2nd ed., Cambridge University Press, Cambridge, 1997.

[55] van Lint, J.H. and Seidel, J.J. Equilateral point sets in elliptic geometry, *Nederl. Akad. Wetensch. Proc. Ser. A* **69** (= *Indag. Math.* **28**), (1966), 335–348.

[56] Lüders, G.: Über die Zustandsänderung durch den Meproze, *Ann. Physik* **8** (1951) 322–328.

[57] Marcus, M. and Minc, H.: *A Survey of Matrix Theory and Matrix Inequalities*, Allyn & Bacon, Boston, 1964.

[58] Mittelstaedt, P.: *Quantum Logic*, D. Reidel, Dordrecht, 1978.

[59] Moroz, B.Z.: Reflections on Quantum Logic, *Internat. J. Theoret. Phys.* **22** (1983), 329–340, Erratum, *Internat. J. Theoret. Phys.* **23** (1984), 497–498.

[60] Morton, P.: On the Eigenvectors of Schur's Matrix, *J. Number Theory* **12** (1980), 122–127.

[61] Neumaier, A.: Distances, graphs and designs, *European J. Combin.* **1** (1980), 163–174.

[62] Neumaier, A.: Combinatorial Configurations in terms of distances, Memorandum 81-09, Eindhoven University of Technology, 1981.

[63] Neumaier, A. and Seidel, J.J.: Discrete measures for spherical designs, eutactic stars and lattices, *Nederl. Akad. Wetensch. Proc. Ser. A* **91** (= *Indag. Math.* **50**), (1988), 321–334.

[64] Neumaier, A. and Seidel, J.J.: Measures of strength $2e$ and optimal designs of degree e, *Sankhyā* **54** (1992), 299–309.

[65] Parthasarathy, K. R.: *An introduction to quantum stochastic calculus*, Birkhuser, Basel, 1992.

[66] Raghavarao, D.: *Constructions and Combinatorial Problems in Design of Experiments*, John Wiley & Sons, New York, 1971.

[67] Reed, M. and Simon, B.: *Methods of Modern Mathematical Physics, I: Functional Analysis*, 2nd. ed., Academic Press, New York, 1980.

[68] Schwinger, J.: Unitary Operator Bases, *Proc. Nat. Acad. Sci. U.S.A.* **46** (1960), 570–579.

[69] Seidel, J.J.: Eutactic stars, in: Hajnal, A. and Sos, V.T. (ed.), *Combinatorics*, Colloq. Math. Soc. János Bolyai **18**, North Holland, Amsterdam, (1978), 983–999:

[70] Seidel, J.J.: Isometric embeddings and geometric designs, *Discrete Math.* **136** (1994), 281–293.

[71] Seidel, J.J.: Spherical Designs and Tensors, *Adv. Studies Pure Math.* **24** (1996), 309–321.

[72] Srinivas, M.D.: Foundations of Quantum Probability Theory, *J. Math. Phys.* **16** (1975), 1672–1685.

[73] Stulpe, W. and Singer M.: Some remarks on the determination of Quantum States by Measurement, *Found. Phys. Lett.* **3** (1990), 153–166.

[74] Thirring, W.: *Lehrbuch der Mathematischen Physik, Bd.3*, Springer, Wien, New York, 1979.

[75] Wallis, J.S.: Hadamard Matrices, in: Wallis, W.D., Street, A.P. and Wallis, J.S., *Combinatorics: Room Squares, Sum-free Sets, Hadamard Matrices*, LNM. 292, Springer, Berlin, Heidelberg, New York 1972.

[76] Wallis, W.D.: *Combinatorial Designs*, Marcel Dekker, New York, 1988.

[77] Weyl, H.: *Gruppentheorie and Quantenmechanik*, Nachdruck der 2. Auflage 1931, Wissenschaftliche Buchgesellschaft, Darmstadt, 1981.

[78] Wiesbrock, H.W.: Born's postulate and reconstruction of ψ-functions in nonrelativistic quantum mechanics, *Internat. J. Theoret. Phys.* **26** (1987), 1175–1184.

[79] Zauner, G.: *Orthogonale Lateinische Quadrate und Anordnungen, Verallgemeinerte Hadamard-Matrizen und Unabhngigkeit in der Quanten-Wahrscheinlichkeitstheorie*, Diplomarbeit, Wien, 1991.

[80] Zhang, W.M., Feng, D.H. and Gilmore, R.: Coherent states: Theory and some applications, *Rev. Modern Phys.* **62** (1990), no. 4, 867–927.