Construction and Classification Results for Commuting Squares of Finite Dimensional $*$-Algebras

A Dissertation Presented for the

Doctor of Philosophy

Degree

The University of Tennessee, Knoxville

Chase Thomas Worley

August 2017

© by Chase Thomas Worley, 2017
All Rights Reserved.

To my family

Acknowledgments

I would like to thank my advisor, Dr. Remus Nicoara, for all of help, support and encouragement. Without a doubt, my graduate school experience would have been completely different if I had not taken his courses during my first three years. His honesty and willingness to push helped me grow mathematically beyond what I thought was possible. I am extremely grateful that he chose me as his second Ph.D. student.

I would be remiss not to mention my fellow graduate students in the department. Though there are too many to name, I am deeply indebted to the encouragement and aid that I received from each of you.

I would also like to thank my doctoral committee members Drs. Remus Nicoara, Stefan Richter, Carl Sundberg, and George Siopsis.

Abstract

In this dissertation, we present new constructions of commuting squares, and we investigate finiteness and isolation results for these objects. We also give applications to the classification of complex Hadamard matrices and to Hopf algebras.

In the first part, we recall the notion of commuting squares which were introduced by Popa and arise naturally as invariants in Jones' theory of subfactors. We review some of the main known examples of commuting squares such as those constructed from finite groups and from complex Hadamard matrices. We also recall Nicoara's notion of defect which gives an upper bound for the number of continuous deformations in the space of commuting squares. Finally, we prove new formulas that lead to computations of defects.

In the second part, we prove a finiteness result for circulant core Hadamard matrices (and thus, for their associated commuting squares). We show that the number of such matrices is finite when the order of the matrix is $p+1$ with p a fixed prime number. We then discuss concrete examples of these matrices of small orders.

In the third part, we give an explicit construction of multi-parametric analytic families of commuting squares obtained as deformations of group commuting squares. In the particular case of cyclic groups of non-prime orders, this gives multi-parametric families of complex Hadamard matrices containing the Fourier matrix. This result expands on the work of Nicoara and White. We then give bounds on the number of parameters in any family stemming from our construction method. We also discuss other parametric families containing the Fourier matrix, some of which include our families as (equivalent) sub-families.

In the last part, we construct a new class of commuting squares which we call bismash commuting squares. They are obtained from bismash product Hopf algebras based on exact factorizations of finite groups, L. We then investigate the defect of a bismash commuting

square which leads us to the conjecture that the defect of the commuting square is equal to the defect of the group L. We prove this conjecture when L is the direct or semidirect product of two proper subgroups.

Table of Contents

1 Introduction **1**

1.1 Commuting Squares and the Span Condition 1

1.1.1 The Span Condition 2

1.2 Defect of Group-Type commuting Squares 3

1.3 Hadamard Matrices 9

1.3.1 Introduction to Hadamard Matrices 9

1.3.2 Construction and Examples of Hadamard Matrices 10

1.3.3 Properties of Hadamard Matrices 11

1.3.4 Hadamard Matrices of Order 4 14

2 Circulant Core Hadamard Matrices **18**

2.1 Circulant Core Matrices 18

2.2 A Finiteness Result for Circulant Core Hadamard Matrices 28

2.3 Circulant Core Hadamard Matrices of Small Order 32

3 Construction of Multi-Parametric Families of Commuting Squares Through the Fourier Matrix **36**

3.1 Preliminaries 36

3.2 Construction of Multi-Parametric Families 37

3.3 Construction based on elements of order > 2 42

3.4 Construction based on an element of order 2 48

3.5 Inequivalence of Matrices in a Family 56

4 Bismash Commuting Squares **59**

4.1 Introduction to Hopf Algebras 59

4.2 Examples of Hopf Algebras 62

4.3 Hopf Algebras from a matched pair of groups 65

4.3.1 Matched Pair of Groups 65

4.3.2 The Bismash Product Hopf Algebra 71

4.3.3 Some Bismash Products that are Group Algebras 74

4.4 Commuting squares from bismash products 75

4.5 The Undephased Defect of a Bismash Commuting Square 82

4.5.1 Defect Computations 83

4.5.2 Calculating $d(\mathbb{C}^G \# \mathbb{C}[F])$ when $L = F \times G$ 85

4.5.3 Calculating $d(\mathbb{C}^G \# \mathbb{C}[F])$ when $L = F \rtimes G$ 87

4.5.4 Towards calculating $d(\mathbb{C}^G \# \mathbb{C}[F])$ when $L = F \bowtie G$ 89

Bibliography **90**

Vita **95**

List of Figures

4.1 Multiplication Table for the bismash product $\mathbb{C}^{\mathbb{Z}_2}\#\mathbb{C}[\mathbb{Z}_3]$ associated to the group $\mathbb{Z}_6$ (using trivial actions). 73

4.2 Multiplication Table for the bismash product $\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2]$ associated to the group D_3. 73

4.3 A typical element in the bismash product $\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]$ associated to the group A_5. 78

4.4 A typical element in the bismash product $\mathbb{C}^{A_4}\#\mathbb{C}[\mathbb{Z}_5]$ as the dual to $\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]$ associated to the group A_5. 80

Chapter 1

Introduction

Throughout this dissertation, we study commuting squares of finite dimensional von Neumann algebras. We present new construction and finiteness results of commuting squares. Commuting squares were introduced in [29] as invariants and construction data in Jones' subfactor theory [12]. From a given commuting square, one can construct a subfactor by repeating a procedure known as the basic construction.

1.1 Commuting Squares and the Span Condition

We begin by recalling the definition of a commuting square.

Definition 1.1. *A commuting square of matrix algebras is a square of inclusions of the following form:*

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

where P_{-1}, P_0, Q_{-1}, Q_0 *are finite dimensional von Neumann algebras of the form* $\bigoplus_j M_{n_j}(\mathbb{C})$, *and* τ *a positive faithful trace on* P_0 *such that* $\tau(1) = 1$ *satisfying the condition that*

$$(P_{-1} \ominus Q_{-1}) \perp (Q_0 \ominus Q_{-1}),$$

i.e. the algebras P_{-1} and Q_0 are orthogonal modulo their intersection. The inner product on P_0 is defined by the trace on P_0 via $\langle x, y\rangle = \tau(xy^*)$.

An important class of commuting squares are the so called group-type commuting square (or just group commuting square) which we recall. Let G be a group with n elements. For each $g \in G$, let $e_g \in \mathbb{C}^n$ be the column vector with a 1 position g and 0 otherwise. Then we have that the group algebra $\mathbb{C}[G] = \text{span}\{u_g : g \in G\}$ where $u_g \in M_n(\mathbb{C})$ satisfies the relationship $u_g(e_h) = e_{gh}$ for each $h \in G$. In other words, we have that $u_g = \sum_{h\in G} e_{h,g^{-1}h}$ where $\{e_{a,b} : a, b \in G\}$ is the set of standard matrix units of $M_n(\mathbb{C})$ indexed over $G \times G$.

Each finite group G with n elements can be encoded in a group commuting square:

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

where $D \approx \ell^\infty(G)$ is the algebra of $n \times n$ diagonal matrices, and $\mathbb{C}[G]$ denotes the group algebra of G. In this case, $\tau = \frac{1}{n}\text{Tr}$ where Tr is cannonical matrix trace. Throughout this thesis we will refer to this commuting square as the group-type commuting square.

1.1.1 The Span Condition

Nicoara introduced a sufficient condition for a commuting square to be isolated in the class of all non-isomorphic commuting squares, which he called the span condition.

Definition 1.2. *(Span Condition [21]) We say a commuting square as in 1.1 satisfies the span condition if*

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

Recall that $Q' \cap P = \{a \in P : ab = ba \text{ for all } b \in Q\}$.

In the case of the group commuting square, we have that the span condition can be read as

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

where $\mathbb{C}[G]' = \{a \in M_n(\mathbb{C}) : au_g = u_g a \text{ for all } g \in G\}$ and $[D, \mathbb{C}[G]] = span\{du - ud : d \in D, u \in \mathbb{C}[G]\}$. Furthermore, Nicoara in [21] and [23] showed where all possible directions of convergence of sequences containing $\mathfrak{C}_G$ lie when it is not isolated. From this work, all possible directions of convergence of sequences converging to $\mathfrak{C}_G$ must be contained in the vector space

$$M_n(\mathbb{C}) \ominus [D, \mathbb{C}[G]]$$

and all possible directions of convergence of sequences of non-isomorphic commuting squares converging to the group commuting square is contained in the vector space

$$M_n(\mathbb{C}) \ominus ([D, \mathbb{C}[G]] + \mathbb{C}[G] + \mathbb{C}[G]' + D).$$

Recall that $P \ominus Q = P \cap Q^{\perp}$ where the orthogonal complements are given by the inner product defined by τ, the normalized trace on $M_n(\mathbb{C})$ when ever P and Q are subalgebras of $M_n(\mathbb{C})$.

In general, finding commuting squares can be a difficult but important task. With Jones' Basic Construction in [12], we can generate a subfactor from each commuting square. However, it may be the fact that the subfactor found via the basic construction is equivalent to a subfactor generated from a different commuting square. In Chapter 4, we find a new class of commuting squares which involve two groups which we call bismash commuting squares. These commuting squares rely on groups, L, which can be exactly factored by two subgroups, F and G.

1.2 Defect of Group-Type commuting Squares

In [25], Nicoara and White defined the undephased and dephased defects of a group G as the dimensions of the previous two vector spaces above.

Definition 1.3. *The undephased defect of a finite group G with $|G| = n$ is*

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

and the dephased defect of G is

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

Nicoara and White also showed that

Theorem 1.1. *For G a finite group,*

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

and

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

where $|g|$ is the order of the element $g \in G$, $cl(G)$ denotes the class number of G.

Remark 1.1.1. *The span condition is equivalent (in the case for a finite group G) to $d'(G) = 0$. Thus, for a finite group G, if $d'(G) = 0$, then $\mathfrak{C}_G$ is isolated in the class of all non-isomorphic commuting squares.*

Remark 1.1.2. *For $G = \mathbb{Z}_n$, we can easily find the defect by using the Euler Phi function. It follows that*

$$d(G) = \sum_{g \in G} \frac{|G|}{|g|} = \sum_{d|n} \frac{|G|}{d} \varphi(d)$$

where the last sum is taken over all divisors of n. Recall that $\varphi(d)$ can be interpreted as the number of relatively prime numbers less than d, but it will also give us the number of elements of order d in the group G.

Example 1.1. *For p prime, the defect of $\mathbb{Z}_p$ is*

$$d(\mathbb{Z}_p) = \left(\frac{p}{1} + \frac{p}{p} \cdot \varphi(p) \right) = p + (p-1) = 2p - 1.$$

Remark 1.1.3. *Let G be a finite abelian group with n elements giving us that $cl(G) = n$. Then we have that $d'(G) = d(G) - 2n + 1$. If $G = \mathbb{Z}_p$ for some prime p, then*

$$d'(\mathbb{Z}_p) = (2p - 1) - 2p + 1 = 0.$$

In fact, Nicoara showed that $d'(G) = 0$ if and only if $G = \mathbb{Z}_p$ for prime p.

Example 1.2. *Let $G = \mathbb{Z}_{p^r}$ where p is prime and $r \in \mathbb{N}$. Then it follows that*

$$d(G) = p^{r-1}(p(r+1) - r).$$

This follows directly from Remark 1.1.2 and the fact that the Euler phi function of power of a prime is $\varphi(p^k) = p^k - p^{k-1}$.

Example 1.3. *The defect of the quaternion group, Q_8, is $d(Q_8) = 24$. This is easily calculated since there is one element of order 1, one element of order 2, and six elements of order 4.*

We will need the following theorem from group theory:

Theorem 1.2. *(Schur-Zassenhauss) Let H be a normal subgroup of a finite group G such that the order of H and $[G : H]$ are relatively prime. Then there exists a subgroup K of G, called the complement of H in G, such that the order of K is equal to $[G : H]$. Furthermore, K is isomorphic to the group G/H, and all such subgroups of G of order equal to $[G : H]$ are conjugate to each other.*

It should be noted that this implies that G is isomorphic to the semidirect product of H and K, $H \rtimes K$. In the case, when K is also a normal subgroup of G, then G is isomorphic to $H \times K$ (really $H \times G/H$). The Schur-Zassenhaus Theorem allows us to prove a nice property about the defect in a large class of finite groups.

Theorem 1.3. *Let G be a finite group. Let H be a normal subgroup of G. Suppose that the order of H and the index of H in G, $[G : H]$, are relatively prime with G/H isomorphic to a normal subgroup of G. In this case, we have that G is isomorphic to $H \times G/H$. Under these conditions, it follows that*

$$d(G) = d(H)d(G/H).$$

Proof. Let G be a finite group with H a normal subgroup of G. Suppose that H and $[G : H]$ are relatively prime. Then by the Schur-Zassenhaus Theorem, there exists a subgroup K of

order $[G : H]$. Then for each $g \in G$, we can write $g = hk$ for some $h \in H$ and $k \in K$ and $|g| = |hk| = lcm(|h|, |k|) = |h||k|$ (see section 4.3.1 for more information on groups of this form). Hence, by Theorem 1.1

$$\begin{aligned} d(G) &= \sum_{g \in G} \frac{|G|}{|g|} = \sum_{\substack{h \in H \\ k \in K}} \frac{|H|[G : H]}{|hk|} \\ &= \sum_{h \in H} \frac{H}{|h|} \sum_{k \in K} \frac{|K|}{|k|} \\ &= d(H)d(G/H). \end{aligned}$$

□

Example 1.4. *Using this theorem, we can now easily find the defect of the group $G = S_3 \times \mathbb{Z}_5$. Since S_3 is a normal subgroup of G (as a direct factor) and since the groups S_3 and $\mathbb{Z}_5$ have coprime orders, we have that*

$$d(G) = d(S_3)d(\mathbb{Z}_5) = 19(9) = 171.$$

Remark 1.3.1. *Let G be a finite nilpotent group. In this case, $G = P_1 \times \cdots \times P_r$ where P_i is a Sylow p_i-subgroup for primes $p_i \neq p_j$ when $1 \neq i \neq j \leq r$. Then it follows that*

$$d(G) = \prod_{i=1}^{r} d(P_i).$$

Clearly we can use the same idea in remark 1.1.2 in order to find the defect of any cyclic group, but if we can also use the previous remark to calculate the defect of the group. For example, we can easily calculate the defect of the group $\mathbb{Z}_{30}$.

Example 1.5. *Using Remark 1.1.2, the defect of the group $G = \mathbb{Z}_{30}$ is*

$$d(G) = \frac{30}{1} + \frac{30}{2} + \frac{30}{3} \cdot 2 + \frac{30}{5} \cdot 4 + \frac{30}{6} \cdot 2 + \frac{30}{10} \cdot 4 + \frac{30}{15} \cdot 8 + \frac{30}{30} \cdot 8 = 135.$$

Similarly, using Remark 1.3.1, we have that the defect of $G = \mathbb{Z}_{30}$ *is*

$$d(G) = d(\mathbb{Z}_2)d(\mathbb{Z}_3)d(\mathbb{Z}_5) = (2 \cdot 2 - 1)\,(2 \cdot 3 - 1)\,(2 \cdot 5 - 1) = 3 \cdot 5 \cdot 9 = 135.$$

Example 1.6. *We calculate the defects of the group* $\mathbb{Z}_4$ *and* $\mathbb{Z}_2 \times \mathbb{Z}_2$*. It follows that from Example 1.2*

$$d(\mathbb{Z}_4) = 8 \text{ and } d(\mathbb{Z}_2 \times \mathbb{Z}_2) = 10 > 9 = d(\mathbb{Z}_2)d(\mathbb{Z}_2).$$

Notice that $\mathbb{Z}_2 \times \{0\}$ *is a normal subgroup of* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *and* $(\mathbb{Z}_2 \times \mathbb{Z}_2)/(\mathbb{Z}_2 \times \{0\})$ *is isomorphic to* $\mathbb{Z}_2$*. Since the index* $[\mathbb{Z}_2 \times \mathbb{Z}_2 : \mathbb{Z}_2 \times \{0\}] = 2$ *is not relatively prime to 2, we do not have a contradiction to Theorem 1.3. Also, recall that since* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *is a p-group, we have that* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *is itself a Sylow 2-subgroup. In cases such as this, if* G *is a p-group, we will not be able to reduce the calculation of* $d(G)$ *by subgroups of* G *as in Remark 1.3.1.*

Example 1.7. *(Defect of groups of order pq) Let* G *be a group of order pq for primes* p *and* q*. Suppose that* $q < p$*. If* $q \nmid (p-1)$*, then it is an easy exercise to show that* G *must be cyclic. In this case it is easy to show that* G *is isomorphic to* $\mathbb{Z}_p \times \mathbb{Z}_q$*, hence,* G *is nilpotent and therefore we have that*

$$d(G) = d(\mathbb{Z}_p \times \mathbb{Z}_q) = (2p-1)(2q-1) = d(\mathbb{Z}_p)d(\mathbb{Z}_q).$$

If $q|(p-1)$*, then we have that* G *is isomorphic to* $\mathbb{Z}_p \rtimes_\theta \mathbb{Z}_q$ *where* θ *is any non-trivial automorphism. We know that there is only one element of order 1 (namely the identity) and no elements of order pq since the group* G *is not cyclic. Using the Sylow theorems, we know that there is only one Sylow p-subgroup of order p (by normality of* $\mathbb{Z}_p$*). In this case, we have that there must be* $p-1$ *elements of order p. This gives us the fact that there must be* $p(q-1)$*. We can also use the fact that there must be p Sylow q-subgroups each of which has* $q-1$ *elements of order q. Therefore, we have that the defect of* G *in this case is*

$$d(G) = d(\mathbb{Z}_p \rtimes \mathbb{Z}_q) = pq + \frac{pq}{q} \cdot p(q-1) + \frac{pq}{p} \cdot (p-1) + \frac{pq}{pq} \cdot 0 = pq + p^2(q-1) + q(p-1).$$

Notice in the case when $q|(p-1)$, G is not a product of its Sylow subgroups since there is more than one Sylow q-subgroup.

Using the above properties for defect, we can prove the formula for the defect of $\mathbb{Z}_n$ for any n. The formula attained matches exactly the formula found by Tadej and Zyckowski found in [36] in calculating the defect for the Fourier matrix of order n.

Theorem 1.4. *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where $p_1 < p_2 < \cdots < p_r$ are prime numbers, $\alpha_i \geq 1$ for all $1 \leq i \leq r$. It follows that the dephased defect*

$$d'(\mathbb{Z}_n) = n\left(\prod_{i=1}^{r}\left(\alpha_i - \frac{\alpha_i}{p_i} + 1\right) - 2\right) + 1.$$

Proof. Recall from above that the dephased defect can be found via

$$d'(\mathbb{Z}_n) = d(\mathbb{Z}_n) - 3n + 1 - cl(\mathbb{Z}_n) = d(\mathbb{Z}_N) - 2n + 1$$

since $\mathbb{Z}_n$ is an abelian group. By the Chinese Remainder theorem, we have that $\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}$. By Theorem 1.3 and Remark 1.3.1, we have that

$$d(\mathbb{Z}_n) = d(\mathbb{Z}_{p_1^{\alpha_1}}) \cdots d(\mathbb{Z}_{p_r^{\alpha_r}}).$$

Recall from Example 1.2 that

$$d(\mathbb{Z}_{p_j^{\alpha_j}}) = p_j^{\alpha_j - 1}(p_j(\alpha_j + 1) - \alpha_j) = p_j^{\alpha_j}\left(\alpha_j - \frac{\alpha_j}{p_j} + 1\right).$$

Therefore, the undephased defect of $\mathbb{Z}_n$ is

$$d(\mathbb{Z}_n) = n\prod_{i=1}^{r}\left(\alpha_j - \frac{\alpha_j}{p_j} + 1\right).$$

Finally, the dephased defect is

$$d'(\mathbb{Z}_n) = n\prod_{i=1}^{r}\left(\alpha_j - \frac{\alpha_j}{p_j} + 1\right) - 2n + 1 = n\left(\prod_{i=1}^{r}\left(\alpha_i - \frac{\alpha_i}{p_i} + 1\right) - 2\right) + 1.$$

It should be noted that if $n = p$ for some prime p, using this formula, we do in fact get that $d'(\mathbb{Z}_p) = 0$. □

1.3 Hadamard Matrices

1.3.1 Introduction to Hadamard Matrices

One of the simplest and nicest examples of commuting squares is the group commuting square, $\mathfrak{C}_G$, when $G = \mathbb{Z}_n$. In this case, we have that $\mathbb{C}[G] = F_n D F_n^*$ where F_n is the Fourier matrix of size n. We have that $F_n = \frac{1}{\sqrt{n}} \left(\epsilon^{jk}\right)_{j,k=0}^{n-1}$ where $\epsilon = e^{\frac{2\pi \mathrm{i}}{n}}$. This gives us the fact that $\mathbb{C}[G]$ is the set of circulant matrices of size n.

Suppose we have a commuting square of the type

$$\begin{pmatrix} D & \subset & M_n(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C}I_n & \subset & UDU^* \end{pmatrix}$$

where U is a unitary matrix. Then the commuting square property reads for each i, j that

$$0 = \tau((d_i - \frac{1}{n} I_n) U d_j U^*) = \tau(d_i U d_j U^*) - \frac{1}{n}\tau(d_j) = \frac{|u_{i,j}|^2}{n} - \frac{1}{n^2}$$

where $d_i = e_{i,i}$ is one of the canonical basis elements of the diagonal matrices. We can renormalize so that the entries of the matrix are unimodular, and in this case, we have that U must be a Hadamard matrix. When we have a commuting square of this type, we call the commuting square a *spin model* commuting square (see [3], [23], [38]).

Definition 1.4. *A (complex) Hadamard matrix is a matrix with unimodular entries and whose rows are mutually orthogonal.*

In this case, we have that if $H \in M_n(\mathbb{C})$ is a Hadamard matrix, then $HH^* = nI_n$. We have a few basic immediate examples.

Example 1.8. *For each $n \in \mathbb{N}$, the Fourier matrix of size n, $F_n = \frac{1}{\sqrt{n}} \left(\epsilon^{jk}\right)_{j,k=0}^{n-1}$, where $\epsilon = e^{\frac{2\pi \mathrm{i}}{n}}$ is an example of a (complex) Hadamard matrix.*

Since we require the entries of a Hadamard matrix to be unimodular, we have that the entires of a real Hadamard matrix are ± 1. For a matrix H to be a real Hadamard matrix, we have that the size of the matrix is either 1, 2 or a multiple of 4.

It is an obvious fact that the size of a real Hadamard matrix is even since the entries are ± 1, it is necessary that there are the same number of 1's as there are -1's. Since we require the rows of the matrix to be mutually orthogonal, we have that the size of the matrix must be divisible by 4. Because of this fact, we have the following

Conjecture 1.4.1. *(Hadamard Conjecture [27]) There exists a real $n \times n$ Hadamard matrix for $n = 4m$ for every $m \in \mathbb{N}$.*

1.3.2 Construction and Examples of Hadamard Matrices

We can construct Hadamard matrices of larger orders based on Hadamard matrices of smaller orders. For instance, we have the following:

Lemma 1.4.1. *If $A \in M_n(\mathbb{C})$ and $B \in M_m(\mathbb{C})$ are Hadamard matrices, then it follows that their Kronecker product $A \otimes B \in M_{nm}(\mathbb{C})$ is also a Hadamard matrix.*

Proof. Since A and B are Hadamard matrices, we have that $AA^* = nI_n$ and $BB^* = mI_m$. So, it follows that

$$\begin{aligned}(A \otimes B)(A \otimes B)^* &= (A \otimes B)(A^* \otimes B^*) \\ &= AA^* \otimes BB^* \\ &= nI_n \otimes mI_m \\ &= nm(I_n \otimes I_m) \\ &= nmI_{nm}\end{aligned}$$

□

Recall that the Kronecker product of two matrices A and B, $A \otimes B$, will be a block matrix whose $(i,j)^{\text{th}}$ block is $(A)_{i,j}B$. The above method allows us to find the following example due to Sylvester [32] in 1867:

Example 1.9. *We may construct a Hadamard matrix of order 2^k for every $k \in \mathbb{N}$. Let*

$$H_1 = \begin{bmatrix} 1 \end{bmatrix}$$
$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$
$$H_{2^k} = \begin{bmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{bmatrix} = H_2 \otimes H_{2^{k-1}} \quad \textit{for all } 2 \leq k \in \mathbb{N}$$

Hadamard gave examples of Hadamard matrices of order 12 and 20 in 1893 [11]. In 1933, the Payley construction [27] gives Hadamard matrices of order $p+1$ when $p = 3 \mod 4$ and prime, and of order $2(p+1)$ when p is a prime equivalent to $1 \mod 4$. His method uses finite fields. We will revisit this construction in the next chapter.

The smallest order not given by Sylvester or Payley is $92 = 4 \cdot 23$. A Hadamard matrix of order 92 was found in 1962 by Baumart, Golomb, and Hall using computers. In 2005, a matrix of order 428 was found [13]. By 2008, there were 13 multiples of 4 less than 2000 for no Hadamard matrix is known for that order. Those were

$$668, 716, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1916, 1948, 1964$$

1.3.3 Properties of Hadamard Matrices

Let H be a Hadamard matrix of order n. Since the rows of H are mutually orthogonal, we have that

$$HH^* = nI_n.$$

This follows from the inner product defined on $\mathbb{C}^n$. We should also note the following property:

Proposition 1.4.1. *Let H be a Hadamard matrix of order n. Then it follows that*

$$|\det(H)| = n^{n/2}.$$

Proof. It follows that

$$n^n = \det(nI_n) = \det(HH^*) = |\det(H)|^2.$$

□

We can always find "new" Hadamard matrices given a Hadamard matrix H.

Proposition 1.4.2. *If H is a Hadamard matrix, then so too is H^*, H^T, and $\overline{H}$.*

These are fairly straightforward. Notice that if $HH^* = nI_n$. Then $\frac{1}{n}H$ is a unitary matrix, therefore it is normal, meaning that it commutes with its conjugate transpose. Therefore, $H^*H = nI_n$. The other two are straightforward as well.

There is a notion of equivalence of Hadamard matrices defined by $H \sim K$.

Definition 1.5. *The complex Hadamard matrices H and K are called equivalent if there are permutation matrices P_1 and P_2 and unitary diagonal matrices D_1 and D_2 such that*

$$P_1 D_1 H D_2 P_2 = K.$$

In this case, we say that $H \sim K$.

This notion of equivalence uses the fact that the rearrangement of rows and columns and multiplying each element in a given row or column by an element of absolute value 1 does not change the properties of the Hadamard matrix. The rows and columns will still be mutually orthogonal and the elements will still have values on the unit circle. We usually write the Hadamard matrix in its dephased form.

Definition 1.6. *A Hadamard matrix, H, of order n is dephased if every entry of the first row and column of H is equal to 1. The lower right $(n-1) \times (n-1)$ submatrix is called the core of H.*

It is clear to see that

Lemma 1.4.2. *Every Hadamard matrix is equivalent to a dephased matrix.*

Due to this lemma, we will mainly consider only dephased Hadamard matrices. Most examples are of permutation type meaning that the core is determined by the first row (of the core) and a set of permutations. In fact all real Hadamard matrices are of this type. This is due to the fact that each row of the core must contain $(n-1)$ 1's and n (-1)'s. The nicest example of permutation type matrices is when the core is circulant. In the next chapter, we will show that the number of Hadamard matrices with a circulant core of a particular size is in fact finite.

As mentioned at the beginning of this section, when G is a cyclic group of order n, we have that the group algebra, $\mathbb{C}[G] = F_n D F_n^*$ where D is the algebra of diagonal matrices of order n. Recall from group theory that $G = \mathbb{Z}_n$ can be decomposed as $\mathbb{Z}_n = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ (when n is non-prime). There are at least two ways that we can write this decomposition. One way is for each n_i to be coprime to n_j when $i \neq j$ and $1 \leq i, j \leq r$. We may ask when can we decompose F_n as a Kronecker product of Fourier matrices of smaller order. We have the following theorem:

Theorem 1.5. *(Tadej [34]) Let $F = F_{n_1} \otimes \cdots \otimes F_{n_r}$ be a Kronecker product of Fourier matrices. Then F is equivalent to $F_{m_1} \otimes \cdots \otimes F_{m_s}$ if and only if the sequence $(m_1, \cdots, m_s)$ is obtained from the sequence $(n_1, \cdots, n_r)$ using a series of operations from the list below:*

1. *permuting a sequence;*
2. *replacing a subsequence n_a, n_b by $n_c = n_a n_b$ if n_a and n_b are relatively prime;*
3. *replacing a sequence element n_c by a subsequence n_a, n_b, if $n_c = n_a n_b$ and n_a, n_b are relatively prime.*

This allows to see immediately that the Fourier matrices F_4 and $F_2 \otimes F_2$ are inequivalent. Recall that

$$F_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix} \text{ and } F_2 \otimes F_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Without the use of this theorem, it would be difficult to determine if these two matrices are not equivalent. Later in Chapter 3, we will introduce another method for determining that the matrices F_4 and $F_2 \otimes F_2$ are in fact inequivalent using the Haagerup-set.

1.3.4 Hadamard Matrices of Order 4

We have seen that there are at least two examples of Hadamard matrices of order 4. We may ask if F_4 and $F_2 \otimes F_2$ are the only two Hadamard matrices of order 4. If H is a Hadamard matrix of order 4, we may assume that it is in dephased form. Therefore, H will have the form

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & x_0 & x_1 & x_2 \\ 1 & y_0 & y_1 & y_2 \\ 1 & z_0 & z_1 & z_2 \end{bmatrix}.$$

Lemma 1.5.1. *Let $x_0, x_1, x_2 \in \mathbb{T}$ with $1 + x_0 + x_1 + x_2 = 0$, then $x_0 \in \{-1, -x_1, -x_2\}$.*

Proof. It follows that

$$\begin{aligned}(x_0+1)(x_0+x_1)(x_0+x_2) &= x_0^3 + x_0^2x_1 + x_0^2x_2 + x_0x_1x_2 + x_0^2 + x_0x_1 + x_0x_2 + x_1x_2 \\ &= x_0^2(1 + x_0 + x_1 + x_2) + x_0x_1x_2(1 + \overline{x_0} + \overline{x_1} + \overline{x_2}) \\ &= x_0^2 \cdot 0 + x_0x_1x_2 \cdot 0 = 0\end{aligned}$$

Hence, we have that $x_0 \in \{-1, -x_1, -x_2\}$. □

Therefore, we may assume in H that $x_0 = -1$ which would imply that $x_2 = -x_1$ since the second row of H must be orthogonal to the first row of H. Let $x_1 = a$. Substituting these values in H, we have that

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \\ 1 & y_0 & y_1 & y_2 \\ 1 & z_0 & z_1 & z_2 \end{bmatrix}.$$

In the third row, we can play the same game. Set $y_0 = -1$. In this case, we need row three and row one giving us that $y_1 = -y_2$. Since the third row must be orthogonal to the second row as well, it must be the case that $y_1 = -a$. This yields the matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \\ 1 & -1 & -a & a \\ 1 & z_0 & z_1 & z_2 \end{bmatrix}.$$

At this point, we cannot play the same game with the last row. Notice first that since H is Hadamard, then so too is H^*. This tells us that the columns of H must be orthogonal as well as its rows. Therefore, z_0 must be equal to 1. Using the fact that row three is orthogonal to row one yields

$$z_1 + z_2 = -2,$$

and furthermore using the orthogonality to row two yields

$$az_1 - az_2 = 0 \implies z_1 = z_2.$$

In this case, we have that $z_1 = z_2 = -1$. Therefore, the matrix is

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \\ 1 & -1 & -a & a \\ 1 & 1 & -1 & -1 \end{bmatrix}.$$

Rearranging the columns and rows of H to write it in an equivalent form, we have that

$$H \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & a & -1 & -a \\ 1 & -1 & 1 & -1 \\ 1 & -a & -1 & a \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & a & -1 & -a \\ 1 & -a & -1 & a \end{bmatrix}.$$

In order for H to be a Hadamard matrix, we need a to be an element of absolute value equal to 1. It is clear to see that if $a = i$, then H is equivalent to F_4, and if $a = 1$, then H is equivalent to $F_2 \otimes F_2$.

We have shown that there are infinitely many Hadamard matrices of order 4. In fact, we have found a one-parameter family of Hadamard matrices. In fact, each of the matrices in the above family are inequivalent. This is not an easy fact to immediately see, but as mentioned earlier we will see a method to show that all matrices in this family are inequivalent. In Chapter 3, we will show explicit construction methods for finding multi-parameter families containing the Fourier matrix of non-prime sizes.

Notice that we can always create a parametric family that contains any Hadamard matrix that we choose. For instance, we have the following example.

Example 1.10. *Let F_3 be the Fourier matrix of order 3. We have that F_3 belongs to the family*

$$F_3(\alpha, \beta) = \begin{bmatrix} 1 & 1 & \alpha \\ \beta & \beta\omega & \alpha\beta\omega^2 \\ 1 & \omega^2 & \alpha\omega \end{bmatrix}.$$

It is clear however that for each value of α, β the matrix is equivalent to the Fourier matrix F_3. Therefore, we really haven't gained any new information. For this reason, each time we find a new family we will write it in its equivalent dephased form.

In fact, it is a well known that there is no family of Hadamard matrices containing the Fourier matrix of order 3. This is due to a result found by Petrescu and independently proved by Nicoara. This is due to the fact that the Fourier matrix of order 3 is isolated in the class of Hadamard matrices.

Definition 1.7. *A Hadamard matrix H is isolated in the class of Hadamard matrices if there is no parametric family of Hadamard matrices containing H.*

Theorem 1.6. *(Petrescu [28]) Let F_n be the Fourier matrix of order n. Then F_n is isolated in the class of Hadamard matrices if and only if n is prime.*

This result follows from the following fact:

Theorem 1.7. *The dephased defect of $\mathbb{Z}_n$ is 0 if and only if n is prime.*

Why do we look at the defect in this case? We us Nicoara's result that the undephased defect of $\mathbb{Z}_n$ gives an upper bound for the number of parameters in a parametric family containing F_n. In fact, we also have that the dephased defect gives an upper bound for the number of parameters in a parametric family of inequivalent Hadamard matrices containing F_n [25].

Chapter 2

Circulant Core Hadamard Matrices

In this chapter, we prove a finiteness result for circulant core Hadamard matrices. This result is interesting due to the fact that we will be able to construct only finitely many spin model commuting squares where the upper left corner has a certain dimension. We start by recalling the definition of circulant core matrices.

2.1 Circulant Core Matrices

Definition 2.1. *A **circulant core** matrix is a matrix with all entries in the first row and column equal to one and whose submatrix formed by deleting the first row and column is circulant.*

A typical circulant core matrix has the form

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & x_0 & x_1 & \cdots & x_{n-2} \\ 1 & x_{n-2} & x_0 & \cdots & x_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 1 & x_1 & x_2 & \cdots & x_0 \end{bmatrix}$$

Let A' be a circulant matrix, then the matrix $A = \begin{bmatrix} 1 & 1 \\ 1 & A' \end{bmatrix}$ is a circulant core matrix. Then it follows that $A^* = \begin{bmatrix} 1 & 1 \\ 1 & (A')^* \end{bmatrix}$ is a circulant core matrix since $(A')^*$ is circulant whenever A' is circulant.

For our purposes, we will only examine the circulant core matrices whose elements in the second row sum to 0. We will call this set, $\mathcal{Q}$. It can be shown that elements of $\mathcal{Q}$ commute, and are therefore simultaneously diagonalizable. Let X be a circulant core matrix with core defined by the vector $(x_0, \cdots, x_{n-2})$. Unless otherwise noted, all subscripts are to be taken modulo $n-1$ for n the order of the matrix. It follows that for $1 \leq j \leq n-1$

$$(X^*X)_{0j} = \sum_{k=0}^{n-1} X^*_{0k} X_{kj} = \sum_{k=0}^{n-1} X_{kj} = 1 + \sum_{k=1}^{n-1} x_{(j-k) \mod (n-1)} = 1 + \sum_{k=0}^{n-2} x_k.$$

If we require that X is Hadamard, then it must be the case that $(X^*X)_{0j} = 0$. Hence, when X is Hadamard, then $\sum_{k=1}^{n-1} x_k = -1$, or in other words, the sum of the elements in the second row (every row but the first). If we can show that the number of matrices in $\mathcal{Q}$ is finite, then we have that the number of Hadamard circulant core matrices is finite since they are contained in $\mathcal{Q}$. If $X \in \mathcal{Q}$, then $X^* \in \mathcal{Q}$ since X^* is a circulant core matrix by the above argument and $\sum_{k=0}^{n-2} x_k = -1 \implies \sum_{k=0}^{n-2} \overline{x}_k = \overline{\sum_{k=0}^{n-2} x_k} = -1$.

Example 2.1. *(Paley Construction [27], see [33] as well) We want to construct a Hadamard circulant core matrix of order $p+1$ where p is an odd prime. For $p \equiv 3 \mod 4$, define the core of the matrix Circ(x), the circulant matrix with first row x, where x has the following form:*

$$x_n = \begin{cases} -1 & , n = 0 \\ \left(\frac{n}{p}\right) & , 1 \leq n \leq p-1 \end{cases}$$

where $\left(\frac{n}{p}\right)$ is the Legendre symbol modulo p. Specifically, if n is a quadratic residue modulo p, then $\left(\frac{n}{p}\right) = 1$, and otherwise $\left(\frac{n}{p}\right) = -1$. (Note that there are the same number of quadratic residues as nonresidues modulo p.)

For $p \equiv 1 \mod 4$, define the core by the vector x where

$$x_n = \begin{cases} -1 & , n = 0 \\ i\left(\frac{n}{p}\right) & , 1 \leq n \leq p-1 \end{cases}$$

where $i = \sqrt{-1}$.

Note that the sum of the elements of vector x is in fact -1 since it is a well known fact that $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0$. For these matrices to be Hadamard, we also need the second row (the first row that isn't all 1's) to be orthogonal to the remaining rows. In other words for $1 \leq k \leq p-1$,

$$1 + \sum_{n=1}^{p-1} x_n \overline{x_{n-k}} = 0.$$

Let $X, Y \in \mathcal{Q}$ with circulant cores X' and Y' respectively. Since X' and Y' are circulant matrices, we know that $X'Y' = Y'X'$.

If $i \neq 0 \neq j$, then we have

$$\begin{aligned} (XY)_{ij} &= \sum_{k=0}^{n-1} x_{ik} y_{kj} \\ &= 1 + \sum_{k=1}^{n-1} x_{k-i} y_{j-k} \\ &= 1 + (X'Y')_{ij} \\ &= 1 + (Y'X')_{ij} \\ &= (YX)_{ij} \end{aligned}$$

If $i = 0, j \neq 0$, then

$$(XY)_{0j} = \sum_{k=0}^{n-1} x_{0k} y_{kj} = \sum_{k=0}^{n-1} y_{kj} = 1 + \sum_{k=1}^{n-1} y_{j-k}$$
$$(YX)_{0j} = \sum_{k=0}^{n-1} y_{0k} x_{kj} = \sum_{k=0}^{n-1} x_{kj} = 1 + \sum_{k=1}^{n-1} x_{j-k}$$

A similar calculation can be shown when $i \neq 0, j = 0$, the difference being that $(XY)_{i0}$ is based on the sum of the x_k's and $(YX)_{i0}$ is based on the sum of the y_k's. Note that

$$(XY)_{00} = \sum_{k=0}^{n-1} x_{0k}y_{k0} = \sum_{k=0}^{n-1} 1 = n = \sum_{k=0}^{n-1} 1 = \sum_{k=0}^{n-1} y_{0k}x_{k0} = (YX)_{00}.$$

Therefore, if we want the matrices X and Y commute, then we need $\sum_{k=1}^{n-1} y_{j-k} = \sum_{k=1}^{n-1} x_{j-k}$. In particular, all elements of $\mathcal{Q}$ will commute since we have that $\sum_{k=1}^{n-1} x_{j-k} = \sum_{k=1}^{n-1} y_{j-k} = -1$.

In the rest of this section, we will prove a technical result that we need in later sections. We find the diagonal form of a circulant core Hadamard matrix. To diagonalize the elements of $\mathcal{Q}$, we use the following matrix:

$$w = \begin{bmatrix} 1-\sqrt{n} & 1+\sqrt{n} & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & \lambda_1 & \lambda_2 & \cdots & \lambda_{n-2} \\ 1 & 1 & (\lambda_1)^2 & (\lambda_2)^2 & \cdots & (\lambda_{n-2})^2 \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & 1 & (\lambda_1)^{n-1} & (\lambda_2)^{n-1} & \cdots & (\lambda_{n-1})^{n-2} \\ 1 & 1 & (\lambda_1)^{n-2} & (\lambda_2)^{n-2} & \cdots & (\lambda_{n-2})^{n-2} \end{bmatrix}$$

where $\lambda_j = e^{i2\pi j/(n-1)}$.

In other words, the matrix which diagonalizes $\mathcal{Q}$ is

$$w = \begin{bmatrix} 1-\sqrt{n} & 1+\sqrt{n} & 0 & \cdots & 0 \\ 1 & & & & \\ \vdots & & & F_{n-1} & \\ 1 & & & & \end{bmatrix}$$

where F_{n-1} is the Fourier matrix of size $n-1$. Throughout, unless otherwise noted, we will take $\hat{x}_j$ to be the j^{th} entry of the Fourier Transform of the vector $x = (x_0, x_1, \cdots, x_{n-2})$. Note that

$$\hat{x}_j = \sum_{k=0}^{n-2} e^{i2\pi kj/(n-1)} x_k.$$

Note

$$F_{n-1}^* \text{Diag}(x) F_{n-1} = \text{Diag}(\hat{x}_0, \hat{x}_1, \cdots, \hat{x}_{n-2}).$$

An interesting property of the matrix w is that

$$\det(w) = (1-\sqrt{n})\det(F_{n-1}) - (1+\sqrt{n})\det(F_{n-1}) = -2\sqrt{n}\det(F_{n-1}).$$

We calculate the determinant using the first row. Since the first and second columns are filled have a one in every position except for the the first, when we delete the first row with either the first or second column, we are left with the Fourier matrix of order $n-1$.

We will now examine the elements of w, w_{jk}.

$$\begin{aligned}
w_{00} &= 1-\sqrt{n} \\
w_{01} &= 1+\sqrt{n} \\
w_{0k} &= 0 \text{ for } 2 \le k \le n-1 \\
w_{j0} &= 1 \text{ for } 1 \le j \le n-1 \\
w_{jk} &= e^{i2\pi(j-1)(k-1)/(n-1)} \text{ for } 1 \le j,k \le n-1
\end{aligned}$$

Let $w = u|w|$ where u is a unitary matrix and $|w| = \sqrt{w^*w}$. This is the polar decomposition of the matrix w. In this case, $u = w|w|^{-1}$ (if $|w|^{-1}$ is well-defined). Clearly, by using a simple calculation, we can see that $u^*u = uu^* = I$.

Since $|w|^{-1}$ is a diagonal matrix (see the calculation for w^*w that follows shortly), we have that $u_{jk} = w_{jk}|w|_{kk}^{-1}$. We now examine the elements of u^*u.

Notice that if w diagonalizes $a \in \mathcal{Q}$, then the matrix u also diagonalizes a. This follows by

$$\begin{aligned} u^* a u &= u^{-1} a u \\ &= (w|w|^{-1})^{-1} a w |w|^{-1} \\ &= |w| w^{-1} a w |w|^{-1} \\ &= |w| d |w|^{-1} \\ &= |w| |w|^{-1} d \\ &= d \end{aligned}$$

where d is the diagonal matrix obtained by conjugating a by w and since $|w|$ is a diagonal matrix, we have that $|w|,\ |w|^{-1}$, and d all commute.

Notice also that if u diagonalizes the matrix a, then w also diagonalizes a since (using the same notation as above)

$$\begin{aligned} w^{-1} a w &= (u|w|)^{-1} a (u|w|) \\ &= |w|^{-1} u^{-1} a u |w| \\ &= |w|^{-1} u^* a u |w| \\ &= |w|^{-1} d |w| \\ &= |w|^{-1} |w| d \\ &= d. \end{aligned}$$

Hence, w diagonalizes $a \in \mathcal{Q}$ if and only if u diagonalizes the matrix a.

We need to examine the matrix w^*w. It follows that $(w^*w)^* = w^*w$, and

$$
\begin{aligned}
(w^*w)_{00} &= (1-\sqrt{n})^2 + (n-1) = 2(n-\sqrt{n}) \\
(w^*w)_{10} &= (w^*w)_{01} = (1+\sqrt{n})(1-\sqrt{n}) + (n-1) = 0 \\
(w^*w)_{k0} &= (w^*w)_{0k} = 0 + \sum_{k=1}^{n-1} e^{i2\pi k/(n-1)} = 0 \text{ for } 2 \le k \le n-1 \\
(w^*w)_{11} &= (1+\sqrt{n})^2 + (n-1) = 2(n+\sqrt{n}) \\
(w^*w)_{kk} &= 0 * 0 + \sum_{k=0}^{n-2} e^{i2\pi k/(n-1)} e^{-i2\pi k/(n-1)} = n-1 \text{ for } 2 \le k \le n-1 \\
(w^*w)_{21} &= (w^*w)_{12} = \sum_{j=0}^{n-1} (w^*)_{2j} w_{j1} = 0(1+\sqrt{n}) + \sum_{j=1}^{n-1} e^{-i2\pi(k-1)/(n-1)} \cdot 1 = 0 \\
(w^*w)_{2k} &= (w^*w)_{k2} = \sum_{j=0}^{n-1} \overline{w}_{j2} w_{jk} = \sum_{j=1}^{n-1} \overline{w}_{j2} w_{jk} = \sum_{j=1}^{n-1} e^{-i2\pi(j-1)/(n-1)} \cdot e^{i2\pi(k-1)(j-1)/(n-1)} \\
&= \sum_{j=1}^{n-1} e^{i2\pi(j-1)(k-2)/(n-1)} = (n-1)\delta_{2k} \text{ for } 2 \le k \le n-1 \\
(w^*w)_{jk} &= \sum_{m=0}^{n-1} \overline{w}_{mj} w_{mk} = \sum_{m=1}^{n-1} \overline{w}_{mj} w_{mk} = \sum_{m=1}^{n-1} e^{i2\pi(m-1)(k-j)/(n-1)} \\
&= (n-1)\delta_{jk} \text{ for } 2 \le j,k \le n-1
\end{aligned}
$$

Hence, we have that

$$
w^*w = \begin{bmatrix}
2(n-\sqrt{n}) & 0 & 0 & 0 & \cdots & 0 \\
0 & 2(n+\sqrt{n}) & 0 & 0 & \cdots & 0 \\
0 & 0 & n-1 & 0 & \cdots & 0 \\
0 & 0 & 0 & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & n-1 & 0 \\
0 & 0 & 0 & \cdots & 0 & n-1
\end{bmatrix}
$$

Therefore, the matrix $|w|^{-1}$ is in fact well-defined meaning that we can actually find the matrix u using the method described. Given the matrix w^*w, we may now explicitly right

down the matrix u as the following

$$u = \begin{bmatrix} \frac{1-\sqrt{n}}{\sqrt{2(n-\sqrt{n})}} & \frac{1+\sqrt{n}}{\sqrt{2(n+\sqrt{n})}} & 0 & \cdots & 0 \\ \frac{1}{\sqrt{2(n-\sqrt{n})}} & \frac{1}{\sqrt{2(n+\sqrt{n})}} & \frac{1}{\sqrt{n-1}} & \cdots & \frac{1}{\sqrt{n-1}} \\ \frac{1}{\sqrt{2(n-\sqrt{n})}} & \frac{1}{\sqrt{2(n+\sqrt{n})}} & \frac{\lambda_1}{\sqrt{n-1}} & \cdots & \frac{\lambda_{n-2}}{\sqrt{n-1}} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ \frac{1}{\sqrt{2(n-\sqrt{n})}} & \frac{1}{\sqrt{2(n+\sqrt{n})}} & \frac{\lambda_1^{n-2}}{\sqrt{n-1}} & \cdots & \frac{\lambda_{n-2}^{n-2}}{\sqrt{n-1}} \end{bmatrix}$$

where $\lambda_j = e^{i2\pi j/(n-1)}$.

We want to show that u diagonalizes $a \in \mathcal{Q}$. This is will be equivalent to showing that w conjugates a by multiplying by w^* on the left and w on the right. Then by using the definition of u, we will find the "nice" entries of the diagonalization. Notice first that

$$(w^*aw)_{jk} = \sum_{m=0}^{n-1}\sum_{r=0}^{n-1} \overline{w}_{mj} a_{mr} w_{rk},$$

and define $d_{jk} := (u^*au)_{jk} = (w^*aw)|w|_{jj}^{-1}|w|_{kk}^{-1}$.

It follows that

$$\begin{aligned}
(w^*aw)_{00} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m0}a_{m0}w_{00} + \sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{r0}\right] = \sum_{m=0}^{n-1}\left[\overline{w}_{m0}\left((1-\sqrt{n}) + \sum_{r=1}^{n-1}a_{mr}\right)\right] \\
&= (1-\sqrt{n})\left((1-\sqrt{n}) + \sum_{r=1}^{n-1}a_{0r}\right) + \sum_{m=1}^{n-1}\left[\overline{w}_{m0}\left((1-\sqrt{n}) + \sum_{r=1}^{n-1}a_{mr}\right)\right] \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + \sum_{m=1}^{n-1}(1-\sqrt{n}) + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}a_{mr} \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + \sum_{m=1}^{n-1}(1-\sqrt{n}) + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}x_{(r-m) \mod (n-1)} \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + (1-\sqrt{n})(n-1) + (n-1)\sum_{k=0}^{n-2}x_k \\
&= (1-\sqrt{n})((1-\sqrt{n}) + (n-1)) + (1-\sqrt{n})(n-1) + (n-1)(-1) \\
&= -2n(1-\sqrt{n})
\end{aligned}$$

Therefore,

$$d_{00} = \frac{-2n(1-\sqrt{n})}{2(n-\sqrt{n})} = -\sqrt{n}.$$

We continue with

$$\begin{aligned}
(w^*aw)_{11} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m1}a_{m0}w_{01} + \sum_{r=1}^{n-1}\overline{w}_{m1}a_{mr}w_{r1}\right] \\
&= \sum_{m=0}^{n-1}\left[\overline{w}_{m1}\left((1+\sqrt{n}) + \sum_{r=1}^{n-1}a_{mr}\right)\right] \\
&= \overline{w}_{01}((1+\sqrt{n}) + \sum_{r=1}^{n-1}a_{0r}) + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m1}(1+\sqrt{n}) + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m1}a_{mr} \\
&= (1+\sqrt{n})((1+\sqrt{n}) + (n-1)) + (1+\sqrt{n})(n-1) + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m1}a_{mr} \\
&= (1+\sqrt{n})((1+\sqrt{n}) + (n-1)) + (1+\sqrt{n})(n-1) - (n-1) \\
&= 2n(1+\sqrt{n}) \\
\implies d_{11} &= \frac{2n(1+\sqrt{n})}{2(n+\sqrt{n})} = \sqrt{n}
\end{aligned}$$

and

$$\begin{aligned}
(w^*aw)_{01} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m0}a_{m0}w_{01} + \sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}\right] \\
&= \overline{w}_{00}a_{00}w_{01} + \sum_{r=1}^{n-1}\overline{w}_{00}a_{0r} + \sum_{m=1}^{n-1}\overline{w}_{m0}a_{m0}w_{01} + \sum_{m=1}^{n-1}\sum_{m=1}^{n-1}\overline{w}_{m0}a_{mr} \\
&= (1-\sqrt{n})(1)(1+\sqrt{n}) + (1-\sqrt{n})(n-1) + (1+\sqrt{n})(n-1) + (-1)(n-1) \\
&= 0 \\
\implies d_{01} &= d_{10} = 0
\end{aligned}$$

Let $2 \leq j \leq n-1$, then we have that

$$\begin{aligned}
(w^*aw)_{0j} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m0}a_{m0}w_{0j} + \sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj}\right] = \sum_{m=0}^{n-1}\left[\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj}\right] \\
&= \sum_{r=1}^{n-1}\overline{w}_{00}a_{0r}w_{rj} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj} \\
&= (1-\sqrt{n})\sum_{m=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj} \\
&= \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m0}a_{mr}w_{rj} = \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)}x_{(r-m) \mod (n-1)} \\
&= \sum_{r=1}^{n-1}\left[e^{i2\pi(r-1)(j-1)/(n-1)}\sum_{m=1}^{n-1}x_{(r-m) \mod (n-1)}\right] = -\sum_{r=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)} = 0
\end{aligned}$$

$$\implies d_{0j} = d_{j0} = 0 \text{ for } 2 \leq j \leq n-1$$

$$\begin{aligned}
(w^*aw)_{1j} &= \sum_{m=0}^{n-1}\left[\overline{w}_{m1}a_{m0}w_{0j} + \sum_{r=1}^{n-1}\overline{w}_{m1}a_{mr}w_{rj}\right] \\
&= \overline{w}_{01}a_{00}w_{0j} + \sum_{r=1}^{n-1}\overline{w}_{01}a_{0r}w_{rj} + \sum_{m=1}^{n-1}\overline{w}_{m1}a_{m0}w_{0j} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{m1}a_{mr}w_{rj} \\
&= (1+\sqrt{n})(1)(0) + \sum_{r=1}^{n-1}(1+\sqrt{n})(1)e^{i2\pi(r-1)(j-1)/(n-1)} \\
&\qquad + \sum_{m=1}^{n-1}(1)(1)(0) + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}(1)a_{mr}w_{rj} \\
&= \sum_{r=1}^{n-1}\sum_{m=1}^{n-1}a_{mr}w_{rj} = \sum_{r=1}^{n-1}\left[w_{rj}\sum_{m=1}^{n-1}a_{mr}\right] \\
&= (-1)\sum_{r=1}^{n-1}e^{i2\pi(r-1)(j-1)/(n-1)} = 0
\end{aligned}$$

$$\implies d_{1j} = d_{j1} = 0 \text{ for } 2 \leq j \leq n-1$$

Note that $a_{mr} = a_{(m+1)(r+1)}$ for $m, r \geq 1$. For $2 \leq j, k \leq n-1$, we have that

$$
\begin{aligned}
(w^*aw)_{jk} &= \sum_{m=0}^{n-1}\left[\overline{mj}a_{m0}w_{0k} + \sum_{r=1}^{n-1}\overline{w}_{mj}a_{mr}w_{rk}\right] \\
&= \sum_{m=0}^{n-1}\left[\sum_{r=1}^{n-1}\overline{w}_{mj}a_{mr}w_{rk}\right] = \sum_{r=1}^{n-1}\overline{w}_{0j}a_{0r}w_{rk} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{mj}a_{mr}w_{rk} \\
&= \sum_{r=1}^{n-1}(0)(1)w_{rk} + \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{mj}a_{mr}w_{rk} = \sum_{m=1}^{n-1}\sum_{r=1}^{n-1}\overline{w}_{mj}a_{mr}w_{rk} \\
&= \sum_{m=0}^{n-2}\sum_{r=0}^{n-2} e^{i2\pi[-m(j-1)+r(k-1)]/(n-1)}x_{(r-m) \mod (n-1)} \\
&= (n-1)\hat{x}_{j-1}\delta_{jk} \\
\implies d_{jk} &= d_{kj} = \frac{(n-1)\hat{x}_{j-1}}{(n-1)}\delta_{jk} = \hat{x}_{j-1}\delta_{jk}
\end{aligned}
$$

Thus, we have that u^*au is a diagonal matrix, and

$$
u^*au = \begin{bmatrix}
-\sqrt{n} & 0 & 0 & 0 & \cdots & 0 \\
0 & \sqrt{n} & 0 & 0 & \cdots & 0 \\
0 & 0 & \hat{x}_1 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & \hat{x}_{n-3} & 0 \\
0 & 0 & 0 & \cdots & 0 & \hat{x}_{n-2}
\end{bmatrix}
$$

2.2 A Finiteness Result for Circulant Core Hadamard Matrices

In this section, we prove that the number of circulant core Hadamard matrices of order $p+1$ for p a prime number is finite. We first recall the following lemma which is adapted from a result found in a paper of Tao [37]:

Lemma 2.0.1. *(Uncertainty Principle [37]) Let $n = p+1$ where p is a prime number. Then for $a \in \mathcal{Q}$ with core $x = (x_0, \cdots, x_{p-1})$, u as above, and $\tilde{x} = u^*au$ (realizing $\tilde{x}$ as a vector in*

$\mathbb{C}^n$, *we have that*

$$|supp(\tilde{x})| + |supp(x)| \geq n + 1.$$

Proof. By simple calculation, we see that $\tilde{x} = (-\sqrt{n}, \sqrt{n}, \hat{x}_1, \hat{x}_2, \cdots, \hat{x}_{p-1})$. It follows from Tao that

$$|supp(\tilde{x})| + |supp(x)| = 2 + |supp(\hat{x})| - 1 + |supp(x)| \geq 2 - 1 + p + 1 = n + 1.$$

□

Theorem 2.1. *The number of circulant core Hadamard matrices of order $n = p+1$ for p a prime number is finite.*

Proof. This proof imitates the Haagerup's proof of finiteness of cyclic p-roots [10]. Let a be a circulant core Hadamard matrix. Then it follows that $a \in \mathcal{Q}$. Then we have that $aa^* = nI_n$. It follows that $(a^*)_{ij} = \frac{1}{a_{ji}}$, and if $i = 0$, or $j = 0$, then we have that $a_{ij} = 1$. So we have that both a and a^* are circulant core matrices of order n. Diagonalizing the matrices, we have that $a \rightsquigarrow \tilde{x} = (-\sqrt{n}, \sqrt{n}, \hat{x}_1, \cdots, \hat{x}_{p-1})$, and $a^* \rightsquigarrow \tilde{y_-} = (-\sqrt{n}, \sqrt{n}, \hat{y}_{-1}, \cdots, \hat{y}_{-(p-1)})$, where $x = (x_0, \cdots, x_{p-1})$ defines the core of a and $x_k y_k = 1$ for $k = 0, \cdots, p-1$. Since a is Hadamard, we have the following system

$$x_k y_k = 1 \quad \text{for } k = 0, \cdots, p-1$$
$$\hat{x}_k \hat{y}_{-k} = n \quad \text{for } k = 1, \cdots, p-1$$

where the indices are taken modulo p. Since we are interested in the Hadamard Matrices, we know if a is defined by x and a^* is defined by y, we have that a^* is also a Hadamard matrix, so we must have the normalization that

$$\sum_{k=0}^{p-1} x_k = \sum_{k=0}^{p-1} y_k = -1.$$

Therefore, we are interested in the solutions to the following system:

$$\sum_{k=0}^{p-1} x_k = \sum_{k=0}^{p-1} y_k = -1$$
$$x_k y_k = 1 \quad \text{for } k = 0, \cdots, p-1$$
$$\hat{x}_k \hat{y}_{-k} = n \quad \text{for } k = 1, \cdots, p-1$$

Let W be the set of solutions to the above system. We want $|W|$ to be finite. Suppose that $|W|$ is infinite. Then we have that $|W|$ is unbounded since it is a complex algebraic variety [30]. We may choose a sequence $(x^{(m)}, y^{(m)})$, where $x^{(m)} = (x_0^{(m)}, \cdots, x_{p-1}^{(m)})$ and $\left\|x^{(m)}\right\|_2^2 + \left\|y^{(m)}\right\|_2^2 \to \infty$. Notice that by Cauchy-Schwartz, we have the following inequalities for every m:

$$\frac{1}{\sqrt{p}} \leq \left\|x^{(m)}\right\|_2$$
$$\frac{1}{\sqrt{p}} \leq \left\|y^{(m)}\right\|_2$$
$$p \leq \left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2$$

Suppose that no subsequence of $\left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2$ converges to infinity. Then we have that $\left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2 \leq M$ for some $M > 0$ and for all $m > 0$. Then we have that

$$\left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2 \leq M$$
$$\left\|x^{(m)}\right\|_2 \leq \frac{M}{\left\|y^{(m)}\right\|_2}$$
$$\left\|x^{(m)}\right\|_2 \leq M\sqrt{p}$$

Likewise, we have that for all m, $\left\|y^{(m)}\right\|_2 \leq M\sqrt{p}$. Hence, it would be the case that

$$\left\|x^{(m)}\right\|_2^2 + \left\|y^{(m)}\right\|_2^2 \leq 2M^2 p$$

which contradicts the fact that $\left\|x^{(m)}\right\|_2^2 + \left\|y^{(m)}\right\|_2^2 \to \infty$. Therefore, there is at least one subsequence where $\left\|x^{(m)}\right\|_2 \left\|y^{(m)}\right\|_2 \to \infty$. Note that we have renamed the sequence as the subsequence here for simplification purposes. We will use this notion throughout the rest of the proof.

Working with this subsequence, we may also find at least one subsequence such that $\left\|\widehat{x^{(m)}}\right\|_2 \left\|\widehat{y^{(m)}}\right\|_2 \to \infty$.

Define $u^{(m)} = \frac{x^{(m)}}{\left\|x^{(m)}\right\|_2}$, and $v^{(m)} = \frac{y^{(m)}}{\left\|y^{(m)}\right\|_2}$. Since $u^{(m)}$ and $v^{(m)}$ are both in the unit sphere, we have by compactness and by passing to a subsequence if necessary, that the limits of both sequences exist, and we define $u = \lim_{m\to\infty} \frac{x^{(m)}}{\left\|x^{(m)}\right\|_2}$, and $v = \lim_{m\to\infty} \frac{y^{(m)}}{\left\|y^{(m)}\right\|_2}$.

It follows that for $k = 0, \cdots, p-1$,

$$u_k v_k = \lim_{m\to\infty} \frac{x_k^{(m)}}{\|x^{(m)}\|_2} \frac{y_k^{(m)}}{\|y^{(m)}\|_2} = \lim_{m\to\infty} \frac{1}{\|x^{(m)}\|_2 \|y^{(m)}\|_2} = 0.$$

By a similar method, for $k = 1, \cdots, p-1$,

$$\widehat{u}_k \widehat{v}_{-k} = 0.$$

Hence, we have that

$$\operatorname{supp}(u) \cap \operatorname{supp}(v) = \emptyset$$
$$\operatorname{supp}(\hat{u}) \cap -(\operatorname{supp}(\hat{v})) = \emptyset$$

giving us that

$$|\operatorname{supp}(u)| + |\operatorname{supp}(v)| \leq p$$
$$|\operatorname{supp}(\hat{u})| + |\operatorname{supp}(\hat{v})| \leq p - 1 + 2, \text{ we add 2 from our normalization}$$

implying

$$|\operatorname{supp}(u)| + |\operatorname{supp}(v)| + |\operatorname{supp}(\hat{u})| + |\operatorname{supp}(\hat{v})| \leq 2p + 1.$$

We know that

$$\begin{aligned} 2p+4 &\leq |\text{supp}(u)| + |\text{supp}(v)| + |\text{supp}(\tilde{u})| + |\text{supp}(\tilde{v})| \\ &= |\text{supp}(u)| + |\text{supp}(v)| + |\text{supp}(\hat{u})| + |\text{supp}(\hat{v})| + 2(2-1) \\ &\leq 2p+1+2 = 2p+3, \end{aligned}$$

which is impossibile.

Note that in the second line we must add 2(2-1) since the first two entries of $\tilde{u}$ are constant $\pm\sqrt{n}$ so we add 2 to supp($\hat{u}$), but because of our normalization, we have that $\hat{u}_1 = -1$ meaning that we must subtract 1 as well from supp($\hat{u}$) which will then give us supp($\tilde{u}$). The same holds for v. Therefore, we have that $|W|$ must be finite since we reached a contradiction using the fact that $|W|$ was infinite. □

Corollary 2.1.1. *The system*

$$\begin{cases} x_0 = -1 - x_1 - x_2 - \cdots - x_{p-1} \\ \frac{x_1}{x_0} + \frac{x_2}{x_1} + \cdots + \frac{x_0}{x_{p-1}} = -1 \\ \frac{x_2}{x_0} + \frac{x_3}{x_1} + \cdots + \frac{x_1}{x_{p-1}} = -1 \\ \qquad\qquad \vdots \\ \frac{x_{p-1}}{x_0} + \frac{x_0}{x_1} + \cdots + \frac{x_{p-2}}{x_{p-1}} = -1 \end{cases}$$

has finitely many solutions.

Proof. Let $x = (x_0, \cdots, x_{p-1})$. Let A be the circulant core matrix with core Circ(x). Note that the off diagonal entries of AA^* yield the equations of the system. Then by the previous theorem, there are only finitely many such matrices. Thus, there are only finitely many x's. □

2.3 Circulant Core Hadamard Matrices of Small Order

We will now look at the Hadamard circulant core matrices of small order. Recall that we must have that for matrices of order $n \geq 2$, $\sum_{k=0}^{n-2} x_k = -1$. For $n = 2$, we have only one

matrix, namely the Fourier matrix of order 2, F_2,

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

For $n = 3$, we have look at a typical circulant core matrix,

$$a = \begin{bmatrix} 1 & 1 & 1 \\ 1 & x_0 & x_1 \\ 1 & x_1 & x_0 \end{bmatrix}.$$

For this matrix to be Hadamard, we have the following system which follows from $aa^* = 3I$ where I is the identity:

$$\begin{aligned} 1 + x_0 + x_1 &= 0 \\ x_0x_1 + x_1 + x_0 &= 0 \\ x_0x_1 + x_0^2 + x_1^2 &= 0 \end{aligned}$$

It follows that

$$0 = x_0x_1 + x_1 + x_0 = -x_0(1 + x_0) - (1 + x_0) + x_0 = -(x_0^2 + x_0 + 1)$$

which implies $x_0 = e^{i2\pi/3},\ e^{-i2\pi/3}$, and $x_1 = e^{-i2\pi/3},\ e^{i2\pi/3}$. This gives us that there is only one non-equivalent Hadamard circulant core matrix of order 3, namely for $\omega = e^{i2\pi/3}$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}$$

which is the Fourier matrix of order 3.

For $n = 4$, we again have only one solution. This follows from the fact

$$1 + x_0 + x_1 + x_2 = 0$$
$$x_0x_1x_2 + x_0^2x_1 + x_0x_2^2 + x_1^2x_2 = 0$$

We want to determine the possible solutions on the unit circle to above system.

By Lemma 1.5.1, we have that $x_0 \in \{-1, -x_1, -x_2\}$. If $x_0 = -1$, then we have that $x_1 = -x_2$ from the first equation. Substituting what we know into the second equation and simplifying, we have that

$$x_2 - x_2^3 = 0$$

implying that $x_2 = \pm 1$ and $x_1 = \mp 1$. The other cases follow a similar method, since if $x_0 = -x_1$, we have that $x_2 = -1$ from the first equation implying that $x_0 = \pm 1$ and $x_1 = \mp 1$. So up to equivalence of the matrix, we really have one solution. $x_0 = -1$, $x_1 = 1$, and $x_2 = -1$ yielding the matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{bmatrix}.$$

Notice that this matrix is equivalent to $F_2 \otimes F_2$ (seen by interchanging the second and fourth columns).

At the $n = 5$ level, we would expect the matrix F_5 to be (at least equivalent to) a circulant core matrix. From Haagerup [10], we know that any dimension five Hadamard matrix is equivalent to the matrix F_5. Clearly, we see that in its original form F_5 is not a

circulant core matrix, but we have that

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & w^3 & w^4 \\ 1 & w^2 & w^4 & w & w^3 \\ 1 & w^3 & w & w^4 & w^2 \\ 1 & w^4 & w^3 & w^2 & w \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^3 & w^4 & w^2 \\ 1 & w^2 & w & w^3 & w^4 \\ 1 & w^4 & w^2 & w & w^3 \\ 1 & w^3 & w^4 & w^2 & w \end{bmatrix}$$

where $w = e^{i2\pi/5}$ giving us that $P_1F_5P_2$ is a circulant core matrix. Here P_1 and P_2 are permutation matrices. Hence, we have shown that F_5 is equivalent to a circulant core matrix. Therefore, up to equivalence, we have that for $2 \leq n \leq 5$, the Hadamard circulant core matrices of order increasing in n are $F_2,\ F_3,\ F_2 \otimes F_2$, and F_5.

Chapter 3

Construction of Multi-Parametric Families of Commuting Squares Through the Fourier Matrix

In this chapter we construct new multi-parametric deformations of group-type commuting squares and Hadamard matrices expanding on the results of Nicoara and White [26]. This is particularly interesting when G is a cyclic group of order n as it gives us families of Hadamard matrices containing the Fourier matrix of order n (for n nonprime).

3.1 Preliminaries

Let G be a finite group with n elements. Throughout this chapter, we will reserve g, g', h, h' to be elements of the group G, and we will use i, j as natural numbers. For each $g \in G$, we define $e_g \in \mathbb{C}^n$ to be the column vector with a 1 on position g and 0 otherwise. (Here the the vectors are indexed by the group elements.) Then the group algebra of G is $\mathbb{C}[G] = span\{u_g : g \in G\}$ where $u_g \in M_n(\mathbb{C})$ satisfies the condition $u_g(e_h) = e_{gh}$ for all $h \in G$. In this case, we may write $u_g = \sum_{h \in G} e_{h,g^{-1}h}$ where $\{e_{g,h} : g, h \in G\}$ is the set of matrix units in $M_n(\mathbb{C})$. Throughout this section, we will follow the methods laid out by Nicoara and White in [26].

3.2 Construction of Multi-Parametric Families

We begin by giving a natural basis for $[D, \mathbb{C}[G]]^{\perp}$ as in [26].

Theorem 3.1. *Let G be a finite group with $|G| = n$, and $g, h \in G$ be fixed. Define $a^{h,g} \in M_n(\mathbb{C})$ by*

$$(a^{h,g})_{p,q} = \begin{cases} 1 & \text{if } p = h^k g \text{ and } q = h^{k+1} g \text{ for } k = 1, \cdots, |h| \\ 0 & \text{otherwise} \end{cases}$$

For each $h \in G$, let $g_1^h, \cdots, g_{n(h)}^n$ be a choice of representatives of the right cosets of $G/\langle h \rangle$, where $n(h) = |G|/|h|$ is the number of elements in $G/\langle h \rangle$. Then the matrices $\{a^{h,g_i^h} : h \in G, 1 \leq i \leq n(h)\}$ form a basis for $M_n(\mathbb{C}) \ominus [D, \mathbb{C}[G]]$ where $n = |G|$.

Remark 3.1.1. *Note that if $h' \in \langle h \rangle$ then for $g \in G$,*

$$a^{h,g} = a^{h',g}.$$

This follows from the fact that $h' = h^m$ for some m, then as k runs through the set $\{1, \cdots, |h|\}$ so too does $k + m$.

Remark 3.1.2. *Let $h', g' \in G$. Then it follows that*

$$(a^{h,g} a^{h',g'})_{p,q} = \sum_{r \in G} (a^{h,g})_{p,r} (a^{h',g'})_{r,q}$$

Note that the product will have a 1 exactly when $(a^{h,g})_{p,r} = 1 = (a^{h',g'})_{r,q}$. Hence, we have the following relations

$$p = h^k g \text{ and } r = h^{k+1} g \text{ for some } k \in \{1, \cdots, |h|\}$$
$$r = h'^l g' \text{ and } q = h'^{l+1} g' \text{ for some } l \in \{1, \cdots, |h'|\}$$

So we may define

$$(a^{h,g}a^{h',g'})_{p,q} = \begin{cases} 1 & \text{if } p = h^k g \text{ and } q = h'h^{k+1}g \text{ for } k = 1, \cdots, |h| \\ 0 & \text{otherwise} \end{cases}$$

Using this, we can determine the powers of $a^{h,g}$.

Theorem 3.2. *Let* $h, g \in G$ *and* $n \in \mathbb{N}$. *Then*

$$((a^{h,g})^n)_{p,q} = \begin{cases} 1 & \text{if } p = h^k g \text{ and } q = h^{k+n}g \text{ for } k = 1, \cdots, |h| \\ 0 & \text{otherwise} \end{cases}$$

Proof. This follows directly from the definition of $a^{h,g}$ for $h, g \in G$ and matrix multiplication. □

We may write $a^{h,g}$ in matrix notation for easier calculations.

Remark 3.2.1. *Let* $h, g \in G$. *Then* $a^{h,g}$ *can be written in matrix notation as*

$$a^{h,g} = \sum_{k=1}^{|h|} e_{h^k g, h^{k+1} g}$$

where $e_{p,q}$ *is the matrix with 1 on position* p, q *and 0 otherwise.*

Remark 3.2.2. *This form allows us to determine* $(a^{h,g})^*$. *It follows that*

$$(a^{h,g})^* = \sum_{k=1}^{|h|} e_{h^{k+1}g, h^k g} = \sum_{k=1}^{|h|} e_{h^k g, h^{k-1} g}.$$

Then we can determine that $(a^{h,g})^* = (a^{h,g})^{|h|-1} = a^{h^{-1},g}$ *in alternate forms.*

Remark 3.2.3. *Note that for* $h, g \in G$,

$$\begin{aligned} (a^{h,g})^0 := a^{h,g}(a^{h,g})^* &= \sum_{k=1}^{|h|} e_{h^k g, h^{-1}h^{k+1}g} \\ &= \sum_{k=1}^{|h|} e_{h^k g, h^k g} \end{aligned}$$

Corollary 3.2.1. *For $h, g \in G$, it follows that $(a^{h,g})^0$ is the identity in $M_n(\mathbb{C})$ if only if $\langle h \rangle g = G$. We also have that*

$$(a^{h,g})^0 a^{h,g} = a^{h,g} = a^{h,g}(a^{h,g})^0.$$

Proof. (Idea) We have that $(a^{h,g})^0$ is a diagonal matrix with entries equal to 1 or 0 for each $h, g \in G$. □

Remark 3.2.4. *It must also be noted that for $h, g \in G$*

$$(a^{h,g})^{|h|} = (a^{h,g})^0.$$

We may express negative powers of a matrix $a^{h,g}$ by a similar method. The inverse of $a^{h,g}$ may not exist as a matrix on the full space, but $a^{h,g}$ will be invertible on a certain subspace.

Theorem 3.3. *Let $h, g \in G$ and $n \in \mathbb{N}$, then*

$$(a^{h,g})^{-n} = \sum_{k=1}^{|h|} e_{h^k g, h^{k-n} g}.$$

Note that the left-hand side may not make sense, but the right-hand side will make sense since group elements are invertible. Therefore, we can actually raise the matrix $a^{h,g}$ to a negative power. Note that we can always replace $-n$ with $m|h| - n$ where $m \in \mathbb{N}$ such that $m|h| - n > 0$.

Theorem 3.4. *(Nicoara [26]) Let $h, g \in G$ be fixed, and $h', g' \in G$ such that $|h'| = |h|$ and $g' \in \langle h \rangle g$, then*

$$a^{h,g} = a^{h',g'}$$

We would like to know when two such matrices commute. We have the following:

Theorem 3.5. *Let $h, h', g, g' \in G$.*

1. *For $a^{h,g}$ to commute with $a^{h',g'}$ with nonzero product, we need $|h| = |h'|$ and $hh' = h'h$.*

2. *If* $\langle h\rangle g \cap \langle h'\rangle g' = \emptyset$, *then*

$$a^{h,g}a^{h',g'} = 0 = a^{h',g'}a^{h,g}.$$

In particular, they commute.

Proof. 1. We have that $(a^{h,g}a^{h',g'})_{p,q} = 1$ when $p = h^k g$ and $q = h'h^{k+1}g$ for some $k \in \{1, \cdots, |h|\}$. For $a^{h,g}a^{h',g'} = a^{h',g'}a^{h,g}$, we would need

$$h^k g = h'^m g'$$
$$h'h^{k+1}g = hh'^{m+1}g'$$

where k is as above, $m \in \{1, \cdots, |h'|\}$. We would need $|h| = |h'|$ so that we have the same number of nonzero entries in each product. The above equations give us that $\langle h\rangle g \cap \langle h'\rangle g' \neq \emptyset$, and we need $h'h = hh'$.

2. Let $h, h', g, g' \in G$ and suppose that $\langle h\rangle g \cap \langle h'\rangle g' = \emptyset$. Then it follows that $h^k g \neq h'^m g'$ for any $k \in \{1, \cdots, |h|\}$ and $m \in \{1, \cdots, |h'|\}$. It follows that

$$a^{h,g}a^{h',g'} = \sum_{k=1}^{|h|}\sum_{m=1}^{|h'|} e_{h^k g, h^{k+1}g}e_{h'^m g', h'^{m+1}g'} = 0$$

since $h^{k+1}g \neq h'^m g'$ for k and m described above. Reversing the roles of h with h' and g with g', we have that $a^{h,g}$ commutes with $a^{h',g'}$.

□

We would like to know when these matrices commute so that we can construct unitary matrices of the form $U_t = e^{ith}$ for $t \in \mathbb{R}$ and h, a Hermitian matrix. These matrices will give us a one parameter family. Our ultimate goal is to find multiparametric families. For instance, we wish to find $U_{t,s} = e^{i(th_1+sh_2)}$, where t and s the parameters, and h_1 and h_2 are hermitian matrices.

Nicoara [26] showed that $U_t = e^{ith}$ for $h = a^{h,g} + (a^{h,g})^*$ produces a one parameter family which gives a commuting square. We want to show the following theorem:

Theorem 3.6. *Fix $l, k, l', k' \in G$ such that the cyclic subgroups generated by l and l' are equal to each other, and $k' \in \langle l \rangle k$. Let $a = a^{l,k}$ and $b = a^{l',k'}$. For $t, s \in \mathbb{R}$, let $U_{t,s} = e^{it(a+a^*)+is(b+b^*)}$. Then $U_{t,s}$ produces a commuting square.*

Proof. Let $g, h \in G$, and $p, q \in \mathbb{Z}$. From above we know that a and b and their respective powers (and hence a^* and b^*) commute by choice of l and l'. Then it follows that

$$U_{t,s} = I + \sum_{r \geq 1} \frac{(it(a+a^*) + is(b+b^*))^r}{r!} = I + \sum_{r \geq 1} \frac{i^r}{r!} \sum_{m=0}^{r} \binom{r}{m} t^m (a+a^*)^m s^{r-m} (b+b^*)^{r-m}.$$

From Nicoara [26], we know that we can use the binomial theorem again to show that $U_{t,s}$ is in the linear span of I, a^n, b^n, $(a^*)^n$, and $(b^*)^n$ for $n \geq 0$. However, we have shown that a^* is a power of a, and likewise b^* is a power of b. Hence, to show that $U_{t,s}$ yields a commuting square, we need to calculate $\tau(d_g U_{t,s} u_h U_{t,s}^*)$ and $\tau(d_g u_h U_{t,s} U_{t,s}^*)$, but from the previous statement about $U_{t,s}$ we need only show that

$$\tau(d_g a^p u_h b^q) = \tau(d_g u_h a^p b^q).$$

It follows that

$$\tau(d_g a^p u_h b^q) = \tau\left(d_g \sum_{j=1}^{|l|} e_{l^j k, l^{j+p} k} \sum_{m \in G} e_{m, h^{-1} m} \sum_{i=1}^{|l'|} e_{l'^i k, l'^{i+q} k} \right)$$

Calculating this trace, we need $g = l^j k$ (implying only one j), $m = l^{j+p} k$ (also fixed), $h^{-1} m = l'^i k$ (implying only one i since there can only be one j), and $g = l'^{i+q} k'$ (which by assumption such a g exists). It then follows that

$$h^{-1} m = l'^i k$$
$$h^{-1}(l^{j+p} k) = l'^{-q} l'^{i+q} k$$
$$h^{-1} l^p g = l'^{-q} g$$
$$l^p l'^q = h$$

Hence,

$$\tau(d_g a^p u_h b^q) = \delta_h^{lpl'q} |\{g\} \cap \langle l \rangle k || \{g\} \cap \langle l' \rangle k'|.$$

□

Lemma 3.6.1. *Let G be a finite abelian group of order n. For each $h \in G$, let $g_1^h, \cdots, g_{n(h)}^h$ be a choice of representatives of the right cosets of $G/\langle h \rangle$, where $n(h) = |G|/|h|$ is the number of elements of $G/\langle h \rangle$. Then $\sum_{j=1}^{n(h)} a^{h,g_j^h} \in \mathbb{C}[G]$.*

Proof. First notice for each $1 \leq i < j \leq n(h)$, $(a^{h,g_i^h})_{p,q} = 1$ implies $(a^{h,g_j^h})_{p,q} = 0$. Otherwise if $(a^{h,g_i^h})_{p,q} = 1$ and $(a^{h,g_j^h})_{p,q} = 1$, then $h^k g_i^h = p = h^r g_j^h$ for some $1 \leq k, r \leq |h|$ which would imply that $g_j^h \in \langle h \rangle g_i^h$, a contradiction.

This fact implies that

$$\left(\sum_{j=1}^{n(h)} a^{h,g_j^h} \right)_{p,q} = \begin{cases} 1 & , p = h^k g_j^h, \text{ and } q = h^{k+1} g_j^h \text{ for some } k \\ 0 & , \text{ else} \end{cases}$$

Notice as well that for each $g \in G$, we have that multiplying the elements of the set $\{g_1^h, \cdots, g_{n(h)}^h\}$ by g will permute the element of the set. This implies that

$$\left(\sum_{j=1}^{n(h)} a^{h,g_j^h} \right)_{p,q} = \left(\sum_{j=1}^{n(h)} a^{h,g_j^h} \right)_{pg^{-1},qg^{-1}}.$$

Therefore, it must be the case that $\sum_{j=1}^{n(h)} a^{h,g_j^h} \in \mathbb{C}[G]$. □

3.3 Construction based on elements of order > 2

Our goal is to construct multi-parameter families of non-equivalent Hadamard matrices containing the Fourier matrix of any given size. In this case, we will let our group be $G = \mathbb{Z}_n$ and for each m which divides n, we know that there are exactly $\varphi(n)$ where φ is the Euler Phi function. Since we want non-equivalent matrices, we want proper divisors of n, i.e. $m \neq 1, n$. Since in the case when $m = 1$, we have that the identity is the only element

of order 1 and the matrices $a^{e,g}$ for any $g \in G$ are diagonal. In the case where $h \in G$ and $|h| = |G|$, then $a^{h,g} \in \mathbb{C}[G]$ which will lead us to equivalent matrices. For the time being, we will look only at elements that do not have order 2. We will revisit this case later.

Theorem 3.7. *Let $G = \mathbb{Z}_n$ with n square free. Let $h \in G$ with $|h| = m > 2$. Then there exists a $\frac{\varphi(m)}{2}(\frac{n}{m} - 1)$-parameter family of Hadamard matrices containing the Fourier matrix, F_n.*

Note that when n is prime, we have no parametric family containing F_n.

Proof. Let $m \neq 2$ be a divisor of n. Consider the set

$$\mathcal{S} = \{h_i \in G \ : \ |h_i| = m, h_i \neq h_j \text{ for } i \neq j, \text{ and } h_i \neq h_j^{-1}\}.$$

Since G is a cyclic group, we have that there are $\varphi(m)$ elements in G of order m. Thus, $\mathcal{S}$ must have $\varphi(m)/2$ elements. Our goal is to construct a multi-paramter family with these $h \in \mathcal{S}$. In order to do so, we need to take advantage of the matrix $a^{h,g} + (a^{h,g})^* = a^{h,g} + a^{h^{-1},g} =: A^{h,g}$ for each $h \in \mathcal{S}$. Note that $A^{h,g} = (A^{h,g})^* = A^{h^{-1},g}$. Since we need A^{h_1,g_1} to commute with A^{h_2,g_2}, we need $|h_1| = |h_2|$. This tells us that $\mathcal{S}$ will allow us find the largest set of $h \in G$ with the same order that will give us different $A^{h,g}$. For $h_i \in \mathcal{S}$, let $\{g_j^{h_i} \ : 1 \leq j \leq |G|/m\}$ be representatives of the right cosets of $G/\langle h_i \rangle$. From the previous theorem, we know that $\sum_{j=1}^{n(h)} a^{h,g_j^h} \in \mathbb{C}[G]$. Using a linear span of the elements $a^{h_i,g_j^{h_i}}$ will be equivalent to choosing another matrix $a^{h,g}$ for some $h, g \in G$. However, this is not the case if we only use $n/m - 1$ elements in the set $\{g_j^{h_i} \ : 1 \leq j \leq n/m\}$. Therefore, we can construct a family with at most $\frac{\varphi(m)(n/m-1)}{2}$ elements. It may be the case that some of the parameters may collapse, or it may be the case that the family that we attain are all equivalent. The explicit construction for the unitary matrix is

$$U_{t_{1,1},\cdots,t_{\frac{\varphi(m)}{2},(n/m-1)}} = e^{\left(i \sum_{k=1}^{\frac{\varphi(m)}{2}} \sum_{j=1}^{\frac{n}{m}-1} t_{k,j} A^{h_k,g_j^{h_k}} \right)}$$

□

One may ask what is the maximal number of parameters we may choose for $G = \mathbb{Z}_n$. We need to find a proper divisor m of n (so that $m \neq 1, n$) which maximizes $\frac{\varphi(m)}{2}(\frac{n}{m} - 1)$.

Example 3.1. *We can construct a family of Hadamard matrices containing the Fourier matrix F_6. It can be shown that each time we construct try to construct a multi-parameter family using group elements which do not have order 2, we find that each family is equivalent to a 1-parameter family. An example of a family that we would like to be a 2-parameter family is*

$$F_6(\lambda, \gamma) = \begin{bmatrix} \lambda & \gamma & \lambda & \gamma & \lambda & \gamma \\ 1 & e^{\frac{i\pi}{3}} & e^{\frac{2i\pi}{3}} & -1 & e^{-\frac{2i\pi}{3}} & e^{-\frac{i\pi}{3}} \\ 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} \\ \lambda & -\gamma & \lambda & -\gamma & \lambda & -\gamma \\ 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} \\ 1 & e^{-\frac{i\pi}{3}} & e^{-\frac{2i\pi}{3}} & -1 & e^{\frac{2i\pi}{3}} & e^{\frac{i\pi}{3}} \end{bmatrix}, (|\gamma|, |\lambda| = 1).$$

However, it is easy to see that this family is equivalent to the 1-parameter family

$$F_6(\gamma) = \begin{bmatrix} 1 & \gamma & 1 & \gamma & 1 & \gamma \\ 1 & e^{\frac{i\pi}{3}} & e^{\frac{2i\pi}{3}} & -1 & e^{-\frac{2i\pi}{3}} & e^{-\frac{i\pi}{3}} \\ 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} & e^{-\frac{2i\pi}{3}} \\ 1 & -\gamma & 1 & -\gamma & 1 & -\gamma \\ 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} & 1 & e^{-\frac{2i\pi}{3}} & e^{\frac{2i\pi}{3}} \\ 1 & e^{-\frac{i\pi}{3}} & e^{-\frac{2i\pi}{3}} & -1 & e^{\frac{2i\pi}{3}} & e^{\frac{i\pi}{3}} \end{bmatrix}, (|\gamma| = 1).$$

Theorem 3.8. *Let $G = \mathbb{Z}_n$ with $n = pqr$ and $p > q > r$. Then if $m > 2$ is a divisor of n, $\frac{\varphi(m)(\frac{n}{m}-1)}{2}$ is maximized when $m = p$.*

Proof. Let m be a divisor of $n = pqr$. First assume that m is prime. Let $m \in \{p, q, r\}$ and let $m \neq s \in \{p, q, r\}$. Without loss of generality, we may assume that $m > s$. Then it follows

that

$$\begin{aligned} sm &< pqr \\ m - s &< pqr\frac{m-s}{sm} \\ (m-s) &< pqr(1/s - 1/m) \\ m + pqr/m &< s + pqr/s \\ -m - pqr/m &> -s - pqr/s \\ pqr - m - pqr/m + 1 &> pqr - s - pqr/s + 1 \\ (m-1)(pqr/m - 1) &> (s-1)(pqr/s - 1) \end{aligned}$$

Therefore, we have that the largest value that $\frac{(m-1)(pqr/m-1)}{2}$ can attain when m is a prime divisor is $\frac{(p-1)(qr-1)}{2} = \frac{\varphi(p)(n/p-1)}{2}$.

Suppose now that m is a product of two primes. If $m = ps$ for $s = q, r$, we have that

$$\begin{aligned} 2 &< qr/s + s \\ qr - s - qr/s + 1 &< qr - 1 \\ (s-1)(qr/s - 1) &< qr - 1 \\ (p-1)(s-1)(qr/s-1) &< (p-1)(qr-1) \\ \frac{\varphi(m)(n/m-1)}{2} &< \frac{\varphi(p)(n/p-1)}{2} \end{aligned}$$

If $m = qr$, we have that $\frac{\varphi(m)(n/m-1)}{2} = \frac{(q-1)(r-1)(p-1)}{2} < \frac{(p-1)(qr-1)}{2} = \frac{\varphi(p)(n/p-1)}{2}$. Note that this follows since $(r-1)(q-1) < qr - 1$. Therefore, we have that the maximal value of $\frac{\varphi(m)(n/m-1)}{2}$ is attained when m is the largest prime divisor. □

Theorem 3.9. *Let n be a square free integer with at least two prime divisors. Then for $m > 2$ a divisor of n, $\frac{\varphi(m)(\frac{n}{m}-1)}{2}$ is maximized when m is the largest prime divisor of n.*

Proof. We proceed by induction on the number of prime divisors of n. We have seen that the base cases are held true when the number of prime divisors is 2 or 3. We will assume that the hypothesis is true when n has k prime factors for some $k \geq 3$. Suppose that $n = p_1 \cdots p_{k+1}$

where $p_i < p_{i+1}$ for $1 \leq i \leq k$. From the proof of the previous theorem, we see that if m is prime divisor of n, then $\frac{\varphi(m)(\frac{n}{m}-1)}{2}$ is maximized when $m = p_{k+1}$.

Assume that m is divisor of n such that $m = p_j r$ for some p_j and $r > 1$. It follows that

$$\frac{\varphi(m)(\frac{n}{m}-1)}{2} = \frac{\varphi(p_j r)(\frac{n}{p_j r}-1)}{2}$$

Since $\frac{n}{p_j}$ has k factors, the induction hypothesis holds true, and since r is a divisor of $\frac{n}{p_j}$, we have that

$$\frac{\varphi(r)(\frac{n/p_j}{r}-1)}{2} \leq \frac{\varphi(p_i)(\frac{n/p_j}{p_i}-1)}{2} = \frac{\varphi(p_i)(\frac{n}{p_j p_i}-1)}{2}$$

where p_i is the largest prime divisor of $\frac{n}{p_j}$. Therefore, we have that

$$\frac{\varphi(m)(\frac{n}{m}-1)}{2} \leq \frac{\varphi(p_j p_i)(\frac{n}{p_j p_i}-1)}{2}.$$

Note that the Euler Totient function splits over distinct primes.

If we can show that

$$\frac{\varphi(p_j p_i)(\frac{n}{p_j p_i}-1)}{2} \leq \frac{\varphi(p_{k+1})(\frac{n}{p_{k+1}}-1)}{2},$$

then we would be done. Without loss of generality, we may assume that $p_j > p_i$. If $p_j = p_{k+1}$, then we have that

$$\begin{aligned}
&\frac{\varphi(p_j p_i)(\frac{n}{p_j p_i}-1)}{2} \leq \frac{\varphi(p_{k+1})(\frac{n}{p_{k+1}}-1)}{2} \\
\iff\ &\varphi(p_{k+1})\varphi(p_i)(\frac{n}{p_{k+1}p_i}-1) \leq \varphi(p_{k+1})(\frac{n}{p_{k+1}}-1) \\
\iff\ &(p_i-1)(\frac{n}{p_{k+1}p_i}-1) \leq \frac{n}{p_{k+1}}-1 \\
\iff\ &-p_i - \frac{n}{p_{k+1}p_i}+1 \leq -1 \\
\iff\ &2 \leq p_i + \frac{n}{p_{k+1}p_i}
\end{aligned}$$

We have that the last statement is true since p_i is a prime, so $p_i \geq 2$ and $\frac{n}{p_{k+1}p_i} > 0$. Therefore, we have that

$$\frac{\varphi(p_jp_i)(\frac{n}{p_jp_i}-1)}{2} \leq \frac{\varphi(p_{k+1})(\frac{n}{p_{k+1}}-1)}{2}$$

is true when $p_j = p_{k+1}$.

Assume now that $p_j < p_{k+1}$. It follows that

$$\frac{\varphi(p_jp_i)(\frac{n}{p_jp_i}-1)}{2} \leq \frac{\varphi(p_jp_{k+1})(\frac{n}{p_jp_{k+1}}-1)}{2}$$

by the induction hypothesis since $\frac{n}{p_j}$ has k divisors and $p_i < p_j < p_{k+1}$. It follows that

$$\begin{aligned}
&\frac{\varphi(p_jp_{k+1})(\frac{n}{p_jp_{k+1}}-1)}{2} \leq \frac{\varphi(p_{k+1})(\frac{n}{p_{k+1}}-1)}{2} \\
\iff\ &(p_j-1)(\frac{n}{p_jp_{k+1}}-1) \leq \frac{n}{p_{k+1}}-1 \\
\iff\ &-p_j - \frac{n}{p_jp_{k+1}} + 1 \leq -1 \\
\iff\ &2 \leq p_j + \frac{n}{p_jp_{k+1}}
\end{aligned}$$

where the last statement is true since $p_j \geq 2$ and $\frac{n}{p_jp_{k+1}} > 0$.

Thus, we have that

$$\frac{\varphi(m)(\frac{n}{m}-1)}{2} \leq \frac{\varphi(p_jp_i)(\frac{n}{p_jp_i}-1)}{2} \leq \frac{\varphi(p_{k+1})(\frac{n}{p_{k+1}}-1)}{2}$$

when m is any divisor of $n = p_1 \cdots p_{k+1}$. Therefore, by induction it must be the case that $\frac{\varphi(m)(\frac{n}{m}-1)}{2}$ is maximized when m is the largest prime divisor of n whenever n is a square free positive integer. □

Using our method of constructing multi-parametric families, we have shown that we can construct a family with at most $\frac{\varphi(p)(n/p-1)}{2}$ parameters when n is square-free and p is its largest prime divisor. We claim that this is an upper bound on the number of parameters since it may be the case that some of the parameters may "collapse" meaning that a family

with more than one parameter may be equivalent to a family with less parameters as was seen in the $n = 6$ case above.

One can ask if n has to be square-free to achieve this bound. For certain numerical examples, it seems that this bound holds for most n. In fact, we have the following:

Conjecture 3.9.1. *Let n be any integer with at least two prime divisors. Then for $m > 2$ a divisor of n, $\frac{\varphi(m)(n/m-1)}{2}$ is maximized when m is the largest prime divisor of n.*

We do have the following

Theorem 3.10. *Let $G = \mathbb{Z}_n$ with $n = p^\alpha$ for some p, prime, and $2 \leq \alpha \in \mathbb{N}$. If $m = p^\beta$ is a divisor of n, then $\frac{\varphi(m)(\frac{n}{m}-1)}{2}$ is maximized when $m = p$.*

Proof. Let $n = p^\alpha$ for some prime p and $\alpha \geq 2$. Let $m = p^\beta$ be a proper divisor of n so that $1 \leq \beta \leq \alpha - 1$. We have that

$$\begin{aligned} & \frac{\varphi(m)(\frac{n}{m}-1)}{2} \leq \frac{\varphi(p)(\frac{n}{p}-1)}{2} \\ \iff & p^{\beta-1}(p-1)(p^{\alpha-\beta}-1) \leq (p-1)(p^{\alpha-1}-1) \\ \iff & p^{\alpha-1} - p^{\beta-1} \leq p^{\alpha-1} - 1 \\ \iff & p^{\beta-1} \geq 1 \end{aligned}$$

The last statement is true since $\beta - 1 \geq 0$. □

This theorem is true for any prime p, but when $p = 2$ the bound we get is not an integer using this method.

3.4 Construction based on an element of order 2

We will know look at what happens when we use elements of order 2. We have the following theorem which is similar to Theorem 3.7:

Theorem 3.11. *Suppose that $n = 2p$ for p an odd prime. Then we can construct a family of Hadamard matrices containing the Fourier matrix F_n with $p - 1$ parameters.*

Proof. Note that in the group $G = \mathbb{Z}_n$ there is only one element of order 2. Let $h \in G$ be the element of order 2. It follows that $a^{h,g} = a^{h^{-1},g} = (a^{h,g})^*$ for all $g \in G$. Since $|G/\langle h\rangle| = p$, we choose p representatives of the right cosets of $G/\langle h\rangle$. Let $\{g_j^h \ : \ 1 \leq j \leq p\}$ be these representatives. Recall Lemma 3.6.1 which states that $\sum_{j=1}^{p} a^{h,g_j^h}$ is a circulant matrix (being an element of $\mathbb{C}[\mathbb{Z}_n]$). This sum will give us a family of equivalent matrices. Therefore, dropping one of the a^{h,g_j^h} from the sum will give us a family of non-equivalent matrices giving us a total $p-1$ matrices in the sum. Note that we can not increase this sum any further since there is no other element of order 2. In this case the explicit construction for this family is

$$U_{t_1,\cdots t_{p-1}} = e^{\left(i\sum_{j=1}^{p-1} t_j a^{h,g_j^h}\right)}$$

which yields the family

$$F_n^{(p-1)}(t_1,\cdots,t_{p-1}) = U_{t_1,\cdots t_{p-1}} F_n$$

□

This construction tells us for $n = 6$, we in fact get 2 parameter family.

Example 3.2. *One of the 2-parameter families that we construct for $n = 6$ is*

$$F_6^{(2)}(t,s) = \begin{bmatrix} e^{it} & e^{-it} & e^{it} & e^{-it} & e^{it} & e^{-it} \\ e^{is} & e^{\frac{i\pi}{3}-is} & e^{is+\frac{2i\pi}{3}} & -e^{-is} & -e^{is+\frac{i\pi}{3}} & -e^{\frac{2i\pi}{3}-is} \\ 1 & e^{\frac{2i\pi}{3}} & -e^{\frac{i\pi}{3}} & 1 & e^{\frac{2i\pi}{3}} & -e^{\frac{i\pi}{3}} \\ e^{it} & -e^{-it} & e^{it} & -e^{-it} & e^{it} & -e^{-it} \\ e^{is} & -e^{\frac{i\pi}{3}-is} & e^{is+\frac{2i\pi}{3}} & e^{-is} & -e^{is+\frac{i\pi}{3}} & e^{\frac{2i\pi}{3}-is} \\ 1 & -e^{\frac{2i\pi}{3}} & -e^{\frac{i\pi}{3}} & -1 & e^{\frac{2i\pi}{3}} & e^{\frac{i\pi}{3}} \end{bmatrix}$$

where $t, s \in \mathbb{R}$. Note that it is possible for us to construct other families which may or may not be equivalent to this family. Writing this family in its equivalent dephased form (one of

the equivalent forms) and renaming, we have that

$$F_6^{(2)}(t,s) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & e^{-2is+2it+\frac{i\pi}{3}} & e^{\frac{2i\pi}{3}} & -e^{2it-2is} & -e^{\frac{i\pi}{3}} & -e^{-2is+2it+\frac{2i\pi}{3}} \\ 1 & e^{2it+\frac{2i\pi}{3}} & -e^{\frac{i\pi}{3}} & e^{2it} & e^{\frac{2i\pi}{3}} & -e^{2it+\frac{i\pi}{3}} \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -e^{-2is+2it+\frac{i\pi}{3}} & e^{\frac{2i\pi}{3}} & e^{2it-2is} & -e^{\frac{i\pi}{3}} & e^{-2is+2it+\frac{2i\pi}{3}} \\ 1 & -e^{2it+\frac{2i\pi}{3}} & -e^{\frac{i\pi}{3}} & -e^{2it} & e^{\frac{2i\pi}{3}} & e^{2it+\frac{i\pi}{3}} \end{bmatrix}.$$

In this case, we have that

$$U_{t,s} = \begin{bmatrix} \cos(t) & 0 & 0 & i\sin(t) & 0 & 0 \\ 0 & \cos(s) & 0 & 0 & i\sin(s) & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ i\sin(t) & 0 & 0 & \cos(t) & 0 & 0 \\ 0 & i\sin(s) & 0 & 0 & \cos(s) & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Remark 3.11.1. *Note that the 2-parameter family found is equivalent to another well-known 2-parameter family (see [33]). It is clear after a change of variable that the family $F_6^{(2)}(t,s)$ is equivalent to (and so we will rename the family)*

$$F_6^{(2)}(\gamma,\lambda) = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \gamma & \gamma\omega & \gamma\omega^2 \\ 1 & \omega^2 & \omega & \lambda & \lambda\omega^2 & \lambda\omega \\ \hline 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \omega & \omega^2 & -\gamma & -\gamma\omega & -\gamma\omega^2 \\ 1 & \omega^2 & \omega & -\lambda & -\lambda\omega^2 & -\lambda\omega \end{array}\right]$$

where $\omega = e^{2\pi i/3}$ and the parameters λ and γ are complex valued with absolute value equal to 1.

Theorem 3.12. *Let $n = 2p_1 \cdots p_k$ for some $k \geq 1$ be square-free. Then the maximal number of parameters in any family of Hadamard matrices containing the Fourier matrix F_n using our construction method is $\frac{n}{2} - 1$.*

Proof. Let $m > 2$ be a divisor of $n = 2p_1 \cdots p_k$. In this case, the largest number of parameters in a family that we can construct using our methods is $\frac{(p_k-1)(\frac{n}{p_k}-1)}{2}$. If we choose to construct a family using a element of order 2, we will get $\frac{n}{2} - 1$ elements in a family. It follows that

$$\begin{aligned} & \frac{n}{2} - 1 > \frac{(p_k - 1)(\frac{n}{p_k} - 1)}{2} \\ \iff \quad & n - 2 > n - p_k - \frac{n}{p_k} + 1 \\ \iff \quad & p_k + \frac{n}{p_k} > 3 \end{aligned}$$

The last statement is true since $p_j > 2$ for each $1 \leq j \leq k$. Then $p_k + \frac{n}{p_k} > 2 + 2^k > 3$ since $k \geq 1$. □

This tells us that we cannot increase the number of parameters in our construction. The max number of parameters that we get when $n = 6$ is two parameters! We would like to have a four parameter family since the dephased defect of $\mathbb{Z}_6$ (which gives us the max number of one-parameter families) is 4. It is natural to ask if after finding the 2-parameter family, can we increase the parameters by using one of the elements in $\mathbb{Z}_6$ of order 3? The answer is no. Introducing the third parameter into the matrix using our construction, yields a family that is in fact equivalent to the two parameter family.

Theorem 3.13. *Let $n = 2^\alpha$ for some $\alpha \geq 2$. Then we can construct a family of Hadamard matrices containing the Fourier matrix F_n with $2^{\alpha-1} - 1$ parameters.*

(Sketch of proof) See Theorem 3.10. The proof is much the same. Since the prime we have is 2, we need to use the expression $2^{\alpha-1} - 1$.

Example 3.3. *For $n = 8$, we construct a 3-parameter family containing the Fourier matrix:*

$$F_8^{(3)}(\alpha,\beta,\gamma) = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & i\beta & -i\beta & i\beta & -i\beta \\ 1 & -1 & i & -i & \alpha\omega & \alpha\omega^3 & -\alpha\omega & -\alpha\omega^3 \\ 1 & -1 & -i & i & \gamma\omega^3 & \gamma\omega & -\gamma\omega^3 & -\gamma\omega \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -i\beta & i\beta & -i\beta & i\beta \\ 1 & -1 & i & -i & -\alpha\omega & -\alpha\omega^3 & \alpha\omega & \alpha\omega^3 \\ 1 & -1 & -i & i & -\gamma\omega^3 & -\gamma\omega & \gamma\omega^3 & \gamma\omega \end{array}\right]$$

where the parameters all have absolute value equal to 1 and $\omega = e^{\pi i/4}$.

There are many questions that we can ask about these bounds on the number of parameters. First of all does the bound $\frac{n}{2} - 1$ hold for all n using our construction method? We know that there are other methods for constructing multi-parametric families of Hadamard matrices containing the Fourier matrix F_n. Using our method, we can only construct a 3-parameter family containing F_8. Interestingly, we can superficially introduce a fourth parameter into our family $F_8^{(3)}(\alpha,\beta,\gamma)$. If we replace i with $i\delta$ in the left-hand blocks, it is easy to check that we have a family of Hadamard matrices.

Example 3.4. *(A family of Hadamard matrices containing the Fourier matrix F_8 with four parameters)*

$$F_8^{(4)}(\alpha,\beta,\gamma,\delta) = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & i\beta & -i\beta & i\beta & -i\beta \\ 1 & -1 & i\delta & -i\delta & \alpha\omega & \alpha\omega^3 & -\alpha\omega & -\alpha\omega^3 \\ 1 & -1 & -i\delta & i\delta & \gamma\omega^3 & \gamma\omega & -\gamma\omega^3 & -\gamma\omega \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -i\beta & i\beta & -i\beta & i\beta \\ 1 & -1 & i\delta & -i\delta & -\alpha\omega & -\alpha\omega^3 & \alpha\omega & \alpha\omega^3 \\ 1 & -1 & -i\delta & i\delta & -\gamma\omega^3 & -\gamma\omega & \gamma\omega^3 & \gamma\omega \end{array}\right]$$

Using a change of variables and writing the family in an equivalent form, we have that

$$F_8^{(4)}(\alpha,\beta,\delta,\epsilon) = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & \delta & \delta & -\delta & -\delta \\ 1 & -1 & \beta & -\beta & \alpha & -\alpha & i\alpha & -i\alpha \\ 1 & -1 & -\beta & \beta & \epsilon & -\epsilon & -i\epsilon & i\epsilon \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -\delta & -\delta & \delta & \delta \\ 1 & -1 & \beta & -\beta & -\alpha & \alpha & -i\alpha & i\alpha \\ 1 & -1 & -\beta & \beta & -\epsilon & \epsilon & i\epsilon & -i\epsilon \end{array}\right]$$

It is also well known that F_8 belongs to a 5-parameter family. This can be found in the Complex Hadamard Matrices Catalogue [35].

Example 3.5. *It is know that the Fourier matrix F_8 belongs to the 5-parameter family*

$$F_8^{(5)}(\alpha,\beta,\chi,\delta,\epsilon) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & e^{\frac{i\pi}{4}}\alpha & i\beta & e^{\frac{3i\pi}{4}}\chi & -1 & e^{-\frac{3i\pi}{4}}\alpha & -i\beta & e^{-\frac{i\pi}{4}}\chi \\ 1 & i\delta & -1 & -i\delta & 1 & i\delta & -1 & -i\delta \\ 1 & e^{\frac{3i\pi}{4}}\epsilon & -i\beta & e^{\frac{i\pi}{4}}\epsilon\chi\bar{\alpha} & -1 & e^{-\frac{i\pi}{4}}\epsilon & i\beta & e^{-\frac{3i\pi}{4}}\epsilon\chi\bar{\alpha} \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & e^{-\frac{3i\pi}{4}}\alpha & i\beta & e^{-\frac{i\pi}{4}}\chi & -1 & e^{\frac{i\pi}{4}}\alpha & -i\beta & e^{\frac{3i\pi}{4}}\chi \\ 1 & -i\delta & -1 & i\delta & 1 & -i\delta & -1 & i\delta \\ 1 & e^{-\frac{i\pi}{4}}\epsilon & -i\beta & e^{-\frac{3i\pi}{4}}\epsilon\chi\bar{\alpha} & -1 & e^{\frac{3i\pi}{4}}\epsilon & i\beta & e^{\frac{i\pi}{4}}\epsilon\chi\bar{\alpha} \end{bmatrix}$$

where $\alpha,\beta,\chi,\delta,\epsilon \in \mathbb{C}$ with absolute value 1. Using a change of variables, and rewriting this family into an equivalent form (and once again renaming), we have that

$$F_8^{(5)}(\alpha,\beta,\gamma,\delta,\epsilon) = \left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & \delta & \delta & -\delta & -\delta \\ 1 & -1 & \beta & -\beta & \alpha & -\alpha & \chi & -\chi \\ 1 & -1 & -\beta & \beta & \epsilon & -\epsilon & -\epsilon\chi\overline{\alpha} & \epsilon\chi\overline{\alpha} \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -\delta & -\delta & \delta & \delta \\ 1 & -1 & \beta & -\beta & -\alpha & \alpha & -\chi & \chi \\ 1 & -1 & -\beta & \beta & -\epsilon & \epsilon & \epsilon\chi\overline{\alpha} & -\epsilon\chi\overline{\alpha} \end{array}\right]$$

It should also be noted that the family $F_8^{(4)}(\alpha,\beta,\delta,\epsilon)$ is a member of the family $F_8^{(5)}(\alpha,\beta,\chi,\delta,\epsilon)$. In fact, $F_8^{(4)}(\alpha,\beta,\delta,\epsilon) = F_8^{(5)}(\alpha,\beta,i\alpha,\delta,\epsilon)$. This tells us that $F_8^{(4)}(\alpha,\beta,\delta,\epsilon)$ is not a maximal family, and for the same reason, $F_8^{(3)}(\alpha,\beta,\gamma)$ is not a maximal family.

We know that the above family contains the maximum number of parameters since the dephased defect of $\mathbb{Z}_8$, $d'(\mathbb{Z}_8)$, is 5. Recall that

$$d'(\mathbb{Z}_n) = d(\mathbb{Z}_n) - 2n + 1.$$

In the case when $n = 6$, we have that $d'(\mathbb{Z}_6) = 4$. To date, it is known that there are four 1-parameter families of Hadamard matrices containing the Fourier matrix F_6. We have shown that there is at least one 2-parameter family. There are two 2-parameter families containing F_6 listed on the Complex Hadamard Matrix Catalogue. It is possible that our family is equivalent to one of the families listed on the catalogue. What is unknown to date is if there exists a 4-parameter family of Hadamard matrices containing the Fourier matrix F_6. There is numerical evidence of the existence of such a family in a paper written by Skinner, Newell, and Sanchez [31], but it is unknown to the author at the time if this family has been explicitly written.

Beyond the $n = 6$ case, our method provides parametric families with the same number of parameters of families that are already known when $n = 2p$ for $p > 2$ prime. For $n = pq$ odd and square-free, our method seems to give a parametric family with half as many parameters as currently known families containing F_n. In fact for small values of n when $n = pq$ for any

primes, the known multi-parameter families containing F_n have exactly $\varphi(n)$ parameters. Therefore, it remains to be seen if there is a method similar to our construction which will allow us to construct a $\varphi(n)$-parameter family for any $n = pq$ with p and q distinct primes. We can also ask if the bound we gave before on the number of parameters can be increased using a similar method for any square-free number n.

Of course the ultimate goal would be to construct a multi-parametric family with exactly $d'(\mathbb{Z}_n)$ parameters for every n. Once again we have for small values of n that this bound is achieved when n is divisible by p^2 for some prime p. However, when n is square free, there is no known $d'(\mathbb{Z}_n)$-parameter family containing F_n for small values of n.

Most of the families that we have given when $n = 2m$ for some $m \geq 3$ have all had the same form following the Kronecker product of $F_2 \otimes F_m$ with some modifications. This allows us to construct the following family:

Example 3.6. *For $n = 12$, we can construct a 7-parameter family of Hadamard matrices containing F_{12}. The family is*

$$F_{12}^{(7)} = \left[\begin{array}{ccc|ccc||ccc|ccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega & \omega^2 & \gamma & \gamma\omega & \gamma\omega^2 & \alpha & \alpha\omega & \alpha\omega^2 & \alpha\gamma & \alpha\gamma\omega & \alpha\gamma\omega^2 \\
1 & \omega^2 & \omega & \lambda & \lambda\omega^2 & \lambda\omega & \beta & \beta\omega^2 & \beta\omega & \beta\lambda & \beta\lambda\omega^2 & \beta\lambda\omega \\
\hline
1 & 1 & 1 & -1 & -1 & -1 & \chi & \chi & \chi & -\chi & -\chi & -\chi \\
1 & \omega & \omega^2 & -\gamma & -\gamma\omega & -\gamma\omega^2 & \delta & \delta\omega & \delta\omega^2 & -\gamma\delta & -\gamma\delta\omega & -\gamma\delta\omega^2 \\
1 & \omega^2 & \omega & -\lambda & -\lambda\omega^2 & -\lambda\omega & \epsilon & \epsilon\omega^2 & \epsilon\omega & -\epsilon\lambda & -\epsilon\lambda\omega^2 & -\epsilon\lambda\omega \\
\hline\hline
1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & \omega & \omega^2 & \gamma & \gamma\omega & \gamma\omega^2 & -\alpha & -\alpha\omega & -\alpha\omega^2 & -\alpha\gamma & -\alpha\gamma\omega & -\alpha\gamma\omega^2 \\
1 & \omega^2 & \omega & \lambda & \lambda\omega^2 & \lambda\omega & -\beta & -\beta\omega^2 & -\beta\omega & -\beta\lambda & -\beta\lambda\omega^2 & -\beta\lambda\omega \\
\hline
1 & 1 & 1 & -1 & -1 & -1 & -\chi & -\chi & -\chi & \chi & \chi & \chi \\
1 & \omega & \omega^2 & -\gamma & -\gamma\omega & -\gamma\omega^2 & -\delta & -\delta\omega & -\delta\omega^2 & \gamma\delta & \gamma\delta\omega & \gamma\delta\omega^2 \\
1 & \omega^2 & \omega & -\lambda & -\lambda\omega^2 & -\lambda\omega & -\epsilon & -\epsilon\omega^2 & -\epsilon\omega & \epsilon\lambda & \epsilon\lambda\omega^2 & \epsilon\lambda\omega
\end{array}\right]$$

where $\omega = e^{2\pi i/3}$.

Of course, this construction method is based on using the 2-parameter family $F_6^{(2)}(\gamma, \lambda)$ and following the ideas laid out in the previous examples.

3.5 Inequivalence of Matrices in a Family

In order to show that the families that we have constructed give inequivalent Hadamard matrices, we will make use of the following invariant introduced by Haagerup in his search for classification of the 5×5 Hadamard matrices.

Definition 3.1. *The Haagerup-set of a complex Hadamard matrix H of order n is the set*

$$\Lambda(H) := \{h_{ij}h_{kl}\overline{h_{il}h_{kj}} \ : \ i, j, k, l = 1, \cdots, n\}.$$

It is clear that if H and K are equivalent Hadamard matrices, i.e. there exist permutation matrices P_1, P_2 and diagonal matrices with unimodular entries D_1, D_2 such that

$$P_1 D_1 H D_2 P_2 = K,$$

then

$$\Lambda(H) = \Lambda(K).$$

This follows from the fact that elements in the same row are multiplied by the same number, and elements in the same column are all multiplied by the same number. Since a permutation of the set $\{1, \cdots, n\}$ is the set $\{1, \cdots, n\}$, it is clear that $\Lambda(H) = \Lambda(K)$. Recall that when $\alpha \in \mathbb{C}$ is unimodular $\overline{\alpha} = \frac{1}{\alpha}$. Recall that $F_2 \otimes F_2$ and F_4 are two inequivalent Hadamard matrices belonging to the family

$$U(a) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & a & -a \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -a & a \end{bmatrix}.$$

We have that $U(1) = F_2 \otimes F_2$ and $U(i)$ is a matrix equivalent to F_4. Calculating the Haagerup set for $U(a)$, we have that

$$\Lambda(U(a)) = \{\pm 1, \pm a, \pm \overline{a}\}.$$

Since the Haagerup-set of $U(a)$ depends on the parameter a, it must be the case that any two matrices in this family are inequivalent. In fact, we have that $\Lambda(F_2 \otimes F_2) = \{\pm 1\}$ whereas $\Lambda(F_4) = \{\pm 1, \pm i\}$.

Using the Haagerup-set to show that two Hadamard matrices are inequivalent is one of the most common methods. Our goal is to use the Haagerup-set to determine if we can reduce the number of parameters in any of our families. Recall Example 3.2 and Remark 3.11.1 with the family $F_6^{(2)}(\lambda, \gamma)$ which contains two parameters. We have that the Haagerup-set for this family is

$$\begin{aligned}\Lambda(F_6^{(2)}(\lambda,\gamma)) = \Big\{ & \pm 1, -e^{\frac{\pi i}{3}}, e^{\frac{2\pi i}{3}}, \pm\lambda, \pm\overline{\lambda}, -\gamma, -\overline{\gamma}, \pm\lambda\overline{\gamma}, \pm\overline{\lambda}\gamma, \\ & \pm e^{\frac{\pi i}{3}}\lambda, \pm e^{\frac{2\pi i}{3}}\lambda, \pm e^{\frac{\pi i}{3}}\overline{\lambda}, \pm e^{\frac{2\pi i}{3}}\overline{\lambda}, e^{\frac{\pi i}{3}}\gamma, e^{\frac{\pi i}{3}}\overline{\gamma}, \\ & -e^{\frac{2\pi i}{3}}\gamma, -e^{\frac{2\pi i}{3}}\overline{\gamma}, \pm e^{\frac{\pi i}{3}}\gamma\overline{\lambda}, \pm e^{\frac{2\pi i}{3}}\gamma\overline{\lambda}, \pm e^{\frac{\pi i}{3}}\lambda\overline{\gamma}, \pm e^{\frac{2\pi i}{3}}\lambda\overline{\gamma} \Big\}.\end{aligned}$$

Using this fact, we find that the Haagerup-set for F_6 (which corresponds $\gamma = \lambda = 1$ in the above family) is

$$\Lambda(F_6) = \left\{\pm 1, \pm e^{\frac{\pi i}{3}}, e^{\frac{2\pi i}{3}}\right\}.$$

Notice in $\Lambda(F_6(\lambda, \gamma))$ both parameters γ and λ appear in the Haagerup-set. This gives us hope that this is in fact a two-parameter family.

In Example 3.1, we saw that the 2-parameter family was actually equivalent to a 1-parameter family. (Instead of using $F_6^{(2)}(\lambda, \gamma)$, we will use $F_6'(\lambda, \gamma)$. It should be noted that we have already shown in the example that this family is equivalent to a 1 parameter family.) Indeed using this family, we see that

$$\Lambda(F_6'(\lambda,\gamma) = \left\{\pm 1, \pm e^{\frac{\pi i}{3}}, \pm e^{\frac{2\pi i}{3}}, \pm\lambda\overline{\gamma}, \pm\gamma\overline{\lambda}, \pm e^{\frac{\pi i}{3}}\lambda\overline{\gamma}, \pm e^{\frac{\pi i}{3}}\gamma\overline{\lambda}, \pm e^{\frac{2\pi i}{3}}\lambda\overline{\gamma}, \pm e^{\frac{2\pi i}{3}}\gamma\overline{\lambda}\right\}.$$

Notice in this Haagerup-set, we can replace $\gamma\overline{\lambda}$ with α which would imply that the Haagerup-set relies only on one parameter, not both. Thus, the family in Example 3.1 is indeed equivalent to a one parameter family of Hadamard matrices containing F_6. Therefore, using a change of variable in the Haagerup-set will allow us to determine if a family with m parameters is equivalent to a family with k parameters where $k \leq m$ as we did in the case of Example 3.1.

Chapter 4

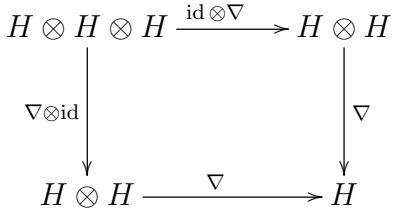
Bismash Commuting Squares

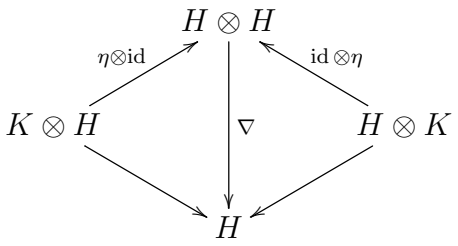
In this chapter, we construct a new class of commuting squares based on the bismash product Hopf algebra. Part of this chapter is based on joint work with Ian Francis and Remus Nicoara.

4.1 Introduction to Hopf Algebras

We will begin by giving the definition of a Hopf algebra and give a few examples. We will then generalize the idea of the commuting square associated to one group using Hopf algebras. For an introduction and construction of algebras, coalgebras, bialgebras, and Hopf algebras refer to [7].

Definition 4.1. *A K-algebra structure is a triple (H, ∇, η), where H is a K-vector space, $\nabla : H \otimes H \to H$ (the multiplication map) and $\eta : K \to H$ (the unit map) are morphisms of K-vector spaces such that the following diagrams are commutative:*

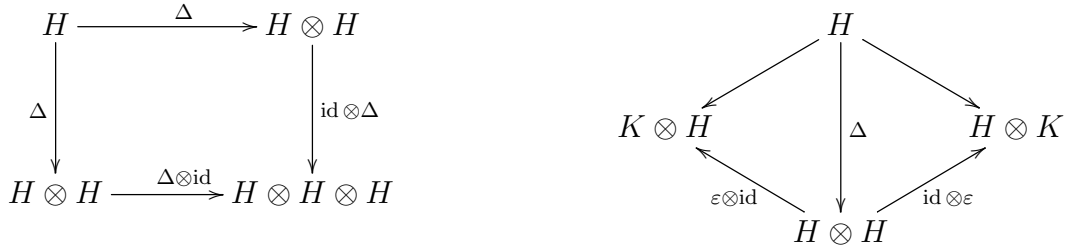




It should be noted here that for the first diagram to commute the multiplication of the

algebra must be associative. In the second diagram, the bottom two arrows are the canonical isomorphisms.

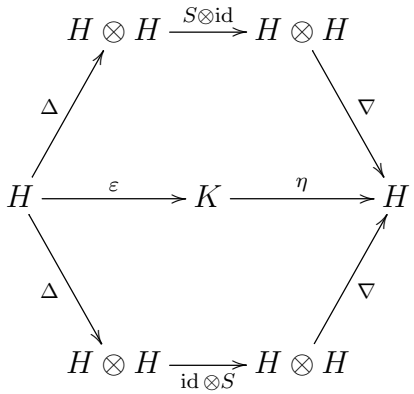
Definition 4.2. *A K-coalgebra structure is a triple (H, Δ, ε), where H is a K-vector space, $\Delta : H \to H \otimes H$ (the comultiplication map) and $\varepsilon : H \to K$ (the counit map) are morphisms of K-vector spaces such that the following diagrams are commutative:*



As before, the commutativity of the first diagram shows that the coalgebra is coassociative, and the unnamed maps in the second diagram are the canonical isomorphisms.

Definition 4.3. *A bialgebra is a K-vector space H, endowed with an algebraic structure (H, ∇, η) and a coalgebra structure (H, Δ, ε). In this case, we also need ∇ and η to be morphisms of coalgebras (this will also show that Δ and ε are morphisms of algebras, Prop 4.1.1 in [7]).*

Definition 4.4. *A Hopf Algebra, H, is a bialgebra over a field K together with a K-linear map $S : H \to H$ such that the following diagram commutes.*



where S is called the antipode map, Δ is the comultiplication of the bialgebra, ε is the counit, η is the unit, and ∇ is the multiplication map.

The following information can be found in [7]. In a Hopf algebra, the antipode is unique since it is the inverse of the element I in the algebra $Hom(H^c, H^a)$ where H^c is the coalgebra structure of H, and H^a is the algebra structure of H. To say that S is the antipode is that $S * I = I * S = \eta\varepsilon$ (here $*$ is the multiplication in the algebra $Hom(H^c, H^a)$), and using the common sigma notation for any $h \in H$:

$$\sum S(h_1)h_2 = \sum h_1 S(h_2) = \varepsilon(h)1.$$

Remark 4.0.1. *(Sigma Notation) Let (H, Δ, ε) be a coalgebra. For $h \in H$, we denote*

$$\Delta(h) = \sum h_1 \otimes h_2$$

where by standard notation the index of the summation is suppressed.

We now give some of the properties of the antipode S.

Proposition 4.0.1. *Let H be a Hopf algebra with antipode S. Then TFAE:*

1. $\sum S(h_1)h_2 = \varepsilon(h)1$ *for any* $h \in H$
2. $\sum h_1 S(h_2) = \varepsilon(h)1$ *for any* $h \in H$
3. $S^2 = I$ *namely the composition of S with itself is I.*

Proposition 4.0.2. *Let H be a Hopf algebra with antipode S. Then we have the following:*

1. $S(hg) = S(g)S(h)$ *for any* $h, g \in H$
2. $S(1) = 1$
3. $\Delta(S(h)) = \sum S(h_2) \otimes S(h_1)$.
4. $\varepsilon(S(h)) = \varepsilon(h)$.

The first two properties mean that S is an antimorphism of algebras, and the last two properties mean that S is an antimorphism of coalgebras.

4.2 Examples of Hopf Algebras

We will now give some examples of Hopf algebras that are of importance to us. For more examples and properties see [1], [2], [16], [17], [18].

Example 4.1. *Let G be a group, and $\mathbb{C}[G]$ the associated group algebra. Then $\mathbb{C}[G]$ is a Hopf algebra.*

For $\mathbb{C}[G]$ to be a Hopf algebra, we need to describe the maps $S, \Delta, \varepsilon, \nabla$, and η and determine whether the diagram at the beginning of the chapter commutes. Recall that $\mathbb{C}[G]$ is a $\mathbb{C}$- vector space with basis $\{g|\ g \in G\}$. Usually we write $\mathbb{C}[G]$ as the linear span of the elements $u_g \in M_n(\mathbb{C})$ described in the previous chapter. However, for convenience , we will write $\mathbb{C}[G]$ as the linear span of the elements of G for ease of notation. In this case, we have a typical element of $\mathbb{C}[G]$ is $\sum_{g\in G} \alpha_g g$ where only finitely many of the α_g's are nonzero (in the case that G is infinite). Note that we may use the left regular representation of the group elements (u_g where $g \in G$) in order to realize $\mathbb{C}[G]$ as a subalgebra of the full matrix algebra.

We define $\Delta : \mathbb{C}[G] \to \mathbb{C}[G] \otimes \mathbb{C}[G]$ only on the basis elements by $\Delta(g) = g \otimes g$. Likewise, for $S : \mathbb{C}[G] \to \mathbb{C}[G]$, it is defined on the basis elements by $S(g) = g^{-1}$. Let $t \in \mathbb{C}[G] \otimes \mathbb{C}[G]$, then $t = \sum \alpha_g g \otimes \beta_h h$, and $\nabla(t) = \sum \alpha_g \beta_h gh$. In other words, for simple tensors of the form $g \otimes h$, $\nabla(g \otimes h) = gh$. For the counit, ε, we have $\varepsilon(g) = 1_{\mathbb{C}}$, and lastly, for $\alpha \in \mathbb{C}$, we have $\eta(\alpha) = \alpha 1_G$ where $1_G \in G$ is the identity element.

It follows then that

$$
\begin{aligned}
(\nabla \circ (S \otimes \mathrm{id}) \circ \Delta)(g) &= (\nabla \circ (S \otimes \mathrm{id}))(g \otimes g) = \nabla(g^{-1} \otimes g) = 1_G \\
(\eta \circ \varepsilon)(g) &= \eta(1_{\mathbb{C}}) = 1_G \\
(\nabla \circ (\mathrm{id} \otimes S) \circ \Delta)(g) &= (\nabla \circ (\mathrm{id} \otimes S))(g \otimes g) = \nabla(g \otimes g^{-1}) = 1_G
\end{aligned}
$$

Hence, the diagram commutes giving us that $\mathbb{C}[G]$ together with the maps defined is a Hopf Algebra. Note that for S defined above S^2 is the identity map giving us that S is indeed the antipode of $\mathbb{C}[G]$.

There is another well known example of Hopf algebras that we have already encountered as well.

Example 4.2. *The dual of* $\mathbb{C}[G]$, $(\mathbb{C}[G])^*$ *when* G *is a finite group is a Hopf Algebra where* $\{\rho_g |\ \rho_g(h) = \delta_g^h\ \forall g, h \in G\}$ *is an orthogonal (idempotent) basis for* $(\mathbb{C}[G])^*$ *with the maps* $\Delta(\rho_g) = \sum_{h \in G} (\rho_{gh^{-1}} \otimes \rho_h)$, $\varepsilon(\rho_g) = \delta_g^{1_G}$, *and* $S(\rho_g) = \rho_{g^{-1}}$.

Recall that when $|G| = n < \infty$, $(\mathbb{C}[G])^* = Hom(\mathbb{C}[G], \mathbb{C})$ is isomorphic to the algebra of $n \times n$ diagonal matrices. It is standard notation to use $\mathbb{C}^G$ instead of $(\mathbb{C}[G])^*$.

Example 4.3. *([17]) Let* H *be a semisimple Hopf algebra and* p *an odd prime number such that the dimension of* H *over* $\mathbb{C}$ *is* p^2 *then* H *is isomorphic to* $\mathbb{C}[\mathbb{Z}_{p^2}]$ *or* $\mathbb{C}[\mathbb{Z}_p \times \mathbb{Z}_p]$.

For the purposes of this paper, an important example of a Hopf Algebra associated to an action of a Hopf Algebra H on another algebra A is given by the following

Definition 4.5. *If* A *is an* H*-module algebra (*A *is a (left)* H*-module), the smash product of* A *and* H, *denoted* $A\#H$, *is, as a vector space* $A\#H = A \otimes H$, *together with the following operation*

$$(a\#h)(b\#g) = \sum a(h_1 \cdot b)\#h_2 g$$

where $\Delta(h) = \sum h_1 \otimes h_2$. *We denote the element* $a\#h$ *instead of* $a \otimes h$ *to emphasize the Hopf algebra structure.*

We will now explore some examples of smash products $A\#H$ where H is either $\mathbb{C}[G]$ and $(\mathbb{C}[G])^*$ for G a finite group.

Let G be a group acting on an algebra A by a group homomorphism $\alpha : G \to Aut_{\mathbb{C}}(A)$. It is standard practice to denote $\alpha(g) = \alpha_g : A \to A$ for $g \in G$. We have the following propositon:

Proposition 4.0.3. *Any action of* G *on an algebra* A *makes* A *into a* $\mathbb{C}[G]$*-module algebra. Conversely, if* A *is a* $\mathbb{C}[G]$*-module algebra, then there is an action of* G *onto* A.

Let G be a group acting on an algebra A via α. Then we have that the smash product $A\#\mathbb{C}[G]$ has multiplication determined by

$$(a\#g)(b\#h) = a\alpha_g(b)\#gh$$

for $a, b \in A$ and $g, h \in G$ since the comultiplication of $\mathbb{C}[G]$ has the property $\Delta(g) = g \otimes g$ for all $g \in G$. In this case, we have that $A\#\mathbb{C}[G] = A * G$ the skew group ring with multiplication

$$(ag)(bh) = a(g \cdot b)gh$$

for all $a, b \in A$ and $g, h \in G$.

Example 4.4. *Let G be a group acting on the group F via $\alpha : G \to Aut(F)$. Then we have that G acts on the group algebra $\mathbb{C}[F]$ and therefore it makes $\mathbb{C}[F]$ a $\mathbb{C}[G]$ module. Hence, we may define the smash product $\mathbb{C}[F]\#\mathbb{C}[G]$ which has multiplication defined by*

$$(f\#g)(f'\#g') = f\alpha_g(f')\#gg'$$

for $f, f' \in F$ and $g, g' \in G$.

In this case, we have that $\mathbb{C}[F]\#\mathbb{C}[G]$ is isomorphic to the group algebra $\mathbb{C}[F \rtimes_\alpha G]$ where $F \rtimes_\alpha G$ is the semidirect product of F and G. Because of this fact, the smash product $A\#H$ is sometimes referred to as the semidirect product.

Instead of using $\mathbb{C}[G]$ as our Hopf algebra, how are things different if we use $(\mathbb{C}[G])^*$? We need to find an algebra A which is a $(\mathbb{C}[G])^*$-module. In this case, we need to have A to be graded by G [19] (see [5] as well). When A is graded by G, we define the multiplication in $A\#(\mathbb{C}[G])^*$ for $a, b \in A$ and $\rho_g, \rho_h \in (\mathbb{C}[G])^*$ by

$$(a\#\rho_g)(b\#\rho_h) = \sum_{l \in G} a(\rho_{gl^{-1}} \cdot b)\#(\rho_l\rho_h) = ab_{gh^{-1}}\#\rho_h$$

using $\Delta(\rho_g) = \sum_{h \in G}(\rho_{gh^{-1}} \otimes \rho_h)$ for ρ_g a basis element of $(\mathbb{C}[G])^*$. Note that $\rho_g \cdot a$ signifies the action of $(\mathbb{C}[G])^*$ on A, and it is essentially the projection onto a subspace of A determined by g since A being graded by G means that each $a \in A$ can be written in the form $a = \sum_{g \in G} a_g$.

4.3 Hopf Algebras from a matched pair of groups

In this section, we will recall an important class of Hopf algebras, namely the bismash product $\mathbb{C}^G\#\mathbb{C}[F]$ where G and F are both finite groups that form a matched pair. We introduce some results from group theory and provide the exact definition of the bismash product. Later in the next section, we will introduce the commuting square associated to a matched pair of groups by using the bismash product $\mathbb{C}^G\#\mathbb{C}[F]$.

4.3.1 Matched Pair of Groups

We will begin by recalling the definition and properties of groups that can be exactly factored by two proper subgroups. These properties can be found in many exercises in graduate algebra textbooks. They are also recalled in many papers that construct the so called bismash product Hopf algebra which we introduce in Section 4.3.2.

Definition 4.6. *An exact factorization of a group L is a pair of proper subgroups F, G such that $L = FG$ and $F \cap G = \{e\}$. We say that F and G factor L exactly.*

We have the following theorem to test for exact factorization:

Theorem 4.1. *Let F and G be proper subgroups of a group L. Then F and G factor L exactly if and only if $|L| = |F| \cdot |G|$ and $F \cap G = \{e\}$.*

Corollary 4.1.1. *If $L = FG$ is an exact factorization of L, then so too is $L = GF$.*

Corollary 4.1.2. *$L = FG$ is an exact factorization of L if and only if for each $l \in L$, $l = fg$ for some uniquely determined $f \in F$ and $g \in G$.*

Example 4.5. *Let $L = A_5$ the alternating group with 60 elements. We may embed A_4, the alternating group with 12 elements, into A_5, and we have the subgroup generated by the 5-cycle (12345) which is isomorphic to $\mathbb{Z}_5$. Then it follows that $A_4 \cap \mathbb{Z}_5 = \{(1)\}$ and $|A_4| \cdot |\mathbb{Z}_5| = 12 \cdot 5 = 60 = |A_5|$. Therefore, we have that $A_4\mathbb{Z}_5$ is an exact factorization of A_5. Also, note that since A_n is a simple group (no non-trivial proper normal subgroups) for $n \geq 5$ neither A_4 nor $\mathbb{Z}_5$ are normal subgroups of A_5.*

Let $L = FG$ be an exact factorization. Then we may define set maps $\lhd : G \times F \to G$ and $\rhd : G \times F \to F$ in the following manner: every $l \in L$ may be written uniquely as $l = f'g'$ for some $f' \in F$ and $g' \in G$, but since F and G are both subgroups of L we have that the element $gf \in L$. We want to find the unique elements $f' \in F, g' \in G$ such that $gf = l = f'g'$. So we define $g \rhd f := f'$ and $g \lhd f := g'$. Since an exact factorization of each element of L is unique, the maps are well defined.

Lemma 4.1.1. *For an exact factorization $L = FG$, the set maps $\lhd : G \times F \to G$ and $\rhd : G \times F \to F$, we have $g \rhd e = e$ and $e \lhd f = e$ for all $f \in F$ and $g \in G$.*

Proof. Let $f \in F$ and $g \in G$ for F and G satisfying the above conditions. Then it follows that

$$eg = g = ge = (g \rhd e)(g \lhd e)$$

where $e \in L = FG$ is the identity element. By the uniqueness of the factorization of the elements of L, we have that $g \rhd e = e$. A similar method works for $e \lhd f = e$. □

Corollary 4.1.3. *For an exact factorization $L = FG$, the set maps $\lhd : G \times F \to G$ and $\rhd : G \times F \to F$, we have $e \rhd f = f$ and $g \lhd e = g$ for all $f \in F$ and $g \in G$.*

Theorem 4.2. *For an exact factorization $L = FG$, the set maps $\lhd : G \times F \to G$ and $\rhd : G \times F \to F$ defined via $(g \rhd f)(g \lhd f) =: gf \in L$ for every $g \in G$ and $f \in F$ are group actions. Furthermore, we have that for every $a, b \in F$ and $x, y \in G$,*

1. $x \rhd (ab) = (x \rhd a)((x \lhd a) \rhd b)$
2. $(xy) \lhd a = (x \lhd (y \rhd a))(y \lhd a)$

Proof. We will prove part 1 here only. Part 2 will follow in a similar manner.

Let $x \in G$ and $a, b \in F$. Then it follows that

$$\begin{aligned} x(ab) &= (x \rhd ab)(x \lhd ab) \\ (xa)b &= ((x \rhd a)(x \lhd a))b = (x \rhd a)((x \lhd a)b) \\ &= (x \rhd a)((x \lhd a) \rhd b)(x \lhd a \lhd b) = (x \rhd a)((x \lhd a) \rhd b)(x \lhd ab) \end{aligned}$$

Equating $x(ab)$ and $(xa)b$ and multiplying by $(x \triangleright ab)^{-1}$ on the right, we have

$$(x \triangleright ab) = (x \triangleright a)((x \triangleleft a) \triangleright b).$$

□

Definition 4.7. *Let F, G be groups with group actions $\triangleleft : G \times F \to G$ and $\triangleright : G \times F \to F$ satisfying the conditions in Theorem 4.2. We say that $(F, G, \triangleright, \triangleleft)$ form a matched pair of groups.*

Example 4.6. *We saw above that for each odd $n \in \mathbb{N}$, we have that $A_n = A_{n-1}\mathbb{Z}_n$ is an exact factorization of the alternating group A_n where in this case $\mathbb{Z}_n$ is isomorphic to the cyclic subgroup generated by the n-cycle $(12\cdots n)$. Note that we need n to be odd so that the n-cycle $(12\cdots n)$ is an element of A_n. We also have that $(A_{n-1}, \mathbb{Z}_n, \triangleright, \triangleleft)$ is a matched pair of groups. We need to define the maps $\triangleright$ and $\triangleleft$, since we know that $gf = (g \triangleright f)(g \triangleleft f)$ for all $g \in \mathbb{Z}_n$ and $f \in A_{n-1}$. With the help of Mathematica, we can find $g \triangleright f$ and $g \triangleleft f$ for the matched pair $(A_4, \mathbb{Z}_5, \triangleright, \triangleleft)$ using the code:*

```
n = 5;
L = AlternatingGroup[n];
F = AlternatingGroup[n - 1];
G = PermutationGroup[{Cycles[{Table[i, {i, 1, n}]}]}];
w[g_, f_] := Module[{gf, gfPos, index, FPos, GPos},
        gf = PermutationProduct[f, g];
        gfPos = GroupElementPosition[L, gf];
        index = Position[Table[GroupElementPosition[L,
                PermutationProduct[Part[GroupElements[G], i],
                Part[GroupElements[F], j]]],
                {j, 1, GroupOrder[F]}, {i, 1, GroupOrder[G]}],
                gfPos];
        FPos = index[[1, 1]];
        GPos = index[[1, 2]];
```

```
{GroupElements[F][[FPos]], GroupElements[G][[GPos]]}]
```

For eaxmple, if we wish to know $(14253) \triangleright (14)(23)$ *and* $(14253) \triangleleft (14)(23)$ *for the matched pair* $(A_4, \mathbb{Z}_5, \triangleright, \triangleleft)$*, we input the cycles into the function. The first value it prints will give us the element in* A_4 *and the second element the function prints will be in the subgroup generated by* (12345)*. Hence we have that*

```
w[Cycles[{{1, 4, 2, 5, 3}}], Cycles[{{1, 4}, {2, 3}}]]

{Cycles[{{1,4},{2,3}}], Cycles[{{1,3,5,2,4}}]}
```

It follows that $(14253) \triangleright (14)(23) = (14)(23)$ *and* $(14253) \triangleleft (14)(23) = (13524)$*.*

Lemma 4.2.1. *Let* $(F, G, \triangleright, \triangleleft)$ *be a matched pair of groups with* $L = FG$ *with* F *normal in* L*. Then it follows that* $g \triangleright f = gfg^{-1}$ *and* $g \triangleleft f = g$ *for all* $g \in G$ *and* $f \in F$*.*

Proof. Let $g \in G$ and $f \in F$ with $L = FG$ so that F is a normal subgroup of L. Then there exists an $f' \in F$ such that $f'g = gf$ since F is normal in L. Then $f'g = gf = (g \triangleright f)(g \triangleleft f)$, we have that $f' = g \triangleright f$ and $g = g \triangleleft f$ by uniqueness of the factorization of the elements of L. Furthermore,

$$gf = (g \triangleright f)(g \triangleleft f) = (g \triangleright f)g \implies gfg^{-1} = g \triangleright f.$$

□

Lemma 4.2.2. *Let* $(F, G, \triangleright, \triangleleft)$ *be a matched pair of groups with* $L = FG$ *and* G *normal in* L*. Then for* $g \in G$ *and* $f \in F$*,* $g \triangleright f = f$*. Furthermore,* $g \triangleleft f = f^{-1}gf$*.*

Proof. Similar calculations as in the previous proof. □

Combining the previous two lemmas, we have the following theorem:

Lemma 4.2.3. *Let* $(F, G, \triangleright, \triangleleft)$ *be a matched pair of groups with* $L = FG$ *with both* F *and* G *normal subgroups of* L*. Then it follows that for all* $f \in F$ *and* $g \in G$*,* $g \triangleright f = f$ *and* $g \triangleleft f = g$*. Namely,* L *is a direct product of* F *and* G*.*

Proof. The statement of this theorem is really asking that L be a direct product of F and G. Let $f \in F$ and $g \in G$ with both F and G normal subgroups of L. Then $fgf^{-1} \in G$ and $gfg^{-1} \in F$. Hence $g(fgf^{-1}) = (gfg^{-1})f^{-1} \in F \cap G = \{e\}$ implying that

$$(g \rhd f)(g \lhd f) = gf = fg$$

and by uniqueness of the factorization of elements in L by F and G, we have $g \rhd f = f$ and $g \lhd f = g$. □

We will need the following lemma for future calculations.

Lemma 4.2.4. *Let $(F, G, \rhd, \lhd)$ be a matched pair of finite groups with $L = FG$. Let $a \in F$, $x, y \in G$, then $x = y \lhd a^{-1}$ implies $y = x \lhd a$. In addition, if $f, a \in F$ and $g \in G$ such that $f = g \rhd a$, then $a = g^{-1} \rhd f$.*

Proof. Since L is factorizable, we can write each $l \in L$ as the product of an element of F and G. Then it follows that

$$\begin{aligned} x = y \lhd a^{-1} &\implies (y \rhd a^{-1})x = (y \rhd a^{-1})(y \lhd a^{-1}) = ya^{-1} \\ &\implies xa = (y \rhd a^{-1})^{-1}y \\ &\implies (x \rhd a)(x \lhd a) = xa = (y \rhd a^{-1})^{-1}y \\ &\implies x \lhd a = y \end{aligned}$$

where the last line follows by the uniqueness of the product decomposition of elements in L. For the second statement, we continue in a similar method.

$$\begin{aligned} f = g \rhd a &\implies f(g \lhd a) = (g \rhd a)(g \lhd a) = ga \\ &\implies g^{-1}f = a(g \lhd a)^{-1} \implies g^{-1} \rhd f = a \end{aligned}$$

by uniqueness. □

Lemma 4.2.5. *Let $(F, G, \rhd, \lhd)$ be a matched pair of finite groups with $L = FG$. For $g \in G$ and $f \in F$, we have that $(g \rhd f)^{-1} = (g \lhd f) \rhd f^{-1}$ and $(g \lhd f)^{-1} = g^{-1} \lhd (g \rhd f)$.*

Proof. Since for any $g \in G$ and $f \in F$, $gf = (g \rhd f)(g \lhd f)$ we have that

$$\begin{aligned}
(g \rhd f)^{-1} &= (g \lhd f) f^{-1} g^{-1} \\
&= ((g \lhd f) \rhd f^{-1})((g \lhd f) \lhd f^{-1}) g^{-1} \\
&= ((g \lhd f) \rhd f^{-1})(g \lhd f f^{-1}) g^{-1} \\
&= ((g \lhd f) \rhd f^{-1})(g \lhd e) g^{-1} \\
&= ((g \lhd f) \rhd f^{-1}) g g^{-1} \\
&= (g \lhd f) \rhd f^{-1}.
\end{aligned}$$

In a similar fashion,

$$\begin{aligned}
(g \lhd f)^{-1} &= f^{-1} g^{-1} (g \rhd f) \\
&= f^{-1}((g^{-1} \rhd (g \rhd f))(g^{-1} \lhd (g \rhd f))) \\
&= f^{-1}((g^{-1} g \rhd f)(g^{-1} \lhd (g \rhd f))) \\
&= f^{-1}(e \rhd f)(g^{-1} \lhd (g \rhd f)) \\
&= f^{-1} f (g^{-1} \lhd (g \rhd f)) \\
&= g^{-1} \lhd (g \rhd f)
\end{aligned}$$

□

How should we view the actions $\lhd$ and $\rhd$ for $L = FG$? Throughout this dissertation, we view the groups F and G as being isomorphic to subgroups of L. In actuality, we should really look at $F \times \{1_L\}$ and $\{1_L\} \times G$ as the subgroups of L so that $L = F \times G$ as sets and not necessarily as groups. The multiplication of L will be defined via:

$$\begin{aligned}
(f, g)(f', g') &= (f, 1_G)(1_F, g)(f', 1_G)(1_F, g') \\
&= (f, 1_G)(g \rhd f', 1_G)(1_F, g \lhd f')(1_F, g') \\
&= (f(g \rhd f'), (g \lhd f') g')
\end{aligned}$$

for all $f, f' \in F$ and $g, g' \in G$. This is the same multiplication rule when $L = F \times G$ as groups (in this case $\triangleleft, \triangleright$ are trivial), when L is the semidirect product of F and G ($L = F \rtimes G$ or $L = F \ltimes G$), or when L is the Zappa-Szép Product of F and G, $L = F \bowtie G$. For more information of the Zappa-Szèp product, also known as bicrossed product or knit product see [1].

4.3.2 The Bismash Product Hopf Algebra

Let $(F, G, \triangleright, \triangleleft)$ be a matched pair of finite groups with $L = FG$. Then we have that the maps $\triangleright, \triangleleft$ induce actions onto $\mathbb{C}^F$ and $\mathbb{C}^G$ from $\mathbb{C}[G]$ and $\mathbb{C}[F]$ respectively. Let $\{\rho_g |\ g \in G\}$ be a basis for $\mathbb{C}^G$, and let $\{\rho_f |\ f \in F\}$ be a basis for $\mathbb{C}^F$. In both cases, we use ρ_x as a basis for the algebras $\mathbb{C}^G$ and $\mathbb{C}^F$ using the index x to know which algebra we are using. We need to induce left actions onto $\mathbb{C}^F$ and $\mathbb{C}^G$ using the actions $\triangleright$ (which is a left action) and $\triangleleft$ which is a right action. We have for all $g \in G$ and $f \in F$, $\mathbb{C}^F$ is a (left) $\mathbb{C}[G]$-module via the action

$$g \cdot \rho_f := \rho_{g \triangleright f}$$

and $\mathbb{C}^G$ is a (left) $\mathbb{C}[F]$-module via the action

$$f \cdot \rho_g := \rho_{g \triangleleft f^{-1}}.$$

Definition 4.8. *Let $(F, G, \triangleright, \triangleleft)$ form a matched pair of finite groups with $L = FG$. Then the bismash product associated to the matched pair of groups is the Hopf algebra $\mathbb{C}^G \# \mathbb{C}[F]$ and has dual $(\mathbb{C}^G \# \mathbb{C}[F])^* = \mathbb{C}^F \# \mathbb{C}[G]$.*

Theorem 4.3. *Let $(F, G, \triangleright, \triangleleft)$ form a matched pair of finite groups with $L = FG$. Then it follows that the dual of $\mathbb{C}^G \# \mathbb{C}[F]$ is $(\mathbb{C}^G \# \mathbb{C}[F])^* = \mathbb{C}^F \# \mathbb{C}[G]$.*

Proof. Let $(F, G, \triangleright, \triangleleft)$ and L be as above. Then we have that the bismash product algebra $\mathbb{C}^G \# \mathbb{C}[F]$ is an example of abelian extension, i.e. there is a short exact sequence of the form

$$0 \to \mathbb{C}^G \to \mathbb{C}^G \# \mathbb{C}[F] \to \mathbb{C}[F] \to 0.$$

The dual of the above short exact sequence is

$$0 \leftarrow (\mathbb{C}^G)^* \leftarrow (\mathbb{C}^G \# \mathbb{C}[F])^* \leftarrow (\mathbb{C}[F])^* \leftarrow 0.$$

Applying the definition of the duals of the group algebras of $\mathbb{C}[G]$ and $\mathbb{C}[F]$ and a similar short exact sequence to the first one, we have the following diagram:

$$\begin{array}{ccccccccc} 0 & \to & (C[F])^* & \to & (\mathbb{C}^G \# \mathbb{C}[F])^* & \to & (\mathbb{C}^G)^* & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathbb{C}^F & \to & \mathbb{C}^F \# \mathbb{C}[G] & \to & \mathbb{C}[G] & \to & 0 \end{array}$$

Since the top and bottom rows are both short exact sequences and the left and right vertical maps are isomorphisms (they are the identity morphism), by the Short Five Lemma, we have that the the middle morphism is in fact an isomorphism. □

The multiplication on $\mathbb{C}^G \# \mathbb{C}[F]$ is defined using the usual smash product multiplication (see Definition 4.5) and is given explicitly as

$$(\rho_x \# a)(\rho_y \# b) = \rho_x (a \cdot \rho_y) \# ab = \rho_x \rho_{y \triangleleft a^{-1}} \# ab = \delta_x^{y \triangleleft a^{-1}} \rho_x \# ab$$

for all $x, y \in G$ and $a, b \in F$ where δ is the Kronecker delta function.

Example 4.7. *Let $L = \mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$. Then $(\mathbb{Z}_2, \mathbb{Z}_3, \triangleright, \triangleleft)$ forms a matched pair with $\triangleright$ and $\triangleleft$ both trivial actions.*

We want to construct the multiplication table for the bismash product $\mathbb{C}^{\mathbb{Z}_2} \# \mathbb{C}[\mathbb{Z}_3]$.

Example 4.8. *Let $L = D_3$ the dihedral group of 6 elements. We have that $L = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ is an exact factorization, so $(\mathbb{Z}_3, \mathbb{Z}_2, \triangleright, \triangleleft)$ is a matched pair. Since $\mathbb{Z}_3$ has index in L equal to 2, we have that $\mathbb{Z}_3$ is normal in L. Therefore, we have that the action $\triangleleft$ is trivial. Therefore, the multiplication table in Figure 4.1 is the multiplication table associated to $L = D_3 \approx \mathbb{Z}_3 \rtimes \mathbb{Z}_2$.*

In the previous, examples we found that the bismash product $\mathbb{C}^{\mathbb{Z}_2} \# \mathbb{C}[\mathbb{Z}_3]$ associated to the groups $\mathbb{Z}_6 \approx \mathbb{Z}_3 \times \mathbb{Z}_2$ and $D_3 \approx \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ have the same structure. In fact, if the

	$\rho_0\#\bar{0}$	$\rho_0\#\bar{1}$	$\rho_0\#\bar{2}$	$\rho_1\#\bar{0}$	$\rho_1\#\bar{1}$	$\rho_1\#\bar{2}$
$\rho_0\#\bar{0}$	$\rho_0\#\bar{0}$	$\rho_0\#\bar{1}$	$\rho_0\#\bar{2}$	0	0	0
$\rho_0\#\bar{1}$	$\rho_0\#\bar{1}$	$\rho_0\#\bar{2}$	$\rho_0\#\bar{0}$	0	0	0
$\rho_0\#\bar{2}$	$\rho_0\#\bar{2}$	$\rho_0\#\bar{0}$	$\rho_0\#\bar{1}$	0	0	0
$\rho_1\#\bar{0}$	0	0	0	$\rho_1\#\bar{0}$	$\rho_1\#\bar{1}$	$\rho_1\#\bar{2}$
$\rho_1\#\bar{1}$	0	0	0	$\rho_1\#\bar{1}$	$\rho_1\#\bar{2}$	$\rho_1\#\bar{0}$
$\rho_1\#\bar{2}$	0	0	0	$\rho_1\#\bar{2}$	$\rho_1\#\bar{0}$	$\rho_1\#\bar{1}$

Figure 4.1: Multiplication Table for the bismash product $\mathbb{C}^{\mathbb{Z}_2}\#\mathbb{C}[\mathbb{Z}_3]$ associated to the group $\mathbb{Z}_6$ (using trivial actions).

action necessary for the multiplication of elements in the algebra is trivial, we have that the bismash product is the tensor product. Where the two bismash products in the example above will differ will be in their duals. We have that the dual algebras $\mathbb{C}^F\#\mathbb{C}[G]$ will have the multiplication defined via

$$(\rho_a\#x)(\rho_b\#y) = \rho_a(x\cdot\rho_b)\#xy = \delta_a^{x\triangleright b}\rho_a\#xy$$

for all $x, y \in G$ and $a, b \in F$.

Note that the group $\mathbb{Z}_2$ acts on the group $\mathbb{Z}_3$ in two ways: trivially, and by conjugation. In the case of $L = \mathbb{Z}_6$, $x \triangleright b = b$ for all $x \in \mathbb{Z}_2$ and $b \in \mathbb{Z}_3$. In the case of $L = D_6$, $x \triangleright b$ has two possibilities. If $x = \bar{0} \in \mathbb{Z}_2$, then $x \triangleright b = b$ for all $b \in \mathbb{Z}_3$. If $x = \bar{1} \in \mathbb{Z}_2$, then $x \triangleright b = b^{-1}$ for all $b \in \mathbb{Z}_3$. Hence, the two bismash products are different. Since the action $\triangleright$ is trivial for the $L = \mathbb{Z}_6$ example, we have that $\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2] = \mathbb{C}^{\mathbb{Z}_3} \otimes \mathbb{C}[\mathbb{Z}_2]$. In figure 4.2, we give the multiplication table for the bismash product $\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2]$ associated to the group $L = D_3 \approx \mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

	$\rho_0\#\bar{0}$	$\rho_0\#\bar{1}$	$\rho_1\#\bar{0}$	$\rho_1\#\bar{1}$	$\rho_2\#\bar{0}$	$\rho_2\#\bar{1}$
$\rho_0\#\bar{0}$	$\rho_0\#\bar{0}$	$\rho_0\#\bar{1}$	0	0	0	0
$\rho_0\#\bar{1}$	$\rho_0\#\bar{1}$	$\rho_0\#\bar{0}$	0	0	0	0
$\rho_1\#\bar{0}$	0	0	$\rho_1\#\bar{0}$	$\rho_1\#\bar{1}$	0	0
$\rho_1\#\bar{1}$	0	0	0	0	$\rho_1\#\bar{1}$	$\rho_1\#\bar{0}$
$\rho_2\#\bar{0}$	0	0	0	0	$\rho_2\#\bar{0}$	$\rho_2\#\bar{1}$
$\rho_2\#\bar{1}$	0	0	$\rho_2\#\bar{1}$	$\rho_2\#\bar{0}$	0	0

Figure 4.2: Multiplication Table for the bismash product $\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2]$ associated to the group D_3.

4.3.3 Some Bismash Products that are Group Algebras

When one first starts looking at bismash products associated to a matched pair of groups, one may ask if in fact you get something other than a group algebra. It turns out that in some cases, the bismash product is in fact a group algebra. The following proposition can be found in [4].

Proposition 4.3.1. *Let $L = FG$ be an exact factorization with $(F, G, \triangleright, \triangleleft)$ forming a matched pair of groups with $L = F \bowtie G$. Then the bismash product $\mathbb{C}^G\#\mathbb{C}[F]$ is isomorphic (as algebras) to the group algebra $\mathbb{C}[\mathbb{Z}_{|G|} \times F]$.*

An immediate example is

Example 4.9. *We have that the dihedral group of $2n$ elements, $D_n = \mathbb{Z}_n \bowtie \mathbb{Z}_2$. Then it follows that the bismash product $\mathbb{C}^{\mathbb{Z}_2}\#\mathbb{C}[\mathbb{Z}_n]$ is isomorphic as algebras to the group algebra $\mathbb{C}[\mathbb{Z}_2 \times \mathbb{Z}_n]$.*

Theorem 4.4. *([19]) A finite-dimensional semisimple Hopf algebra over $\mathbb{C}$ is a group Hopf algebra if and only if it is cocommutative.*

Corollary 4.4.1. *Let $(F, G, \triangleright, \triangleleft)$ be a matched pair of finite groups with $L = FG$. Then we have that the bismash product $\mathbb{C}^G\#\mathbb{C}[F]$ is a group algebra if and only if G is an abelian normal subgroup of L.*

Lemma 4.4.1. *([4]) Let $(F, G, \triangleright, \triangleleft)$ be a matched pair of groups with $L = FG$. Then we have that the bismash product $\mathbb{C}^G\#\mathbb{C}[F]$ is semisimple.*

Proof. (of Corollary 4.4.1) We have that $\mathbb{C}^G\#\mathbb{C}[F]$ is a finite-dimensional semisimple Hopf algebra. To show that $\mathbb{C}^G\#\mathbb{C}[F]$ is a group algebra, we will show that it is cocommutative. Let $g \in G$ and $f \in F$, let Δ be the comultiplication and σ be defined via $\sigma(a \otimes b) = b \otimes a$, then

$$\Delta(\rho_g\#f) = \sum_{h\in G} \rho_{gh^{-1}}\#(h \triangleright f) \otimes \rho_h\#f = \sum_{h\in G} \rho_{gh^{-1}}\#f \otimes \rho_h\#f$$

$$\sigma(\Delta(\rho_g\#f)) = \sum_{h\in G} \rho_h\#f \otimes \rho_{gh^{-1}}\#f = \sum_{h\in G} \rho_{h^{-1}g}\#f \otimes \rho_h\#f$$

Since G is abelian, we have that $\sigma \circ \Delta = \Delta$. Hence, $\mathbb{C}^G\#\mathbb{C}[F]$ is cocommutative a hence a group algebra. $\square$

We have the following theorem of Masuoka [17]:

Theorem 4.5. *A semisimple Hopf algebra of dimension p^2 with a prime p is isomorphic to the group algebra $\mathbb{C}[\mathbb{Z}_{p^2}]$ or $\mathbb{C}[\mathbb{Z}_p \times \mathbb{Z}_p]$.*

Therefore, we immediately know that the bismash product $\mathbb{C}^{\mathbb{Z}_p}\#\mathbb{C}[\mathbb{Z}_p]$ (which is self-dual) is isomorphic to a group algebra, specifically $\mathbb{C}[\mathbb{Z}_p \times \mathbb{Z}_p]$.

Recall from basic group theory that there are only two groups of order p^2 (both of which are abelian). In fact, both groups must be abelian, and the groups are $\mathbb{Z}_{p^2}$, and $\mathbb{Z}_p \times \mathbb{Z}_p$ which is an exact factorization of a group with both maps $\triangleright, \triangleleft$ trivial (since abelian). We also have that both copies of $\mathbb{Z}_p$ in $\mathbb{Z}_p \times \mathbb{Z}_p$ are normal since the group is abelian, and therefore we have that

$$\mathbb{C}^{\mathbb{Z}_p}\#\mathbb{C}[\mathbb{Z}_p] \approx \mathbb{C}[\mathbb{Z}_p] \otimes \mathbb{C}[\mathbb{Z}_p] \approx \mathbb{C}[\mathbb{Z}_p \times \mathbb{Z}_p].$$

4.4 Commuting squares from bismash products

In this section, we associate to any bismash product a commuting square, similarly to constructing commuting squares from groups. We begin by defining the bismash commuting square.

Definition 4.9. *Let $(F, G, \triangleleft, \triangleright)$ be an exact pair of finite groups with $L = FG$ and $n = |L| = |F||G|$. We construct a new class of commuting squares called the bismash commuting square given by*

$$\mathcal{C}^L_{\mathbb{C}^G\#\mathbb{C}[F]} = \begin{pmatrix} \mathbb{C}^F\#\mathbb{C}[G] & \subset & M_n(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C}I_n & \subset & \mathbb{C}^G\#\mathbb{C}[F] \end{pmatrix}.$$

Note that one has to keep track of the original group L associated to the bismash product $\mathbb{C}^G\#\mathbb{C}[F]$ due to what was seen in the examples in the previous section with the groups $\mathbb{Z}_6$ and D_3 which both can be exactly factored with the subgroups isomorphic to $\mathbb{Z}_3$ and $\mathbb{Z}_2$. We will prove that this construction does in fact give a commuting square.

In order to construct the commuting squares, we need to represent the elements in the bismash product algebra with elements in $M_n(\mathbb{C})$ where $n = |F||G| < \infty$. We will use the same idea as group algebras, namely the left regular representation. So for a typical element $\rho_g \# f \in \mathbb{C}^G \# \mathbb{C}[F]$, we have $u_{\rho_g \# f} = \left(z_{(x,a),(y,b)}\right)_{\substack{x,y \in G \\ a,b \in F}} \in M_n(\mathbb{C})$ where

$$z_{(x,a),(y,b)} = \begin{cases} 1, & (\rho_g \# f)(\rho_y \# b) = \rho_x \# a \\ 0, & \text{else} \end{cases}$$

It follows from the multiplication of the elements in the bismash product and from Lemma 4.2.4 that we may write $u_{(g,f)}$ (we use this abbreviated version for ease of notation) as

$$u_{\rho_g \# f} := u_{(g,f)} = \sum_{a \in F} e_{(g,fa),(g \triangleleft f,a)}.$$

The bismash product $\mathbb{C}^{\mathbb{Z}_2} \# \mathbb{C}[\mathbb{Z}_3]$ associated to the groups $\mathbb{Z}_6$ and D_3 (the Dihedral group of 6 elements) has the same representation. In fact, since the action $\triangleleft$ is trivial in both groups, we have that $u_{(g,f)}$ for both groups will be a block circulant matrix. This tells us that a typical element in the bismash product algebra will look like a block diagonal matrix whose entries are circulant matrices.

Example 4.10. *For the bismash product $\mathbb{C}^{\mathbb{Z}_2} \# \mathbb{C}[\mathbb{Z}_3]$ associated to the group $\mathbb{Z}_6$, we have that the element $u_{\rho_0 \# 1}$ will have the form*

$$\left[\begin{array}{ccc|c} 0 & 1 & 0 & \\ 0 & 0 & 1 & 0I_3 \\ 1 & 0 & 0 & \\ \hline & 0I_3 & & 0I_3 \end{array}\right]$$

Example 4.11. *Let $L = A_5 = FG$ where $F = A_4$ and $G = \mathbb{Z}_5$. A typical element in the bismash product $\mathbb{C}^{\mathbb{Z}_5} \# \mathbb{C}[A_4]$ where the larger group is A_5 can be depicted using Mathematica to achieve a matrix plot. The code below will help represent the simple elements as matrices. Note that it makes use of the Mathematica code used above to find the maps $\triangleright$ and $\triangleleft$. The code used to find $u_{\rho_g \# f}$ is*

```
uu[g_, f_] := Module[{gPos, a, fa, faPos, wgf2Pos, eG, eF, eFG},
    gPos= GroupElementPosition[G, g];
    a[k_]:= GroupElements[F][[k]];
    fa[k_]:= PermutationProduct[a[k], f];
    faPos[k_]:= GroupElementPosition[F, fa[k]];
    wgf2Pos= GroupElementPosition[G, w[g, f][[2]]];
    eG[i_,k_]:= Table[Piecewise[{{0, s != i || t != k},
            {1, s == i && t == k}}],{s,1,GroupOrder[G]},
            {t, 1, GroupOrder[G]}];
    eF[j_,l_]:=Table[Piecewise[{{0, s != j || t != l},
            {1,s == j && t == l}}],{s,1,GroupOrder[F]},
            {t,1,GroupOrder[F]}];
    eFG[i_,j_,k_,l_]:=KroneckerProduct[eG[i,k],eF[j,l]];
    Sum[eFG[gPos,faPos[k],wgf2Pos,k],{k,1,GroupOrder[F]}]]
```

Since a typical element will be a linear combination of the elements $u_{\rho_g \# f}$, we see that a typical element will have the form seen in Figure 4.3. In the figure, the same number is represented by similar shading. The value of 0 is represented by the white areas.

We also need to represent the dual bismash product algebra $\mathbb{C}^F \# \mathbb{C}[G]$ in much the same way. Note that the multiplication in the dual algebra is

$$(\rho_f \# g)(\rho_b \# y) = \rho_f(g \cdot \rho_b) \# gy = \delta_f^{g \triangleright b} \rho_f \# gy.$$

Recall that if $g \triangleright b = f$ then $b = g^{-1} \triangleright f$ for all $g \in G$ and $b, f \in F$.

Let F, G be a matched pair of groups with $L = FG$. A typical element in $\mathbb{C}^F \# \mathbb{C}[G]$ looks like $\rho_f \# g$ for $g \in G$ and $f \in F$. Note that we can make sense of the element $g \# \rho_f$ in $\mathbb{C}[G] \# \mathbb{C}^F$ (note that we should change the multiplication so that multiplication is the same as in the original smash product). We have that

$$\mathbb{C}[G] \# \mathbb{C}^F \approx \mathbb{C}^F \# \mathbb{C}[G]$$

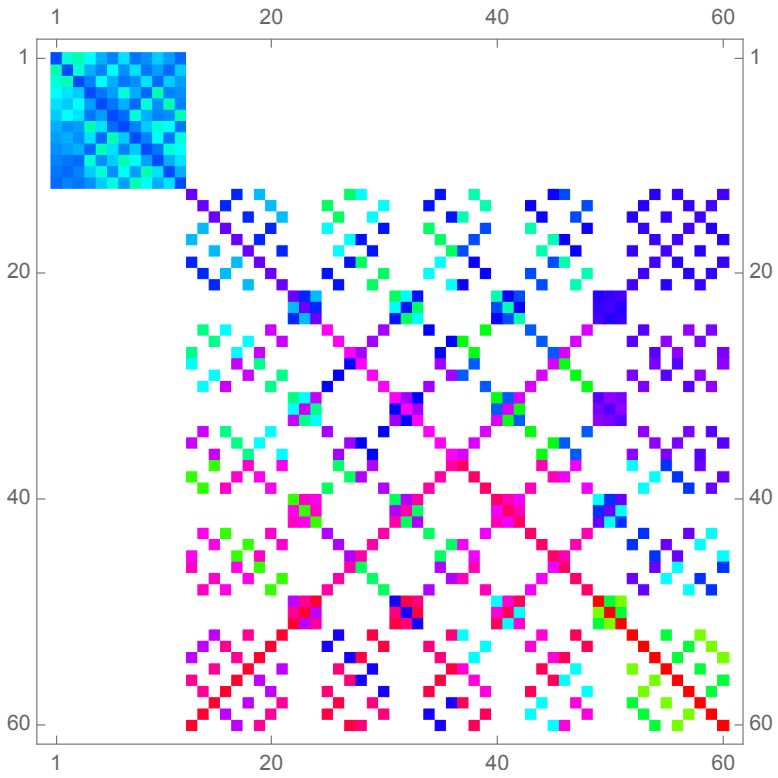


Figure 4.3: A typical element in the bismash product $\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]$ associated to the group A_5.

by $\rho_f\#g \mapsto g\#\rho_{g^{-1}\triangleright f}$. We define the multiplication in $\mathbb{C}[G]\#\mathbb{C}^F$ by

$$(g_1\#\rho_{f_1})(g_2\#\rho_{f_2}) = \delta^{g_2^{-1}\triangleright f_2}_{g_2^{-1}g_1^{-1}\triangleright f_1} g_1g_2\#\rho_{g_2^{-1}g_1^{-1}\triangleright f_1}.$$

The multiplication rule is not entirely important for what we want to do. We really can deal with the multiplication in $\mathbb{C}^F\#\mathbb{C}[G]$ and then map into $\mathbb{C}[G]\#\mathbb{C}^F$. It should be noted that this is the same multiplication since if we look at the image of the typical element and then multiply, we achieve the same result as we do as we multiply first and then look at the image. This is due to the fact that

$$\begin{aligned}
\delta^{g_2^{-1}\triangleright f_2}_{g_2^{-1}g_1^{-1}\triangleright f_1} = 1 &\iff g_2^{-1}\triangleright f_2 = g_2^{-1}g_1^{-1}\triangleright f_1 \\
&\iff f_2 = g_1^{-1}\triangleright f_1 \\
&\iff f_1 = g_2\triangleright f_2 \iff \delta^{g_2\triangleright f_2}_{f_1} = 1
\end{aligned}$$

which is the factor that is need for the multiplication to be nonzero in $\mathbb{C}^F\#\mathbb{C}[G]$.

The main reason that we wish to change the coordinates is so we can make sense of the multiplication of embeddings of typical elements as matrices. Recall that we can represent an element $\rho_f\#g \in \mathbb{C}^F\#\mathbb{C}[G]$ as an element in $M_{|F||G|}(\mathbb{C})$ by

$$v_{\rho_f\#g} = \sum_{y\in G} e_{f\#gy,g^{-1}\triangleright f\#y} = \sum_{y\in G} e_{f,g^{-1}\triangleright f} \otimes e_{gy,y}$$

and similarly for $\rho_g\#f \in \mathbb{C}^G\#\mathbb{C}[F]$ as $v_{\rho_g\#f} = \sum_{x\in F} e_{g\#fx,g\triangleleft f\#x}$.

Example 4.12. *Let $L = A_5 = FG$ where $F = A_4$ and $G = \mathbb{Z}_5$. A typical element in the bismash product $\mathbb{C}^{A_4}\#\mathbb{C}[\mathbb{Z}_5]$ can be found using Mathematica much as we did for the algebra $\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]$. The code below will find the representation for simple elements as matrices. Figure 4.4 shows the form of a typical element in the dual algebra. Again, similar shading represents the same number. The white area represents the value of zero.*

```
vv[f_,g_]:=Module[{x,wxInvf1Pos,gInvxPos,eG,eF,eFG,gInv,gInvx},
        x[k_] := GroupElements[G][[k]];
        wxInvf1Pos[k_]:=GroupElementPosition[F,
                        w[InversePermutation[x[k]],f][[1]]];
        gInv = InversePermutation[g];
        gInvx[k_]:=PermutationProduct[x[k],gInv];
        gInvxPos[k_]:=GroupElementPosition[G,gInvx[k]];
        eG[i_,k_]:=Table[Piecewise[{{0, s != i || t != k},
                {1,s == i && t == k}}],{s,1,GroupOrder[G]},
                {t,1,GroupOrder[G]}] ;
        eF[j_,l_]:=Table[Piecewise[{{0, s != j || t != l},
                {1,s == j && t == l}}], {s,1,GroupOrder[F]},
                {t,1,GroupOrder[F]}];
        eFG[i_,j_,k_,l_]:=KroneckerProduct[eG[i,k],eF[j,l]];
        Sum[eFG[k,wxInvf1Pos[k],gInvxPos[k],wxInvf1Pos[k]],
                {k,1,GroupOrder[G]}]]
```

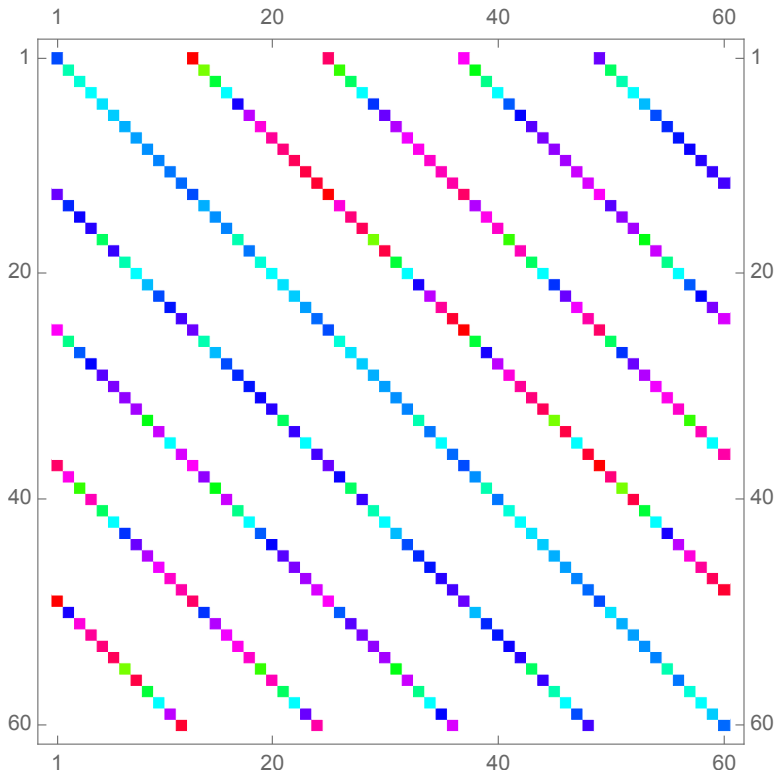


Figure 4.4: A typical element in the bismash product $\mathbb{C}^{A_4}\#\mathbb{C}[\mathbb{Z}_5]$ as the dual to $\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]$ associated to the group A_5.

Let $A = \mathbb{C}^F\#\mathbb{C}[G]$ and $A^* = \mathbb{C}^G\#\mathbb{C}[F] \approx \mathbb{C}[F]\#\mathbb{C}^G$. Then we can represent an element in the dual as

$$v_{\rho_g\#f} = \sum_{x\in F} e_{fx\#g\triangleleft fx, x\#g\triangleleft fx} = \sum_{x\in F} e_{fx,x} \otimes e_{g\triangleleft fx, g\triangleleft fx}.$$

Theorem 4.6. *Let $L = FG$ be a finite group such that $(F, G, \triangleleft, \triangleright)$ is a matched pair of groups.. Then it follows that*

$$\mathbb{C}^G\#\mathbb{C}[F] \cap \mathbb{C}^F\#\mathbb{C}[G] = \mathbb{C}I_n$$

where $n = |F| \cdot |G|$.

Proof. (Sketch) Typical elements in $\mathbb{C}^G\#\mathbb{C}[F]$ and $\mathbb{C}^F\#\mathbb{C}[G]$ will be linear combinations of elements of $u_{\rho_f\#g}$ and $v_{\rho_{g'}\#f'}$ for $f, f' \in F$ and $g, g' \in G$. In order to determine when an element in is in the intersection, we need only to find when $v_{\rho_{g'}\#f'} = u_{\rho_f\#g}$. It is easy to check that when this happens $g = 1_G$ and $f' = 1_F$. In this case, we have an element in the

intersection must be constant along the diagonal on the matrix. So the intersection must be $\mathbb{C}I_n$. $\square$

Theorem 4.7. *Let $L = FG$ be a finite group such that $(F, G, \triangleleft, \triangleright)$ is a matched pair of groups. It follows that*

$$\mathcal{C}^L_{\mathbb{C}^G \# \mathbb{C}[F]} = \begin{pmatrix} \mathbb{C}^F \# \mathbb{C}[G] & \subset & M_n(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C}I_n & \subset & \mathbb{C}^G \# \mathbb{C}[F] \end{pmatrix}$$

is a commuting square.

Proof. In order for $\mathcal{C}^L_{\mathbb{C}^G \# \mathbb{C}[F]}$ to be a commuting square, we need to show that $(\mathbb{C}^G \# \mathbb{C}[F]) \ominus \mathbb{C}I_n \perp (\mathbb{C}^F \# \mathbb{C}[G]) \ominus \mathbb{C}I_n$. So we want to calculate the inner product between a basis element of H and H^*. So we calculate the following trace:

$$\begin{aligned}
\tau(v_{\rho_g \# f} u^*_{\rho_{f'} \# g'}) &= \tau\left(\sum_{x \in F} \sum_{y \in G} e_{fx,x} e_{g'^{-1} \triangleright f', f'} \otimes e_{g \triangleleft fx, g \triangleleft fx} e_{y, g'y} \right) \\
&= \tau(e_{f(g'^{-1} \triangleright f'), f'} \otimes e_{g \triangleleft f(g'^{-1} \triangleright f'), g'(g \triangleleft f(g'^{-1} \triangleright f'))}) \\
&= \tau(e_{f(g'^{-1} \triangleright f'), f'}) \tau(e_{g \triangleleft f(g'^{-1} \triangleright f'), g'(g \triangleleft f(g'^{-1} \triangleright f'))}) \\
&= \frac{1}{|F||G|} \delta^{f'}_{f(g'^{-1} \triangleright f')} \delta^{g \triangleleft f(g'^{-1} \triangleright f')}_{g'(g \triangleleft f(g'^{-1} \triangleright f'))} \\
&= \frac{1}{|F||G|} \delta^{f'}_{f(g'^{-1} \triangleright f')} \delta^{1_G}_{g'} \\
&= \frac{1}{|F||G|} \delta^{f'}_{ff'} \delta^{1_G}_{g'} \\
&= \frac{1}{|F||G|} \delta^{1_F}_{f} \delta^{1_G}_{g'}
\end{aligned}$$

Note that if we want these elements to be orthogonal to $\mathbb{C}$ we need f to not be the identity in F and g' to not be the identity element in G. Hence, we have that $H \ominus \mathbb{C} \perp H^* \ominus \mathbb{C}$. $\square$

4.5 The Undephased Defect of a Bismash Commuting Square

We now give some computations of the undephased defect of the newly constructed bismash commuting squares. Recall from Nicoara [23] that the defect is an upper bound for the number of parameters in a family of commuting squares containing the given bismash commuting square.

Let $A = span\{u_{(g,f)} = \sum_{a\in F} e_{(g,fa),(g\triangleleft f,a)}\}$, $A^* = span\{v_{f,g} = \sum_{x\in G} e_{(x,x^{-1}\triangleright f),(g^{-1}x,x^{-1}\triangleright f)}\}$, and $[A, A^*] = span\{e_{(g,f((g\triangleleft f)^{-1}\triangleright f')),(g'^{-1}(g\triangleleft f),(g\triangleleft f)^{-1}\triangleright f')} - e_{(g'g,g^{-1}g'^{-1}\triangleright f'),(g\triangleleft f,f^{-1}(g^{-1}g'^{-1}\triangleright f'))}\}$. Then A is the representation of the algebra $\mathbb{C}^G\#\mathbb{C}[F]$, and A^* is the representation of the algebra $\mathbb{C}^F\#\mathbb{C}[G]$. Note that the dimensions of A and A^* are both n, where $n = |F||G|$. Then the defect of A is defined as

$$d(A) := n^2 - \dim_{\mathbb{C}}[A, A^*] = \dim_{\mathbb{C}}[A, A^*]^{\perp} = \dim_{\mathbb{C}} V,$$

where

$$V := \left\{ (z_{(g,f),(g',f')})_{\substack{g,g'\in G\\ f,f'\in F}} \in M_n(\mathbb{C}) : \sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')}[u_{(g,f)}, v_{(f',g')}] = 0 \right\}.$$

It follows that

$$\sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')}[u_{(g,f)}, v_{(f',g')}] = 0$$

$$\Longleftrightarrow$$

$$\sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')} e_{(g,f((g\triangleleft f)^{-1}\triangleright f')),(g'^{-1}(g\triangleleft f),(g\triangleleft f)^{-1}\triangleright f')}$$

$$= \sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')} e_{(g'g,g^{-1}g'^{-1}\triangleright f'),(g\triangleleft f,f^{-1}(g^{-1}g'^{-1}\triangleright f'))}$$

4.5.1 Defect Computations

With the use of a computer, we can calculate the number of distinct coefficients in V. First, we use the bismash product coming from $L = A_5 = FG$ where $F = A_4$ and $G = \mathbb{Z}_5$, namely $\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]$.

Example 4.13. *Using a computer, we can calculate the defect of* $\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]$ *coming from the group* $A_5 = A_4\mathbb{Z}_5$. *It follows that*

$$d(\mathbb{C}^{\mathbb{Z}_5}\#\mathbb{C}[A_4]) = 1168.$$

It should be noted that the defect of the group A_5 *is* $d(A_5) = 1168$. *The defect was calculated by finding the number of distinct coefficients* $z_{(g,f),(g',f')}$ *for* $g, g' \in \mathbb{Z}_5$ *and* $f, f' \in A_4$ *satisfying*

$$\sum_{\substack{g,g'\in\mathbb{Z}_5\\ f,f'\in A_4}} z_{(g,f),(g',f')}[u_{(g,f)}, v_{(f',g')}] = 0.$$

Another way that we could calculate the defect using a computer is a method discussed in [25] by Nicoara and White. We can find the $\dim_{\mathbb{C}}(W)$ where

$$W = span\{[u_{(g,f)}, v_{(f',g')}] : g, g' \in G, \text{ and } f, f' \in F\}.$$

We have that if s is the $n^2 \times n^2$ matrix indexed by $(G \times F) \times (G \times F)$ whose $((g, f), (g', f'))^{\text{th}}$ row is given by $[u_{(g,f)}, v_{(f',g')}]$ (really we are flattening the $n \times n$ matrix, $[u_{(g,f)}, v_{(f',g')}]$, to be a vector of length n^2). Recall $n = |L| = |F||G|$. It follows that rank of s will give us the dimension of W. Therefore,

$$\dim_{\mathbb{C}}(V) = \dim_{\mathbb{C}}(W^{\perp}) = n^2 - rank(s).$$

Therefore, we also have that $\dim_{\mathbb{C}}(V)$ is the nullity of the matrix s.

Example 4.14. *We have that* $L = S_3$ *can be exactly factored as* $S_3 = \mathbb{Z}_2\mathbb{Z}_3$. *Note that one of the actions is trivial while the other is conjugation. This follows from the fact that*

$S_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$. *The defect of the algebra* $\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2]$ *is* $d(\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2]) = 19$ *as found using the method described before this example. In fact, we already know that* $d(S_3) = 19$ *as well.*

Example 4.15. *Using any of the methods from the previous two examples, we find that the defect of* $\mathbb{C}^{\mathbb{Z}_2}\#\mathbb{C}[\mathbb{Z}_3]$ *when* $\mathbb{Z}_6 = \mathbb{Z}_3\mathbb{Z}_2 = \mathbb{Z}_2\mathbb{Z}_3$ *is*

$$d(\mathbb{C}^{\mathbb{Z}_2}\#\mathbb{C}[\mathbb{Z}_3]) = d(\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2]) = 15 = d(\mathbb{Z}_6).$$

In all the examples that we have seen so far, the defect of the bismash product algebra has been equal to the defect of the group that forms the algebra. This leads us to the following conjecture:

Conjecture 4.7.1. *Let* $L = FG$ *be an exact factorization of a group* L*. Then the defect of* $\mathbb{C}^G\#\mathbb{C}[F]$ *is*

$$d(\mathbb{C}^G\#\mathbb{C}[F]) = d(L).$$

This gives us another reason why we should keep track of the original group that forms the bismash product. Notice that for groups that are decomposable as $L = \mathbb{Z}_2\mathbb{Z}_3$, we know that L can be equal to $\mathbb{Z}_6$ or S_3. In the first case, the defect is 15, and in the second case the defect is 19. Due to this fact, it may be necessary to write $\mathbb{C}^G\#_L\mathbb{C}[F]$ where $L = FG$ unless it is clearly stated what group L determines the actions $\triangleleft$, and $\triangleright$. Throughout this dissertation, we will forgo writing the group L in the algebra as we clearly state which groups we have in each example.

It may be the case that Conjecture 4.7.1 is only true for certain groups. Since we know the actions $\triangleright$ and $\triangleleft$ for certain factorizable groups $L = FG$, we can calculate the defect the bismash product coming from L. The following example seems to give us a problem.

Example 4.16. *Let* $L = S_3 = \mathbb{Z}_3\mathbb{Z}_2$*. We know that* $S_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$*. Proposition 4.3.1 tells us that* $\mathbb{C}^{\mathbb{Z}_2}\#\mathbb{C}[\mathbb{Z}_3]$ *is isomorphic as an algebra to* $\mathbb{C}[\mathbb{Z}_2 \times \mathbb{Z}_3]$*. Recall that* $d(\mathbb{Z}_2 \times \mathbb{Z}_3) = 15$*. We should expect* $d(\mathbb{C}^{\mathbb{Z}_2}\#\mathbb{C}[\mathbb{Z}_3])$ *to be equal to* $d(\mathbb{C}^{\mathbb{Z}_3}\#\mathbb{C}[\mathbb{Z}_2]) = 19 = d(S_3)$*. We do not have a problem in this case since the defect takes into its calculations the corners of the commuting square. Recall that when we calculate the defect in the group algebra case, one corner is*

isomorphic to the diagonal matrices. In the case of the bismash algebra commuting squares, both corners are bismash algebras not necessarily isomorphic to the diagonal matrices.

4.5.2 Calculating $d(\mathbb{C}^G \# \mathbb{C}[F])$ when $L = F \times G$

In this subsection, we would like to prove Conjecture 4.7.1 when $L = FG$ is the direct product of F and G.

Theorem 4.8. *Let $L = FG$ be an exact factorization of a finite group, L, where both F and G are normal subgroups. In this case, $L = F \times G$. Then it follows that*

$$d(\mathbb{C}^G \# \mathbb{C}[F]) = d(L).$$

Proof. Let $L = F \times G$ be a finite group. From Lemma 4.2.3, we have that both $\lhd$ and $\rhd$ are trivial, i.e. $g \rhd f = f$ and $g \lhd f = g$ for all $f \in F$ and $g \in G$. In other words, every element in F commutes with every element in G (this does not say that L is abelian).

Notice from the calculations above and using the our specific actions, we have that

$$\sum_{\substack{g,g' \in G \\ f,f' \in F}} z_{(g,f),(g',f')}[u_{(g,f)}, v_{(f',g')}] = 0$$

$$\iff \sum_{\substack{g,g' \in G \\ f,f' \in F}} z_{(g,f),(g',f')} e_{(g,ff'),(g'^{-1}g,f')} - \sum_{\substack{g,g' \in G \\ f,f' \in F}} z_{(g,f),(g',f')} e_{(g'g,f'),(g,f^{-1}f')}) = 0$$

Using the change of variables, where in the first sum $x = g, a = ff', y = g'^{-1}g,$ and $b = f'$ and in the second sum $x = g'g, a = f', y = g,$ and $b = f^{-1}f'$, we get that

$$z_{(x,ab^{-1}),(xy^{-1},b)} = z_{(y,ab^{-1}),(xy^{-1},a)}.$$

Using another change of variable with $g = x, f = ab^{-1}, g' = xy^{-1}$ and $f' = b$, we get that

$$z_{(g,f),(g',f')} = z_{(g'^{-1}g,f),(g',ff')}.$$

Iterating this relationship, we have that

$$\begin{aligned} z_{(g,f),(g',f')} &= z_{(g'^{-1}g,f),(g',ff')} \\ &= z_{(g'^{-2}g,f),(g',f^2f')} \\ &\vdots \\ &= z_{(g'^{-n}g,f),(g',f^nf')} \end{aligned}$$

The smallest n that will give us $g = g'^{-n}g$ and $f' = f^n f'$ is $n = lcm(|g'|, |f|)$ for each $g \in G$ and $f' \in F$. Therefore, the number of distinct values of $z_{(g,f),(g',f')}$ is equal to

$$\sum_{\substack{g \in G \\ f' \in F}} \frac{|G||F|}{lcm(|g'|, |f|)}.$$

Recall that $|L| = |G||F|$ and since for each $l \in L$ $l = fg$, we have that $|l| = lcm(|g|, |f|)$ for some $g \in G$ and $f \in F$ whenever $L = F \times G$. Therefore, we have that

$$d(\mathbb{C}^G \# \mathbb{C}[F]) = \sum_{\substack{g \in G \\ f' \in F}} \frac{|G||F|}{lcm(|g'|, |f|)} = \sum_{l \in L} \frac{|L|}{|l|} = d(L).$$

□

This result allows us to have the following:

Corollary 4.8.1. *Let $L = FG$ be an exact factorization of a finite group, L, where both F and G are normal subgroups. In this case, $L = F \times G$. Suppose further that the orders of F and G are coprime. Then it follows that*

$$d(\mathbb{C}^G \# \mathbb{C}[F]) = d(G)d(F).$$

Proof. Use Theorem 1.3. We have that $d(\mathbb{C}^G \# \mathbb{C}[F]) = d(L) = d(G)d(F)$. □

4.5.3 Calculating $d(\mathbb{C}^G\#\mathbb{C}[F])$ when $L = F \rtimes G$

The next more complicated example for which we want to calculate the defect of the bismash product is when the group L is the semidirect product of two subgroups.

Theorem 4.9. *Let $L = F \rtimes G$. In this case, we have that the undephased defect of $\mathbb{C}^G\#\mathbb{C}[F]$ is*

$$d(\mathbb{C}^G\#\mathbb{C}[F]) = d(L).$$

Proof. Let $L = F \rtimes G$. By Lemma 4.2.1, we have that $g \triangleright f = gfg^{-1}$ and $g \triangleleft f = g$ for all $f \in F$ and $g \in G$. Using this fact, we can begin calculating the defect as in the previous proof. It follows that

$$\sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')}[u_{(g,f)}, v_{(f',g')}] = 0$$

$$\Longleftrightarrow$$

$$\sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')} e_{(g,f(g^{-1}f'g)),(g'^{-1}g,g^{-1}f'g)} = \sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')} e_{(g'g,g^{-1}g'^{-1}f'g'g),(g,f^{-1}(g^{-1}g'^{-1}f'g'g))}$$

Replacing g with $g'^{-1}g$ in the second sum, we get that the above is true if and only if

$$\sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')} e_{(g,f(g^{-1}f'g)),(g'^{-1}g,g^{-1}f'g)} = \sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g'^{-1}g,f),(g',f')} e_{(g,g^{-1}f'g),(g'^{-1}g,f^{-1}(g^{-1}f'g))}$$

Replacing f' with $gf'g^{-1}$ in both sums, we have

$$\sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',gf'g^{-1})} e_{(g,ff'),(g'^{-1}g,f')} = \sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g'^{-1}g,f),(g',gf'g^{-1})} e_{(g,f'),(g'^{-1}g,f^{-1}f')}$$

We will use the change of variables $x = g$, $a = ff'$, $y = g'^{-1}g$, and $b = f'$ in the first sum, and in the second sum, we use $x = g$, $a = f'$, $y = g'^{-1}g$, and $b = f^{-1}f'$. This gives us the relation that

$$\sum_{\substack{x,y\in G\\ a,b\in F}} z_{(x,ab^{-1}),(xy^{-1},xbx^{-1})} e_{(x,a),(y,b)} = \sum_{\substack{x,y\in G\\ a,b\in F}} z_{(y,ab^{-1}),(xy^{-1},xax^{-1})} e_{(x,a),(y,b)}$$

This allows us to move the relationship to the coefficients. In other words, we have that the above is true if and only if

$$z_{(x,ab^{-1}),(xy^{-1},xbx^{-1})} = z_{(y,ab^{-1}),(xy^{-1},xax^{-1})}$$

for all $x, y \in G$ and $a, b \in F$. Using one more change of variable with $g = x$, $f = ab^{-1}$, $g' = xy^{-1}$, and $f' = xbx^{-1}$ yields for all $g, g' \in G$ and $f, f' \in F$

$$z_{(g,f),(g',f')} = z_{(g'^{-1}g,f),(g',(gfg^{-1})f')}.$$

Iterating this relationship gives us

$$z_{(g,f),(g',f')} = z_{(g'^{-n}g,f),(g',(g'^{-(n-1)}gfg^{-1}g'^{n-1})\cdots(gfg^{-1})f')}.$$

We need to know what value of n gives us

$$g'^{n} = 1_G \text{ and } (g'^{-(n-1)}gfg^{-1}g'^{n-1})\cdots(gfg^{-1}) = 1_F.$$

Let $l = (gf^{-1}g^{-1}, g'^{-1}) \in L$. If follows that

$$l^m = ((gf^{-1}g^{-1})(g'^{-1}gf^{-1}g^{-1}g')\cdots(g'^{-(m-1)}gf^{-1}g^{-1}g'^{(m-1)}), g'^{-m}).$$

If $m = |l|$, then $(gf^{-1}g^{-1})(g'^{-1}gf^{-1}g^{-1}g')\cdots(g'^{-(m-1)}gf^{-1}g^{-1}g'^{(m-1)}) = 1_F$ which implies that $(g'^{-(m-1)}gfg^{-1}g'^{(m-1)})\cdots(g'^{-1}gfg^{-1}g')(gfg^{-1}) = 1_F$ by taking the inverse of the previous relationship. Therefore, finding the number of distinct coefficients for fixed $g \in G$ and $f' \in F$, is equivalent to finding the order of an element $l \in L$. This gives us that the defect is

$$d(\mathbb{C}^G \# \mathbb{C}[F]) = \sum_{l \in L} \frac{|F||G|}{|l|} = \sum_{l \in L} \frac{|L|}{|l|} = d(L).$$

□

We also have that

Theorem 4.10. *Let $L = F \rtimes G$. In this case, we have that the undephased defect of $\mathbb{C}^F\#\mathbb{C}[G]$ is*

$$d(\mathbb{C}^F\#\mathbb{C}[G]) = d(L).$$

Proof. This follows from the previous case. Since $[u_{(g,f)}, v_{(f',g')}] = -[v_{(f',g')}, u_{(g,f)}]$ for all $g, g' \in G$ and $f, f' \in F$, it follows that

$$\sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')}[u_{(g,f)}, v_{(f',g')}] = 0 \iff \sum_{\substack{g,g'\in G\\ f,f'\in F}} z_{(g,f),(g',f')}[v_{(f',g')}, u_{(g,f)}] = 0.$$

Therefore, the restrictions on the coefficients in the first sum are exactly the same as they are in the second sum. □

4.5.4 Towards calculating $d(\mathbb{C}^G\#\mathbb{C}[F])$ when $L = F \bowtie G$

Notice in both proofs of calculating the defect of $\mathbb{C}^G\#\mathbb{C}[F]$ so far have included essentially the same change of variables at some point. This could mean for a positive result of Conjecture 4.7.1 for any finite group $L = FG$. Currently, calculating the undephased defect of $\mathbb{C}^G\#\mathbb{C}[F]$ when $L = F \bowtie G$ has proven to be complicated. However, it is our hope that 4.7.1 is true for any finite group $L = FG$.

We can use similar change of variables to calculate $d(\mathbb{C}^G\#\mathbb{C}[F])$ when $L = F \rtimes G$, but the problem arises in finding an element of L which has the correct order needed to finish the proof of the conjecture for general groups $L = F \bowtie G$.

Bibliography

[1] Agore, A. L., Chirvasitu, A., Ion, B., and Militaru, G. (2009). Bicrossed products for finite groups. *ArXiv e-prints*. 62, 71

[2] Andruskiewitsch, N. (2014). On finite-dimensional Hopf Algebras. arXiv:1403.7838. 62

[3] Banica, T. (1999). Compact Kac Algebras and commuting squares. arXiv. 9

[4] Clarke, M. C. (2009). On the algebra structure of some bismash products. *Journal of Algebra*, 322:2590–2600. 74

[5] Cohen, M. and Montgomery, S. (1984). Group-graded rings, smash products and group actions. *Transactions of the American Mathematical Society*, 282(1). 64

[6] Collins, M. (2007). Some bismash products that are not group algebras. *Journal of Algebra*, 316:297–302.

[7] Dasclescu, S., Nastasescu, C., and Raianu, S. (2001). *Hopf Algebras: An Introduction*. Number 235 in Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, Inc. 59, 60, 61

[8] e Sá, N. B. and Bengtsson, I. (2012). Families of complex Hadamard matrices. ArXiv:1202.1181v2.

[9] Haagerup, U. (1996). Orthogonal maximal abelian $*$-subaglebras of the $n \times n$ matrices and cyclic n-roots. *Institut for Matematik, U. of Southern Denmark*, 29:296–322.

[10] Haagerup, U. (2008). Cyclic p-roots of prime lengths p and related complex hadamard matrices. *ArXiv e-prints*. 29, 34

[11] Hadamard, J. (1893). Resolution d'une question relative aux determinants. *Bulletin des Science Mathematiques*, 17:240–246. 11

[12] Jones, V. (1983). Index for subfactors. *Invent. math.*, 72:1–25. 1, 3

[13] Kharaghani, H. and Tayfeh-Rezaie, B. (2005). A Hadamard matrix of order 428. *Journal of Combinatorial Designs*, 13:435–440. 11

[14] Klupsch, M. and Lundes, J. (2015). On a class of finite-dimensional semisimple Hopf Algebras. *Communications in Algebra*, 43:2932–2942.

[15] Kobayashi, T. and Masuoka, A. (1997). A result extended from groups to Hopf Algebras. *Tsukuba J. Math.*, 21(1):55–58.

[16] Majid, S. (1990). Physics for algebraists: Non-commutative Hopf Algebras by a bicrossproduct construction. *Journal of Algebra*, 130:17–64. 62

[17] Masuoka, A. (1996). The p^n theorem for semisimple Hopf Algebras. *Proceedings of the American Mathematical Society*, 124(3). 62, 63, 75

[18] Masuoka, A. (2000). Extensions of Hopf Algebras and Lie Bialgebras. *Transactions of the American Mathematical Society*, 352(8):3837–3879. 62

[19] Montgomery, S. (1993). *Hopf Algebras and Their Actions on Rings*. Number 82 in Regional Conference Series in Mathematics. American Mathematical Society. 64, 74

[20] Ng, S.-H. (2004). Hopf Algebras of dimension pq. *Journal of Algebra*, 276:399–406.

[21] Nicoara, R. (2006). A finiteness result for commuting squares of matrix algebras. *Journal of Operator Theory*, 55(2):295–310. 2, 3

[22] Nicoara, R. (2010). Subfactors and Hadamard matrices. *Journal of Operator Theory*, 64.

[23] Nicoara, R. (2011). Limit points of commuting squares. *Indiana University Math Journal*, 60. 3, 9, 82

[24] Nicoara, R. and Beauchamp, K. (2008). Maximal abelian $*$-algebras of the 6×6 matrices. *Journal of Linear Algebra and Applications*, 428:1833–1853.

[25] Nicoara, R. and White, J. (2014). The defect of a group-type commuting square. *Revue Romaine Math.*, (2). 3, 17, 83

[26] Nicoara, R. and White, J. (2017). Analytic deformations of group commuting squares and complex Hadamard matrices. *Journal of Functional Analysis*, 272(8):3486–3505. 36, 37, 39, 40, 41

[27] Paley, R. (1933). On orthogonal matrices. *Journal of Mathematics and Physics*, 12:311–320. 10, 11, 19

[28] Petrescu, M. (1997). *Existence of continuous families of complex Hadamard matrices of certain prime dimensions*. PhD thesis, UCLA. 16

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

[30] Rudin, W. (2009). *Function Theory in the Unit Ball of* $\mathbb{C}^n$. Classics in Mathematics. Springer Science & Business Media. 30

[31] Skinner, A., Newell, V., and Sanchez, R. (2009). Unbiased bases (Hadamards) for six-level systems: Four ways from Fourier. *J. Math. Phys.*, 50. 54

[32] Sylvester, J. J. (1867). 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. *Philophical Magazine*, 34:461–475. 10

[33] Szollosi, F. (2011). *Construction, classification and parameterization of complex Hadamard matrices*. PhD thesis, Central European University. 19, 50

[34] Tadej, W. (2006). Permutation equivalence classes of Kronecker products of unitary Fourier matrices. *Linear Algebra and its Applications*, 418:719–736. 13

[35] Tadej, W. and Zyczkowski, K. (2006). A concise guide to complex Hadamard matrices. *Open Syst. Inf. Dyn*, 13:133–177. 53

[36] Tadej, W. and Zyczkowski, K. (2008). Defect of a unitary matrix. *Linear Algebra and its Applications*, 429:447–481. 8

[37] Tao, T. (2003). An uncertainty principle for cyclic groups of prime order. *ArXiv e-prints*. 28

[38] White, J. (2013). *Isolation and Deformation Results for Commuting Squares of Finite Dimensional Matrix Algebras*. PhD thesis, University of Tennessee, Knoxville. 9

Vita

Chase Thomas Worley was born November 10, 1988 at The University of Tennessee Medical Center in Knoxville, Tennessee. His family moved multiple times finally settling in Cumberland, Virginia on his family's commercial farm. He graduated from the Fuqua School in Farmville, Virginia in 2007. He matriculated at Maryville College where he graduated in 2011 with a Bachelor of Arts degree in mathematics. While attending Maryville, he was a member of the Fighting Scots Football program. He was named to the Academic All-Conference team 2008-2011 and was named to the All-Sportsmanship Team in the Fall of 2010. Immediately after graduation in 2011, Chase attended the University of Tennessee in Knoxville for graduate school. In December 2014, Chase completed a Master of Science in Mathematics. After completion of his doctoral degree, he will begin teaching mathematics at Maryville College.