12-2013

Isolation and Deformation Results for Commuting Squares of Finite Dimensional Matrix Algebras

Joseph Robert White
University of Tennessee - Knoxville, white@math.utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Joseph Robert White entitled "Isolation and Deformation Results for Commuting Squares of Finite Dimensional Matrix Algebras." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Remus I. Nicoara, Major Professor

We have read this dissertation and recommend its acceptance:

Robert Mee, Stefan Richter, Carl Sundberg

Accepted for the Council:

Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

12-2013

Isolation and Deformation Results for Commuting Squares of Finite Dimensional Matrix Algebras

Joseph Robert White
white@math.utk.edu

To the Graduate Council:

I am submitting herewith a dissertation written by Joseph Robert White entitled "Isolation and Deformation Results for Commuting Squares of Finite Dimensional Matrix Algebras." I have examined the final electronic copy of this dissertation for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Doctor of Philosophy, with a major in Mathematics.

Remus I. Nicoara, Major Professor

We have read this dissertation and recommend its acceptance:

Robert Mee, Stefan Richter, Carl Sundberg

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

Isolation and Deformation Results for Commuting Squares of Finite Dimensional Matrix Algebras

A Dissertation Presented for the

Doctor Of Philosophy

Degree

The University of Tennessee, Knoxville

Joseph Robert White

December 2013

Dedication

I dedicate this dissertation to my family; my wife, Sarah, my daughter, Hannah, and my son, Adam. Their love, support, and encouragement have helped me tremendously. Mainly, I dedicate this dissertation to Hannah as I was not able to be the father I wanted to be for her during the first few years of her precious life. Also, when things were not going well, her smile and playful demeanor always cheered me up and kept me going.

Acknowledgements

I would like to thank Professor Remus Nicoara, my thesis advisor, for all of his help, support and encouragement during my graduate studies. His academic expertise, as well as his honesty and especially his patience, have been invaluable to my obtaining a PhD. Without his guidance, writing this dissertation would have been impossible. I especially am grateful that he accepted (and kept) me as his first PhD student.

I am also very grateful to all of the teachers in the analysis group who have done a very wonderful job teaching me and instilling an enthusiasm for analysis that I previously lacked before attending the University of Tennessee. Especially, I would like to thank Professor Carl Sundberg for all of the special topics courses he taught throughout the years. Those courses were very challenging and stimulating. The ideas presented in some of those courses have helped tremendously in the development of this dissertation.

Abstract

Commuting squares arise as algebraic-combinatorial invariants in Jones' theory of subfactors. They can also be used to construct subfactors via iterating the basic construction, and a lot of the known examples of subfactors are obtained this way. In this thesis, we use deformation techniques to investigate the structure of the moduli space of commuting squares, and of a larger class of generalized commuting squares.

In the first part of the thesis, we consider generalizations of commuting squares, called twisted commuting squares, obtained by having the commuting square orthogonality condition hold with respect to the inner product given by a faithful state on a finite dimensional matrix algebra. We present various examples of twisted commuting squares, most of which are computationally easy to work with, and we prove an isolation result. We also give an application to the theory of associative deformations of the matrix multiplication.

In the second part of the thesis, we investigate commuting squares arising from finite groups. We define the undephased defect $d(G)$ and the dephased defect $d(G)$ for a finite group G, which generalize the existing notions of defect for Fourier matrices. The undephased and dephased defects give upper bounds on the number of independent directions in which the commuting square associated to G can be deformed by any (possibly isomorphic) commuting squares, respectively by non-isomorphic commuting squares. We find a canonical basis of independent directions in which the commuting square associated to G can be deformed, and we explicitly construct parametric families of commuting squares in each of the $d(G)$ directions of this basis. In particular, we obtain parametric families of complex Hadamard matrices stemming from the Fourier matrix of non-prime dimension.

Table of Contents

Chapter 1

Summary of Main Results

In this dissertation we study commuting squares of finite dimensional von Neuman algebras; i.e. squares of inclusions of finite dimensional matrix algebras:

$$\mathfrak{C} = \begin{pmatrix} P_{-1} & \subset & P_0 & \\ \cup & & \cup, & \tau \\ Q_{-1} & \subset & Q_0 & \end{pmatrix}$$

with a faithful trace τ on P_0 such that the vector space $P_{-1} \ominus Q_{-1}$ is orthogonal to $Q_0 \ominus Q_{-1}$ with respect to the inner product defined by τ on P_0. Note that all of our traces are assumed to be normalized, i.e. $\tau(1) = 1$.

Commuting squares were introduced by Popa in [28], as invariants in Jones' theory of subfactors ([15], [13]). They encode the generalized symmetries of the subfactor and in a lot of situations are complete invariants ([28], [29]). In particular, any finite group G or order n can be encoded in a commuting square:

$$\mathfrak{C}_G = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & , \tau \\ \mathbb{C} & \subset & \mathbb{C}[G] & \end{pmatrix}$$

where $\mathrm{D} \cong \mathrm{l}^{\infty}(\mathrm{G})$ is the algebra of $n \times n$ diagonal matrices, and $\mathbb{C}[G]$ denotes the group algebra of G. It can be shown that two group commuting squares are isomorphic if and only if the corresponding groups are isomorphic. The subfactor associated to $\mathfrak{C}_G$ by iterating Jones' basic construction is a cross product subfactor. Moreover, if G is abelian, then $\mathfrak{C}_G$ is a *spin model* commuting square, and the associated subfactor is a Hadamard subfactor in the sense of [20].

In [19], Nicoara initiated a study of the deformations of a commuting square, in the class of commuting squares. It was shown that if a commuting square satisfies a certain *span condition*, then it is isolated among all non-isomorphic commuting squares. In the case of $\mathfrak{C}_G$, the span condition asks that V be equal to $\mathrm{M_n}(\mathbb{C})$, where V is the subspace of $\mathrm{M_n}(\mathbb{C})$ given by :

$$V = \mathrm{span}\{du - ud \,:\, d \in \mathrm{D}, \mathrm{u} \in \mathbb{C}[\mathrm{G}]\} + \mathbb{C}[\mathrm{G}] + \mathbb{C}[\mathrm{G}]' + \mathrm{D}.$$

When the span condition fails, the dimension $d'(G)$ of $V^{\perp} = \mathrm{M_n} \ominus \mathrm{V}$ can be interpreted as an upper bound for the number of independent directions in which $\mathfrak{C}_G$ can be deformed by non-isomorphic commuting squares. We define the following:

Definition 1.0.1. *The undephased defect of a finite group G is*

$$d(G) = n^2 - \dim_{\mathbb{C}}([\mathrm{D}, \mathbb{C}[\mathrm{G}]]).$$

The dephased defect of G is

$$d'(G) = n^2 - \dim_{\mathbb{C}}([\mathrm{D}, \mathbb{C}[\mathrm{G}]] + \mathbb{C}[\mathrm{G}] + \mathbb{C}[\mathrm{G}]' + \mathrm{D}).$$

We calculate the dephased and undephased defects of G. Let $cl(G)$ denote the class number of G; i.e. $cl(G)$ is the number of distinct conjugacy classes of G. We prove the following two theorems:

Theorem 1.1.

$$d(G) = \sum_{g \in G} \frac{|G|}{ord(g)}.$$

Theorem 1.2. *The dephased and the undephased defects of a finite group G are related as follows:*

$$d'(G) = \sum_{g \in G} \frac{|G|}{ord(g)} - 3n + 1 + cl(G).$$

We also show that $d(G)$ is the best possible bound in the following sense: there exists a basis for $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]^{\perp}$, such that for every a in the basis there is an analytic family of commuting squares containing $\mathfrak{C}_G$ and of direction a.

Theorem 1.3. *There is a basis for $\{a : a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]\}$ such that for every a in the basis there is an analytic family of commuting squares containing $\mathfrak{C}_G$ and of direction a. More precisely, for each a in the basis and $t \in \mathbb{R}$, if $U_t = e^{\mathrm{ita}}$, then*

$$\mathfrak{C}_t = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & , \tau \\ \mathbb{C} & \subset & U_t \mathbb{C}[G] U_t^* & \end{pmatrix}$$

is a commuting square.

However, we show that it is not true in general that every (hermitian of unit length) $a \in [\mathrm{D}, \mathbb{C}[\mathrm{G}]]^{\perp}$ is a direction of convergence. We also investigate what other conditions such a should satisfy. In the case of $G = \mathbb{Z}_n$, we prove that the 'second order conditions', in the sense of Nicoara ([21]), don't change the number of directions.

Theorem 1.4. *Let $G = \mathbb{Z}_n$ and $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$, then there exits $b \in \mathrm{M_n}$ such that*

- $b + b^* = a$
- $\tau(b[p, q]) = \tau(pqa^2) - \tau(paqa)$ *for all $p \in \mathrm{D}$ and $q \in \mathbb{C}[G]$.*

We also introduce a generalization of commuting squares which we call twisted commuting squares. We discuss some analogous results for them.

Chapter 2

Preliminaries

In this chapter, we cover preliminary results. We start with the span condition.

2.1 Span condition preliminaries

We now recall some definitions and results due to Nicoara (see [19]) about commuting squares that will aid in answering the question "when is a Hadamard matrix isolated?" In [5], Christensen gives the following definition:

Definition 2.1.1. *Let A be a finite dimensional von Neumann algebra with identity I and normalized trace τ. Denote by $S(A)$ the set of all $*$-subalgebras of A containing I. For B_1, $B_2 \in S(A)$ and $\delta > 0$ we say B_1 is* δ-contained *in B_2 if for every $x \in B_1$ with $||x|| = 1$ there exists $y \in B_2$ such that $||x - y||_2 < \delta$ (where $||x||_2 = \sqrt{\tau(x^*x)}$). If B_1 is δ-contained in B_2 and B_2 is δ-contained in B_2, we write $||B_1 - B_2||_{2,A} < \delta$.*

Remark 2.1.2. *Arguments from [5] show that there exists a continuous increasing function $f : [0, \infty) \to [0, \infty)$, $f(0) = 0$ such that if δ is small and $||B_1 - B_2||_{2,A} < \delta$ then $B_2 = Ad(U)(B_1) = UB_1U^*$ for some unitary $U \in A$, $||U - I||_2 < f(\delta)$.*

Definition 2.1.3. *We say that the commuting square of matrix algebras*

$$\mathfrak{C} = \begin{pmatrix} P_{-1} & \subset & P_0 & \\ \cup & & \cup, & \tau \\ Q_{-1} & \subset & Q_0 & \end{pmatrix}$$

is isolated *if there exists* $\delta > 0$ *such that if*

$$\widetilde{\mathfrak{C}} = \begin{pmatrix} \widetilde{P}_{-1} & \subset & \widetilde{P}_0 & \\ \cup & & \cup, & \tau \\ \widetilde{Q}_{-1} & \subset & \widetilde{Q}_0 & \end{pmatrix}$$

is a commuting square and $\varphi : P_0 \to \widetilde{P}_0$ *is a trace-invariant* $*$*-isomorphism satisfying*

$$||\varphi(P_{-1}) - \widetilde{P}_{-1}||_{2,\widetilde{P}_0} < \delta, \quad ||\varphi(Q_{-1}) - \widetilde{Q}_{-1}||_{2,\widetilde{P}_0} < \delta, \quad ||\varphi(Q_0) - \widetilde{Q}_0||_{2,\widetilde{P}_0} < \delta$$

then $\widetilde{C}$ *is isomorphic to* $\mathfrak{C}$*.*

For algebras $B \subset A$, we will use the notation

$$B' \cap A = \{a \in A : ab = ba, \forall b \in B\}.$$

Lemma 2.0.1. *Let*

$$\mathfrak{C} = \begin{pmatrix} P_{-1} & \subset & P_0 & \\ \cup & & \cup, & \tau \\ Q_{-1} & \subset & Q_0 & \end{pmatrix}$$

be a commuting square of finite dimensional von Neumann algebras, with trace τ*. Then* $\mathfrak{C}$ *is isolated if and only if there exists* $\epsilon > 0$ *such that if* $U \in Q_{-1}' \cap P_0$ *is a unitary with* $||U - I||_2 < \epsilon$*, and*

$$\mathfrak{C}(U) = \begin{pmatrix} P_{-1} & \subset & P_0 & \\ \cup & & \cup, & \tau \\ Q_{-1} & \subset & UQ_0U^* & \end{pmatrix}$$

is a commuting square, then $\mathfrak{C}(U)$ *is isomorphic to* $\mathfrak{C}$*.*

Now, to get a condition for isolation the idea is that if the commuting square $\mathfrak{C}$ is not isolated then there exists unitaries U_n converging to I such that $U_n \neq I$ and $\mathfrak{C}(U_n)$ are non-isomorphic commuting squares, then we may write out the commuting square condition for each n and take the "derivative" of this relationship along some "direction of convergence" of U_n. By a direction of convergence, we mean the following: let $U_n = \exp(\mathrm{ih_n}) \in \mathrm{P_0}$ for some nonzero hermitians $h_n \in P_0$ converging to 0. By the compactness of the unit ball (in the finite dimensional algebra P_0), we may assume, after passing to a subsequence, that $\frac{h_n}{||h_n||} \to h \in P_0$, $||h|| = 1$. We will refer to h as a *direction of convergence* of $(U_n)_n$.

Finally, note that $\frac{U_n - I}{\mathrm{i||h_n||}} \to h$ implies that $\frac{||U_n - I||}{||h_n||} \to ||h|| = 1$ and consequently

$$h = \lim_{n\to\infty} \frac{U_n - I}{\mathrm{i||U_n - I||}}.$$

Note the inclusion of i in the definition of h ensures that h is hermitian.

2.1.1 Span condition

For subalgebras A and B of an algebra C, let

$$[A, B] = \mathrm{span}\{ab - ba : a \in A, b \in B\}.$$

Definition 2.1.4. *We say that the commuting square*

$$\mathfrak{C}(U) = \begin{pmatrix} P_{-1} & \subset & P_0 & \\ \cup & & \cup, & \tau \\ Q_{-1} & \subset & Q_0 & \end{pmatrix}$$

satisfies the span condition *if:*

$$[P_{-1}, Q_0] + (Q'_{-1} \cap P_{-1}) + (Q'_{-1} \cap Q_0) + (P'_{-1} \cap P_0) + (Q'_0 \cap P_0) = P_0.$$

Note that in general $\dim[P_{-1}, Q_0] \leq \dim(P_0) - \dim(Q'_{-1} \cap P_{-1} + Q'_{-1} \cap Q_0 + P'_{-1} \cap P_0 + Q'_0 \cap P_0)$, so the span condition simply asks for the dimension of the commutator $[P_{-1}, Q_0]$ to be maximal.

Theorem 2.1.5. *(Nicoara 2007) If the commuting square of finite dimensional von Neumann algebras*

$$\mathfrak{C} = \begin{pmatrix} P_{-1} & \subset & P_0 \\ \cup & & \cup \, , \tau \\ Q_{-1} & \subset & Q_0 \end{pmatrix}$$

satisfies the span condition of 2.1.4, then $\mathfrak{C}$ *is isolated.*

2.2 Hadamard matrices

One of the simplest examples of commuting squares is:

$$\mathfrak{C}(U) = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup, & \tau \\ \mathbb{C} & \subset & U\mathrm{DU}^* & \end{pmatrix}$$

where D is the algebra of diagonal matrixes, $U = F_n = \frac{1}{\sqrt{n}} (\epsilon^{ij})_{0 \leq i,j \leq n-1}$ with $\epsilon = e^{\frac{2\pi \mathrm{i}}{n}}$ ([27]). Note that $U\mathrm{DU}^*$ is precisely the algebra of circulant permutation matrices.

We call F_n the *standard biunitary* of order n. More generally, one can ask for which U is $\mathfrak{C}(U)$ a commuting square. The commuting square condition asks that D and $U\mathrm{DU}^*$ be orthogonal modulo their intersection $\mathbb{C}$. For $0 \leq i \leq n-1$, let $d_i = e_{i,i}$ where $\{e_{i,j}\}_{0 \leq i,j \leq n-1}$ are the standard matrix units of $\mathrm{M_n}(\mathbb{C})$. Then for each i and j, we have

$$0 = \tau((d_i - \frac{1}{n}I)Ud_jU^*) = \tau(d_iUd_jU^*) - \frac{1}{n}\tau(d_j) = \frac{|u_{i,j}|^2}{n} - \frac{1}{n^2}.$$

Thus, U is a unitary having all entries of the same absolute value $\frac{1}{\sqrt{n}}$. Such a matrix is called a *biunitary matrix.* If we renormalize U so that all entries of U are unimodular, then we say U is a *(complex) Hadamard matrix.* Note that we will interchangeably use H is a complex Hadamard matrix if $HH^* = nI_n$ and all entries of H are unimodular.

Two Hadamard matrices, H_1 and H_2, are *equivalent* if there exists unitary diagonal matrices D_1, D_2 and permutation matrices P_1, P_2 such that

$$H_2 = P_1D_1H_2D_2P_2.$$

It is easy to see that H_1 and H_2 are equivalent if and only if $\mathfrak{C}(H_1)$ and $\mathfrak{C}(H_2)$ are isomorphic as commuting squares, i.e. conjugate by a unitary from $\mathrm{M_n}(\mathbb{C})$. Note that the operations allowed in this definition are precisely the operations one can do to H_2 in order to maintain the orthogonality of D and $H_2\mathrm{DH}_2^*$ modulo $\mathbb{C}$. Furthermore, it is clear that any Hadamard matrix is equivalent to a Hadamard matrix with the first row and first column consisting of 1s.

Definition 2.2.1. *A complex Hadamard matrix is called* dephased *if the entries of its first row and column are all equal to 1:*

$$H_{1,i} = H_{i,1} = 1 \quad \textit{for } i = 1, \ldots, n.$$

For every n composite, one may construct infinitely many non-equivalent Hadamard matrices by certain modifications of the elements of the Fourier matrix. For example, if $n = 4$

$$U(\lambda) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \lambda & -\lambda \\ 1 & -1 & -\lambda & \lambda \end{pmatrix}$$

where $|\lambda| = 1$ is a one-parameter family of Hadamard matrices.

Now we apply Theorem 2.1.5 to commuting squares given by Hadamard matrices. Since the algebras D and $U\mathrm{DU}^*$ are abelian and orthogonal modulo their intersection $\mathbb{C}I$ the span condition becomes:

$$\dim([\mathrm{D}, \mathrm{UDU}^*]) = \mathrm{n}^2 - 2\mathrm{n} + 1 = (\mathrm{n} - 1)^2.$$

Thus, we have the following:

Proposition 2.2.2. *If $U \in \mathrm{M_n}(\mathbb{C})$ is a biunitary matrix such that the dimension of the vector space $[\mathrm{D}, \mathrm{UDU}^*]$ is $n^2 - 2n + 1$, then U is isolated among all biunitaries (up to equivalence).*

Note that intuitively, the quantity $(n-1)^2 - \dim[\mathrm{D}, \mathrm{UDU}^*]$ measures *how many parametric families* should pass through U (1 for each possible direction of convergence). Furthermore, the theorem is only one implication. It is currently unknown whether the span condition is both necessary and sufficient.

Independently, Tadej and Życzkowski ([33]) found an equivalent way to decide when a Hadamard matrix was isolated.

Definition 2.2.3. *The* defect *$d(H)$ of an $n \times n$ complex Hadamard matrix H is the dimension of the solution space of the real linear system with respect to a matrix variable $R \in \mathbb{R}^{n^2}$:*

$$R_{1,j} = 0 \quad j \in \{2, \dots, n\}$$

$$R_{i,1} = 0 \quad i \in \{2, \dots, n\}$$

$$\sum_{k=1}^{n} H_{i,k}\overline{H}_{j,k}(R_{i,k} - R_{j,k}) = 0 \quad 1 \leq j, k \leq n.$$

Using the defect, we may formulate a condition that ensures isolation:

Lemma 2.0.2. *A dephased complex Hadamard matrix H is isolated if $d(H) = 0$.*

Next, we will give a little background for how the idea of the defect came about. Let U_n denote the unitary group of matrices of order n. Let C_n denote the set of complex Hadamard matrices and note that

$$C_n = \mathrm{M_n}(\mathbb{T}) \cap \sqrt{\mathrm{n}}\mathrm{U_n}$$

is a real algebraic manifold. Tadej and Życzkowski compute the "enveloping tangent space" at a complex Hadamard matrix $H \in \mathrm{M_n}$, given by:

$$\tilde{T}_H C_N = T_H \mathrm{M_n}(\mathbb{T}) \cap \mathrm{T_H}\sqrt{\mathrm{n}}\mathrm{U_n}.$$

In [1], Banica gives a strict algebraic interpretation in our setting of the results of Tadej and Życzkowski. Let $\mathrm{M'_n}(\mathbb{C}) \subset \mathrm{M_n}(\mathbb{C})$ be the set of matrices which have 1s on the first row and column. Let $D_n = C_n \cap \mathrm{M'_n}(\mathbb{C})$. Then D_n is simply the submanifold of C_n consisting of dephased matrices. We get the following theorem by using some basic differential geometry:

Theorem 2.2.4. *We have a canonical identification*

$$\tilde{T}_H C_n = \{A \in \mathrm{M_n}(\mathbb{R}) : \sum_{\mathrm{k}} \mathrm{H_{i,k}}\overline{\mathrm{H}}_{\mathrm{j,k}}(\mathrm{A_{i,k}} - \mathrm{A_{j,k}}) = 0\}$$

and $\tilde{T}_H D_n$ consists of the matrices $A \in \tilde{T}_H C_n$ having 0 on the first row and column.

It is a fact that for a Hadamard matrix H and if $U = \frac{1}{\sqrt{n}}H$, the defect and the span condition are related by

$$d(H) = (n-1)^2 - \dim[\mathrm{D}, \mathrm{UDU}^*].$$

In the following sections, we give an overview of some of the known results related to Hadamard matrices.

2.2.1 Real Hadamard matrices

Hadamard matrices were first introduced in 1867 by Sylvester in [32]. Originally, all entries were required to be ± 1; i.e. a *real Hadamard matrix.* Unlike complex Hadamard matrices, real Hadamard matrices can only exist when $n = 1$, 2 or is a multiple of 4. Indeed, for $n > 2$, suppose H is a normalized Hadamard matrix (all entries in the first row are 1). Consider the first three rows of H. Since H is normalized, each column of the first three rows must have one of the following four forms:

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}.$$

Let the numbers of columns of such forms be denoted by x, y, z, and w. Since the rows are orthogonal, x, y, z, and w satisfy

$$\begin{aligned} x + y + z + w &= 1 \\ x + y - z - w &= 0 \\ x - y + z - w &= 0 \\ x - y - z + w &= 0 \end{aligned}$$

which has only one solution, $x = y = z = w = \frac{n}{4}$. Thus, n is a multiple of 4.

Conjecture 2.2.5. *(Hadamard) For $n = 4k$, there exists a real Hadamard matrix.*

It has been verified that the conjecture holds for every multiple of 4 up to 664. In fact, 668, 716 and 892 are the only multiples up to 1000 for which there is no known Hadamard matrix. The real Hadamard matrices play an important role in statistics (mainly in designs of experiments). Let S be a set of s symbols or levels. We recall the following definition:

Definition 2.2.6. *An $N \times k$ array A with entries from S is said to be an* orthogonal array *with s levels, strength t (for $0 \leq t \leq k$), and index λ if every $N \times t$ subarray of A contains each t-tuple based on S exactly λ times as a row.*

Note that the term levels is frequently used because these arrays arise in designs of experiments where the symbols typically indicate the levels or settings of the factors (variables) whose effects on the response variable are of interest in the experiment. It is a fact that λ is determined by the other parameters since $\lambda = \frac{N}{s^t}$. Therefore, we notate such an orthogonal array by $OA(N, k, s, t)$. It is easy to see that $\mathrm{OA}(4\lambda, 4\lambda - 1, 2, 2)$ exists if and only if there is a Hadamard matrix of order 4λ. There are several constructions yielding various orders of *real* Hadamard matrices (see Chapter 14 of [10]). In [10], constructions producing the following orders where p is an odd prime are described:

- 2^r
- $p^r + 1 \equiv 0 \pmod 4$
- $h(p^r + 1)$, h the order of a Hadamard matrix
- $h(h - 1)$, h a product of numbers of the form 2^r and $p^r + 1 \equiv 0 \pmod 4$
- $h(h + 3)$ with h and $h + 4$ as above
- $h_1 h_2 (p^r + 1) p^r$ where h_1 and h_2 are orders of Hadamard matrices
- $h_1 h_2 s(s + 3)$ with h_1, h_2 as above and s, $s + 4$ of the form $p^r + 1$
- $q(q + 2) + 1$, q and $q + 2$ of the form p^r.

Most of these constructions use constructions due to Paley. In [25], we get:

Theorem 2.2.7. *Let p be a prime, $p \equiv 3 \pmod 4$, and consider the matrix $Q \in M_p(\mathbb{R})$ defined by:*

$$Q_{i,j} = \begin{cases} 1 & \text{if } i-j \text{ is a quadratic residue mod } p \\ -1 & \text{if } i-j \text{ is a quadratic non-residue mod } p \\ 0 & \text{if } i=j \end{cases}$$

Then

$$H_{p+1} = \begin{pmatrix} 1 & 1_p \\ -1_p^T & Q+I_p \end{pmatrix}$$

where 1_p denotes the $p \times 1$ row matrix of 1s and I_p is the $p \times p$ identity matrix is a Hadamard matrix of order $p+1$.

Recall, $a \neq 0$ is a quadratic mod p if there exists x such that $a \equiv x^2 (\text{mod } p)$. Note that Q is a *conference matrix*. Furthermore, if $p \equiv 1 \pmod 4$, we still can get a Hadamard matrix using the same Q as above. Indeed, by letting

$$S = \begin{pmatrix} 0 & 1_p \\ 1_p^T & Q \end{pmatrix}$$

we get that

$$H_{2(p+1)} = \begin{pmatrix} S+I_{p+1} & S-I_{p+1} \\ S-I_{p+1} & -S-I_{p+1} \end{pmatrix}$$

is a Hadamard matrix of order $2(p+1)$.

2.2.1.1 Application

Real Hadamard matrices are useful in the theory of codes. To each real Hadamard matrix, we may associate a code. We recall some standard definitions from coding theory.

Definition 2.2.8. *Let A be an alphabet. A* code over *A is a subset C of A^n for some positive integer n. We say that n is the length of the code. The elements of C are called* codewords. *We say that $|C|$ is the* size *of the code. The* distance *of a code is the minimum* Hamming distance *between any two distinct codewords, i.e., the minimum number of positions at which two distinct codewords differ.*

Definition 2.2.9. *If C is a code of length n, size M and minimum distance d then C is said to be a (n, M, d)*-code.

Definition 2.2.10. *A* binary code *is a code over* $\{0, 1\}$.

Definition 2.2.11. *Let H_n be a real Hadamard matrix. A Hadamard code of length n, denoted Had_n, is the binary code derived from H_n by replacing all -1 values with 0 in H_n and then taking all the rows of H_n and their complements as codewords.*

Note that since any two rows of H differ in exactly $\frac{n}{2}$ positions, the minimum distance of the code is $\frac{n}{2}$.

Proposition 2.2.12. *Let H_n be a Hadamard matrix. Then, the Hadamard code Had_n derived from H_n is a binary $(n, 2n, \frac{n}{2})$-code.*

To decode a code, we have to unravel it. Let $t = \lfloor (\frac{n}{2} - 1)/2 \rfloor = \frac{n-4}{4}$ be its *error-correcting capacity*. Given a vector y of length n, $y \in \{0, 1\}^n$, let $\hat{y}$ be the result of replacing 0 with -1 in y. First compute $\hat{y}^T H_n$, then take the maximum absolute value as a codeword; if it is positive, the codeword came from H_n and if it is negative, the codeword came from $-H_n$.

The code (32, 64, 16) was used between 1969 and 1972 by the Mariner spacecraft to transmit images of Mars with 6-bit datawords, which represented 64 grayscale values. Note that with this code, errors of up to 7 bits per word can be corrected using this scheme.

2.2.2 Complex Hadamard matrices

A natural question one asks is "how many Hadamard matrices exist (up to equivalence) for each n?" While all Hadamard matrices of orders up to 5 are classified with $n = 5$ done in a paper by Haageruup ([9]), it seems very hard to describe Hadamard matrices of higher orders, such a classification not being known even for $n = 6$. For n composite, some constructions of parametric families of Hadamard matrices whose entries are linear functions (also called affine families, see [33]) are presented in papers by Diţă and Matolcsi and Szöllősi ([6],[17]). There is however no general procedure of constructing such families with non-affine entries, or for n prime. A catalogue of most known complex Hadamard matrices of small order (up to order 16) can be found in [33].

We will show the classification for $n = 3$ and 4. For $n = 5$, the solution is already non-trivial and the computations already require a few lemmas. We recall the following lemmas about algebraic manipulations of complex numbers.

Lemma 2.0.3. *If $x, y, z \in \mathbb{C}$ such that $|x| = |y| = |z| = 1$ and $x + y + z = 0$, then $x = z\epsilon$ and $y = z\epsilon^2$ where $\epsilon \in \{\frac{1}{2} + \frac{\mathrm{i}\sqrt{3}}{2}, \frac{1}{2} - \frac{\mathrm{i}\sqrt{3}}{2}\}$.*

Proof. Conjugating $x + y + z = 0$ we obtain $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 0$. Solving and eliminating x, we get $\frac{1}{y+z} = \frac{1}{y} + \frac{1}{z}$ or equivalently $\left(\frac{y}{z}\right)^2 + \frac{y}{z} + 1 = 0$. Thus, $y = \epsilon z$ with ϵ as above. Since $1 + \epsilon + \epsilon^2 = 0$, $x = -y - z = -z(1 + \epsilon) = \epsilon^2 z$.

■

It is now easy to see that up to equivalence there is only one Hadamard matrix of order 3. Indeed, if H is a Hadamard matrix of order 3 we may normalize it (i.e. put it into dephased form) and assume

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & x_1 & x_2 \\ 1 & y_1 & y_2 \end{pmatrix}.$$

Applying the lemma, we have $x_1 = \epsilon$ and $y_1 = \epsilon^2$ with ϵ with ϵ as defined in the lemma. The orthogonality of the 2nd and 3rd columns gives $x_2 = \epsilon^2$ and $y_2 = \epsilon$. Thus, all order 3 Hadamard matrices are equivalent to F_3.

Lemma 2.0.4. *If $x, y, z, t \in \mathbb{C}$ such that $|x| = |y| = |z| = |t| = 1$ and $x + y + z + t = 0$, then $x \in \{-y, -z, -t\}$.*

Proof. A routine calculation shows

$$\begin{aligned}(x+y)(x+z)(x+t) &= x^2(x+y+z+t) + xyz + xyt + xzt + yzt \\ &= xyz + xyt + xzt + yzt \\ &= xyzt(\overline{x} + \overline{y} + \overline{z} + \overline{t}) = 0.\end{aligned}$$

■

We use this lemma to classify the Hadamard matrices of order 4. After normalizing so that the first row and column are 1s, the lemma says each row and column of H must contain at least one -1. In fact, we must have a column which has two -1s. If this is the case, then H is equivalent to a matrix of the form:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \lambda & -\lambda \\ 1 & -1 & -\lambda & \lambda \end{pmatrix}$$

where $|\lambda| = 1$. Suppose that H doesn't have two -1s in a column. Then H is equivalent to

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & x & -x \\ 1 & -x & -1 & x \\ 1 & x & -x & -1 \end{pmatrix}.$$

The orthogonality of the 2nd and 3rd columns gives $0 = 1 - \overline{x} + x - |x|^2 = x - \overline{x}$. Thus, $x = \pm 1$ and hence H does indeed contain a column with two -1s. Therefore, H is equivalent to:

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \lambda & -\lambda \\ 1 & -1 & -\lambda & \lambda \end{pmatrix}$$

for some $|\lambda| = 1$. Hence, we have a 1−D orbit of Hadamard matrices when $n = 4$.

As n gets bigger, the problem of classifying all equivalence classes gets much more difficult. The difficulty lies in trying to extend these lemmas to higher orders so that we may reduce the number of parameters in the dephased form. In 1996, Haagerup ([9]) showed that for $n = 5$, all Hadamard matrices are equivalent to F_5. The calculations already rely on roughly 12 pages of algebraic manipulations and lemmas. In fact, many of the computations ultimately rely on the following lemma and some careful analysis of what the entries must be:

Lemma 2.0.5. *Let* $|u| = |v| = |s| = |t| = 1$. *Then*

$$(u + v)(\overline{s} + \overline{t})(\overline{u}s + \overline{v}t) \in \mathbb{R}.$$

Proof. The idea is simply to expand the quantity in the lemma and regroup using the basic fact that $z + \overline{z} \in \mathbb{R}$ for all $z \in \mathbb{C}$. Indeed,

$$\begin{aligned}(u + v)(\bar{s} + \bar{t})(\bar{u}s + \bar{v}t) &= (u\bar{s} + v\bar{t} + u\bar{t} + v\bar{s})\,(\bar{u}s + \bar{v}t) \\ &= 2 + (u\bar{v}\bar{s}t + \bar{u}vs\bar{t}) + (\bar{u}v + u\bar{v}) + (\bar{s}t + s\bar{t})\,.\end{aligned}$$

■

For $n = 6$, a complete classification is unknown; however, Beauchamp and Nicoara ([2]) have classified all *self-adjoint* Hadamard matrices. They obtain the following one-parameter non affine family:

$$B_6^{(1)}(\theta) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \overline{x} & -y & -\overline{x} & y \\ 1 & x & -1 & t & -t & -x \\ 1 & -\overline{y} & \overline{t} & -1 & \overline{y} & -\overline{t} \\ 1 & -x & -\overline{t} & y & 1 & \overline{z} \\ 1 & \overline{y} & -\overline{x} & -t & z & 1 \end{pmatrix}$$

where $\theta \in \left[-\pi, -\arccos\left(\frac{-1+\sqrt{3}}{2}\right)\right] \cup \left[\arccos\left(\frac{-1+\sqrt{3}}{2}\right), \pi\right]$ and the variables x, y, z, and t are given by:

$$\begin{aligned} y &= \exp(\mathrm{i}\theta) \\ z &= \frac{1+2y-y^2}{y(-1+2y+y^2)} \\ x &= \frac{1+2y+y^2-\sqrt{2}\sqrt{1+2y+2y^3+y^4}}{1+2y-y^2} \\ t &= \frac{1+2y+y^2-\sqrt{2}\sqrt{1+2y+2y^3+y^4}}{-1+2y+y^2}. \end{aligned}$$

A search for a *symmetric* analogue of the above matrices yields the following classification of symmetric matrices found by Matolcsi and Szöllősi in [18]:

$$M_6^{(1)}(x) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x & x & -x & -x \\ 1 & x & a & b & c & d \\ 1 & x & b & a & d & c \\ 1 & -x & c & d & e & f \\ 1 & -x & d & c & f & e \end{pmatrix}$$

where

$$a = \frac{x^2 - 2x - 1}{4} + \mathrm{i}\frac{(\mathrm{x}^2 - 2\mathrm{x} - 1)\sqrt{16 - |\mathrm{x}^2 - 2\mathrm{x} - 1|^2}}{4\,|\mathrm{x}^2 - 2\mathrm{x} - 1|}$$
$$b = \frac{x^2 - 2x - 1}{4} - \mathrm{i}\frac{(\mathrm{x}^2 - 2\mathrm{x} - 1)\sqrt{16 - |\mathrm{x}^2 - 2\mathrm{x} - 1|^2}}{4\,|\mathrm{x}^2 - 2\mathrm{x} - 1|}$$
$$c = -\frac{x^2 + 1}{4} + \mathrm{i}\frac{(\mathrm{x}^2 + 1)\sqrt{16 - |\mathrm{x}^2 + 1|^2}}{4\,|\mathrm{x}^2 + 1|}$$
$$d = -\frac{x^2 + 1}{4} - \mathrm{i}\frac{(\mathrm{x}^2 + 1)\sqrt{16 - |\mathrm{x}^2 + 1|^2}}{4\,|\mathrm{x}^2 + 1|}$$
$$e = \frac{x^2 + 2x - 1}{4} + \mathrm{i}\frac{(\mathrm{x}^2 + 2\mathrm{x} - 1)\sqrt{16 - |\mathrm{x}^2 + 2\mathrm{x} - 1|^2}}{4\,|\mathrm{x}^2 + 2\mathrm{x} - 1|}$$
$$f = \frac{x^2 + 2x - 1}{4} - \mathrm{i}\frac{(\mathrm{x}^2 + 2\mathrm{x} - 1)\sqrt{16 - |\mathrm{x}^2 + 2\mathrm{x} - 1|^2}}{4\,|\mathrm{x}^2 + 2\mathrm{x} - 1|}$$

and $x \neq \pm \mathrm{i}$ is any unimodular number.

The next example is perhaps the most well-known example of order 6. It is of *Butson-type*.

Definition 2.2.13. *We say that a complex Hadamard matrix H of order n is of* Butson-type*, if H is composed from the $q-th$ roots of unity for some q. This class of matrices is denoted by $BH(n,q)$.*

The following example was found by Butson in [4] and is in $BH(6,3)$:

$$S_6^{(0)} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega^2 & \omega^2 & \omega \\ 1 & \omega & 1 & \omega & \omega^2 & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega & \omega^2 & \omega^2 & \omega & 1 \end{pmatrix}$$

where ω is a primitive third root of unity. The reason this matrix is so well-known is that Tao ([34]) used it to disprove Fuglede's conjecture:

Conjecture 2.2.14. *A domain Ω admits a spectrum if and only if it is possible to tile $\mathbb{R}^n$ by a family of translates $\{t+\Omega : t \in \Lambda\}$ of Ω (ignoring sets of measure 0).*

We recall that $\Lambda \subset \mathbb{R}^n$ is a *spectrum* of Ω if $\{\frac{1}{\sqrt{|\Omega|}} e^{2\pi \mathrm{i} \mathrm{x} \cdot \xi}\}_{\xi \in \Lambda}$ is an orthonormal basis of $L^2(\Omega)$. In [8], Fuglede proved this conjecture (also known as the spectral set conjecture) under the additional assumption that the tiling set or the spectrum are lattice subsets of $\mathbb{R}^n$.

2.2.2.1 Isolation results

It turns out that the span condition is satisfied for $S_6^{(0)}$; so, it is isolated. Randomly chosen members, U, of the other families of Hadamard matrices above all have $(n-1)^2 - \dim[\mathrm{D}, \mathrm{UDU}^*] = 4$. Hence, all of them, except for the single isolated point $S_6^{(0)}$, *might* be part of a larger four-parameter family. Furthermore, numerical experiments done by Skinner, Newell, and Sanchez seem to confirm the presence of a four-parameter family in a neighborhood of the Fourier matrix, F_6 ([31]). Thus, we have the following conjecture, which is widely believed to be true:

Conjecture 2.2.15. *There is a four-parameter family of complex Hadamard matrices of order 6 containing the Fourier matrix or order 6, F_6.*

In fact, recently, in a PhD thesis by Szöllősi ([18]), more evidence has come to light. He *constructs* a family of order 6 matrices that has four parameters; however, the construction is not explicit. Furthermore, it is unclear if the Fourier matrix is included in this four parameter family. Recently, Diţă in [7] has come up with another construction that yields four-parameter families; however, "the peculiarity of all of them is that they are long matrices which can be stored and viewed only in an electronic format". Thus, the question still remains.

Naturally, we should ask the question about whether F_n is isolated as it is a well-known matrix with many applications throughout mathematics. With the span condition, one can get a simple proof (see [19]) of the following result due to Petrescu ([26]):

Theorem 2.2.16. *F_n is isolated if and only if n is prime.*

We will give some background and interesting results that arose in thinking about this problem.

Problem 2.2.17. *(S. Popa, 1981) For p prime, is F_p the only Hadamard matrix of order p? (Up to equivalence of course)*

It took almost a decade to answer this question. In 1990-1992, de la Harpe-Jones and Munemassa-Watatani constructed another example of a Hadamard matrix for every prime $p > 5$, obtained as a *circulant* matrix with 1st row

$$\begin{pmatrix} x_1 & x_2 & \dots & x_{p-1} & x_p \end{pmatrix}$$

with entries $x_1 = 1$, $x_i = \alpha$ or β for $i > 1$, depending on whether i is or is not a quadratic residue mod p (for some complex numbers $|\alpha| = |\beta| = 1$).

A related problem is due to Enflo:

Problem 2.2.18. *(Enflo, 1983) Is it true that for p prime there exists a unique $x : \mathbb{Z}_p \to \mathbb{T}$ such that x, $\hat{x}$ are both unimodular where $\hat{x}$ is the Fourier transform of $\mathbb{Z}_p$?*

Björck solved this problem for $p > 7$ using the same example that de la Harpe-Jones and Munemassa-Watatani came up with above. It turns out that classifying *circulant* Hadamard matrices is equivalent to Björck's problem of classifying *cyclic n-roots* ([3]).

Consequently, the problem shifted to answering whether or not the number of Hadamard matrices of prime order was *finite*. Haagerup proved that for every n prime there are finitely many *circulant* Hadamard matrices. It would seem that the number of Hadamard matrices of prime order is finite; however, in 1994, Petrescu constructed examples of one-parameter families of inequivalent Hadamard matrices for $n = 7$, 13, 19, 31, and 79. One of the examples found for $n = 7$ is:

$$U(\lambda) = \begin{pmatrix} \lambda\omega & \lambda\omega^4 & \omega^5 & \omega^3 & \omega^3 & \omega & 1 \\ \lambda\omega^4 & \lambda\omega & \omega^3 & \omega^5 & \omega^3 & \omega & 1 \\ \omega^5 & \omega^3 & \overline{\lambda}\omega & \overline{\lambda}\omega^4 & \omega & \omega^3 & 1 \\ \omega^3 & \omega^5 & \overline{\lambda}\omega^4 & \overline{\lambda}\omega & \omega & \omega^3 & 1 \\ \omega^3 & \omega^3 & \omega & \omega & \omega^4 & \omega^5 & 1 \\ \omega & \omega & \omega^3 & \omega^3 & \omega^5 & \omega^4 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

where $|\lambda| = 1$ and ω is a primitive 6-th root of unity.

2.2.2.2 Banica's results

In this section, we give some motivation to the ideas that led to Chapter 3. In [1], Banica gives the following definitions:

Definition 2.2.19. *Associated to a complex Hadamard matrix $H \in \mathrm{M_n}(\mathbb{C})$ are:*

- *the* dephased defect $d'(H) = \dim(\tilde{T}_H D_n)$
- *the* undephased defect $d(H) = \dim(\tilde{T}_H C_n)$

where C_n is the set of complex Hadamard matrices in $\mathrm{M_n}(\mathbb{C})$ (which is a real algebraic manifold) and D_n denotes the set of dephased complex Hadamard matrices which is a real algebraic submanifold of C_n.

Observe that $d'(H)$ is precisely the defect introduced by Tadej and Życzkowski in [33]. It is easy to see that $d(H)$ and $d'(H)$ are related by:

Proposition 2.2.20. $d'(H) = d(H) - 2n + 1$.

In [33], the (dephased) defect of the Fourier matrix is calculated as:

$$d'(F_n) = \begin{cases} 1 - N + 2\sum_{l=1}^{\frac{n-1}{2}} \gcd(n,l) & \text{for } n \text{ odd} \\ 1 - \frac{n}{2} + 2\sum_{l=1}^{\frac{n}{2}-1} \gcd(n,l) & \text{for } n \text{ even.} \end{cases}$$

Note that to a finite abelian group, we may associate a "generalized Fourier matrix". More precisely, suppose $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ is a finite abelian group, then

$$F_G = F_{n_1} \otimes \ldots F_{n_r}.$$

In [1], Banica shows that the defect of F_G is simply

$$d(F_G) = \sum_{g \in G} \frac{|G|}{\operatorname{ord}(g)}.$$

In Chapter 3, we will generalize the notion of the defect associated to a finite abelian group to *any* finite group. In particular, we will obtain a simpler proof to the formula given above.

2.2.2.3 Application

In this section, we will give an application related to Hadamard matrices. From quantum information theory, we have the following definition:

Definition 2.2.21. *Two orthonormal bases of $\mathbb{C}^n$, $\mathcal{B}_1$ and $\mathcal{B}_2$ are called* mutually unbiased *if for every $e \in \mathcal{B}_1$ and $f \in \mathcal{B}_2$ we have $|\langle e, f\rangle| = \frac{1}{\sqrt{n}}$. A collection of orthonormal bases $\{\mathcal{B}_i\}_{1\le i\le m}$ are called (pairwise) mutually unbiased if $\mathcal{B}_i$ and $\mathcal{B}_j$ are mutually unbiased for $i \neq j$.*

Mutually unbiased bases are referred to as MUBs. Clearly, we may identify each $\mathcal{B}_i$ with a unitary matrix B_i of order n, whose rows are simply the basis vectors in $\mathcal{B}_i$. It is easy to see that by fixing $B_1 = I$, every other B_i is a complex Hadamard matrix (up to a scaling factor). Therefore, understanding MUBs requires understanding complex Hadamard matrices and vice-versa.

A natural question one asks is:

Problem 2.2.22. *Decide the maximal number of MUBs in* $\mathbb{C}^n$ *for any* n.

It is easy to see that if $\{I, \frac{1}{\sqrt{n}}H_2, \ldots, \frac{1}{\sqrt{n}}H_m\}$ is a collection of MUBs, then $\frac{1}{\sqrt{n}}H_iH_j^*$ are complex Hadamard matrices for every $2 \leq i < j \leq m$. Note the similarity to maximal abelian subalgebras (MASAs). In $\mathrm{M_n}(\mathbb{C})$, it is easy to see that the only MASAs are $U\mathrm{D_n}\mathrm{U}^*$ where $\mathrm{D_n}$ denotes the diagonal matrices in $\mathrm{M_n}(\mathbb{C})$ and U is a Hadamard matrix. Thus, a collection of MUBs also gives rise to a collection of *orthogonal* MASAs. Therefore, we have the following:

Proposition 2.2.23. *There are at most* $n+1$ *MUBs in* $\mathbb{C}^n$ *and at most* $\frac{n}{2}+1$ *real MUBs in* $\mathbb{R}^n$.

The upper bound of $n+1$ is achieved for prime powers. In [11], we have the following:

Theorem 2.2.24. *For every prime power* $n = p^k$ *there is a complete set of MUBs consisting of* $p^k + 1$ *bases in* $\mathbb{C}^n$.

For n composite, the task remains elusive and does not have an obvious answer either numerically or algebraically. It is easy to find a lower bound using the tensor product of matrices (which preserves Hadamard matrices).

Proposition 2.2.25. *Suppose there are* m_1 *and* m_2 *MUBS in* $\mathbb{C}^{n_1}$ *and* $\mathbb{C}^{n_2}$, *respectively. Then there exists at least* $\min\{m_1, m_2\}$ *MUBs in* $\mathbb{C}^{n_1 n_2}$.

Using the theorem above and noting the smallest prime divisor can be 2, we have the following:

Corollary 2.2.26. *For every* $n > 1$, *there is a triplet of MUBs in* $\mathbb{C}^n$.

Our interest in Hadamard matrices, mainly in obtaining one-parameter families of non-equivalent Hadamard matrices, comes from the possibility of constructing subfactors from the corresponding commuting squares (see for instance [14]). However, it is hard to decide if such subfactors are non-isomorphic, or to compute their principal graphs.

2.3 Subfactors from commuting squares

2.3.1 Preliminaries

In this section we review some concepts and results of subfactor theory. The references we use are [12], [28], [29], [30].

Definition 2.3.1. *A* von Neumann algebra *is a $*$-subalgebra, M, of $B(H)$ such that the identity operator is in M and*

$$M = \overline{M}^{s.o.}.$$

Let $M' = \{T \in B(H) : TM = MT\}$. We have the following algebraic characterization of von Neumann algebras:

Theorem 2.3.2. *(von Neumann's bicommutant theorem) M is a von Neumann algebra if and only if $M = M''$.*

Definition 2.3.3. *We say a von Neumann algebra M is a* factor *if it has trivial center, i.e. $M \cap M' = \mathbb{C}$. A von Neumann algebra N is a* subfactor *of M if N is a factor and $N \subset M$.*

Recall, we say M is *finite* if every isometry $v \in M$ is a unitary. We have the following classification of factors:

- if M has minimal projections, we say it is of type I.
  - If M is finite, then it is of type I_n for some positive integer n and in which case $M = B(H) = \mathrm{M_n}(\mathbb{C})$.

– If M is infinite, then it is of type I_∞. In this case, $M = B(H)$ with $\dim H = \infty$.

- If M has no minimal projections, then we have the following:
  - if M is finite, we say it is of type II_1.
  - if M is infinite, we have the following dichotomy:
    * if M is seminfinite, we say it is of type II_∞. Here, $M = N \otimes B(H)$ where N is a type II_1 factor.
    * if M is purely infinite, we say it is of type III.

We restrict ourselves to the case of M being a von Neumann algebra with a faithful normal trace τ. A faithful normal trace τ is a functional satisfying

- τ is a positive linear functional with $\tau(1) = 1$
- τ is faithful, i.e. for all $x \in M$, $\tau(x^*x) = 0$ implies $x = 0$
- τ is normal, i.e. τ is weakly continuous on $(M)_1$, the unit ball of M with respect to the uniform norm $||\cdot||_\infty$
- τ is a trace, i.e. for all $x, y \in M$, $\tau(xy) = \tau(yx)$.

Let $N \subset M$ be an inclusion of von Neumann algebras with a faithful normal tracial state τ. We will denote by $||x||_2 = \sqrt{\tau(x^*x)}$ the Hilbert norm given by τ on M, and denote by $L^2(M, \tau)$ the completion of M in this norm. Elements $x \in M$ will be denoted $\hat{x}$ when regarded as vectors in $L^2(M, \tau)$.

M acts on $L^2(M, \tau)$ by left and right multiplication, which we will denote as $L(x)$, $R(x) \in B(L^2(M, \tau))$ for $x \in M$. We identify M with $L(M) \subset B(L^2(M, \tau))$. Let $J_M(\hat{x}) = \widehat{x^*}$ be the *canonical conjugation*. Then $J_M L(x) J_M = R(x^*)$ and hence, $J_M L(M) J_m = R(M)$.

2.3.2 Jones' Basic Construction

Let $N \subset M \subset B(L^2(M,\tau))$ be an inclusion of von Neumann algebras. Let $e_N \in B(L^2(M,\tau))$ denote the orthogonal projection of $L^2(M,\tau)$ onto the subspace $L^2(N,\tau)$. So, for $x \in M$ $e_N(\hat{x}) = \widehat{E_N(x)}$ where E_N is the unique τ-preserving conditional expectation from M onto N. We have

(a) $e_N x e_N = E_N(x) e_N$, for all $x \in M$

(b) $N = \{x \in M : [x, e_N] = 0\}$ where $[x, e_N] = x e_N - e_N x$

(c) $y e_N = 0$ with $y \in N$ implies $y = 0$

(d) $J_M e_N = e_N J_M$.

Let $M_1 = \langle M, e_N \rangle$ be the von Neumann algebra generated by M, e_N in $B(L^2(M,\tau))$. We will also denote M_1 by $\langle M, N \rangle$. Let $Tr_{\langle M,N \rangle}$ be the unique semifinite faithful normal trace on M_1 such that $Tr_{\langle M,N \rangle}(x e_N y) = \tau(xy)$ for all $x, y \in M$. $(\langle M,N \rangle, Tr_{\langle M,N \rangle})$ is called the *basic construction* (Jones, [12]). We have the following properties:

(a) $M_1 = \{x e_N y : x, y \in M\}'' = J_M N' J_M$ where $N' = \{x \in B(L^2(M,\tau)) : [x, N] = 0\}$.

(b) $e_N M_1 e_N = N e_N$.

We would like for the trace on $\langle M, e_N \rangle$ to extend τ in a natural way.

Definition 2.3.4. *If P is a subalgebra of $\langle M, e_N \rangle$, a trace τ_1 on $\langle M, e_N \rangle$ is called a* (λ, P) trace *or* λ-Markov trace *if τ_1 extends τ and $\tau_1(e_N x) = \lambda \tau(x)$ for all $x \in P$.*

In the case that such a trace exists for $M_1 = \langle M, e_N \rangle$, we say $N \subset M$ is a λ-*Markov inclusion*. If N, M are finite dimensional and $N \subset M$ has irreducible inclusion matrix T, then the trace τ is Markov if and only if it is given by the unique Perron-Frobenius vector of TT^* ([12]).

Now, suppose that $N \subset M$ is a λ-Markov inclusion. It is a fact if such a λ exists, then $\lambda = [M : N]^{-1}$ defines an index. Note that since N is a factor, so is M_1. Then, we may apply the basic construction to the inclusion $M \subset M_1 \subset M_2 = \langle M_1, e_{M_1} \rangle$. Furthermore, there is a λ-Markov trace for $M_1 \subset M_2$. Thus, we may iterate the basic construction obtaining the *Jones tower*

$$N \subset M \overset{e_0}{\subset} M_1 \overset{e_1}{\subset} M_2 \subset \dots$$

where $M_i = \langle M_{i-1}, M_{i-2} \rangle$, with *Jones projections* $e_i = e_{M_{i-1}}$ for $i \geq 1$ (note, we have used the convention that $N = M_{-1}$ and $M = M_0$) satisfying:

- $e_i^2 = e_i$ for all i

- $e_i e_j = e_j e_i$ if $|i - j| > 1$

- $e_i e_{i\pm 1} e_i = \lambda e_i$ for all i

- $\tau(e_{i+1} x) = \lambda \tau(x)$ for all $x \in M_i$.

2.3.3 Construction of subfactors

In this section, we will describe how one obtains a subfactor from a commuting square. Recall, a commuting square is a square of inclusions of finite dimensional von Neumann algebras:

$$\mathfrak{C} = \begin{pmatrix} P_{-1} & \subset & P_0 & \\ \cup & & \cup, & \tau \\ Q_{-1} & \subset & Q_0 & \end{pmatrix}$$

with a faithful trace τ on P_0 such that the vector space $P_{-1} \ominus Q_{-1}$ is orthogonal to $Q_0 \ominus Q_{-1}$ with respect to the inner product defined by τ on P_0. Note that $P_{-1} \ominus Q_{-1}$ being orthogonal to $Q_0 \ominus Q_{-1}$ is equivalent to

$$E_{P_{-1}} E_{Q_0} = E_{Q_{-1}}$$

where $E_A = E_A^{P_0}$ denotes the τ-invariant conditional expectation of P_0 onto the subalgebra $A \subset P_0$.

First, we will recall how to construct the *hyperfinite II_1 factor* from matrix algebras. Consider the inclusion

$$M_2(\mathbb{C}) \subset M_{2^2}(\mathbb{C}) \subset M_{2^3}(\mathbb{C}) \subset \dots$$

with $x \in M_{2^n}(\mathbb{C})$ being identified with

$$x \otimes I_2 = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \in M_{2^{n+1}}(\mathbb{C}).$$

Let $M_\infty = \cup M_{2^n}$. Then it is clear that M_∞ is a $*$-algebra. Since each inclusion is clearly isometric, there exists a unique tracial state, τ, on R_∞ which restricts on the factor M_{2^n} to the unique tracial state $\tau_{M_{2^n}}$. Let (H, π, Ω) denote the associated GNS triple. We define

$$R_{(2)} = \overline{\pi(R_\infty)}^{\text{w.o.}}.$$

Note that we have a trace on $R_{(2)}$ via $\tau(x) = \langle x\Omega, \Omega \rangle$. Furthermore, this trace is unique and hence, $R_{(2)}$ is a II_1 factor. Note that $R_{(2)}$ is "approximately finite dimensional" in the following sense:

Definition 2.3.5. *A von Neumann algebra M is said to be* approximately finite dimensional, or AFD*, if there exists an increasing sequence*

$$A_1 \subset A_2 \subset \ldots \subset A_n \subset A_{n+1} \subset \ldots$$

of finite dimensional $*$-subalgebras, whose union is weakly dense in M.

Note that there was nothing special about choosing 2 above. We could have done the same construction using $M_\infty = \otimes_n M_{N^n}(\mathbb{C})$ for any $N > 1$ and still obtain a II_1 factor. However, we have the following somewhat surprising theorem due to Murray and von Neumann.

Theorem 2.3.6. *Every AFD II_1 factor is isomorphic to $R_{(2)}$.*

Thus, up to isomorphism, amongst the class of all II_1 factors, there is exactly one with the property that is approximately finite-dimensional. We call this II_1 factor the *hyperfinite II_1 factor* and denote it by R. Now, we are ready to construct subfactors of R.

The commuting square $\mathcal{C}$ is called *non-degenerate* if $P_0 = \text{span } P_{-1}Q_0$. A main feature of non-degenerate commuting squares is how well they behave in terms of iterating the basic construction. If $\mathfrak{C}$ is a commuting square as above with a λ-Markov trace τ, then

$$\begin{array}{ccccc} P_0 & \subset P_1 & = \langle P_0, e_{P_{-1}} \rangle \\ \cup & & \cup \\ Q_0 & \subset Q_1 & = \langle Q_0, e_{P_{-1}} \rangle \end{array}$$

is also a commuting square. Hence, by iterating the basic construction, we obtain an inclusion $\cup_i Q_i = Q \subset P = \cup_i P_i$ of hyperfinite II_1 factors (with index λ^{-1}):

$$\begin{array}{ccccccc} P_{-1} \subset & P_0 \subset & P_1 = \langle P_0, e_1 \rangle \subset & \ldots \nearrow & P \\ \cup & \cup & \cup & & \cup \\ Q_{-1} \subset & Q_0 \subset & Q_1 = \langle Q_0, e_1 \rangle \subset & \ldots \nearrow & Q \end{array}$$

2.3.4 The standard invariant

Let $N \subset M$ be an inclusion of II_1 factors with a finite faithful normal trace τ. Assume that the *Jones index* $[M : N] = \dim_n L^2(M, \tau)$ is finite. As before, e_N denotes the Jones projection and $M_1 = \langle M, e_N \rangle$. Then M_1 is also a II_1 factor and the trace τ extends to M_1 by $\tau_1 = [M : N]^{-1}\tau$ and $[M_1 : M] = [M : N]$. Thus, we may iterate the basic construction.

Definition 2.3.7. *The* standard invariant $\mathcal{G}_{N,M}$ *of the sub factor $N \subset M$ is defined to be the trace preserving isomorphism class of the following sequences of commuting squares of finite dimensional C^*-algebras, together with the trace and the Jones projections $e_n \in N' \cap \mathrm{M_n}$:*

$$\begin{array}{ccccccccc} \mathbb{C} = N' \cap N & \subset & N' \cap M & \subset & N' \cap M_1 & \subset & N' \cap M_2 & \subset & \ldots \\ & & \cup & & \cup & & \cup & & \ldots \\ & & \mathbb{C} = M' \cap M & \subset & M' \cap M_1 & \subset & M' \cap M_2 & \subset & \ldots \end{array}$$

To calculate the standard invariant, one first has to understand what the basic construction yields and then be able to calculate the relative commutants. We do know from the properties of the basic construction, that the Jones projections e_1, e_2, ..., e_n are always contained in $N' \cap \mathrm{M_n}$.

Let's return to the case where N and M arise from a commuting square of the form

$$\mathfrak{C} = \left(\begin{array}{ccc} A_0^1 & \subset & A_1^1 \\ \cup & & \cup \\ A_0^0 & \subset & A_1^0 \end{array}, \tau \right)$$

where A_0^0, A_0^1, A_1^0, and A_1^1 are finite dimensional $*$-algebras and τ is a faithful trace on A_1^1.

In this case, the calculation of the higher order relative commutants in the standard invariant of $N \subset M$ can be expressed in terms of finite dimensional algebras, by using a highly nontrivial result called Ocneanu's compactness argument. One first iterates the basic construction in all possible directions (both vertically and horizontally).

Theorem 2.3.8. *(Ocneanu compactness) Let*

$$\begin{array}{ccccccccccccc}
\dots & \subset & \dots & \subset & \dots & \subset & \dots & \subset & \dots & \subset & \dots & \nearrow & \dots \\
\cup & & \cup & & \cup & & \cup & & \cup & & & & \cup \\
A_0^n & \subset & A_1^n & \subset & A_2^n & \subset & \dots & \subset & A_k^n & \subset & \dots & \nearrow & R_n \\
\cup & & \cup & & \cup & & \cup & & \cup & & & & \cup \\
\dots & \subset & \dots & \subset & \dots & \subset & \dots & \subset & \dots & \subset & \dots & \nearrow & \dots \\
\cup & & \cup & & \cup & & \cup & & \cup & & & & \cup \\
A_0^1 & \subset & A_1^1 & \subset & A_2^1 & \subset & \dots & \subset & A_k^n & \subset & \dots & \nearrow & R_1 \\
\cup & & \cup & & \cup & & \cup & & \cup & & & & \cup \\
A_0^0 & \subset & A_1^0 & \subset & A_2^0 & \subset & \dots & \subset & A_k^n & \subset & \dots & \nearrow & R_0
\end{array}$$

be the result of applying the basic construction in all possible directions. Then for each $n \geq 1$,

$$R_0' \cap R_n = A_1^{0'} \cap A_0^n.$$

Chapter 3

Twisted Commuting Squares

This chapter is based on joint work with Nicoara ([23]). In this chapter we weaken the commuting square condition, by replacing the trace τ with a faithful state φ. We call the resulting structure a twisted commuting square. Our main motivation is the possibility to construct finite index subfactors from twisted commuting squares, which will be discussed in a future paper.

The chapter is organized as follows: In Section 1 we introduce the main definitions and discuss possible normalizations for twisted commuting squares.

In Section 2 we prove an isolation result for twisted commuting squares, which is a generalization of the Span Condition introduced by Nicoara in [19]. This allows us to determine, for many of the examples we consider, if they are isolated or part of parametric families.

Section 3 is dedicated to examples of twisted commuting squares similar to the commuting squares based on (complex) Hadamard matrices. They are obtained for $R = \mathrm{M_n}(\mathbb{C})$, $P = \mathrm{D}$ the diagonals, $Q = u\mathrm{D}u^*$ for some unitary u, and $\varphi(\cdot) = \tau(\cdot a)$ for some $a \in \mathrm{M_n}(\mathbb{C})$ positive invertible. If the twisted commuting square condition is satisfied, we call u an a-Hadamard matrix. When $a = I_n$, this is the same as a Hadamard matrix. While there aren't many Hadamard matrices of small dimensions (see [9], [33]), looking at a-Hadamards provides a richer class of examples - see for instance Proposition 3.3.3.

Finally, in Section 4 we use parametric families of (twisted or not) Hadamard commuting squares to obtain associative deformations m_λ of the matrix multiplication. Our results can also be extended to multiplications on finite dimensional $*$-algebras. It turns out that certain families of (twisted) commuting squares yield associative multiplications of the form

$$m_\lambda(x, y) = m(x, y) + (\lambda - 1)m'(x, y) + (\bar{\lambda} - 1)m''(x, y),\ |\lambda| = 1$$

where m, m' and m'' are all associative multiplications.

Deformations of the multiplication are of interest in Quantum Algebra with applications to High Energy Physics. For instance, the approach to the theory of integrable systems via the Lenard-Magri scheme ([16]) uses compatible Poisson structures, which could be obtained from linear associative deformations of the multiplication (see for instance [24]).

3.1 Preliminaries

Definition 3.1.1. *A* twisted commuting square *of matrix algebras is a square of inclusions:*

$$\begin{pmatrix} P & \subset & R & \\ \cup & & \cup & ,\varphi \\ S & \subset & Q & \end{pmatrix}$$

where R, P, Q, S are finite dimensional $*$-algebras (i.e., of the form $\oplus_{i=1}^{k} \mathrm{M_{n_i}}(\mathbb{C})$) and φ is a faithful state on R, satisfying:

$$\mathrm{proj}_{\varphi,P}\mathrm{proj}_{\varphi,Q} = \mathrm{proj}_{\varphi,Q}\mathrm{proj}_{\varphi,P} = \mathrm{proj}_{\varphi,S}$$

where $\mathrm{proj}_{\varphi,V}$ *denotes the orthogonal projection from* R *to the subspace* V*, with respect to the inner product defined by* φ *on* R*:* $\langle x, y\rangle = \varphi(y^*x)$*.*

Equivalently, the commuting projections condition above can be written as:

$$P \ominus_\varphi S \perp_\varphi Q \ominus_\varphi S$$

where the orthogonal complements and the orthogonality are considered with respect to the inner product defined by φ*.*

One of the simplest (but rich in examples) classes of twisted commuting squares is obtained by letting $P = \mathrm{D}, \mathrm{Q} = \mathrm{uDu}^*$ be two copies of the diagonal matrices $\mathrm{D} \subset \mathrm{R} = \mathrm{M_n}(\mathbb{C})$, where u is a unitary matrix. If we let τ denote the normalized trace on $\mathrm{M_n}(\mathbb{C})$, then the faithful state φ is of the form $\varphi(x) = \tau(xa)$, for some positive invertible matrix $a \in \mathrm{M_n}(\mathbb{C})$. The twisted commuting square condition becomes a relation between u and a, generalizing the notion of complex Hadamard matrix.

Definition 3.1.2. *Let* $a \in \mathrm{M_n}(\mathbb{C})$ *be positive and invertible, with* $\tau(a) = 1$*. We say that a unitary* $u \in \mathrm{M_n}(\mathbb{C})$ *is* a-Hadamard *if*

$$\begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & ,\varphi \\ \mathbb{C}I_n & \subset & u\mathrm{Du}^* & \end{pmatrix}$$

is a twisted commuting square, where $\varphi(x) = \tau(xa)$ *for* $x \in \mathrm{M_n}(\mathbb{C})$*.*

Remark 3.1.3. *Since* $x - \varphi(x)1$ *is orthogonal to* $\mathbb{C}$*, with respect to the inner product defined by* φ*, the commuting square condition can be written as* $\varphi((y - \varphi(y)1)(x - \varphi(x)1)) = 0$*, for all* $x \in \mathrm{D}$ *and* $y \in u\mathrm{Du}^*$*. After taking adjoints it also follows* $\varphi((x - \varphi(x)1)(y - \varphi(y)1)) = 0$*, for all* $x \in \mathrm{D}$ *and* $y \in u\mathrm{Du}^*$*. Equivalently:*

$$\varphi(xy) = \varphi(x)\varphi(y), \text{ for all } x \in \mathrm{D}, \mathrm{y} \in \mathrm{uDu}^*.$$

Note that this is also equivalent to $\varphi(yx) = \varphi(x)\varphi(y)$ *for all* $x \in \mathrm{D}, \mathrm{y} \in \mathrm{uDu}^*$.

Let $(e_{i,j})_{1\leq i,j\leq n}$ denote the matrix units of $\mathrm{M_n}(\mathbb{C})$. It follows that u must satisfy $\tau(ue_{i\,i}u^*e_{j\,j}a) = \tau(ue_{i\,i}u^*a)\tau(e_{j\,j}a)$ for all i, j, or equivalently

$$\sum_{1\leq k\leq n} a_{j\,k}u_{k\,i}\overline{u_{j\,i}} = \frac{a_{j\,j}}{n}\sum_{1\leq l\leq n}\left(\sum_{1\leq k\leq n}\overline{u_{k\,i}}a_{k\,l}\right)u_{l\,i}, \text{ for all } i, j. \tag{3.1}$$

Remark 3.1.4. *Note that for* $a = I_n$*,* u *being* a*-Hadamard is equivalent to* u *being a complex Hadamard matrix, i.e.* u *is unitary and all its entries are of the same absolute value,* $|u_{k\,l}| = \frac{1}{\sqrt{n}}$.

Definition 3.1.5. *We say that the twisted commuting square*

$$\mathfrak{C} = \begin{pmatrix} P & \subset & R & \\ \cup & & \cup & ,\varphi \\ S & \subset & Q & \end{pmatrix}$$

is isomorphic *to the twisted commuting square*

$$\widetilde{\mathfrak{C}} = \begin{pmatrix} \widetilde{P} & \subset & \widetilde{R} & \\ \cup & & \cup & ,\widetilde{\varphi} \\ \widetilde{S} & \subset & \widetilde{Q} & \end{pmatrix}$$

if there exists a $*$*-algebra isomorphism* $\psi : R \to \widetilde{R}$ *such that* $\psi(P) = \widetilde{P}$*,* $\psi(S) = \widetilde{S}$*,* $\psi(Q) = \widetilde{Q}$ *and* $\widetilde{\varphi}(\psi(x)) = \varphi(x)$ *for all* $x \in R$.

We now present the canonical way to normalize twisted commuting squares and a-Hadamard matrices. For algebras $B \subset A$, we recall the notation $B' \cap A = \{a \in A \text{ such that } ab = ba, \forall b \in B\}$.

Lemma 3.0.6. *Let* R*,* P*,* Q*,* S *be finite dimensional* $*$*-algebras with a fixed trace* τ *on* R*, let* $a \in R$ *be positive and invertible and let* $\varphi(x) = \tau(ax)$*,* $x \in R$*. For each unitary element* u *in* R*, let*

$$\mathfrak{C}(u) = \begin{pmatrix} P & \subset & R & \\ \cup & & \cup & ,\varphi \\ S & \subset & uQu^* & \end{pmatrix}.$$

Let $q \in Q$, $q' \in Q' \cap P$, $p \in \{a\}' \cap S' \cap P$, $p' \in \{a\}' \cap P' \cap R$ be unitary elements. Assume that $\mathfrak{C}(u)$ is a twisted commuting square. Then $\mathfrak{C}(pp'uqq')$ is a twisted commuting square isomorphic to $\mathfrak{C}(u)$.

Proof. Modifying u to the right by q, q' does not change the algebra uQu^* and thus does not change the twisted commuting square: $\mathfrak{C}(pp'u) = \mathfrak{C}(pp'uqq')$. By applying $\mathrm{Ad}((pp')^*)$ to $\mathfrak{C}(pp'u)$ (which leaves R, P, S invariant), we see that $\mathfrak{C}(pp'u)$ is isomorphic to $\mathfrak{C}(u)$. Indeed, we have $\varphi(\mathrm{Ad}(pp')(x)) = \varphi(x)$, since p and p' commute with a.

■

Definition 3.1.6. *Let $a \in \mathrm{M_n}(\mathbb{C})$ be a positive, invertible matrix. We say that two a-Hadamard matrices u_1, u_2 are* equivalent*, written $u_1 \sim u_2$, if there exist unitary diagonal matrices d_1, d_2 and permutation matrices p_1, p_2 with $p_1 d_1$ commuting with a, such that $u_2 = p_1 d_1 u_1 d_2 p_2$.*

Remark 3.1.7. *Lemma 3.0.6 shows that equivalent a-Hadamard matrices yield isomorphic twisted commuting squares. The converse is also true, since the normalizer of* D *in* $\mathrm{M_n}(\mathbb{C})$ *is the set of elements of the form pd, with d diagonal unitary and p a permutation matrix. The fact that $p_1 d_1$ commutes with a follows from the preservation of φ in the definition of the isomorphism of twisted commuting squares: $\varphi(Ad(p_1 d_1)) = \varphi$.*

Remark 3.1.8. *It is easy to see that if $u \in \mathrm{M_n}(\mathbb{C})$ is a-Hadamard and if $d \in \mathrm{D}$ is unitary, then dud^* is dad^*-Hadamard. Thus, we may reduce ourselves to the case when a has the entries $a_{11}, a_{12}, ..., a_{1n}$ real.*

While complex Hadamard matrices can be normalized (up to equivalence) to have the first row and column made of 1's, twisted Hadamard matrices do not allow for such nice normalizations. The main problem is that we can modify from the left only by elements which commute with a. The only normalization that we will use is the following.

Remark 3.1.9. *Since we can modify $u \to ud$ by diagonal unitaries d, we may assume (up to equivalence) that the entries $u_{11}, u_{12}, \ldots, u_{1n}$ are all real.*

3.2 An Isolation Result for Twisted Hadamard Matrices

In this section we generalize the isolation result obtained by Nicoara in [19] to twisted commuting squares: we prove that if a certain Span Condition holds, then the twisted commuting square is isolated. For simplicity, we will only do this for twisted commuting squares arising from a-Hadamard matrices. All examples to which we apply the Span Condition in the next section are of this form.

Definition 3.2.1. *Let $a \in \mathrm{M_n}(\mathbb{C})$ be positive and invertible, and let u be an a-twisted Hadamard matrix. We say that u is* isolated *if there exists $\delta > 0$ such that if v is any a-twisted Hadamard with $||v - u|| < \delta$, then v is equivalent to u.*

Let u be a-Hadamard and let $\mathfrak{C}$ be the twisted a-Hadamard commuting square associated to u

$$\mathfrak{C} = \begin{pmatrix} P & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & , \varphi \\ \mathbb{C} & \subset & Q & \end{pmatrix}$$

where $P = \mathrm{D}, \mathrm{Q} = \mathrm{uDu}^*$ and $\varphi(x) = \tau(xa)$.

For two subspaces V, W of a $*$-algebra R we will use the notation

$$[V, W] = \mathrm{span}\{vw - wv : v \in V, w \in W\}.$$

Definition 3.2.2. *We say that* $\mathfrak{C}$ *satisfies* the Span Condition *if*

$$[aP_0, Q] + [P_0 a, Q] + (\{a\}' \cap P) + Q = \mathrm{M_n}(\mathbb{C})$$

where $P_0 = P \ominus_\varphi \mathbb{C}I_n$*.*

Remark 3.2.3. *When* $a = I_n$*, the span condition becomes* $[P, Q] + P + Q = \mathrm{M_n}(\mathbb{C})$*, which is the span condition for Hadamard matrices introduced by the first author in [19].*

Theorem 3.2.4. *Let* u *be an* a*-Hadamard matrix. If the associated twisted commuting square* $\mathfrak{C}$ *satisfies the Span Condition, then* u *is isolated.*

Proof. Assume that the span condition is satisfied, but u is not isolated. Then there exists unitaries u_n, $u_n \to I$, such that $u_n u$ are all a-Hadamard matrices, not equivalent to u. So

$$\mathfrak{C}(\mathfrak{u_n}) = \begin{pmatrix} P & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & , \varphi \\ \mathbb{C} & \subset & u_n Q u_n^* & \end{pmatrix}$$

are all twisted commuting squares. By a compactness argument, we may assume after eventually passing to a subsequence that $h = \lim_{n\to\infty} \frac{u_n - I}{i||u_n - I||}$ exists. Note that $||h|| = 1$. Since u_n are unitaries, it follows that h is self-adjoint. By the same argument as in Lemma 1.8 from [19], after eventually modifying $u_n \to p_n u_n q_n$ with $p_n \in \{a\}' \cap P$ and $q_n \in Q$ unitaries convering to I, we may assume that h is orthogonal to the vector space $(\{a\}' \cap P) + Q$. By orthogonal we mean with respect to the canonical inner product on $\mathrm{M_n}(\mathbb{C})$, given by the trace.

Writing the twisted commuting square condition for each u_n gives $\varphi(p u_n q u_n^*) = \varphi(p)\varphi(u_n q u_n^*)$. For $\varphi(p) = 0$, we can rewrite $\varphi(p u_n q u_n^*) = 0$ as:

$$\varphi(p(u_n - I)q u_n^*) + \varphi(pq(u_n - I)^*) = 0.$$

After dividing by $i||u_n - I||$ and taking the limit as $n \to \infty$, we obtain:

$$\varphi(phq) - \varphi(pqh) = 0.$$

Equivalently: $\tau(phqa) - \tau(pqha) = 0$. Which by using the properties of the trace is equivalent to

$$\tau(h[ap, q]) = 0.$$

This shows that h is orthogonal to $[aP_0, Q]$, where $P_0 = P \ominus_\varphi \mathbb{C}I_n$. Since h is self-adjoint and P_0, Q are closed to $*$, it follows that h will also be orthogonal to $[aP_0, Q]^* = [P_0 a, Q]$. Thus, h is orthogonal to $[aP_0, Q] + [P_0 a, Q] + (\{a\}' \cap P) + Q = \mathrm{M_n}(\mathbb{C})$, which implies $h = 0$, contradicting $||h|| = 1$.

■

Remark 3.2.5. *For most a's that we will apply this result to, we have* $\{a\}' \cap P = \mathbb{C}$*, so the span condition becomes* $[aP_0, Q] + [P_0 a, Q] + Q = \mathrm{M_n}(\mathbb{C})$*.*

3.3 Examples

In this section we present various examples of twisted commuting squares, arising from unitaries u which are a-Hadamard, for some a positive and invertible. We will avoid the examples that yield classical commuting squares (without a twist), i.e. based on complex Hadamard matrices. A catalogue of the known complex Hadamard matrices can be found at [33]. We start by observing that diagonal matrices a will only give Hadamard examples.

Proposition 3.3.1. *Let* $a \in \mathrm{D}$ *be positive and invertible,* $\tau(a) = 1$*. Then,* u *is* a*-Hadamard if and only if* u *is a complex Hadamard matrix.*

Proof. Let e_{ij} denote the matrix units of $\mathrm{M_n}(\mathbb{C})$. Suppose u is a Hadamard matrix. Since $ae_{jj} \in \mathrm{D}$, we have $\tau(ue_{ii}u^*e_{jj}a) = \tau(ue_{ii}u^*)\tau(e_{jj}a) = \tau(ue_{ii}u^*a)\tau(e_{jj}a)$.

Conversely, suppose u is a-Hadamard and $a = \sum_{1\leq k\leq n} \lambda_k e_{kk}$. Then

$$\lambda_j |u_{ji}|^2 = \lambda_j \tau(ue_{ii}u^*e_{jj}) = \tau(ue_{ii}u^*e_{jj}a) = \tau(ue_{ii}u^*a)\tau(e_{jj}a) = \frac{\lambda_j}{n}\tau(ue_{ii}u^*a).$$

Therefore, we have $|u_{j\,i}| = |u_{k\,i}|$ for any fixed i and $1 \leq j, k \leq n$. Because u is unitary, it follows $|u_{j\,i}| = \frac{1}{\sqrt{n}}$ for all j, i. Hence, u is a Hadamard matrix.

■

Remark 3.3.2. *It is possible for a Hadamard matrix to be a-Hadamard, even if a is not diagonal. For instance, if a is the matrix having* 1 *on the diagonal and all the other entries equal to some* $t \in (0,1)$*, then it is easy to see that any Hadamard matrix having the first column made of* $1's$ *(so in particular any Hadamard matrix in normalized form) is also a-Hadamard.*

The next proposition shows that for each $n > 4$ there exists at least one pair (a, u) with a positive invertible, and u an a-Hadamard matrix which is not a complex Hadamard matrix. Moreover, the matrices a, u are circulant matrices. In particular, they commute.

Proposition 3.3.3. *Let* $n > 4$ *and let* e_{ij} *denote the matrix units of* $\mathrm{M_n}(\mathbb{C})$*. Let* $B = \sum_{i,j=1}^{n} e_{ij}$ *and let* $X = \sum_{i=1}^{n} e_{ii+1}$*, where the index* $n+1$ *is identified with* 1*. Let* $u = \frac{2}{n}B - X$ *and let* $a = I_n + \frac{n-4}{2n-4}(B - I_n)$*. Then* u *is* a*-Hadamard.*

Proof. Using $B^2 = nB$, $XB = BX = B$ and $X^*B = BX^* = B$, it is immediate to check that $uu^* = (\frac{2}{n}B - X)(\frac{2}{n}B - X^*) = \frac{4}{n^2}nB + I_n - \frac{4}{n}B = I_n$. Thus u is a unitary. It is easy to see that a is positive and invertible.

We now check that the a-Hadamard condition $\tau(ae_{kk}ue_{ll}u^*) = \tau(ae_{kk})\tau(aue_{ll}u^*)$ holds for all k, l. This is equivalent to

$$(u^*a)_{lk} \cdot u_{kl} = \frac{1}{n} a_{kk} \cdot (u^*au)_{ll}.$$

Since $ua = au$, the right part of the equality above is $\frac{1}{n}$. For the left part, notice that $u^*a = (\frac{2}{n}B - X^*)(I_n + \frac{n-4}{2n-4}(B - I_n)) = \frac{1}{2}B - \frac{n}{2n-4}X^*$. This matrix has all entries equal to $\frac{1}{2}$, except those on positions $k+1, k$, which equal $\frac{1}{2-n}$. Since u has the entries equal to $\frac{2}{n}$, except the entries $u_{k,k+1} = \frac{2-n}{n}$, it follows that $(u^*a)_{lk} \cdot u_{kl} = \frac{1}{n}$.

■

We now classify the unitaries u that are a-Hadamard, for an arbitrary 2×2 positive invertible matrix a, $\tau(a) = 1$. By Remarks 3.1.8 and 3.1.9, we may assume $a = \begin{pmatrix} \alpha & \lambda \\ \lambda & 2-\alpha \end{pmatrix} \in M_2(\mathbb{R})$ where $0 < \alpha < 2$ and $|\lambda| < \sqrt{2\alpha - \alpha^2}$, and $u_{1\,1},\ u_{1\,2} \in \mathbb{R}$. Then (3.1) yields the following equations:

$$\begin{aligned} \alpha u_{1\,k}^2 + \lambda u_{1\,k} u_{2\,k} &= \frac{\alpha}{2}\left(\alpha u_{1\,k}^2 + (2-\alpha)\left|u_{2\,k}\right|^2 + 2\lambda u_{1\,k}\Re u_{2\,k}\right) && (3.2) \\ \lambda u_{1\,k}\overline{u_{2\,k}} + (2-\alpha)\left|u_{2\,k}\right|^2 &= \frac{2-\alpha}{2}\left(\alpha u_{1\,k}^2 + (2-\alpha)\left|u_{2\,k}\right|^2 + 2\lambda u_{1\,k}\Re u_{2\,k}\right). && (3.3) \end{aligned}$$

Since the right hand sides of equations 3.2 and, 3.3 are all real, $u_{2\,k} \in \mathbb{R}$. Using this and the previous equations, we obtain

$$\alpha(2-\alpha)\left(\left|u_{1\,k}\right|^2 - \left|u_{2\,k}\right|^2\right) = 2(\alpha - 1)\lambda u_{1\,k} u_{2\,k}. \tag{3.4}$$

We note that $\alpha = 1$ or $\lambda = 0$ yields $|u_{1\,1}| = |u_{2\,1}|$ and $|u_{1\,2}| = |u_{2\,2}|$ and u unitary would then imply $|u_{1\,1}| = |u_{2\,1}| = |u_{1\,2}| = |u_{2\,2}| = \frac{1}{\sqrt{2}}$. Thus, u is equivalent to the unitary $u = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

For $\lambda \neq 0$ and $\alpha \neq 1$, let $\omega = \frac{2(\alpha-1)}{\alpha(2-\alpha)}\lambda$. Note that each of $|u_{i\,j}| \neq 0$ for $1 \leq i,\ j \leq 2$ (else, a column of u would be 0) and $\omega \neq 0$. Let $r = \frac{u_{1\,k}}{u_{2\,k}}$ and note that $r,\ \omega \in \mathbb{R}$. Dividing equation 3.4 by $u_{2\,k}^2$, we get $r^2 - 1 = \omega r$. Letting $r_1 = \frac{\omega + \sqrt{\omega^2+4}}{2}$, we see that $u_{1\,k} = r u_{2\,k}$ with $r \in \{r_1, \frac{-1}{r_1}\}$. Letting $u_{1\,1} = r u_{2\,1}$ and $u_{1\,2} = r' u_{2\,2}$ with $r,\ r' \in \{r_1, \frac{-1}{r_1}\}$, the unitary conditions are $1 = r^2 u_{2\,1}^2 + (r')^2 u_{2\,2}^2 = u_{2\,1}^2 + u_{2\,2}^2$ and $0 = r u_{2\,1}^2 + r' u_{2\,2}^2$ which imply $r \neq r'$. Hence, u is equivalent to a unitary of the form:

$$\begin{pmatrix} r r_1 & \frac{-1}{r} r_2 \\ r_1 & r_2 \end{pmatrix} \tag{3.5}$$

where $r_1 = \frac{1}{\sqrt{1+r^2}}$, $r_2 = \frac{r}{\sqrt{1+r^2}}$, $\omega = \frac{2(\alpha-1)}{\alpha(2-\alpha)}\lambda$, and $r = \frac{\omega+\sqrt{\omega^2+4}}{2}$.

Example 3.3.4. *For* $a = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{\sqrt{3}}{3} \\ \frac{\sqrt{3}}{3} & \frac{3-\sqrt{5}}{2} \end{pmatrix}$, *we obtain* $u = \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{-1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$. *A calculation via mathematica shows the span condition is satisfied, so u is isolated among the a-Hadamard matrices.*

We now give a degenerate (in the sense that each a is positive but not invertible) parametric family of matrices of order 3 with a corresponding family of twisted Hadamard matrices.

Example 3.3.5. *Let* $a = \begin{pmatrix} 1 & 2t^2-1 & t \\ 2t^2-1 & 1 & t \\ t & t & 1 \end{pmatrix}$ *where* $0 < t < 1$. *Let* $x = -1 + t^4 - t\sqrt{2-3t^2+t^6}$, $y = -1 + t^4 + t\sqrt{2-3t^2+t^6}$, $w = -t + t^3 - \sqrt{2-3t^2+t^6}$, *and* $z = -t + t^3 + \sqrt{2-3t^2+t^6}$. *Then*

$$u = \begin{pmatrix} \frac{1}{\sqrt{2+t^2}} & \sqrt{\frac{x}{2(t^2+2)(t^2-1)}} & \sqrt{\frac{y}{2(t^2+2)(t^2-1)}} \\ \frac{1}{\sqrt{2+t^2}} & -\sqrt{\frac{t^2-1}{2x(t^2+2)}} & -\sqrt{\frac{t^2-1}{2(t^2+2)y}} \\ \frac{t}{\sqrt{2+t^2}} & \frac{1}{w}\sqrt{\frac{2x(t^2-1)}{(t^2+2)}} & \frac{1}{z}\sqrt{\frac{2y(t^2-1)}{(t^2+2)}} \end{pmatrix}$$

is a-Hadamard.

While the example above looks hard to work with in general, certain values of t give unitaries with rational entries.

Example 3.3.6. *For* $t = \frac{1}{2}$, *we obtain* $a = \begin{pmatrix} 1 & -\frac{1}{2} & \frac{1}{2} \\ -\frac{1}{2} & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 1 \end{pmatrix}$ *and* $u = \begin{pmatrix} \frac{2}{3} & \frac{2}{3} & \frac{1}{3} \\ \frac{2}{3} & -\frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & -\frac{2}{3} & \frac{2}{3} \end{pmatrix}$.
A calculation via Mathematica shows the span condition is satisfied, so u is an isolated a-Hadamard matrix.

We now show how for any n non-prime, $n = k \cdot m$, parametric families of a-Hadamards (a fixed) can be constructed from fixed a-Hadamards of smaller orders. This construction is a natural generalization of the Diţă-Haagerup type Hadamard matrices (see [9],[33])

Proposition 3.3.7. *Let $a_1 \in \mathrm{M_m}(\mathbb{C})$ and $a_2 \in \mathrm{M_k}(\mathbb{C})$ be positive, invertible matrices. Suppose that b is a_2-Hadamard and $c_1, c_2, \ldots, c_k$ are a_1-Hadamard. Then*

$$u = \begin{bmatrix} b_{1\,1}c_1 & b_{1\,2}c_2 & \cdots & b_{1\,k}c_k \\ b_{2\,1}c_1 & b_{2\,2}c_2 & \cdots & b_{2\,k}c_k \\ \vdots & \vdots & & \vdots \\ b_{k\,1}c_1 & b_{k\,2}c_2 & \cdots & b_{k\,k}c_k \end{bmatrix} \text{ is } a = a_1 \otimes a_2\text{-Hadamard.}$$

Proof. Let $(e_{i\,j})_{1\leq i,j\leq m}$ and $(f_{i'\,j'})_{1\leq i',j'\leq k}$ be the matrix units for $\mathrm{M_m}(\mathbb{C})$ and $\mathrm{M_k}(\mathbb{C})$ respectively. Making an appropriate identification of $\mathrm{M_{km}}(\mathbb{C})$ with $\mathrm{M_m}(\mathbb{C}) \otimes \mathrm{M_k}(\mathbb{C})$, we have $u = \sum_{p,q} b_{p\,q}c_q \otimes f_{p\,q}$ and $u^* = \sum_{r,s} \overline{b_{r\,s}}c_s^* \otimes f_{s\,r}$. We need to verify that for each i, i', j, j'

$$\tau\left(u(e_{i\,i} \otimes f_{i'\,i'})u^*(e_{j\,j} \otimes f_{j'\,j'})a\right) = \tau\left(u(e_{i\,i} \otimes f_{i'\,i'})u^* a\right)\tau\left((e_{j\,j} \otimes f_{j'\,j'})a\right). \tag{3.6}$$

Using the linearity of τ, we have the left side of equation 3.6 is:

$$\sum_{p,q,r,s} \tau\left(b_{p\,q}c_q e_{i\,i}\overline{b_{r\,s}}c_s^* e_{j\,j}a_1 \otimes f_{p\,q}f_{i'\,i'}f_{s\,r}f_{j'\,j'}a_2\right).$$

Note that $f_{p\,q}f_{i'\,i'}f_{s\,r}f_{j'\,j'} \neq 0 \Leftrightarrow q = i' = s,\ r = j'$. Thus, the left side of (3.6) reduces to

$$\sum_{p} \tau\left(c_{i'}e_{i\,i}c_{i'}^* e_{j\,j}a_1\right)\tau\left(b_{p\,i'}\overline{b_{j'\,i'}}f_{p\,j'}a_2\right). \tag{3.7}$$

Using similar arguments as above, the right side reduces to:

$$\sum_{p,r} \tau\left(c_{i'}e_{i\,i}c_{i'}^* a_1\right)\tau\left(b_{i'\,q}\overline{b_{r\,i'}}f_{p\,r}a_2\right)\tau\left(e_{j\,j}a_1\right)\tau\left(f_{j'\,j'}a_2\right). \tag{3.8}$$

Since $b = \sum_{p\,q} b_{p\,q}f_{p\,q}$ is a_2-Hadamard and for a fixed i', $c_{i'}$ is a_1-Hadamard, we have:

$$\sum_{p} \tau\left(b_{p\,i'}\overline{b_{j'\,i'}}f_{p\,j'}a_2\right) = \sum_{p\,r} \tau\left(b_{p\,i'}\overline{b_{r\,i'}}f_{p\,r}\right)\tau\left(f_{j'\,j'}a_2\right) \tag{3.9}$$

$$\tau\left(c_{i'}e_{i\,i}c_{i'}^* e_{j\,j}a_1\right) = \tau\left(c_{i'}e_{i\,i}c_{i'}^* a_1\right)\tau\left(e_{j\,j}a_1\right). \tag{3.10}$$

Finally, we plug (3.10) and (3.9) into (3.7) to get (3.8).

■

Using the previous proposition, we now give a parametric family of 4×4 of a-Hadamard matrices, with a fixed.

Example 3.3.8. *Let* $a = \begin{pmatrix} \alpha & \lambda \\ \lambda & 2-\alpha \end{pmatrix}$ *where* $0 < \alpha < 2$ *and* $0 < \lambda < \sqrt{2\alpha - \alpha^2}$. *Let* $\omega = \frac{2\lambda(\alpha-1)}{\alpha(2-\alpha)}$ *and* $r = \frac{\omega+\sqrt{\omega^2+4}}{2}$. *Let* $r_1 = \frac{1}{\sqrt{1+r^2}}$, *and* $r_2 = \frac{r}{\sqrt{1+r^2}}$. *Then equation (3.5) gives*

$$c_1 = \begin{pmatrix} rr_1 & -\frac{r_2}{r} \\ r_1 & r_2 \end{pmatrix} \text{ and } c_2(t) = \begin{pmatrix} rr_1 & \frac{-r_2}{r}\exp(it) \\ r_1 & r_2\exp(it) \end{pmatrix}$$

are a-Hadamard for any real number t. Furthermore,

$$u(t) = \frac{1}{\sqrt{2}} \begin{pmatrix} c_1 & c_1 \\ c_2(t) & -c_2(t) \end{pmatrix}$$

is a one parameter family of $a \otimes I_2$-Hadamard matrices.

The simplest parametric family that we were able to obtain is the following:

Example 3.3.9. *Let* $a = \begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{\sqrt{3}}{3} \\ \frac{\sqrt{3}}{3} & \frac{3-\sqrt{5}}{2} \end{pmatrix}$ *and* $\lambda \in \mathbb{T}$. *Then the following is a parametric family of a-Hadamards:*

$$u_\lambda = \frac{1}{\sqrt{2}} \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{-1}{2} & \frac{\sqrt{3}}{2} & \frac{-1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} & \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{-1}{2}\lambda & \frac{-\sqrt{3}}{2} & \frac{1}{2}\lambda \\ \frac{1}{2} & \frac{\sqrt{3}}{2}\lambda & \frac{-1}{2} & \frac{-\sqrt{3}}{2}\lambda \end{pmatrix}.$$

The span condition can not hold for u_λ, as it is not isolated. Indeed, a Mathematica calculation shows that the dimension of the space from the span condition is 14 for $\lambda = 1$.

3.4 Twisted Hadamard Matrices and Associative Deformations of the Matrix Product

Starting from a parametric family of twisted Hadamard commuting squares, we obtain a continuous family m_t ($t \in \mathbb{R}$) of associative multiplications on $\mathrm{M_n}(\mathbb{C})$, where m_0 is the canonical matrix multiplication. Moreover, m_t will coincide with m_0 when restricted to any of the two MASAs which are the corners of the initial twisted commuting square.

Associative deformations of the multiplication are a subject of interest in Quantum Algebra with applications to High Energy Physics. For instance, the approach to the theory of integrable systems via the Lenard-Magri scheme ([16]) uses compatible Poisson structures, which could be obtained from linear associative deformations of the multiplication (see for instance [24]).

Due to the rigidity of semi-simple associative algebras, for t small, the multiplications m_t must be of the form $m_t(x,y) = \varphi_t^{-1}(\varphi_t(x)\varphi_t(y))$, where $\varphi_t : \mathrm{M_n}(\mathbb{C}) \to \mathrm{M_n}(\mathbb{C})$ is a linear isomorphism. We will construct, from twisted commuting squares, such families φ_t for which the structural constants of the multiplications m_t are easy to compute. Moreover, we will see that certain families of commuting squares, such as those arising from Petrescu's Hadamard matrices, yield associative multiplications of the form

$$m_\lambda(x,y) = m(x,y) + (\lambda - 1)m'(x,y) + (\bar{\lambda} - 1)m''(x,y),\ |\lambda| = 1$$

where m, m' and m'' are all associative multiplications, with $m = m_0$. Equivalently, this will give a parametric family of multiplications m_t of degree two in t.

Let $a \in M_n(\mathbb{C})$ be positive invertible, let $\varphi(x) = \tau(ax)$ and let u be an a-Hadamard unitary with no non-zero entries. Denote $P = \mathrm{D}$, $Q = u\mathrm{D}u^*$. Let p_i and $q_i = up_iu^*$, $1 \le i \le n$, denote the minimal projections of P, respectively Q. We begin by finding some easy formulas for the structural constants of the canonical matrix multiplication m, in the bases given by p_i, q_i. Note that $p_i q_j$ span $\mathrm{M_n}(\mathbb{C})$:

Proposition 3.4.1. *Let $u \in \mathrm{M_n}(\mathbb{C})$ be a unitary, $P = \mathrm{D}$ and $Q = u\mathrm{D}u^*$. Then*

$$\mathrm{span}\{\mathrm{pq} : \mathrm{p} \in \mathrm{P}, \mathrm{q} \in \mathrm{Q}\} = \mathrm{M_n}(\mathbb{C})$$

if and only if u has no zero entries.

Proof. $\mathrm{span}\{\mathrm{pq} : \mathrm{p} \in \mathrm{P}, \mathrm{q} \in \mathrm{Q}\} = \mathrm{M_n}(\mathbb{C})$ if and only if $v_{i,j} = p_i q_j, 1 \leq i,j \leq n$ form a basis for $\mathrm{M_n}(\mathbb{C})$. We have: $\tau(v_{k,l} v^*_{k',l'}) = \tau(p_k q_l q_{l'} p_{k'}) = \delta_k^{k'} \delta_l^{l'} \tau(p_k q_l) = \frac{1}{n} \delta_k^{k'} \delta_l^{l'} |u_{kl}|^2$. So the $n^2 \times n^2$ matrix with entries $\tau(v_{k\,l} v^*_{k'\,l'})$ is diagonal and it is invertible if and only if all the diagonal entries $|u_{kl}|^2$ are non-zero.

■

It follows that for all $1 \leq k,l,k',l' \leq n$, the structural coefficients $c^{ij}_{klk'l'}$ of the multiplication satisfy: $(p_k q_l)(p_{k'} q_{l'}) = \Sigma^n_{i,j=1} c^{ij}_{klk'l'} p_i q_j$. By multiplying by p_k to the left and $q_{l'}$ to the right, it follows $(p_k q_l)(p_{k'} q_{l'}) = c^{kl'}_{klk'l'} p_k q_{l'}$, so $c^{kl'}_{klk'l'} = \varphi(p_k q_l p_{k'} q_{l'})/\varphi(p_k)\varphi(q_{l'})$ and $c^{ij}_{klk'l'} = 0$ for $(i,j) \neq (k,l')$. Thus, we obtain:

$$(p_k q_l)(p_{k'} q_{l'}) = \gamma^{k'l'}_{kl} p_k q_{l'}, \text{ where } \gamma^{k'l'}_{kl} = \frac{\varphi(p_k q_l p_{k'} q_{l'})}{\varphi(p_k)\varphi(q_{l'})}. \tag{3.11}$$

Let now u_t ($t \in \mathbb{R}$) be a continuous parametric family of a-Hadamard unitaries, with $u_0 = u$. Denote $Q_t = u_t \mathrm{D} u_t^*$, so $Q_0 = Q$. Let $\varphi_t : \mathrm{M_n}(\mathbb{C}) \to \mathrm{M_n}(\mathbb{C})$ be given by

$$\varphi_t(p_k u p_l u^*) = p_k u_t p_l u_t^*$$

for any $1 \leq k,l \leq n$. For t small, the entries of u_t will also be non-zero, so $p_k u_t p_l u_t^*$, $1 \leq k,l \leq n$ form a basis of $\mathrm{M_n}(\mathbb{C})$. It follows that φ_t extends to a linear isomorphism of $\mathrm{M_n}(\mathbb{C})$, and $\varphi_t(pq) = p\mathrm{Ad}(u_t u_0^*)(q)$ for all $p \in P, q \in Q$. Let $m_t(x,y) = \varphi_t^{-1}(\varphi_t(x)\varphi_t(y))$.

Proposition 3.4.2. *The associative multiplication m_t satisfies: $m_t(x,y) = m(x,y)$ for all (x,y) with $x \in P$ or $y \in Q$.*

Proof. We have $m_t(pq,q') = \varphi_t^{-1}(p\mathrm{Ad}(u_tu_0^*)(q)\mathrm{Ad}(u_tu_0^*)(q')) = \varphi_t^{-1}(p\mathrm{Ad}(u_tu_0^*)(qq')) = pqq' = m(pq,q')$, for all $p \in P$ and $q,q' \in Q$. This shows that $m_t(x,y) = m(x,y)$ for all $y \in Q$. The other equality follows by a similar argument.

■

We now find the structural constants of the multiplication m_t. From the formula for m_t, we have: $m_t(p_kup_lu^*, p_{k'}up_{l'}u^*) = \varphi_t^{-1}(p_ku_tp_lu_t^*p_{k'}u_tp_{l'}u_t^*)$. By arguments similar to those that lead to (3.11), we have

$$p_ku_tp_lu_t^*p_{k'}u_tp_{l'}u_t^* = \gamma_{kl}^{k'l'}(t)p_ku_tp_{l'}u_t^*, \text{ with } \gamma_{kl}^{k'l'}(t) = \frac{\varphi(p_ku_tp_lu_t^*p_{k'}u_tp_{l'}u_t^*)}{\varphi(p_k)\varphi(u_tp_{l'}u_t^*)}.$$

So we obtain:

$$m_t(p_kup_lu^*, p_{k'}up_{l'}u^*) = \gamma_{kl}^{k'l'}(t)p_kup_{l'}u^*.$$

In the case when $a = \frac{1}{n}I_n$, so $u_t = (u_{kl}(t))_{1\le k,l\le n}$ are all Hadamard matrices, we have $\gamma_{kl}^{k'l'}(t) = n^2\tau(p_ku_tp_lu_t^*p_{k'}u_tp_{l'}u_t^*) = n\frac{u_{kl}u_{k'l'}}{u_{k'l}u_{kl'}}$. It follows:

Proposition 3.4.3. *Consider a continuous family of Hadamard matrices $u_t = (u_{kl}(t))_{1\le k,l\le n}$, t real. Then the following is a parametric family of associative multiplications of $\mathrm{M_n}(\mathbb{C})$:*

$$m_t(p_kup_lu^*, p_{k'}up_{l'}u^*) = \gamma_{kl}^{k'l'}(t)p_kup_{l'}u^*, \text{ where } \gamma_{kl}^{k'l'}(t) = n\frac{u_{kl}(t)u_{k'l'}(t)}{u_{k'l}(t)u_{kl'}(t)}.$$

We now observe that certain families of Hadamard matrices, which depend linearly on a parameter $\lambda \in \mathbb{T}$, yield multiplications m_λ linear in $\lambda, \bar{\lambda}$. This is somewhat surprising, as the formula for the structural constants $\gamma_{kl}^{k'l'}(\lambda)$ of m_λ involves products of four entries of u.

We first recall the family of complex Hadamard matrices of order 4 found by Haagerup in [9]:

$$F_4(\lambda) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & \lambda & -\lambda \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -\lambda & \lambda \end{pmatrix}, \lambda \in \mathbb{T}.$$

We also recall the following family of complex Hadamard matrices of order 7 found by Petrescu in [26]. Let $w = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$ and let

$$P_7(\lambda) = \frac{1}{\sqrt{7}}\begin{pmatrix} \lambda w & \lambda w^4 & w^5 & w^3 & w^3 & w & 1 \\ \lambda w^4 & \lambda w & w^3 & w^5 & w^3 & w & 1 \\ w^5 & w^3 & \overline{\lambda} w & \overline{\lambda} w^4 & w & w^3 & 1 \\ w^3 & w^5 & \overline{\lambda} w^4 & \overline{\lambda} w & w & w^3 & 1 \\ w^3 & w^3 & w & w & w^4 & w^5 & 1 \\ w & w & w^3 & w^3 & w^5 & w^4 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \lambda \in \mathbb{T}. \tag{3.12}$$

Proposition 3.4.4. *If $u_\lambda = F_4(\lambda)$ or $u_\lambda = P_7(\lambda)$ ($\lambda \in \mathbb{T}$), then the parametric family of associative multiplications m_λ associated to u_λ, as in Proposition 3.4.3, is of the form*

$$m_\lambda = m + (\lambda - 1)m' + (\bar{\lambda} - 1)m'', \lambda \in \mathbb{T}$$

where m is the canonical matrix multiplication and m', m'' are associative matrix multiplications.

Proof. To show that m_λ can be expressed as $m + (\lambda - 1)m' + (\bar{\lambda} - 1)m''$, it is enough to show that none of the coefficients $\gamma_{k,l}^{k',l'}(\lambda)$ contain λ^2 or $\bar{\lambda}^2$. This is clear, since the families of Hadamard matrices above have the property: no single row or column contains multiples of both λ and $\bar{\lambda}$, and if $u_{kl}(\lambda)$ and $u_{k'l'}(\lambda)$ are both multiples of λ (respectively $\bar{\lambda}$), then so are $u_{kl'}(\lambda)$ and $u_{k'l}(\lambda)$.

The fact that m', m'' must be multiplications follows by writing the associativity of m_λ and identifying the coefficients of $\lambda^2, \bar{\lambda}^2$, which are linearly independent of $1, \lambda, \bar{\lambda}$ for $\lambda \in \mathbb{T}$.

$\blacksquare$

Remark 3.4.5. *The same holds true for the deformation of multiplication arising from the twisted a-Hadamard matrices from Example 3.3.8. It is also true for several other known linear parametric families of Hadamard matrices.*

Remark 3.4.6. *If we use* $\bar{\lambda} = 1/\lambda$*, we can write* λm_λ *in the form* $A + B\lambda + C\lambda^2$*, with* $\lambda \in \mathbb{T}$*. It easily follows that* $A + Bt + Ct^2$ *is an associative multiplication for any parameter* t*. Note that* A *and* C*, but not* B*, are also associative multiplications (for the examples above).*

Chapter 4

Group type commuting squares

Throughout the chapter, let G be a finite group of order n with group algebra $\mathbb{C}[G]$. In the following sections, we will reserve g, g', h, and h' to represent group elements while i and k will be reserved for natural numbers. Fix an ordering on G. For each $g \in G$, let $e_g \in \mathbb{C}^n$ denote the column vector with a 1 in position g and 0 otherwise. Then $\mathbb{C}[G] = \operatorname{span}\{u_g : g \in G\}$ where $u_g \in \mathrm{M_n}(\mathbb{C})$ satisfies $u_g(e_h) = e_{gh}$ for all $h \in G$ (i.e. $\mathbb{C}[G]$ is the left regular representation of G). Let τ denote the normalized trace on $\mathrm{M_n}(\mathbb{C})$. We have the corresponding commuting square

$$\mathfrak{C} = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & ,\tau \\ \mathbb{C}I_n & \subset & \mathbb{C}[G] & \end{pmatrix}.$$

It can be shown that two group commuting squares are isomorphic if and only if the corresponding groups are isomorphic. The span condition for such a commuting square reads

$$[\mathrm{D}, \mathbb{C}[\mathrm{G}]] + \mathbb{C}[\mathrm{G}] + \mathbb{C}[\mathrm{G}]' + \mathrm{D} = \mathrm{M_n}$$

where $\mathbb{C}[G]' = \{a \in \mathrm{M_n} : \mathrm{au_g} = \mathrm{u_g a}\, \forall \mathrm{g} \in \mathrm{G}\}$.

We define the dephased and undephased defect for $\mathfrak{C}_G$, or equivalently, for the group G as follows:

Definition 4.0.7. *Given a finite group, G, the* undephased defect *is*

$$d(G) = n^2 - \dim_{\mathbb{C}}[\mathrm{D}, \mathbb{C}[\mathrm{G}]]$$

and the dephased defect *of G is*

$$d'(G) = n^2 - \dim_{\mathbb{C}}\left([\mathrm{D}, \mathbb{C}[\mathrm{G}]] + \mathbb{C}[\mathrm{G}] + \mathbb{C}[\mathrm{G}]' + \mathrm{D}\right).$$

4.1 The defect of a group-type commuting square

Some of the results in this section will appear in [22].

Our goal now is to relate $d(G)$ and $d'(G)$. We will need a few results about the interactions of the various spaces in the definitions. First, we describe the elements in $\mathbb{C}[G]'$.

Proposition 4.1.1. *A matrix $a \in \mathrm{M_n}(\mathbb{C})$ is in $\mathbb{C}[G]'$ if and only if*

$$a_{g^{-1}g',h} = a_{g',gh}$$

for all g, g', $h \in G$. Furthermore, $\dim_{\mathbb{C}} C[G]' = n$, and $\mathbb{C}[G]' \cap \mathrm{D} = \mathbb{C}\mathrm{I_n}$.

Proof. Fix $g \in G$. Since $(u_g)_{g',h'} = \delta^{g'}_{gh'}$, routine calculations show that

$$(u_g a)_{g',h} = \sum_{h'} (u_g)_{g',h'} a_{h',h} = a_{g^{-1}g',h}$$

and

$$(a u_g)_{g',h} = \sum_{h'} a_{g',h'} (u_g)_{h',h} = a_{g',gh}.$$

Thus, a commutes with all u_g's if and only if $a_{g^{-1}g',h} = a_{g',gh}$ for all g, g', $h \in G$. By taking $g' = e$, we have for any g, $h \in G$, $a_{g,h} = a_{e,g^{-1}h}$ which shows all entries of a depend solely on the first row of a. Conversely, if $(c_g)_{g \in G} \in \mathbb{C}^n$, we can consider the matrix a given by $a_{g,h} = c_{g^{-1}h}$. Then a will have the first row given by the c_g's, and it is easy to see that $a_{g^{-1}g',h} = a_{g',gh}$ for all g, g', $h \in G$. Consequently, $\dim_{\mathbb{C}} \mathbb{C}[G]' = n$. The last statement follows as $a_{g,g} = a_{e,e}$ for each $g \in G$.

■

Corollary 4.0.1. *The algebras* $\mathbb{C}[G]'$ *and* D *are orthogonal modulo their intersection* $\mathbb{C}$.

Proof. Let $g \in G$, $a \in \mathbb{C}[G]'$ and d_g be the diagonal matrix with a 1 in position g, g and 0 elsewhere. Then $\tau(a) = \frac{1}{n}\sum_{h \in G} a_{h,h} = a_{g,g}$ since $a_{h,h} = a_{g,g} = a_{e,e}$ for all $h \in G$. Hence,

$$\tau(a(d_g - \frac{1}{n}I_n)) = \tau(ad_g) - \frac{1}{n}\tau(a) = \frac{a_{g,g}}{n} - \frac{a_{g,g}}{n} = 0.$$

■

Proposition 4.1.2. *The algebras* $\mathbb{C}[G]$, $\mathbb{C}[G]'$, *and* D *are all orthogonal to* $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]$.

Proof. Fix g, $h \in G$. Let $d \in \mathrm{D}$, d_h be the diagonal matrix with a 1 on position h, h and 0 elsewhere, and $u_g, u_h \in \mathbb{C}[G]$ be as before. Since the diagonals commute, it is easy to see that

$$\tau(d[d_h, u_g]) = \tau(dd_h u_g - du_g d_h) = \tau((dd_h - d_h d)u_g) = 0.$$

Next, we know that $u_h u_g = u_{hg}$ has no diagonal entries unless $hg = e$ (and hence, $gh = e$) where e denotes the identity of G. Thus,

$$\tau(u_h[d_h, u_g]) = \tau(d_h u_{gh} - d_h u_{hg}) = 0.$$

Finally, if $x \in \mathbb{C}[G]'$, we have

$$\tau(x[d_h, u_g]) = \tau(xd_h u_g - xu_g d_h) = \tau((u_g x - xu_g)d_h) = 0.$$

■

Let $cl(G)$ denote the class number of G; i.e. $cl(G)$ is the number of distinct conjugacy classes of G. We have the following characterization of $\mathbb{C}[G] \cap \mathbb{C}[G]'$:

Proposition 4.1.3. *A matrix $a = \sum_g c_g u_g \in \mathbb{C}[G]$ is also in $\mathbb{C}[G]'$ if and only if*

$$c_g = c_{hgh^{-1}}$$

for all $g, h \in G$. Thus $\dim_{\mathbb{C}}(\mathbb{C}[G] \cap \mathbb{C}[G]') = cl(G)$.

Proof. Fix $h \in G$. It is easy to see that $au_h = \sum_g c_g u_{gh}$ and $u_h a = \sum_g c_g u_{hg}$. Relabeling, from $au_h = u_h a$ it follows that

$$\sum_{g'} c_{g'h^{-1}} u_{g'} = \sum_{g'} c_{h^{-1}g'} u_{g'}.$$

We conclude that $c_{g'h^{-1}} = c_{h^{-1}g'}$ for all $g', h \in G$. Setting $g = h^{-1}g'$, this is equivalent to

$$c_{hgh^{-1}} = c_g.$$

■

Now, we are ready to relate $d(G)$ and $d'(G)$.

Theorem 4.1. *The dephased and undephased defect of a finite group G are related as follows:*

$$d(G) = d'(G) + 3n - 1 - cl(G).$$

Proof. By repeatedly applying $\dim_{\mathbb{C}}(V + W) = \dim_{\mathbb{C}} V + \dim_{\mathbb{C}} W - \dim_{\mathbb{C}} V \cap W$ for vector spaces V and W and using the propositions, we have

$$\begin{aligned}\dim_{\mathbb{C}}([\mathrm{D},\mathbb{C}[\mathrm{G}]]+\mathbb{C}[G]+\mathbb{C}[G]'+\mathrm{D}) &= \dim_{\mathbb{C}}([\mathrm{D},\mathbb{C}[\mathrm{G}]])+\dim_{\mathbb{C}}(\mathbb{C}[G]+\mathbb{C}[G]'+\mathrm{D})) \\ &= \dim_{\mathbb{C}}([\mathrm{D},\mathbb{C}[\mathrm{G}]])+\dim_{\mathbb{C}}(\mathbb{C}[G]+\mathbb{C}[G]')+\dim_{\mathbb{C}}(\mathrm{D})-\dim_{\mathbb{C}}(\mathbb{C}) \\ &= \dim_{\mathbb{C}}([\mathrm{D},\mathbb{C}[\mathrm{G}]])+\dim_{\mathbb{C}}(\mathbb{C}[G])+\dim_{\mathbb{C}}(\mathbb{C}[G]')) \\ &\quad -\dim_{\mathbb{C}}(\mathbb{C}[G]\cap\mathbb{C}[G]')+n-1 \\ &= \dim_{\mathbb{C}}([\mathrm{D},\mathbb{C}[\mathrm{G}]])+3n-cl(G)-1.\end{aligned}$$

We conclude that

$$d(G)=d'(G)+3n-1-cl(G).$$

■

We now compute $d(G)$ for any finite group in terms of the orders of the elements of g.

Theorem 4.1.4. *The undephased defect of a group algebra* $\mathbb{C}[G]$ *is given by:*

$$d(\mathbb{C}[G])=\sum_{g\in G}\frac{|G|}{ord(g)}.$$

Proof. For $g\in G$, let d_g denote the diagonal matrix with a 1 on position g,g and 0 elsewhere and δ_i^k denote the Kronecker delta. The idea of the proof is that if $W=\operatorname{span}\{[d_g,u_h]:g,h\in G\}$, then $\dim_{\mathbb{C}}W+\dim_{\mathbb{C}}W^{\perp}=n^2$ and we relate this to calculations involving only W. Let $A(g,h)=[d_g,u_h]$ and let $\tilde{A}(g,h)$ denote the "row by row" column vector form of $A(g,h)$. Finally let M be the $n^2\times n^2$ matrix with the (g,h) column equal to $\tilde{A}(g,h)$. Note that the dimension of the set of matrices $C=(c_{g,h})_{g,h\in G}$ satisfying $\sum_{g,h}c_{g,h}A(g,h)=0$ is precisely the dimension of the null space of M and the dimension of the column space of M is precisely $\dim_{\mathbb{C}}W$. Hence, in calculating the defect, it is sufficient to calculate the dimension of the set of matrices $C=(c_{g,h})_{g,h\in G}$ satisfying $\sum_{g,h}c_{g,h}A(g,h)=0$ where $A(g,h)=[d_g,u_h]$.

Routine calculations show that $(d_g u_h)_{g',h'} = \delta_g^{g'}(u_h)_{g,h'} = \delta_g^{g'}\delta_{hh'}^{g}$ and $(u_h d_g)_{g',h'} = \delta_g^{h'}(u_h)_{g',g} = \delta_g^{h'}\delta_{hg}^{g'}$. Thus, $A(g,h)_{g',h'} = (\delta_g^{g'} - \delta_g^{h'})\delta_{hh'}^{g'}$. Then for each $g, h \in G$, we have

$$\begin{aligned} 0 &= \sum_{g,h} c_{g,h}(\delta_g^{g'} - \delta_g^{h'})\delta_{hh'}^{g'} \\ &= \sum_{h}(c_{g',h} - c_{h',h})\delta_{hh'}^{g'}. \end{aligned}$$

For fixed g' and h', there is exactly one h with $hh' = g'$. Hence, we get $c_{g',h} = c_{h',h}$ whenever $hh' = g'$. Consequently, $g' \in \langle h \rangle g$ implies $c_{g',h} = c_{g,h}$. It follows that we have $[G : \langle h \rangle]$ choices to make for the column associated to h.

■

Thus, we see that for fixed $g, h \in G$, defining $c^{h,g} \in M_n(\mathbb{C})$ by

$$\left(c^{h,g}\right)_{p,q} = \begin{cases} 1 & \text{if } p = h^k g \text{ and } q = h \text{ for some } k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

then $c^{h,g}$ is a canonical basis element for $\{C : \sum_{g,h} c_{g,h} A(g,h) = 0\}$.

Corollary 4.1.5. *If G is a finite group, the dephased defect of G is*

$$d'(G) = \sum_{g \in G} \frac{|G|}{ord(g)} - 3n + 1 + cl(G).$$

Before continuing, we relate our results to some results of Banica. Note that if G is abelian, then $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$ for some $r \in \mathbb{N}$ (here $n = n_1 \ldots n_r$). For such G's, it is easy to see that $\mathbb{C}[G] = F_G \mathrm{D} \mathrm{F}_{\mathrm{G}}^*$ where $F_G = F_{n_1} \otimes \ldots \otimes F_{n_r}$ is the Fourier matrix associated to G. In [1], the undephased defect of the generalized Fourier matrix F_G is given by

$$d(F_G) = \sum_{g \in G} \frac{|G|}{\mathrm{ord}(g)}.$$

Thus, we have:

Remark 4.1.6. *When we particularize the defect to* $G = \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_r}$*, our calculation* $d(G)$ *gives a different proof of Banica's result.*

Now, we ask when is the span condition satisfied. Note that the span condition holds if and only if $d'(G) = 0$.

Theorem 4.2. *Let* G *be a finite group with at least 2 elements. Then* $d'(G) = 0$ *if and only if* $G = \mathbb{Z}_p$ *where* p *is a prime number.*

Proof. Suppose G is a group of order n and let e denote the identity of G. We break the proof into two cases for G; either G is cyclic or it is not. Suppose G is cyclic. Then $G \simeq \mathbb{Z}_n$. Hence, $cl(G) = n$ and we have

$$\begin{aligned} d'(G) &= d(\mathbb{C}[G]) - 2n + 1 + (cl(G) - n) \\ &= n + \sum_{g \in G \setminus \{e\}} \frac{n}{\text{ord}(g)} - 2n + 1 \\ &\geq n + (n-1) - 2n + 1 \\ &= 0 \end{aligned}$$

with equality if and only if every non-identity element has order n; i.e. $G = \mathbb{Z}_p$ for some prime p.

Now suppose G isn't cyclic. Then $cl(G) > 1$ and $\text{ord}(g) < n$ for all $g \in G \setminus \{e\}$. Thus,

$$\begin{aligned} d'(G) &= n + \sum_{g \in G \setminus \{e\}} \frac{n}{\text{ord}(g)} - 2n + 1 + (cl(G) - n) \\ &\geq n + 2(n-1) - 2n + 1 + cl(G) - n \\ &= cl(G) - 1 \\ &> 0. \end{aligned}$$

■

Remark 4.1.7. *Since $d'(G) = 0$ is equivalent to $\mathfrak{C}_G$ satisfying the span condition, in this case $\mathfrak{C}_G$ is isolated. Applying this to the group $G = \mathbb{Z}_p$ with p prime, we obtain Petrescu's result ([26]) that the Fourier matrix, F_p, is isolated among all Hadamard matrices.*

4.2 The second order condition for group commuting squares

We now do similar computations to see what a given $a \in \mathrm{M_n}(\mathbb{C})$ with $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ must satisfy.

Theorem 4.2.1. *Let $a \in \mathrm{M_n}(\mathbb{C})$, then $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ if and only if*

$$a_{h^{-1}g,g} = a_{g,hg}$$

for all $g, h \in G$.

Proof. Fix g and h. Then

$$\begin{aligned} 0 &= \tau(aA(g,h)) \\ &= \sum_{g',h'} a_{g',h'} A(g,h)_{h',g'} \\ &= \sum_{g',h'} a_{g',h'} \left(\delta_g^{g'} - \delta_g^{h'}\right) \delta_{hh'}^{g'} \\ &= a_{g,h^{-1}g} - a_{hg,g}. \end{aligned}$$

Note that the last equality is true since there exists a unique h' with $hh' = g$ and a unique g' with $hg = g'$. Thus, we conclude $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ if and only if $a_{g,h^{-1}g} = a_{hg,g}$ for all g, $h \in G$. Replacing h with h^{-1} we se that $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ if and only if $a_{h^{-1}g,g} = a_{g,hg}$.

■

We are now ready to come up with a basis for $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]^{\perp} = \{\mathrm{a} : \mathrm{a} \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]\}$. For fixed g, $h \in G$ we have just shown that $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ if and only if $a_{h^{-1}g,g} = a_{g,hg}$ which implies that $a_{h^{-1}g,g} = a_{g,hg} = a_{hg,h^2g} = \ldots = a_{h^{|h|-1}g,g}$. Thus, a candidate for a canonical basis element is given by:

Definition 4.2.2. *Fix g, $h \in G$. We define $a^{h,g} \in \mathrm{M_n}(\mathbb{C})$ by*

$$\left(a^{h,g}\right)_{p,q} = \begin{cases} 1 & \text{if } p = h^k g \text{ and } q = h^{k+1} g \text{ for some } k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}.$$

Theorem 4.3. *For each $h \in G$, let $g_1^h, \ldots, g_{[G:\langle h\rangle]}^h$ denote coset of represents of $G/\langle h\rangle$. Then*

$$\{a^{h,g_i^h} : h \in G, 1 \leq i \leq [G : \langle h\rangle]\}$$

is a basis for $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]^{\perp}$.

Proof. Linear independence from the following stronger condition: the nonzero entries of $a^{h,g}$ are zero entries for $a^{l,k}$ if either $h \neq l$ or $h = l$ and $k \notin \langle h\rangle g$. Indeed, if $(a^{h,g})_{g',h'} \neq 0 \neq (a^{l,k})_{g',h'}$ then $g' \in \langle h\rangle g \cap \langle l\rangle k$ and $h' = hg' = lg'$ which implies $h = l$ and hence $k \in \langle h\rangle g$.

Next, suppose $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$. Then it follows that for each $h \in G$ and $1 \leq i \leq [G : \langle h\rangle]$, $a_{h^{-1}g_i^h, g_i^h} = a_{g_i^h, hg_i^h} = a_{hg_i^h, h^2 g_i^h} = \ldots = a_{h^{|h|-1}g_i^h, g_i^h}$. We conclude that

$$a = \sum_{h \in G, 1 \leq i \leq [G:\langle h\rangle]} a_{g_i^h, hg_i^h} a^{h, g_i^h}.$$

■

In [21], Nicoara proves the following new restriction that a commuting square must satisfy if it is not isolated:

Theorem 4.2.3. *Let*

$$\mathfrak{C} = \begin{pmatrix} P_{-1} & \subset & P_0 & \\ \cup & & \cup & , \tau \\ Q_{-1} & \subset & Q_0 & \end{pmatrix}$$

be a commuting square of finite dimensional von Neumann algebras, with trace τ. If $\mathfrak{C}$ is not isolated and h is a normalized direction of convergence, then there exists $s \in P_0$ satisfying the conditions:

- $s + s^* = h^2$
- $\tau(s\,[p,q]) = \tau(pqh^2) - \tau(phqh)$ *for all* $p \in P_{-1}$ *and* $q \in Q_0$.

Lemma 4.3.1. *Let $a \in P_0$. To verify the existence of b such that $\tau(b\,[p,q]) = \tau(pqa^2) - \tau(paqa)$ for all $p \in P_{-1}$ and $q \in Q_0$, it is enough to check that whenever $p_i \in P_{-1}$ and $q_i \in Q_0$ ($1 \leq i \leq N$ for some $N \geq 1$) satisfy $\sum_{i=1}^{N}[p_i, q_i] = 0$, we must have $\sum_{i=1}^{N} \tau(p_i q_i a^2) - \tau(p_i a q_i a) = 0$.*

Proof. Since P_{-1} and Q_0 are finite dimensional, it suffices to find b such that $\tau(b\,[p_i, q_j]) = \tau(p_i q_j a^2) - \tau(p_i a q_j a)$ for any p_i in a basis of P_{-1} and q_j in a basis of Q_0. We will write the equations that such a b must satisfy as a system of matrix equations. Let $A(i,j) = [p_i, q_j]$ and $\tilde{A}(i,j)$ denote the row by row row vector of $A(i,j)$. Let $\tilde{b}$ denote the column by column column vector of b. The desired conditions on b require that for each i and j,

$$\tilde{A}(i,j)\tilde{b} = \tau(p_i q_j a^2) - \tau(p_i a q_j a).$$

Hence, if M is the matrix with (i,j) row $\tilde{A}(i,j)$ and v is the column vector with (i,j) row $\tau(p_i q_j a^2) - \tau(p_i a q_j a)$, then $M\tilde{b} = v$. By examining the augmented matrix, we see that the system is consistent (i.e. such a b does indeed exist) if and only if for any linear combination of the rows of M that is 0, then we must have that the same linear combination of the rows of v is 0 which is precisely the statement in the claim.

∎

Lemma 4.3.2. *Suppose $a \in P_0$ is Hermitian (i.e. $a = a^*$) and $b \in P_0$ satisfies $\tau(b[p,q]) = \tau(pqa^2) - \tau(paqa)$ for all $p \in P_{-1}$ and $q \in Q_0$. Then, there exists $\tilde{b} \in P_0$ such that*

- $\tau(\tilde{b}[p,q]) = \tau(pqa^2) - \tau(paqa)$ *for all* $p \in P_0$ *and* $q \in Q_{-1}$

- $\tilde{b} + \tilde{b}^* = a^2$.

Proof. Let $p \in P_{-1}$ and $q \in Q_0$. It follows by taking adjoints of the relation

$$\tau(b[p,q]) = \tau(pqa^2) - \tau(paqa) \tag{4.1}$$

that b^* satisfies

$$\tau(-b^*[p^*,q^*]) = \tau(q^*p^*a^2) - \tau(aq^*ap^*).$$

Since p^* and q^* are generic elements of P_{-1} and Q_0 respectively, it follows that for all $p \in P_{-1}$ an $q \in Q_0$,

$$\tau(-b^*[p,q]) = \tau(qpa^2) - \tau(paqa).$$

Subtracting this relation from 4.1, we obtain

$$\tau((b+b^*)[p,q]) = \tau([p,q]a^2)$$

for all $p \in P_{-1}$ and $q \in Q_0$. Therefore, $b + b^* - a^2$ is orthogonal to $[P_{-1}, Q_0]$. It follows that if $\tilde{b} = b - \frac{1}{2}(b + b^* - a^2)$, we have $\tilde{b} + \tilde{b}^* = a^2$ and $\tau(\tilde{b}[p,q]) = \tau(b[p,q])$ and for all $p \in P_{-1}$ and $q \in Q_0$.

■

In what follows, we give results that partially answer the question "if a is a normalized direction of convergence, then does there exist $b \in \mathrm{M_n}(\mathbb{C})$ with $\tau(b\,[p,q]) = \tau(pqa^2) - \tau(paqa)$ for all $p \in \mathrm{D}$ and $q \in \mathbb{C}[G]$"? We answer the question when $G = Z_n$ and show precisely what

b's work for $a + a^*$ where a is a canonical basis element of $\{h : h \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]\}$ for any group G.

Lemma 4.3.3. *Let G be a group and $\{H_i\}_{i \in I}$ be a family of subgroups of G. Let $g_i \in G$ then either $\cap_{i \in I} g_i H_i$ is empty or a (left) coset of $\cap_{i \in I} H_i$.*

Proof. Let $H = \cap_{i \in I} H_i$. Suppose $\cap_{i \in I} g_i H_i \neq \emptyset$. Let $g \in \cap_{i \in I} g_i H_i$. Then for each $i \in I$, $g = g_i h_i$ for some $h_i \in H_i$. We will show $gH = \cap_{i \in I} g_i H_i$. If $x \in gH$, then $x \in \cap_{i \in I} g_i H_i$ since $g \in \cap_{i \in I} g_i H_i$. Thus, $gH \subset \cap_{i \in I} g_i H_i$.

Conversely, suppose $x \in \cap_{i \in I} g_i H_i$. We want to show that $x \in gH$ or equivalently that $g^{-1}x \in H$. Since $x \in \cap_{i \in I} g_i H_i$, for each $i \in I$, $x = g_i \tilde{h}_i$ for some $\tilde{h}_i \in H_i$. It follows that for each $i \in I$, $g^{-1}x = h_i^{-1} g_i^{-1} g_i \tilde{h}_i = h_i^{-1} \tilde{h}_i \in H_i \subset H$ and consequently, $x \in gH$.

■

Theorem 4.2.4. *Let $G = \mathbb{Z}_n$ and $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$, then there exists $b \in \mathrm{M_n}$ with $\tau(b[p, q]) = \tau(pqa^2) - \tau(paqa)$ for all $p \in \mathrm{D}$ and $q \in \mathbb{C}[G]$.*

Proof. By Lemma 4.3.1, it suffices to show that whenever $\sum_{i=1}^m c_{g_i,h_i}[d_{g_i}, u_{h_i}] = 0$, then $\sum_{i=1}^m c_{g_i,h_i}\tau(d_{g_i}u_{h_i}a^2) = \sum_i^m c_{g,h}\tau(d_{g_i}au_{h_i}a)$. Since these relations are clearly linear in $c_{g,h}$, it is sufficient to prove the result for a basis of matrices $(c_{g,h})$ satisfying $\sum_{g,h} c_{g,h}[d_g, u_h] = 0$. Recall, for fixed g, $h \in G$, that a basis element for when $\sum_{g,h} c_{g,h}[d_g, u_h] = 0$ is given by $c^{h,g}$ (the matrix with 1 on position $hk + g, h$ for $k = 1, \ldots, |h|$ and 0 otherwise). Thus, it suffices to show that

$$\sum_{k=1}^{|h|} \tau(d_{hk+g}u_h a^2) = \sum_{k=1}^{|h|} \tau(d_{hk+g}au_h a) = 0.$$

Let $(a_i)_{1 \leq i \leq N}$ be the canonical basis for $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]^\perp$ described earlier (in some order). Write $a = \sum_k \alpha_k a_k$ for some $\alpha_k \in \mathbb{C}$. It follows that $\tau(d_g u_h a^2) = \sum_{k,l} \alpha_k \alpha_l \tau(d_g u_h a_k a_l)$ and $\tau(d_g a u_h a) = \sum_{k,l} \alpha_k \alpha_l \tau(d_g a_k u_h a_l)$. Therefore, we need to show that for canonical basis elements of $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]^\perp$, a and $\tilde{a}$, we have

$$\sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{h(k-1)+g,h'}\tilde{a}_{h',hk+g} = \sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{hk+g,h'}\tilde{a}_{-h+h',hk+g}.$$

Let $h_0, h_1, g_0, g_1 \in \mathbb{Z}_n$. Then $a = a^{h_0,g_0}$ and $\tilde{a} = a^{h_1,g_1}$ are canonical basis elements of $\{a : a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]\}$. Note that by choosing $h_0 = h_1$ and $g_0 = g_1$, then $a = \tilde{a}$. Let $S_h = \langle h \rangle + g$, $S_{h_0} = \langle h_0 \rangle + g_0$, and $S_{h_1} = \langle h_1 \rangle + g_1$. Then

$$\begin{aligned}
\sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{h(k-1)+g,h'}\tilde{a}_{h',hk+g} &= \sum_{k=1}^{|h|}\sum_{h' \in S_{h_0}\cap S_{h_1}} \delta_{h(k-1)+g}^{h'-h_0}\delta_{hk+g}^{h'+h_1} \\
&= \sum_{k=1}^{|h|}\sum_{h' \in S_{h_0}\cap S_{h_1}} \delta_{hk+g}^{h'+h_1}\delta_{h_1}^{h-h_0} \\
&= \delta_h^{h_0+h_1}\left|S_{h_0} \cap S_{h_1} \cap (S_h - h_1)\right|.
\end{aligned}$$

Similarly, we have

$$\sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{hk+g,h'}\tilde{a}_{-h+h',hk+g} = \delta_h^{h_0+h_1}\left|S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0)\right|.$$

By Lemma 4.3.3, we have that if both $S_{h_0} \cap S_{h_1} \cap (S_h - h_1)$ and $S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0)$ are either both empty or non empty, then $|S_{h_0} \cap S_{h_1} \cap (S_h - h_1)| = |S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0)|$ and hence,

$$\sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{h(k-1)+g,h'}\tilde{a}_{h',hk+g} = \sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{hk+g,h'}\tilde{a}_{-h+h',hk+g}.$$

Thus, it suffices to show that if $h = h_0 + h_1$, then

$$S_{h_0} \cap S_{h_1} \cap (S_h - h_1) \neq \emptyset \Leftrightarrow S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0) \neq \emptyset.$$

Assume $h = h_0 + h_1$ and $x \in S_{h_0} \cap S_{h_1} \cap (S_h - h_1)$. We exhibit a $y \in S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0)$. If we write $y = x+z$, then z will have to satisfy $z \in \langle h_0 \rangle \cap (\langle h_1 \rangle + h) \cap (\langle h \rangle + h_0 + h_1)$, which can be simplified to:

$$\langle h_0 \rangle \cap (\langle h_1 \rangle + h_0) \cap \langle h \rangle.$$

We used here that $h = h_0 + h_1$.

For simplicity of notations, let $r = -h_0$ and $s = h$. Then $h_1 = r + s$. We need to show that:

$$\langle r \rangle \cap (\langle r+s \rangle - r) \cap \langle s \rangle \neq \emptyset, \text{ for any } r, s \in \mathbb{Z}_n.$$

If we rewrite this statement in terms of elements of the group $\mathbb{Z}$, we have to show that for all integers $n > 1$ and r, s, we have:

$$(r\mathbb{Z} + n\mathbb{Z}) \cap (s\mathbb{Z} + n\mathbb{Z}) \cap (-r + (r+s)\mathbb{Z} + n\mathbb{Z}) \neq \emptyset. \tag{4.2}$$

In what follows, we will use the notations (x, y) and $[x, y]$ for the greatest common divisor, respectively the least common multiple of the integers x, y. We have:

$$r\mathbb{Z} + n\mathbb{Z} = (r, n)\mathbb{Z} \text{ and } s\mathbb{Z} + n\mathbb{Z} = (s, n)\mathbb{Z}.$$

It follows that

$$(r\mathbb{Z} + n\mathbb{Z}) \cap (s\mathbb{Z} + n\mathbb{Z}) = [(r, n), (s, n)]\mathbb{Z}.$$

Thus, (4.2) can be rewritten as:

$$[(r, n), (s, n)]\mathbb{Z} \cap (-r + (r+s, n)\mathbb{Z}) \neq \emptyset$$

or equivalently

$$r \in k\mathbb{Z}, \text{ where } k = ([(r, n), (s, n)], (r+s, n))$$

which means that all we have to check is that k divides r. It is a well known identity that $[(r,n),(s,n)] = ([r,s],n)$. Thus $k = (([r,s],n),(r+s,n)) = ([r,s],r+s,n)$. In particular k divides $([r,s],r+s)$, so if we show that $([r,s],r+s)$ divides r we are done.

Let $d = (r,s)$, $r = dr'$, $s = ds'$ with $(r',s') = 1$. Then $([r,s],r+s) = (dr's', dr' + ds') = d(r's', r'+s') = d$, which divides $r = dr'$. We used here that $(r's', r'+s') = 1$, which follows immediately from $(r',s') = 1$. This ends the proof.

■

Remark 4.2.5. *By the previous theorem, the bound on the number of possible directions of convergence around F_n, the Fourier matrix of order n, given by the defect of F_n is not* decreased *by the second order conditions.*

Open Question 4.2.6. *For any direction of convergence $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$, does there exist a sequence of Hadamard matrices converging to F_n with direction of convergence a?*

The result from Theorem 4.2.4 is not true for any finite abelian group G. Indeed, in the case of the group $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ there exist a's satisfying the first order condition, but not satisfying the second order condition.

Remark 4.2.7. *Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. If*

$$a = \begin{pmatrix} 0 & -1 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

then it can easily be checked with Mathematica that no $b \in \mathrm{M_n}(\mathbb{C})$ exists satisfying $\tau(b[d,u]) = \tau(daua) - \tau(dua^2)$ for all $d \in \mathrm{D}$ and $u \in F_G \mathrm{D} \mathrm{F}_{\mathrm{G}}^*$.

Proposition 4.2.8. *Let G be a finite group. Let $k,l \in G$ and $a = a^{k,l}$. Then $\tau(b[p,q]) = \tau(pq(a+a^*)^2) - \tau(p(a+a^*)q(a+a^*))$ for all $p \in \mathrm{D}$ and $q \in \mathbb{C}[G]$ if and only if $b \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$.*

Proof. We show that for any product $a'a''$ with $a', a'' \in \{a, a^*\}$ then $\tau(b[p,q]) = \tau(pqa'a'') - \tau(pa'qa')$, $b \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$.

Fix $g, h \in G$. Let $p = d_g$ and $q = u_h$. We've seen previously that $\tau(b[p,q]) = b_{g,h^{-1}g} - b_{hg,g}$. Also, we have $\tau(d_g u_h a^2) = \sum_{h' \in G} a_{h^{-1}g,h'} a_{h',g}$ and $\tau(d_g a u_h a) = \sum_{h'} a_{g,h'} a_{h^{-1}h',g}$. Let $S_k = \langle k \rangle l$. Note that for $h' \in S_k$, $a_{g',h'} \neq 0$ if and only if $g' \in S_k$ with $g' = k^{-1}h'$ and similarly, $a_{h',g'} \neq 0$ if and only if $g' \in S_k$ with $g' = kh'$. Thus,

$$\begin{aligned}
\tau(d_g u_h a^2) &= \sum_{h' \in S_k} a_{h^{-1}g,h'} a_{h',g} \\
&= \delta_h^{k^2} |S_k \cap \{g\}| \quad \text{ since } a_{h',g} \neq 0 \Leftrightarrow g = kh' \text{ and then } a_{h^{-1}g,h'} \neq 0 \Leftrightarrow h^{-1}g = k^{-1}h'
\end{aligned}$$

and

$$\begin{aligned}
\tau(d_g a u_h a) &= \sum_{h' \in S_k} a_{g,h'} a_{h^{-1}h',g} \\
&= \delta_h^{k^2} |S_k \cap \{g\}| \quad \text{ since } a_{g,h'} \neq 0 \Leftrightarrow g = k^{-1}h' \text{ and then } a_{h^{-1}h',g} \neq 0 \Leftrightarrow h^{-1}h' = k^{-1}g.
\end{aligned}$$

A similar argument shows that $\tau(pq(a^*)^2) = \tau(pa^*qa^*)$.

We now show $\tau(pqaa^*) = \tau(paqa^*)$ (an identical argument shows that $\tau(pqa^*a) = \tau(pa^*qa)$) for any $p \in \mathrm{D}$ and $q \in \mathbb{C}[G]$. If e denotes the identity of G, we have

$$\begin{aligned}
\tau(d_g u_h a a^*) &= \sum_{h' \in G} a_{h^{-1}g,h'} a^*_{h',g} \\
&= \sum_{h' \in S_k} a_{h^{-1}g,h'} a^*_{h',g} \\
&= \delta_h^e |S_k \cap \{g\}| \quad \text{ since } a^*_{h',g} \neq 0 \Leftrightarrow g = k^{-1}h' \text{ and then } a_{h^{-1}g,h'} \neq 0 \Leftrightarrow h^{-1}g = k^{-1}h'
\end{aligned}$$

and

$$\tau(d_g a u_h a^*) = \sum_{h' \in S_k} a_{g,h'} a^*_{h^{-1}h',g}$$
$$= \delta^e_h \, |S_k \cap \{g\}| \quad \text{since } a_{g,h'} \neq 0 \Leftrightarrow g = k^{-1}h' \text{ and then } a^*_{h^{-1}h',g} \neq 0 \Leftrightarrow h^{-1}h' = kg \; .$$

Thus, we see for all p and q, b must satisfy $\tau(b[p,q]) = 0$, i.e. $b \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$.

■

4.3 Construction of commuting squares

In this section, we wish to construct commuting squares from unitaries $U_k \to I$ of the form

$$\mathfrak{C}_k = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & ,\tau \\ \mathbb{C}I_n & \subset & U_k\mathbb{C}[G]U_k^* & \end{pmatrix}$$

and where $h = \lim_k \frac{U_k - I}{\mathrm{i}||\mathrm{U_k - I}||}$ is a canonical hermitian basis element for the hermitians orthogonal to D, $\mathbb{C}[G]$, and $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]$. The idea is that we will construct such unitaries using the matrix exponential of certain elements in $\mathrm{M_n}(\mathbb{C})$. In what follows, we will first construct unitaries from hermitians orthogonal to $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ which give commuting squares of the above form and then extend the result to the other spaces. First, we need a lemma about the powers of canonical basis elements.

Lemma 4.3.4. *Fix g, $h \in G$ and let $a = a^{h,g}$. Then for $m \in \mathbb{N}$, a^m is the matrix satisfying $1 = a_{h^k g, h^{k+m} g}$ for $k = 1, \ldots, |h|$ and 0 otherwise. Furthermore, for $m, n \in \mathbb{N}$, we have*

$$a^m a^{*n} = \begin{cases} a^{m-n} & \text{if } m \geq n \\ a^{*(n-m)} & \text{if } n > m \end{cases}$$

where we define a^0 to be the matrix with $1 = a^0_{h^k g, h^k g}$ for $k = 1, \ldots, |h|$ and 0 otherwise.

Proof. We induct on m. The result is trivial when $m = 1$. Assume for some $m \in \mathbb{N}$, a^m is as claimed. Let $S_h = \langle h \rangle g$. Fix $g', h' \in G$. Clearly if $g' \notin S_h$, we have $(a^{m+1})_{g',h'} = 0$. For $g' \in S_h$, we have $(a^m)_{g',\tilde{h}} = \delta_{\tilde{h}}^{h^m g'}$. Hence, for $g' \in S_h$, $0 \neq (a^{m+1})_{g',h'} = \sum_{\tilde{h} \in G} a^m_{g',\tilde{h}} a_{\tilde{h},h'} \Leftrightarrow h' = h^{m+1} g$.

For $g', h' \in G$, we have $0 \neq (a^m a^{*n})_{g',h'} = \sum_{\tilde{h} \in G} a^m_{g',\tilde{h}} a^{*n}_{\tilde{h},h'}$ if and only if $g' \in S_h$, $\tilde{h} = h^m g'$ and $h' = h^{-n}\tilde{h} = h^{-n+m} g'$. Thus, for $m \geq n$ we have $a^m a^{*n} = a^{m-n}$ and for $m < n$, $a^m a^{*n} = a^{*(n-m)}$.

■

Note that for g, $h \in G$ and $a = a^{h,g}$, we have $aa^* = a^0 = a^* a$. Thus, the binomial theorem will apply to $(a + a^*)^n$ for each $n \in \mathbb{N}$. Hence, we have the following:

Corollary 4.3.1. *Fix g, $h \in G$ and let $a = a^{h,g}$. For $t \in \mathbb{R}$, if $U_t = e^{\mathrm{it}(\mathrm{a}+\mathrm{a}^*)}$ and $V_t = e^{\mathrm{it}\left(\frac{\mathrm{a}-\mathrm{a}^*}{\mathrm{i}}\right)}$, then*

$$U_t = I + \sum_{p \geq 1} \frac{(\mathrm{it})^{\mathrm{p}}}{p!} \sum_{q=0}^{p} \binom{p}{q} a^q a^{*p-q}$$

and

$$V_t = I + \sum_{p \geq 1} \frac{t^p}{p!} \sum_{q=0}^{p} \binom{p}{q} (-1)^{p-q} a^q a^{*p-q}.$$

Theorem 4.3.1. *Fix $k, l \in G$ and let $a = a^{l,k}$. For $t \in \mathbb{R}$, if $U_t = e^{\mathrm{it}(\mathrm{a}+\mathrm{a}^*)}$ or if $U_t = e^{\mathrm{it}\left(\frac{\mathrm{a}-\mathrm{a}^*}{\mathrm{i}}\right)}$, then*

$$\mathfrak{C} = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & , \tau \\ \mathbb{C} I_n & \subset & U_t \mathbb{C}[G] U_t^* & \end{pmatrix}$$

is a commuting square.

Proof. The main idea of the proof is that we know that

$$\mathfrak{C} = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) & \\ \cup & & \cup & , \tau \\ \mathbb{C}I_n & \subset & \mathbb{C}[G] & \end{pmatrix}$$

is a commuting square. Thus, if we can show that for each $p \in \mathrm{D}$ and $q \in \mathbb{C}[G]$, we have $\tau(pq) = \tau(pU_t q U_t^*)$, then the result will follow since by applying to $p \in \mathrm{D} \ominus \mathbb{C}$, we will obtain $\tau(pU_t q U_t^*) = 0$ which is precisely the commuting square condition. We will use that $\tau(pq) = \tau(pqU_t U_t^*)$. Therefore, by Lemma 4.3.4 and the previous corollary, it suffices to show that for each g, $h \in G$, we have $\tau(d_g u_h x y) = \tau(d_g x u_h y)$ for any x and y which are powers of a or a^* and for $y = I_n$. Fix $p, q \in \mathbb{N}$, g, $h \in G$, and let $S_l = \langle l \rangle k$. We first show the result when $y = I_n = I$. Then

$$\begin{aligned} \tau(d_g u_h a^p) &= \sum_{h' \in S_l} a^p_{h^{-1}g, h'} I_{h', g} \\ &= \delta^{l^{-p}g}_{h^{-1}g} \left| S_l \cap \{g\} \right| \\ &= \delta^{l^p}_{h} \left| S_l \cap \{g\} \right| \end{aligned}$$

and

$$\begin{aligned} \tau(d_g a^p u_h) &= \sum_{h' \in S_l} a^p_{g, h'} I_{h^{-1}h', g} \\ &= \delta^{l^{-p}hg}_{g} \left| S_l \cap \{hg\} \right| \\ &= \delta^{l^p}_{h} \left| S_l \cap \{hg\} \right|. \end{aligned}$$

When $h = l^p$, we have $|S_l \cap \{g\}| \neq \emptyset$ if and only if $hg \in S_l$ which shows $\tau(d_g u_h a^p) = \tau(d_g a^p u_h)$.

A similar argument shows that $\tau(d_g u_h a^{*p}) = \tau(d_g a^{*p} u_h)$. Next, we show the result when $y = a^q$. Indeed,

$$\begin{aligned}
\tau(d_g u_h a^p a^q) &= \sum_{h' \in S_l} a^p_{h^{-1}g,h'} a^q_{h',g} \\
&= \sum_{h' \in S_l} \delta_g^{l^q h'} a^p_{h^{-1}l^q h',h'} \\
&= \sum_{h' \in S_l} \delta_g^{l^q h'} \delta_{h^{-1}l^q h'}^{l^{-p}h'} \\
&= \delta_h^{l^{q+p}} \left| S_l \cap \{g\} \right|
\end{aligned}$$

and similarly

$$\begin{aligned}
\tau(d_g a^p u_h a^q) &= \sum_{h' \in S_l} a^p_{g,h'} a^q_{h^{-1}h',g} \\
&= \sum_{h' \in S_l} \delta_g^{l^{-p}h'} \delta_{h^{-1}h'}^{l^{-q}l^{-p}h'} \\
&= \delta_h^{l^{q+p}} \left| S_l \cap \{g\} \right|.
\end{aligned}$$

A nearly identical proof as above establishes $\tau(d_g u_h a^{*p} a^{*q}) = \delta_{h^{-1}}^{l^{p+q}} \left| S_l \cap \{g\} \right| = \tau(d_g a^{*p} u_h a^{*q})$. We now check $\tau(d_g u_h a^p a^{*q}) = \tau(d_g a^p u_h a^{*q})$.

$$\begin{aligned}
\tau(d_g u_h a^p a^{*q}) &= \sum_{h' \in S_l} a^p_{h^{-1}g,h'} a^{*q}_{h',g} \\
&= \sum_{h' \in S_l} \delta_g^{l^{-q}h'} a^p_{h^{-1}l^{-q}h',h'} \\
&= \sum_{h' \in S_l} \delta_g^{l^{-q}h'} \delta_{h^{-1}l^{-q}h'}^{l^{-p}h'} \\
&= \delta_h^{l^{p-q}} \left| S_l \cap \{g\} \right|
\end{aligned}$$

and similarly

$$\begin{aligned}\tau(d_g a^p u_h a^{*q}) &= \sum_{h'\in S_l} a^p_{g,h'} a^{*q}_{h^{-1}h',g}\\ &= \sum_{h'\in S_l} \delta_g^{l^{-p}h'} a^{*q}_{h^{-1}h',l^{-p}h'}\\ &= \sum_{h'\in S_l} \delta_g^{l^{-p}h'} \delta_{h^{-1}h'}^{l^q l^{-p}h'}\\ &= \delta_h^{l^{p-q}} \left|S_l \cap \{g\}\right|.\end{aligned}$$

An identical argument shows $\tau(d_g u_h a^{*p} a^q) = \delta_h^{l^{q-p}} \left|S_l \cap \{g\}\right| = \tau(d_g a^{*p} u_h a^q)$.

■

Fix $k,\ l \in G$ and let $a = a^{l,k}$. In the previous theorem, we proved the existence of a family of commuting squares in the directions $a + a^*$ and $\frac{a-a^*}{\mathrm{i}}$. We have $a^* = a^{l^{-1},k}$. It follows that $a = a^*$ if and only if $|l| = 1$, or 2. For $|l| > 2$, it also follows that $a + a^*$ and $\frac{a-a^*}{\mathrm{i}}$ are both nonzero Hermitians. Note that $a = \frac{1}{2}(a + a^*) + \frac{\mathrm{i}}{2}\left(\frac{a-a^*}{\mathrm{i}}\right)$. It is then clear that the Hermitians orthogonal to $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ are generated by the distinct nonzero elements of the form $a + a^*$ and $\frac{a-a^*}{\mathrm{i}}$ where $a = a^{h,g}$ for some $g,\ h \in G$ and in fact, these form a basis for the Hermitians orthogonal to $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]$ since linear independence follows from the fact that the nonzero entries of $a^{h,g}$ are zero entries for $a^{l,k}$ if either $h \neq l$ or $h = l$ and $k \notin \langle h\rangle g$ which was shown in the proof of Theorem 4.3.

Remark 4.3.2. *From the preceding result it follows that $d(G)$ is the best possible bound for the number of independent directions of convergence, in the following sense: there exists a basis for $[\mathrm{D}, \mathbb{C}[\mathrm{G}]]^{\perp}$, such that for every a in the basis there is an analytic family of commuting squares containing $\mathfrak{C}_G$ and of direction a. However, it is not true in general that every (hermitian of unit length) $a \in [\mathrm{D}, \mathbb{C}[\mathrm{G}]]^{\perp}$ is a direction of convergence.*

Example 4.3.3. *Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. If*

$$a = \begin{pmatrix} 0 & -1 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}.$$

then $a \in [\mathrm{D}, \mathbb{C}[\mathrm{G}]]^{\perp}$, *but* a *is not a direction of convergence.*

We now try to get the same result for basis elements of $\{h : h \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]], \mathrm{D}, \mathbb{C}[\mathrm{G}]\}$. First, we will alter our basis for $\{h : h \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]\}$. Note that for $g \in G$,

$$\begin{aligned} \tau(au_g) &= \sum_{h,h'} a_{h,h'} (u_g)_{h',h} \\ &= \sum_{h} a_{h,gh}. \end{aligned}$$

Let k, $l \in G$, $a = a^{l,k}$ and $S_l = \langle l \rangle k$. We have

$$\begin{aligned} \sum_{h} a_{h,gh} = \sum_{h \in S_l} a_{h,gh} &\neq 0 \\ &\Leftrightarrow gh = lh \\ &\Leftrightarrow g = l. \end{aligned}$$

Therefore, we have the following fact:

Remark 4.3.4. *Let* $h, g_1, g_2 \in G$. *Then* $a^{h,g_1} - a^{h,g_2}$ *is orthogonal to* $\mathbb{C}[G]$.

This leads to the following definition:

Definition 4.3.5. *Let* g, $h \in G$. *We define a matrix* $\alpha^{h,g} \in \mathrm{M_n}(\mathbb{C})$ *by*

$$\alpha^{h,g} = a^{h,e} - a^{h,g}.$$

Thus, for $g,\ h \in G$, it follows that $\alpha^{h,g} \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]] + \mathbb{C}[G]$. Note that $a^{h,g}$ has each diagonal entry equal to 0 unless $h = e$. Furthermore, if $g \in \langle h \rangle$, then $\alpha^{h,g} = 0$. For $h \in G$, let $g_1^h = e, \ldots, g^h_{[G:\langle h \rangle]}$ denote coset representatives of $G/\langle h \rangle$. So, our candidate for a basis is

$$\{\alpha^{h,g_i^h} : h \in G \setminus \{e\}, 2 \leq i \leq [G : \langle h \rangle]\}.$$

Note that linear independence follows from the fact that the nonzero entries of $a^{h,g}$ are zero entries for $a^{l,k}$ if either $h \neq l$ or $h = l$ and $k \notin \langle h \rangle g$ which was proven in the proof of Theorem 4.3. To check they span, suppose $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]\,, \mathrm{D}, \mathbb{C}[\mathrm{G}]$. Then write $a = \sum_{h,i} \beta_{h,g_i} a^{h,g_i^h}$ for some $\beta_{h,g_i} \in \mathbb{C}$ and a^{h,g_i^h} is a canonical basis for $\{a : a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]\}$ for each h and i. Now $a \perp \mathrm{D}$ tells us that none of the h's are e. For $h \in G$, we have $\sum_{h'} a_{h',hh'} = 0$ and it follows that $\beta_{h,e} = -\sum_{i \geq 2} \beta_{h,g_i}$ for each $h \in G$ (since the entries $a_{h',hh'}$ are the nonzero entries of $a^{h,g}$ for some g) and consequently, $\sum_i \beta_{h,g_i} a^{h,g_i^h} = \sum_{i \geq 2} \beta_{h,g_i} \left(a^{h,g_i^h} - a^{h,e}\right)$.

Proposition 4.3.6. *Let $h \in G$ and $g \notin \langle h \rangle$. Then $a^{h,e}a^{h,g} = 0 = a^{h,g}a^{h,e}$ and $a^{h,e}(a^{h,g})^* = 0 = (a^{h,g})^* a^{h,e}$.*

Proof. We check one of the products is 0 as the others follow in a similar fashion. We have $(a^{h,e}a^{h,g})_{g',h'} \neq 0 \Leftrightarrow g' \in \langle h \rangle$, $hg' \in \langle h \rangle g$ and $h' = h^2 g'$. It follows that from $hg' \in \langle h \rangle g$ that $g' \in \langle h \rangle g$ which contradicts the fact that $\langle h \rangle$ and $\langle h \rangle g$ are distinct cosets.

■

Corollary 4.3.7. *Let $h \in G$ and $g \notin \langle h \rangle$. For $m \in \mathbb{N}$, we have*

$$(\alpha^{h,g})^m = (a^{h,e})^m + (-1)^m (a^{h,g})^m.$$

It is easy to see that $\alpha^{h,g}(\alpha^{h,g})^* = (\alpha^{h,g})^* \alpha^{h,g}$ and hence the binomial theorem may be applied to $\left(\alpha^{h,g} + (\alpha^{h,g})^*\right)^n$ for each $n \in \mathbb{N}$.

Corollary 4.3.8. *Let $h \in G$ and $g \notin \langle h \rangle$. If $U_t = e^{it(\alpha^{h,g} + (\alpha^{h,g})^*)}$, then*

$$U_t = I + \sum_{p \geq 1} \frac{(it)^p}{p!} \sum_{q=0}^{p} \binom{p}{q} \left((a^{h,e})^q (a^{h,e})^{*(p-q)} + (-1)^n (a^{h,g})^q (a^{h,g})^{*(p-q)}\right).$$

Theorem 4.3.9. *Let $h \in G$ and $g \notin \langle h \rangle$. For $t \in \mathbb{R}$, if $U_t = e^{it(\alpha^{h,g}+(\alpha^{h,g})^*)}$, then*

$$\mathfrak{C} = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n(\mathbb{C})} \\ \cup & & \cup \\ \mathbb{C}I_n & \subset & U_t\mathbb{C}[G]U_t^* \end{pmatrix}$$

is a commuting square.

Proof. Theorem 4.3.1 tells us $\tau(pqxy) = \tau(pxqy)$ and $\tau(pqx) = \tau(pxq)$ for all $p \in \mathrm{D}$ and $q \in \mathbb{C}[G]$ whenever x and y are powers of $a^{h,e}$ or $(a^{h,e})^*$, whenever x and y are powers of $a^{h,g}$ or $(a^{h,g})^*$, and whenever x is a power of $a^{h,e}$, $(a^{h,e})^*$, $a^{h,g}$, or $(a^{h,g})^*$ and $y = I$. Thus, it suffices to check that $\tau(pxqy) = 0$ whenever x is a power of $a^{h,e}$ or $(a^{h,e})^*$ and y is a power of $a^{h,g}$ or $(a^{h,g})^*$ and vice-versa (as Proposition 4.3.6 shows that $\tau(d_{g'}u_{h'}xy) = 0$). To that end, let $l, m \in \mathbb{N}$. Fix $h', g' \in G$. We show $\tau\left(d_{g'}\left(a^{h,e}\right)^l u_{h'}\left(a^{h,g}\right)^m\right) = 0$. Indeed,

$$\begin{aligned}\tau(d_{g'}(a^{h,e})^l u_{h'}(a^{h,g})^m) &= \sum_k \left((a^{h,e})^l\right)_{g',k}\left((a^{h,g})^m\right)_{(h')^{-1}k,g'} \\ &= 0 \text{ as } g' \in \langle h \rangle \text{ and } g' \in \langle h \rangle g \text{ is impossible.}\end{aligned}$$

The fact that the other mixed powers are 0 is proved in exactly the same way.

■

Let $h \in G$ and $g \notin \langle h \rangle$. The previous theorem gives an analytic family in the direction $\alpha^{h,g} + (\alpha^{h,g})^*$. We ask "are these parametric families isomorphic?" More generally, "can $U_2^k = p_1^k d_1^k U_1^k F p_2^k d_2^k F^*$ for infinitely many k where d_1^k, d_2^k unitary diagonals and p_1^k, p_2^k permutation matrices"? To answer this question, we need a couple of lemmas.

Lemma 4.3.5. *Suppose x_k are unitaries and $x_k \to x$ with $\frac{x_k - x}{\mathrm{i}||\mathrm{x_k - x}||} \to X$. Then there exists $\{\lambda_k\}$ with $\lambda_n \in \mathbb{C}$ and $|\lambda_k| = 1$ such that $\lambda_k x_k \to x$ and $\frac{\lambda_k x_k - x}{\mathrm{i}||\lambda_k \mathrm{x_k - x}||} \to \widetilde{X}$ with $\tau(\widetilde{X}x^*) = 0$.*

Proof. Since $D = \{\lambda : |\lambda = 1|\}$ is compact, for each k there exists λ_k such that

$$||\lambda_k x_k - x||_2 = \inf_{|\lambda|=1} \{||\lambda x_k - x||_2\}.$$

Note that $||\lambda_k x_k - x||_2 \leq ||x_k - x||_2 \to 0$. Therefore, $\lambda_k x_k \to x$. Recall, for u unitary, $||u - I||_2^2 = 2 - 2\mathbb{R}\tau(u)$. Thus, $\mathbb{R}\tau(\lambda_k x_k x^*) \geq \mathbb{R}\tau(\lambda x_k x^*)$ for all $|\lambda| = 1$. Hence,

$$\mathbb{R}\tau(\lambda_k(e^{\mathrm{i}\lambda} - 1)x_k x^*) \leq 0$$

for all $\lambda \in \mathbb{R}$. By dividing with $\lambda > 0$ and taking the limit as λ approaches 0, we obtain $\mathbb{R}\tau(\mathrm{i}\lambda_\mathrm{k}\mathrm{x}_\mathrm{k}\mathrm{x}^*) \leq 0$; doing the same for $\lambda < 0$, we have $\mathbb{R}\tau(\mathrm{i}\lambda_\mathrm{k}\mathrm{x}_\mathrm{k}\mathrm{x}^*) \geq 0$. Thus,

$$\mathbb{R}\tau(\mathrm{i}\lambda_\mathrm{k}\mathrm{x}_\mathrm{k}\mathrm{x}^*) = 0.$$

Equivalently, $\mathbb{R}\tau(\mathrm{i}(\lambda_\mathrm{k}\mathrm{x}_\mathrm{k}\mathrm{x}^* - \mathrm{I})) = 0$. Let $\widetilde{X} = \lim_{k\to\infty} \frac{\lambda_k x_k x^* - I}{\mathrm{i}||\lambda_\mathrm{k}\mathrm{x}_\mathrm{k}\mathrm{x}^* - \mathrm{I}||}$ (after passing to a subsequence if needed). Dividing the previous equality by $||\lambda_k x_k x^* - I||$ and taking the limit, we have $\mathbb{R}\tau(\mathrm{i}(\mathrm{i}\widetilde{\mathrm{X}})) = 0$. Since $\widetilde{X}$ is hermitian, we have $\tau(\widetilde{X}) = \mathbb{R}\tau(\widetilde{X}) = 0$.

■

Lemma 4.3.6. *Suppose d_1, d_2 are diagonal matrices and p_1, p_2 are permutation matrices in $\mathrm{M_n}(\mathbb{C})$ which satisfy*

$$p_1 d_1 F d_2 p_2 F^* = I.$$

Then if σ_1 and σ_2 are permutations associated to p_1 and p_2 respectively, there exists b such that $(b, n) = 1$ such that

$$\sigma_1(k) = \sigma_1(0) - bk$$

and

$$\sigma_2^{-1}(k) = \sigma_2^{-1}(0) - b^{-1}k.$$

Furthermore, if $\epsilon = e^{\frac{2\pi i}{n}}$,

$$d_{1,\sigma_1(k)} = d_{1,0}\epsilon^{bk\sigma_2^{-1}(0)}$$

and

$$d_{2,\sigma_2^{-k}} = d_{2,0}\epsilon^{b^{-1}k\sigma_1(0)}$$

for any k.

Proof. Letting σ_i denote the permutation defining p_i and $\epsilon = e^{\frac{2\pi i}{n}}$, we see that

$$\epsilon^{kl} = \epsilon^{\sigma_1^{-1}(k)\sigma_2^{-1}(l)} d_{1,\sigma_1(k)} d_{2,\sigma_1^{-1}(l)}.$$

We now find necessary and sufficient conditions on the permutations for solutions to exist. Let $x_{k,l} = \epsilon^{kl-\sigma_1(k)\sigma_2^{-1}(l)}$. Suppose d and d' are diagonal matrices satisfying $d_k d'_l = x_{kl}$, then $d'_l = \frac{x_{k'l'}}{d'_k}$ for all k', l'. It follows that $\frac{d_k}{d'_k} = \frac{x_{kl}}{x_{k'l'}}$. Thus, a necessary condition on x_{kl} is that for $1 \leq k, k', l, l'$ we have

$$\frac{x_{kl}}{x_{k'l}} = \frac{x_{kl'}}{x_{k'l'}}.$$

In fact, this is sufficient. Suppose the equality is satisfied. Choose $d_0 d'_0 = x_{00}$ and set $d_k = d_0 \frac{x_{k0}}{x_{00}}$ and $d'_l = d'_0 \frac{x_{0l}}{x_{00}}$. Then

$$d_k d'_l = d_0 \frac{x_{k0}}{x_{00}} d'_0 \frac{x_{0l}}{x_{00}} = \frac{x_{k0}x_{0l}}{x_{00}} = \frac{x_{kl}x_{00}}{x_{00}}.$$

Thus, we get that σ_1 and σ_2 must satisfy

$$kl - \sigma_1(k)\sigma_2^{-1}(l) \equiv \sigma_1(0)\sigma_2^{-1}(0) - \sigma_1(0)\sigma_2^{-1}(l) - \sigma_1(k)\sigma_2^{-1}(l) \text{ for } 0 \leq k, l \leq n-1$$

or equivalently

$$kl \equiv (\sigma_1(0) - \sigma_1(k)) \left(\sigma_2^{-1}(0) - \sigma_2^{-1}(l)\right) \text{ for } 0 \leq k, l \leq n-1.$$

Choose a such that $1 = \sigma_2^{-1}(0) - \sigma_2^{-1}(a)$. Then, we have $ka \equiv \sigma_1(0) - \sigma_1(k)$ for all k. It follows that $(a, n) = 1$. Similarly, we get that $\sigma_2^{-1}(0) - \sigma_2^{-1}(k) \equiv bk$ with $(b, n) = 1$. Since $kl \equiv abkl$ for all k, l, we must have $b = a^{-1}$. Thus, there exists b with $(b, n) = 1$ and

$$\sigma_1(k) = \sigma_1(0) - bk$$

and

$$\sigma_2^{-1}(k) = \sigma_2^{-1}(0) - b^{-1}k.$$

■

Theorem 4.3.10. *Let $h_1, h_2 \in G$, $g_1 \notin \langle h_1 \rangle$, $g_2 \notin \langle h_2 \rangle$ and s_k, $t_k \in \mathbb{R}$. Let $U_k^1 = e^{it_k(\alpha^{h_1,g} + (\alpha^{h_1,g})^*)}$, and $U_k^2 = e^{is_k(\alpha^{h_2,g} + (\alpha^{h_2,g})^*)}$. If $|h_1| \neq |h_2|$, then it is not possible that $\mathfrak{C}_k^1$ is isomorphic to $\mathfrak{C}_k^2$ for infinitely many k where*

$$\mathfrak{C}_k^i = \begin{pmatrix} \mathrm{D} & \subset & \mathrm{M_n}(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C}I_n & \subset & U_k^i \mathbb{C}[G] U_k^{i*} \end{pmatrix}.$$

Then

Proof. Assume there exists permutation matrices p_i^k and unitary diagonal matrices d_i^k for $i = 1, 2$ with $p_1^k d_1^k U_1^k F p_2^k d_2^k F^* = U_2^k$ for all k. By passing to subsequences and using that the set of permutations matrices is finite, we may assume $d_i^k \to d_i$ and $p_i^k = p_i$. First, we find which d_i and p_i can work. Taking the limit, we have

$$p_1 d_1 F d_2 p_2 F^* = I.$$

Applying Lemma 4.3.6, we have there exists b with $(b, n) = 1$ such that

$$\sigma_1(l) = \sigma_1(0) + bl,$$
$$\sigma_2^{-1}(l) = \sigma_2^{-1}(0) + b^{-1}l,$$

and

$$d_{1,\sigma_1(l)} = d_{1,0}\epsilon^{-bl\sigma_2^{-1}(0)} \text{ for all } l.$$

By passing to subsequences, we may assume $\lim_k \frac{d_i^k - d_i}{||d_i^k - d_i||} = D_i$ where D_i is a diagonal matrix. By replacing d_1^k with $\lambda_k d_1^k$ and d_2^k with $\overline{\lambda_k} d_2^k$ as in Lemma 4.3.5, we may assume that $\tau(D_1 d_1^*) = 0$. Note that this does not change the relation $p_1 d_1^k U_1^k F d_2^k p_2 F^* = U_2^k$. Let $r_k = \max\{||d_1^k - d_1||, ||d_2^k - d_2||, ||U_1^k - I||, ||U_2^k - I||\}$. Then there exists constants δ_i and α_i for $i = 1, 2$ with

$$\lim_n \frac{d_i^k - d_i}{r_k} = \delta_i D_i \text{ and } \lim_k \frac{U_i^k - I}{k_n} = \alpha_i \alpha^{h_i, g_i} \text{ for } i = 1, 2.$$

Indeed, $\alpha_i = \lim_k \frac{||U_i^k - I||}{r_k}$ and $\delta_i = \lim_k \frac{||d_i^k - d_i||}{r_k}$ for $i = 1, 2$. Furthermore, $0 \leq \alpha_1, \alpha_2, \delta_1, \delta_2 \leq 1$ and at least one of α_1, α_2, δ_1, and δ_2 are nonzero since the max is achieved for each k; if all are zero, then for large n, we have

$$\frac{||U_i^k - I||}{r_k} < \frac{1}{2} \text{ and } \frac{||d_i^k - d_i||}{r_k} < \frac{1}{2} \text{ for } i = 1, 2$$

which is a contradiction as at least one of them is 1 for each k. Since $p_1 d_1 F d_2 p_2 F^* = I$,

$$U_2^k - I = p_1(d_1^k - d_1)U_1^k F d_2^k p_2 F^* + p_1 d_1 (U_1^k - I) F d_2^k p_2 F^* + p_1 d_1 F (d_2^k - d_2) p_2 F^*.$$

Dividing by r_k and taking the limit, we have

$$\alpha_2\left(\alpha^{h_2,g_2}+(\alpha^{h_2,g_2})^*\right)=p_1(\delta_1 D1)Fd_2p_2F^*+p_1d_1\alpha_1\left(\alpha^{h_1,g_1}+(\alpha^{h_1,g_1})^*\right)Fd_2p_2F^*+p_1d_1F(\delta_2D_2)p_2F^*$$
$$=\delta_1p_1D_1d_1^*p_1^*+\alpha_1p_1d_1\left(\alpha^{h_1,g_1}+(\alpha^{h_1,g_1})^*\right)d_1^*p_1^*+\delta_2Fp_2^*d_2^*D_2p_2F^*.$$

Note that $p_1D_1d_1^*p_1^*$ and $p_2^*d_2^*D_2p_2$ are both diagonal matrices.

We have that $d_{1,\sigma_1(p)}=d_0\epsilon^{-\sigma_2^{-1}(0)bp}$ for any p. Therefore,

$$(p_1d_1\alpha^{h_1,g_1}d_1^*p_1^*)_{k,l}=\epsilon^{-\sigma_2^{-1}(0)b(k-l)}\left(\alpha^{h_1,g_1}+(\alpha^{h_1,g_1})^*\right)_{\sigma_1(k),\sigma_1(l)}.$$

For any $g\in G$, $(a^{h_1,g}+\left(a^{h_1,g}\right)^*)_{\sigma_1(k),\sigma_1(l)}\neq 0$ if and only if $\sigma_1(k)=h_1p+g$ and $\sigma_1(l)=h_1(p\pm 1)+g$ for some $1\le p\le |h_1|$ if and only if $k=b^{-1}h_1p+b^{-1}(g-\sigma_1(0))$ and $b(l-k)=\pm h_1$ for some $1\le p\le |h_1|$. Note that since $(b,n)=1$, $|b^{-1}h_1|=|h_1|$. Letting $a=a^{b^{-1}h_1,-b^{-1}\sigma_1(0)}-a^{b^{-1}h_1,b^{-1}(g-\sigma_1(0))}$, we then have that

$$p_1d_1\left(\alpha^{h_1,g_1}+(\alpha^{h_1,g_1})^*\right)d_1^*p_1^*=\epsilon^{-h_1\sigma_1(0)}a+\left(\epsilon^{-h_1\sigma_1(0)}a\right)^*.$$

By Remark 4.3.4, it follows that $p_1d_1(\alpha^{h_1,g_1}+(\alpha^{h_1,g_1})^*)d_1^*p_1^*$ is orthogonal to D and FDF^*. Hence, we must have $\alpha_2\left(\alpha^{h_2,g_2}+(\alpha^{h_2,g_2})^*\right)-\alpha_1p_1d_1\left(\alpha^{h_1,g_1}+(\alpha^{h_1,g_1})^*\right)d_1^*p_1^*=0$ which can only happen if $\alpha_1=\alpha_2=0$ since $|h_1|\neq|h_2|$. We conclude that

$$0=\delta_1p_1D_1d_1^*p_1^*+\delta_2Fp_2^*d_2^*D_2p_2F^*$$

with both δ_1 and δ_2 nonzero which can only happen only when $D_i=\beta_id_i$ for some constants β_1 and β_2 (since for a diagonal d, FdF^* is circulant). It follows that $\lim_n \frac{d_1^n-d_1}{||d_1^n-d_1||}=\beta_1d_1$ with $0=\tau(\beta_1d_1d_1^*)$ and hence, $\beta_1=0$ which is a contradiction as $||\beta_1d_1||=1$.

■

Bibliography

[1] Teodor Banica. The defect of generalized Fourier matrices. *Linear Algebra Appl.*, 438(9):3667–3688, 2013. 10, 22, 23, 56

[2] Kyle Beauchamp and Remus Nicoara. Orthogonal maximal abelian -subalgebras of the matrices. *Linear Algebra and its Applications*, 428(8-9):1833 – 1853, 2008. 17

[3] Göran Björck. Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and "cyclic n-roots". pages 131–140. 21

[4] A. T. Butson. Generalized hadamard matrices. *Proc. Am. Math. Soc.*, 13:894–898, 1962. 19

[5] Erik Christensen. Subalgebras of a finite algebra. *Mathematische Annalen*, 1978. 4

[6] P Diţă. Some results on the parametrization of complex hadamard matrices. *Journal of Physics A: Mathematical and General*, 37(20):5355, 2004. 15

[7] Petre Diţă. Four-parameter families of complex hadamard matrices of order six. 2012. 20

[8] Bent Fuglede. Commuting self-adjoint partial differential operators and a group theoretic problem. *Journal of Functional Analysis*, 16(1):101–121, May 1974. 20

[9] Uffe Haagerup. Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots. *Institut for Matematik, U. of Southern Denmark*, 29:296–322, 1996. 15, 17, 34, 43, 48

[10] Marshall Hall, Jr. *Combinatorial theory (2nd ed.)*. John Wiley & Sons, Inc., New York, NY, USA, 1998. 12

[11] I.D. Ivanovic. Geometrical description of quantal state determination. *J. Phys. A.*, 14, 1981. 24

[12] V. Jones. Index for subfactors. *Inventiones mathematicae*, 72:1–25, 1983. 25, 27, 28

[13] V. Jones and V.S. Sunder. *Introduction to subfactors.* Cambridge: Cambridge University Press, 1997. 1

[14] V. F. R. Jones. Planar algebras, I. Technical report, 1999. 25

[15] V.F.R. Jones. Index for subfactors. *Invent. Math.*, 72:1–25, 1983. 1

[16] Franco Magri. A Simple model of the integrable Hamiltonian equation. *J.Math.Phys.*, 19:1156–1162, 1978. 34, 46

[17] M. Matolcsi and F. Szöllősi. Constructions of complex hadamard matrices via tiling abelian groups. *Open Syst. Inform. Dynam.*, 14(3):247–264, 2007. 15

[18] M. Matolcsi and F. Szöllősi. Towards the classification of 6×6 complex hadamard matrices. *Open Sys. & Inf. Dyn.*, 15, 2008. 18, 20

[19] Remus Nicoara. A finiteness result for commuting squares of matrix algebras. *J. Operator Theory*, pages 295–310, 2006. 2, 4, 21, 33, 38, 39

[20] Remus Nicoara. Subfactors and Hadamard matrices. *J. Oper. Theory*, 64(2):453–468, 2010. 2

[21] Remus Nicoara. Limit points of commuting squares. *Indiana Univ. Math. J.*, 60(3):847–858, 2011. 3, 59

[22] Remus Nicoara and Joseph White. The defect of a group-type commuting square. *Revue Roumaine de Mathematiques Pures et Appliquees*, page to appear. 52

[23] Remus Nicoara and Joseph White. Twisted commuting squares. *International Journal of Mathematics*, 24(05):1350036, 2013. 33

[24] A V Odesskii and V V Sokolov. Integrable matrix equations related to pairs of compatible associative algebras. *Journal of Physics A: Mathematical and General*, 39(40):12447, 2006. 34, 46

[25] R. E. A. C. Paley. On orthogonal matrices. *J. Math. Phys.*, pages 311–320, 1933. 12

[26] Mihai Petrescu. *Existence of continuous families of complex hadamard matrices of certain prime dimensions and related results*. PhD thesis, University of California, Los Angeles, 1997. AAI9803521. 21, 49, 58

[27] S. Popa. Orthogonal pairs of $*$-subalgebras in finite von Neumann algebras. *Journal of Operatory Theory*, 9:253–268, 1983. 7

[28] S. Popa. Classification of subfactors: the reduction to commuting squares. *Inventiones mathematicae*, 101(1):19–43, 1990. 1, 25

[29] S. Popa. Classification of amenable subfactors of type II. *Acta Mathematica*, 172:163–255, 1994. 1, 25

[30] S. Popa. Universal construction of subfactors. *J. Reine Angew. Math.*, 543:39–81, 2002. 25

[31] A. J. Skinner, V. A. Newell, and R. Sanchez. Unbiased bases (hadamards) for 6-level systems: Four ways from fourier. 2008. 20

[32] James Joseph Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, (232):461–475. 11

[33] Wojciech Tadej and Karol Życzkowski. A concise guide to complex Hadamard matrices. *eprint arXiv:quant-ph/0512154*, December 2005. 9, 15, 22, 23, 34, 40, 43

[34] Terence Tao. Fuglede's conjecture is false in 5 and higher dimensions. *Math. Res. Lett.*, 11(2-3):251–258, 2004. 20

Vita

Joseph Robert Halley White was born December 25, 1983 and grew up in Dallas, TX and Atlanta, GA. He received Bachelor of Arts degrees in Mathematics and French and a Bachelor of Science degree in Economics from Georgia College and State University, The Public Liberal Arts University of Georgia in 2005. In 2007, he received a Master of Science degree in Mathematics from Clemson University. While completing the Doctorate of Philosophy in Mathematics at the University of Tennessee, he completed a Master of Science in Statistics through the Intercollegiate Graduate Statistics Program. He married Sarah Alice Baker in January 2007. In January of 2008, their eldest child, Hannah Halley White, was born and in October 2012, their youngest child, Adam Hugh White, was born.