Association Schemes, Codes, and Difference Sets

Thesis by

Carlos H. Salazar-Lazaro

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

2007

(Defended December 5, 2006)

To my mother Margarita, my stepdad Russell, and my sisters Nelly, Kelly, and Johanna.

Acknowledgments

I cannot thank enough my advisor Professor Richard Wilson for his guidance and support throughout my years as a graduate student. I am grateful for his suggestions on the different topics that I have pursued while working on my thesis. I am even more grateful for his patience and kindness.

I thank Cheng-Yeaw Ku, Dinakar Ramakrishnan, and David Wales, the other members of my committee, for their time and patience. I also thank the graduate students who have listened, who have helped me with technical questions, and who have provided invaluable friendships. Specifically, I would like to thank Daniel Katz, Kimball Martin, Jay Bartroff, David Whitehouse, Chris Lee, David Grynkiewicz, Jennifer Johnson, Matthew Gealy, Antonio Hernandez, Rupert Venzke, and many others.

I thank the Caltech mathematics department for supporting me through graduate school. I also thank the math department staff for their invaluable assistance. Specifically, I thank Elizabeth Woods, Kathy Carreon, Stacey Croomes, Cherry Galvez, and Seraj Muhammed. I give my special gratitude to Pamela Fong and Sara Mena for being good friends and colleagues. I thank the postdocs whom I befriended, and who helped me in one way or another. Specifically, I thank Vladimir Baranovsky, Cheng-Yeaw Ku, Peter Keevash, Ada Chan, Monica Varizani, Eric Wambach, Eric Rains, David Damanik, and many others.

I thank the Northrop Grumman Corporation for providing me with financial assistance during my fifth year. I thank my friends, who have given me much encouragement, and who have helped me. Specifically, I thank Vijay Vyas, Jane Nguyen, David Sandler, Curtis Horn, Vu Duong, John Avery, Jason Brighterman, Kevin Lee, and many others.

I thank my family for their much-needed support: Kelly Lazaro, Nelly Lazaro, Johanna Salazar-Lazaro, Margarita Lazaro, and Russell Beebe. Finally, I would like to thank my girlfriend Gina Kuchler Litts for her constant encouragement and support.

Abstract

Adviser: Richard Wilson.

This thesis consists of an introductory chapter and three independent chapters. In the first chapter, we give a brief description of the three independent chapters: abelian n-adic codes; generalized skew hadamard difference sets; and equivariant incidence structures.

In the second chapter, we introduce n-adic codes, a generalization of the Duadic Codes studied by Pless and Rushanan, and we solve the corresponding existence problem. We introduce n-adic groups, canonical pplitters, and Margarita Codes to generalize the "self-dual" codes of Rushanan and Pless, and we solve the corresponding existence problem.

In the third chapter, we consider the generalized skew hadamard difference set (GSHDS) existence problem. We introduce the combinatorial matrices A_{G,G_1}, where $G_1 = (\mathbb{Z}/exp(G)\mathbb{Z})^*$ and G is a group, to reduce the existence problem to an integral equation. Using a special finite-dimensional algebra or Association Scheme, we show $A^2_{G,G_1} = \frac{|G|}{p} I$ for general G. With the aid of A_{G,G_1}, we show some necessary conditions for the existence of a GSHDS D in the group $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^{2\alpha+1}$, we provide a proof of Johnsen's exponent bound, we provide a proof of Xiang's exponent bound, and we show a necessary existence condition for general G.

In the fourth chapter, we study the incidence matrices $W_{t,k}(v)$ of t-subsets of $\{1, \ldots, v\}$ vs. k-subsets of $\{1, \ldots, v\}$. Also, given a group G acting on $\{1, \ldots, v\}$, we define analogous incidence matrices $M_{t,k}$ and $M'_{t,k}$ of k-subsets' orbits vs. t-subsets' orbits. For general G, we show that $M_{t,k}$ and $M'_{t,k}$ have full rank over $\mathbb{Q}$, we give a bound on the exponent of the Smith Group of $M_{t,k}$ and $M'_{t,k}$, and we give a partial answer to the integral preimage problem for $M_{t,k}$ and $M'_{t,k}$. We propose

the Equivariant Sign Conjecture for the matrices $W_{t,k}(v)$ using a special basis of the column module of $W_{t,k}$ consisting of columns of $W_{t,k}$; we verify the Equivariant Sign Conjecture for small cases; and we reduce this conjecture to the case $v = 2k + t$. For the case $G = (\mathbb{Z}/n\mathbb{Z})$, we conjecture that $M'_{t,k}$ has a basis of the column module of $M'_{t,k}$ that consists of columns of $M'_{t,k}$. We prove this conjecture for $(t, k) = (2, 3), (2, 4)$, and we use these results to calculate the Smith Group of $M_{2,4}$, $M'_{2,4}$, $M_{2,3}$, and $M'_{2,3}$ for general n.

Contents

List of Figures

Chapter 1

Introduction

1.1 Abelian n-adic Codes

In [21], Pless and Rushanan introduced a family of cyclic binary codes called the Duadic Codes to generalize the cyclic binary Quadratic Residue Codes. Using the language of primitive idempotents[1] in $\mathbb{F}_q[G]$, where $\mathbb{F}_q$ is the finite field of q elements and G is an abelian group, Duadic Codes were introduced as in definition 1.1.1.

Definition 1.1.1. *Let $\mu \in Aut(G)$, and let $e = \sum_{g\in G} e_g[g]$ be a primitive idempotent in $\mathbb{F}_q[G]$. Define $\mu \cdot \mathrm{e}$ as $\sum_{g\in G} e_g[\sigma(g)]$. Let $e_1 = e$ and $e_2 = \mu \cdot e$. If*

$$e_1 + e_2 \;=\; 1 - \frac{1}{|G|}\sum_{g\in G}[g],$$

then we say that e_1, e_2, μ forms a Duadic Code *and we call μ the* splitting of the code.

Duadic Codes were of special importance since they provided a construction for Finite Projective Planes. This link is sumarized in the following result that is found in [23] in its most general form.

Theorem 1.1.2. *Let C be a duadic code with splitting given by μ_{-1} then the minimum distance for oddlike[2] code words, d_0, satisfies*

$$d_0^2 - d_0 + 1 \geq v.$$

[1] An idempotent is primitive, if for every other idempotent f, $ef = fe = f \neq 0 \Rightarrow e = f$.
[2] A word $w = \sum_{g\in G} c_g[g]$ is oddlike, if $\sum_{g\in G} c_g \neq 0$.

If equality holds then the supports of the minimum-weight oddlike codewords of weight d_0 are the blocks of a projective plane of order $(d_0 - 1)$. Furthermore, d_0 is the minimum distance of C, and the minimum weight codewords are precisely those codewords that are constant on the supports of the blocks of the finite projective plane.

Originally, Duadic Codes were introduced in the cyclic binary case. Since their introduction, there has been various generalizations with respect to:

1. Parity of the characteristic of the field,
2. Number of idempotents used, and
3. The cyclic and noncyclic abelian case.

The following is a history of these generalizations:

1. **The family of Duadics in even characteristic**, by Rushanan in [22]. These are codes in $\mathbb{F}_q[G]$ where G is an arbitrary abelian group, q is even, and 2 idempotents are used in its definition. The existence problem is solved.
2. **The family of Duadics in odd characteristic**, by Smid in [25]. These are codes in $\mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]$ where q is odd and 2 idempotents are used in its definition. The existence problem is solved.
3. **The family of Triadic Codes**, by Pless and Rushanan in [21]. These are codes in $\mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]$ where q is even and 3 idempotents are used in its definition. The existence problem is solved.
4. **The family of Polyadic Codes**, by Brualdi and Pless in [4]. These are codes in $\mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]$ and m idempotents are used in its definition. The existence problem is solved.
5. **The family of m-adic Polyadic Codes**, by Ling and Xing in [18]. These are codes in $\mathbb{F}_q[G]$ where G is a general abelian group, and m idempotents are used in its definition. The existence problem is solved for the "nondegenerate" case.

We will provide for a different generalization of Duadic Codes that will parallel the family of m-adic Polyadic Codes of San Ling, and the Duadic Codes of Rushanan. This will be the family of n-adic codes defined by:

Definition 1.1.3. *Let n be a prime and G be an abelian group. An* n-adic code *is a pair e, μ where e is an idempotent and $\mu \in Aut(G)$ satisfying $Stab_{\langle\mu\rangle}(e) = \{\mu^k | \mu^k \cdot e = e\} = \langle\mu^n\rangle$, under the action of $Aut(G)$ on the primitive idempotents of $\mathbb{F}_q[G]$, and*

$$\begin{aligned} \langle e_1, \ldots, e_n\rangle &= \mathbb{F}_q[G], \\ \langle e_1\rangle \cap \langle e_2\rangle \cap \cdots \cap \langle e_n\rangle &= \langle d_{g_0}\rangle \\ &= \langle \frac{1}{|G|}\sum_{g\in G}[g]\rangle, \end{aligned}$$

where $e_i = \mu^{i-1} \cdot e$.

Remark: The term n-adic, introduced in definition 1.1.3, is not related to p-adic numbers.

We will solve the existence problem for n-adic codes as it is given by the next theorem.

Theorem 1.1.4. *Let n be a prime, then the following are true:*

1. *There is an n-adic code in $\mathbb{F}_q[G]$ if and only if there is an n-adic code in $\mathbb{F}_q[S]$ for every sylow subgroup S of G.*
2. *There are no n-adic codes in $\mathbb{F}_q[G]$ when G is an n-group.*
3. *Let G be an s-group where $(s, n) = 1$. Let $t_s(k) = |\mu_k|$ in $Aut(\mathbb{Z}/s\mathbb{Z})$. Then,*
   (a) *Let s be an odd prime and assume n divides $\frac{s-1}{t_q(s)}$, then there is an n-adic code in $\mathbb{F}_q[G]$.*
   (b) *Let s be an odd prime, assume n does not divide $\frac{s-1}{t_q(s)}$, and $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times (\mathbb{Z}/s^2\mathbb{Z})^{\pi_2} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$. Then,*
      i. *If $s = 1$ modulo n there is an n-adic code in $\mathbb{F}_q[G]$ if and only if $\pi_i = 0$ modulo n for all i.*

ii. If $s \neq 1$ modulo n there is an n-adic code in $\mathbb{F}_q[G]$ if and only if $t_s(n)$ divides π_i for all i.

(c) Let $s = 2$ be such that $(2, n) = 1$. Let $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times (\mathbb{Z}/s^2\mathbb{Z})^{\pi_2} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$. There is an n-adic code in $\mathbb{F}_q[G]$ if and only if $t_n(2)$ divides π_i for all i.

We will continue our study of n-adic codes by providing conditions under which n-adic codes become Triadic Codes, Polyadic Codes, and m-adic Polyadic Codes. This will put the concept of n-adic codes into perspective with the current generalizations of duadic codes.

We will also provide a generalization of proposition 1.1.2, given as proposition 1.1.5 below, by introducing the concept of n-adic groups for which there will always be a canonical splitter of order n, and by calling the analogous "self-dual" codes Margarita codes.

Theorem 1.1.5. *Let e, μ_l give a Margarita code in $\mathbb{F}_q[G]$ where G is an n-adic group and μ_l a canonical splitter of order n. Let d_0 be the minimum weight of all oddlike vectors of $\langle e \rangle$. Let $w \in \langle e \rangle$ be an oddlike vector of weight d_0. Let $w = \sum_{g \in B} \beta_g[g]$ where $B \subset G$ is the support of w. Let $\widetilde{B} = \sum_{g \in B}[g]$ be the characteristic function of the support of w. Define $r_{n,\mu_l,G} : G \to \mathbb{Z}$ as,*

$$r_{n,\mu_l,G}(g) \;=\; |H_g \cap (B \times \ldots \times B)|,$$

where

$$H_g \;=\; \{(g_1, \ldots, g_n) \in G \times \cdots \times G | g_1 + \mu_l(g_2) + \cdots + \mu_{l^{n-1}}(g_n) = g\}.$$

Then,

1. *The constant d_0 satisfies $d_0^n - r_{n,\mu_l,G}(1) + 1 \geq |G|$,*
2. *If $d_0^n - r_{n,\mu_l,G}(1) + 1 = |G|$, then:*
   (a) The oddlike word satisfies $w = \alpha * \widetilde{B}$ for some $\alpha \in \mathbb{F}_q$,

(b) The characteristic function of the support of w satisfies,

$$\widetilde{B} * (\mu_l \cdot \widetilde{B}) * \cdots * (\mu_l^{n-1} \cdot \widetilde{B}) \;=\; (r_{n,\mu_l,G}(1) - 1)[1] + \sum_{g \in G} [g].$$

3. The constant $r_{n,\mu_l,G}(1)$ satisfies $r_{n,\mu_l,G}(1) = d_0$ modulo n.

1.2 Generalized Skew Hadamard Difference Sets

We will assume that the reader is familiar with the theory of Difference Sets as it can be found in Jungnickel's book in [12], and in Lander's book in [17]. Also, we will assume that G is an abelian group, and we will use the additive notation for its group operation.

Skew Hadamard Difference Sets (SHDS) are subsets D of an abelian group G such that in the group algebra $\mathbb{Z}[G]$:

$$\begin{aligned} D(x)D(x^{-1}) &= (k - \lambda)[0] + \lambda G(x), \\ D(x) + D(x^{-1}) &= G(x) - 1. \end{aligned}$$

The following is what is known about the existence problem for SHDSs. This can be found in Chen, Sehgal, and Xiang's paper in [6].

Theorem 1.2.1. *A SHDS has parameters $(v, k, \lambda) = (v, \frac{v-1}{2}, \frac{v-3}{4})$. Also, if $D \subset G$ is a SHDS, and G is abelian, then:*

1. The order of the group v has the form $v = p^{2\alpha+1}$, where $p = 3$ mod 4,

2. If χ is any nonprincipal character, then:

$$\chi(D) \;=\; \frac{-1 + \epsilon_\chi \sqrt{-v}}{2},$$

where $\epsilon_\chi \in \{+1, -1\}$,

3. *If* $G = \mathbb{Z}/p^{a_1}\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_r}\mathbb{Z}$ *where:* $a_1 \geq a_2 \geq \cdots \geq a_r$ *and* $a_1 \geq 2$, *then:*

   (a) *The exponents* a_1 *and* a_2 *are the same, i.e. ,* $a_1 = a_2$,

   (b) *The exponents* $a_i s$ *satisfy,*

$$a_1 \leq \frac{a_1 + \cdots + a_r + 1}{4}.$$

   This is Xiang's exponent bound.

We introduce the concept of a Generalized Skew Hadamard Difference Set (GSHDS), given by:

Definition 1.2.2. *A* generalized skew hadamard difference set *(GSHDS) is an element of the group algebra* $D(x) \in \mathbb{Z}[G]$ *such that:*

$$\begin{aligned} D(x)D(x^{n_o}) &= (k_o - \lambda)[1] + \lambda G(x), \\ D(x) + D(x^{n_o}) &= G(x) - [1], \end{aligned}$$

where $[1] = x^0$ *is the multiplicative unit of* $\mathbb{Z}[G]$, $k_o = |D(x) \cap D(x^{-n_o})|$, *and* n_o *is a Non-Quadratic Residue of* $(\mathbb{Z}/exp(G)\mathbb{Z})^*$.

In our study of GSHDSs, we introduce the concept of Quadratic Residue Slices (QRS) defined by:

Definition 1.2.3. *Let* G *be an abelian p-group, and* $G_1 = (\mathbb{Z}/exp(G)\mathbb{Z})^*$ *be the numerical multipliers of* G. *Let* $\Omega_{g_1}, \ldots, \Omega_{g_r}$ *be the distinct orbits of the action of* G_1 *on* $\widetilde{G} = G \backslash \{0\}$. *A* Quadratic Residue Slice *(QRS) is any formal sum of the form:*

$$\sum_{i=1}^{r} \epsilon_{\Omega_{g_i}} \Omega_{g_i},$$

where $\epsilon_{\Omega_{g_i}} \in \{\pm 1\}$.

Using the language of QRSs, we extend the existence conjecture of SHDS to GSHDS.

Conjecture 1.2.4. *If G is an abelian group that affords a GSHDS, then G is elementary abelian.*

We prove the analog of proposition 1.2.1 for GSHDS using a unified framework in the language of Quadratic Residue Slices (QRS).

We introduce a combinatorial matrix A_{G,G_1} that is well defined in any abelian p-group and depends on the choice of a set of representatives of the action of G_1 on $G\backslash\{0\}$.

Definition 1.2.5. *Let G be an abelian p-group with exponent p^{a_1}. Let $\theta : G \to \widehat{G}$ be an noncanonical isomorphism such that $\theta(g)(g') = \theta(g')(g)$. Let Ω_g be an orbit of $G_1 = (\mathbb{Z}/exp(G)\mathbb{Z})^*$ on $\widetilde{G} = G\backslash\{0\}$ and Ω_χ an orbit of $G_1 = (\mathbb{Z}/exp(G)\mathbb{Z})^*$ on $\widetilde{\widehat{G}} = \widehat{G}\backslash\{\chi_0\}$. Then, $\mathrm{A_{G,G_1}}$ is defined on the set of orbits of G_1 on $\widetilde{G}$ versus the set of orbits of G_1 on $\widetilde{\widehat{G}}$ using θ by:*

$$A_{G,G_1}(\Omega_{\theta(g')}, \Omega_g) \;=\; \begin{cases} (\frac{n}{p})o(p\cdot g) & \text{if } \theta(g')(g) = \eta_p^n, \\ 0 & \text{else,} \end{cases}$$

where $(\frac{n}{p})$ is the quadratic residue symbol, $o(g)$ is the order of g in the group G, χ_0 is the principal character, η_p is a fixed primitive pth root of unity, and $p \cdot g = p \cdot g = g + g + \cdots + g$ is g added to itself p times.

Using the matrix A_{G,G_1}, we introduce the concept of difference coefficients as:

Definition 1.2.6. *Let d be the vector representation of a QRS $D \subset G$, i.e., a vector of ± 1. The* difference coefficients of D *are given by the vector $A_{G,G_1}d$.*

We show the following properties of A_{G,G_1}:

Theorem 1.2.7. *The following hold:*

1. *The incidence matrix A_{G,G_1} satisfies,*

$$A_{G,G_1}^2 \;=\; \frac{|G|}{p} I_{r,r},$$

where $I_{r,r}$ is the identity matrix.

2. *There is a GSHDS D in G if and only if there is a vector d of ± 1s such that $A_{G,G_1} d = \sqrt{\frac{|G|}{p}} \bar{d}$ for some integral vector $\bar{d}$.*

We proceed to study difference coefficients, and we show integral formulas involving them. In our study of difference coefficients, we prove Xiang's exponent bound for GSHDS, and we introduce the concept of difference intersection numbers.

Definition 1.2.8. *Let D be a QRS in G, and let $L \subset G$ be a subgroup with $\frac{G}{L} = \{g_1' L, \ldots, g_s' L\}$. The* difference intersection numbers of D with respect to L in G *are defined as:*

$$\nu_{G,L}(D, g_i') \quad = \quad |D \cap g_i' L| - |D^{(n_0)} \cap g_i' L|.$$

Using part 1 of theorem 1.2.7 and the structure of Galois Rings, we find necessary conditions for the existence of a GSHDS in the family of groups $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^{2\alpha+1}$. We achieve this by first using the multiplicative structure of the Galois Ring $GR(p^2, \alpha)$ to deduce a "Canonical Form" for A_{H,H_1}, where $H = (\mathbb{Z}/p^2\mathbb{Z})^{2\alpha}$. Using the "Canonical Form" of A_{H,H_1}, we deduce the following existence conditions:

Theorem 1.2.9. *Let $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^3$, and $D \subset G$ a GSHDS. Let $H = \{0\} \times (\mathbb{Z}/p^2\mathbb{Z})^3 \subset G$ and $L = p \cdot H \simeq (\mathbb{Z}/p\mathbb{Z})^3$. Let $D' = H \cap D$, and $D'' = L \cap D$. Let,*

1. *The vector of ± 1s representing D' be d'.*

2. *Decompose d' by $d' = (d_0'^T, d_1'^T, \ldots, d_{p^2}'^T)$ where d_i' is a $(p^2 + p + 1) \times 1$ vector of ± 1s representing disjoint H_1 classes of D'.*

3. *The vector of difference coefficients of the H_1 classes of d_i' be $\widetilde{d_i}'$.*

Then, there is a ordering of the H_1 classes of H and a set of H_1-orbit representatives such that:

1. *The set D'' is a GSHDS in L.*

2. *The image of* d_0 *under* A_{L,L_1} *has form* $A_{L,L_1}d_0 = p\bar{d_0}$ *where* $\bar{d_0}$ *is a* $p^2+p+1\times 1$ *vector of* ± 1*s. Define* $\bar{d_0}$ *the "dual" of* D''.

3. *The image of* $\widetilde{d_0}$ *under* A_{L,L_1} *has form* $A_{L,L_1}\widetilde{d_0} = p\bar{\widetilde{d}}_0$*, for some integral* $\bar{\widetilde{d}}_0$.

4. *The vector* $\bar{\widetilde{d}}_0$ *of the previous part satisfies* $\bar{\widetilde{d}}_0 = \sum_{i=1}^{p^2} d_i$.

5. *The vector of* ± 1*s of part 2 satifies* $p\bar{d_0} = \sum_{i=1}^{p^2} \widetilde{d}_i$.

Theorem 1.2.10. *Let* D *be a GSHDS in* $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^{2\beta+1}$*, and let* $K = (\mathbb{Z}/p\mathbb{Z})^{2\beta}$*. Then, there are elements* $A, B \in \mathbb{Z}[K]$ *that depend on* D*, and there is an element* $L_0 \in \mathbb{Z}[K]$ *that depends on the structure of* G *such that:*

1. *The elements* A *and* B *satisfy* $p^{2\beta}A = \chi_0(A)K(x) + L_0 * B^{(-1)}$*, where* χ_0 *is the principal character of* K.

2. *The elements* A *and* B *satisfy* $p^{2\beta}B = \chi_0(B)K(x) + pL_0 * A^{(-1)}$*, where* χ_0 *is the principal character of* K.

3. *All the coefficients of* A *are odd, and* $\chi_0(A)$ *is odd.*

4. *All the coefficients of* B *are odd, and* $\chi_0(B)$ *is odd.*

5. *The principal character of* A *has value* $\chi_0(A) = p^{\beta-1}\epsilon_0 b_0$*; where* ϵ_0 *is* ± 1*, and* b_0 *is an odd integer.*

6. *The principal character of* B *has value* $\chi_0(B) = p^{\beta}\epsilon_0 a_0$*; where* ϵ_0 *is* ± 1 *and equal to the* ϵ_0 *of part 5, and* a_0 *is an odd integer.*

We close the chapter with a proof of Johnsen's exponent bound using the matrix A_{G,G_1}, and with a necessary existence condition between the Difference Coefficients and the difference intersection numbers of a GSHDS D in a general abelian p-group G.

1.3 Equivariant Incidence Structures

We consider the incidence matrices $W_{t,k}$ defined on the t-subsets vs. k-subsets of $\{1, \ldots, v\}$ by:

$$W_{t,k}(e_T, e_K) = \begin{cases} 1 & \text{if } T \subset K, \\ 0 & \text{else.} \end{cases}$$

The following problems concerning the matrices $W_{t,k}$ have been solved in the literature:

1. What is the rank of $W_{t,k}$? When is $W_{t,k}$ onto? When is $W_{t,k}$ injective?
2. How can the kernel of $W_{t,k}$ be characterized? Do we know a canonical basis for the kernel?
3. Does $W_{t,k}$ allow for a column $\mathbb{Z}$-basis? That is, is there a subset of the columns of $W_{t,k}$ that is a basis for the column space of $W_{t,k}$ over $\mathbb{Z}$? This is the concept of a (t, k)-basis.
4. What is the Smith Normal Form of $W_{t,k}$?
5. What is a left inverse of $W_{t,k}$ when $W_{t,k}$ is injective?
6. What is a right inverse of $W_{t,k}$ when $W_{t,k}$ is surjective?
7. When does an integral vector have an integral preimage under $W_{t,k}$?

Questions 1, 5, and 6 have been answered by Kramer in [13, 14, 15]. Questions 3, 4, and 7 have been answered by Wilson in [26]. Question 2 has been answered by Ajoodani-Namini and Khosrovshahi in [1], and by Bier in [3].

We consider these questions when there is an action of a group G. That is, we ask the same questions for $M_{t,k} = (W_{t,k})_0$, and for $M'_{t,k} = ((W^T_{t,k})_0)^T$; where $M_{t,k}$ is defined by

$$M_{t,k}(e_{\Omega_T}, e_{\Omega_K}) = |\{K' \in \Omega_K | T \subset K'\}|,$$

and $M'_{t,k}$ is defined by

$$M'_{t,k}(e_{\Omega_T}, e_{\Omega_K}) \;=\; |\{T' \in \Omega_T | T' \subset K\}|,$$

where Ω_T is an orbit of G on the t-subsets, and Ω_K is an orbit of G on the k-subsets.

1.3.1 General G

For general G:

1. We show $M_{t,k}$ and $M'_{t,k}$ have full rank.
2. We provide a partial answer to the integral preimage problem of $M_{t,k}$ for arbitrary G.
3. We provide some bounds on the exponent of the Smith Group of $M_{t,k}$ and $M'_{t,k}$ for arbitrary G.
4. We provide a left inverse of $M_{t,k}$ when $M_{t,k}$ is injective.
5. We provide a right inverse of $M_{t,k}$ when $M_{t,k}$ is surjective.
6. We provide a left inverse of $M'_{t,k}$ when $M'_{t,k}$ is injective.
7. We provide a right inverse of $M'_{t,k}$ when $M'_{t,k}$ is surjective.
8. We solve for the Smith Group of $M'_{t,k}$ provided that for $t < k$:
   (a) The matrix $M'_{t,t+1}(n)$ affords a $(t, t+1)$-basis.
   (b) A vector z has an integral preimage under $M'_{t,t+1}$ if and only if $\binom{t+1-i}{t-i}$ divides $M'_{i,t}z$ for $i = 1, \ldots, t$.

1.3.2 Case G = Stab(Ω)

We propose the following property of $L_{t,k} = W_{t,k}, M_{t,k}, M'_{t,k}$ that we call "trivial positive equivariant signing."

Definition 1.3.1. *Let β be a (t,k)-basis of $L'_{t,k}$. We say that ϵ is a* trivial positive equivariant signing for $(L_{t,k},\beta)$, *if for every $K' \in_{\sim} \beta$,*

$$L_{t,k}e_{K'} \;=\; \sum_{K\in\beta} C(K',K)\epsilon(K)L_{t,k}e_K,$$

we have $\epsilon \in \{-1,0,1\}$ and $C(K',K) \geq 0$.

*We say the signing ϵ is G-*invariant*, where $G \subset S_v$, whenever $\epsilon(\sigma \cdot K) = \epsilon(K)$ for all $\sigma \in G$ and $K \in \beta_{t,k}$.*

We consider the action of the group $G = Stab(\Omega)$, where Ω is a partition of $\{1,\ldots,v\}$. By introducing the concepts of: monotone families, compatible sets, equivariant compatible sets, and inclusion maps; we give reduction criteria to show for a given G-invariant family $\beta_{t,k}$ of columns of $W_{t,k}(v)$:

1. When $\beta_{t,k}$ is a (t,k)-basis of $W_{t,k}(v)$.
2. When the set of G-orbits in β, i.e., $\beta^G_{t,k}$, is a (t,k)-basis for $M'_{t,k}$.
3. When the set $\beta_{t,k}$ admits a trivial positive equivariant signing for $W_{t,k}$ that is G-invariant.
4. When the set $\beta^G_{t,k}$ admits a trivial positive equivariant signing for $M'_{t,k}$.

We show the Bier-Frankl (B-F) basis and the Khosorovshahi-Ajoodani (KAj) basis allow a stabilizer group G of the form $Stab(\Omega_{t,k})$ where

$$\begin{aligned}\Omega_{t,k} \;&=\; \{1,\ldots,v-k-t\} \cup \{v-k-t+1, v-k-t+2\} \cup \cdots \\ &\quad \cup \{v-k+t-1, v-k+t\} \cup \{v-k+t+1,\ldots,v\},\end{aligned}$$

for the KAj basis, and

$$\begin{aligned}\Omega_{t,k} \;&=\; \{v,\ldots,k+t+1\} \cup \{k+t, k+t-1\} \cup \cdots \\ &\quad \cup \{k-t+2, k-t+1\} \cup \{k-t,\ldots,1\},\end{aligned}$$

for the B-F basis. We also show that these bases are equivalent.

Using the reduction results, we prove that these bases admit a trivial positive equivariant signing that is G-invariant for the cases: $(1,2),(2,3)$, by providing a proof; $(3,4),(5,6)$, via a computer program. We also show:

Proposition 1.3.2. *Let $\beta_{t,k}$ be the KAj (t,k)-basis or the B-F (t,k)-basis, then: $\beta_{t,k}(v)$ admits a trivial positive equivariant signing that is $G = Stab(\Omega_{t,k}(v))$-invariant for all $v \geq k+t+1$ if and only if $\beta_{t,k}(v)$ admits a trivially positive equivariant signing that is $G = Stab(\Omega_{t,k}(2k+t))$-invariant for $v = 2k+t$.*

We propose the following conjecture that we call the "Equivariant Sign Conjecture."

Conjecture 1.3.3. *Let $\beta_{t,k}$ be the KAj (t,k)-basis or the B-F (t,k)-basis, then $\beta_{t,k}$ admits a trivial positive equivariant signing that is $G = Stab(\Omega_{t,k})$-invariant.*

1.3.3 Case $\mathbf{G = (Z/nZ)}$

For the group $G = (\mathbb{Z}/n\mathbb{Z})$:

1. We solve the integral preimage problem for $M_{t,k}$ when $G = \mathbb{Z}/n\mathbb{Z}$ and n is a prime.

2. We calculate the Smith Group of $M'_{2,3}$ and of $M_{2,3}$ for arbitrary n by solving for a $(2,3)$-basis.

3. We calculate the Smith Group of $M'_{2,4}$ and of $M_{2,4}$ for arbitrary n by solving for a $(2,4)$-basis.

4. We give some partial results for a generating set of the column space of $M'_{3,4}$.

We also propose the following conjectures that we call the "(t,k)-basis Conjectures."

Conjecture 1.3.4. (Weak version) *Let $\gcd(tk,n) = 1$, and let $t < k \leq n-k$. Then, $M'_{t,k}$ admits a (t,k)-basis.*

Conjecture 1.3.5. (Strong version) *Let $t < k \leq n - k$. Then, $M'_{t,k}$ admits a (t, k)-basis.*

We close the chapter by showing how the (t, k)-basis conjectures can be used to calculate the Smith Group of $M'_{t,k}$.

Proposition 1.3.6. *Let $\gcd(n, (2(k-1))!) = 1$, and $1 \leq t < k \leq n - k \leq n - t$. Assume the (t, k)-basis conjecture holds for n, and for all $(i-1, i)$ where $i = 1, \ldots, k$. Then, $M'_{t,k}(n)$ has Smith Group given by:*

$$(\mathbb{Z}/\binom{k}{t}\mathbb{Z}) \times (\mathbb{Z}/\binom{k-2}{t-2}\mathbb{Z})^{r_2(n)-1} \times (\mathbb{Z}/\binom{k-3}{t-3}\mathbb{Z})^{r_3(n)-r_2(n)} \times \cdots \times (\mathbb{Z}/\binom{k-(t-1)}{t-(t-1)}\mathbb{Z})^{r_{t-1}(n)-r_{t-2}(n)},$$

where $r_i(n) = \frac{\binom{n}{i}}{n}$ is the number of orbits on the i-subsets for $i = 2, \ldots, t$.

Chapter 2

Abelian n-adic Codes

2.1 Preliminaries

We will consider abelian group codes that are given by ideals in $\mathbb{F}_q[G]$ and are also known as G-codes. We will assume that $(q, |G|) = 1$, where q is a prime power, and that G is abelian. This will make $\mathbb{F}_q[G]$ a semisimple algebra and all ideals in $\mathbb{F}_q[G]$ principal (generated by idempotents, unique up to units).

We will assume the natural action of $Aut(G)$ on the idempotents e of G defined for any $\sigma \in Aut(G)$ as:

$$\mu \cdot e \;\; = \;\; \sum_{g \in G} e_g[\sigma(g)],$$

where $e = \sum_{g \in G} e_g[g]$.

We will also assume the natural action of $Aut(G)$ on $\widehat{G}$ defined for any $\sigma \in Aut(G)$ and $\chi \in \widehat{G}$ as $\sigma \cdot \chi = \chi \circ \sigma^{-1}$.

As $\mathbb{F}_q[G]$ is semisimple, every G-invariant subspace I_1 splits. That is, there is a G-invariant subspace I_2 such that $\mathbb{F}_q[G] = I_1 \oplus I_2$. In particular, if $I_1 = \langle e \rangle$, then $I_2 = \langle 1 - e \rangle$ and $\mathbb{F}_q[G] = \langle e \rangle \oplus \langle 1 - e \rangle$. Hence, $\mathbb{F}_q[G] = \langle e_1 \rangle \oplus \cdots \oplus \langle e_r \rangle$; where $\langle e_i \rangle$ are ideals that cannot be written as the sum of 2 proper ideals, i.e., irreducible. The idempotents $e_1, \ldots, e_r$ are called primitive idempotents. We note that it can be shown that any idempotent of $\mathbb{F}_q[G]$ is the sum of some irreducible idempotents, that is, $e = e_{i_1} + \cdots + e_{i_k}$.

By considering a splitting field for G, i.e., $\mathbb{F}_{q^r}$ where $\mathbb{F}_{q^r}^*$ has all $exp(G)$th roots of unity, one can show that in $\mathbb{F}_{q^r}[G] \supseteq \mathbb{F}_q[G]$ there are $|G|$ irreducible idempotents given by the irreducible characters of G into $\mathbb{F}_{q^r}^*$; where the idempotent corresponding to the character χ is given by:

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi(g^{-1})[g].$$

One can show that the Galois group of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ is generated by the Frobenious Map $x \mapsto x^q$. We will denote the Frobenious Map by σ_q. We note that, one can show that if $\chi(g)$ is an irreducible character, then $\sigma_q(\chi(g))$ is another irreducible character. Thus, σ_q induces an action on the irreducible characters of G.

The following is a well-known result in Character Theory, and it can be found in Isaacs' book in [10], chapter 9.

Theorem 2.1.1. *Let e be the an irreducible idempotent in $\mathbb{F}_q[G]$, let $\mathbb{F}_{q^r}$ be a splitting field of G. Then, in $\mathbb{F}_{q^r}[G]$, $e = e_{\chi_1} + \cdots + e_{\chi_l}$ where $\chi_1, \ldots, \chi_l$ forms an orbit of σ_q acting on the irreducible characters of G.*

By using theorem 2.1.1, we will proceed to calculate the irreducible idempotents of $\mathbb{F}_q[G]$ by introducing the concept of cyclotomic cosets.

Note that $\sigma_q(\chi(g)) = (\chi(g))^q = \chi^q(g)$. Hence, in $\widehat{G}$, σ_q acts like raising to the qth power. This map $g \mapsto g^q$, a numerical multiplier, is clearly in $Aut(\widehat{G})$ as $(q, |G|) = 1$.

By using any noncanonical isomorphism $\eta : G \mapsto \widehat{G}$, where $\widehat{G}$ is the group of characters, we can identify any $\chi = \chi_g \in \widehat{G}$ with a $\eta(g)$. By using this identification, we can identify the orbit of $\chi = \chi_{g_1}$ under σ_q in $\widehat{G}$ with the orbit of g_1 under μ_q in G.

Thus, by theorem 2.1.1, if e is an irreducible idempotent in $\mathbb{F}_q[G]$, then there is some orbit of μ_q acting on G, say C_{g_o}, such that

$$e = \sum_{g \in C_{g_o}} e_{\chi_g},$$

where the above equation is taken in $\mathbb{F}_{q^r}[G]$. The orbits of μ_q on G are called the qth

cyclotomic cosets of G.

We will call the irreducible idempotent $d_{g_0} = \sum_{g' \in C_1} e_{\chi^1} = \frac{1}{|G|} \sum_{g \in G} [g]$ which corresponds to the trivial cyclotomic coset $C_1 = \{1\}$ the trivial irreducible idempotent, clearly a primitive idempotent in $\mathbb{F}_q[G]$.

It can be shown that if $X = \{C_{g_o}, \ldots, C_{g_r}\}$ are all the distinct μ_q orbits of G, then X forms an Association Scheme. That is, if in $\mathbb{Z}[G]$ we let $C'_{g_i} = \sum_{g \in C_{g_i}} g$, then there are $p^k_{i,j} \in \mathbb{Z}$ such that:

$$C'_{g_i} * C'_{g_j} = \sum_{k=0}^{r} p^k_{i,j} C'_{g_k}.$$

Thus, the algebra generated by $X' = \{C'_{g_o}, \ldots, C'_{g_r}\}$ in $\mathbb{F}_q[G]$ is finite dimensional of dimension $r+1$. One can show that this subalgebra is also semisimple and has as idempotents the primitive idempotents of $\mathbb{F}_q[G]$. In particular, this shows that primitive idempotents, and for that matter any idempotent, are constant on the qth cyclotomic cosets of G. However, there is an easy way of seeing this. Let e be an idempotent, then:

$$\begin{aligned} e &= e^q \\ &= (\sum_{g \in G} c_g [g])^q \\ &= \sum_{g \in G} (c_g)^q [g^q] \\ &= \sum_{g \in G} c_g [g^q] \\ &= \mu_q \cdot e, \end{aligned}$$

which says that μ_q is a multiplier of e. Thus, the coefficients of e are μ_q invariant; that is, they are constant on the qth cyclotomic classes. Note also that $Aut(G)$ induces an action on the primitive idempotents of $\mathbb{F}_q[G]$. We can show this by considering a primitive idempotent $d_{g_i} = \sum_{g \in C_{g_i}} e_{\chi_g}$ of $\mathbb{F}_q[G] \subseteq \mathbb{F}_{q^r}[G]$, where $\mathbb{F}_{q^r}$ is a splitting field for G. Consider:

$$\begin{aligned}\mu \cdot d_{g_i} &= (\sum_{g \in C_{g_i}} \mu \cdot e_{\chi_g}) \\ &= \sum_{g \in C_{g_i}} (\mu \cdot e_{\chi_g}),\end{aligned}$$

where, $e_{\chi_g} = \frac{1}{|G|} \sum_{g' \in G} \chi_g((g')^{-1})[g']$. Thus,

$$\begin{aligned}\mu \cdot e_{\chi_g} &= \frac{1}{|G|} \sum_{g' \in G} \chi_g((g')^{-1})[\mu(g')] \\ &= \frac{1}{|G|} \sum_{g' \in G} \chi_g((\mu^{-1}(g'))^{-1})[g'] \\ &= \frac{1}{|G|} \sum_{g' \in G} \chi_g(\mu^{-1}((g')^{-1}))[g'] \\ &= \frac{1}{|G|} \sum_{g' \in G} (\mu \cdot \chi_g)((g')^{-1})[g'].\end{aligned}$$

Define $\mu^*(\chi)(g') = (\mu \cdot \chi)(g')$. Note that $\mu^*(\chi)$ is again an irreducible character since $\mu \in Aut(G)$. One can show that μ^* is an automorphism of the group of irreducible characters, i.e., $\mu^* \in Aut(\widehat{G})$, and that the map $\mu \rightarrow \mu^*$ is an anti-isomorphism from $Aut(G)$ to $Aut(\widehat{G})$.

Clearly, $\mu \cdot e_{\chi_g} = e_{\mu^*(\chi_g)}$, and

$$\begin{aligned}\mu \cdot d_{g_i} &= \sum_{g \in C_{g_i}} e_{\mu^*(\chi_g)} \\ &= \sum_{g \in \mu^*(C_{g_i})} e_{\chi_g},\end{aligned}$$

where $\mu^*(C_{g_i})$ is defined in the following way: since $\mu^* \in Aut(\widehat{G})$, and $\{\chi_g | g \in C_{g_i}\}$ form a cyclotomic coset in $\widehat{G}$, $\mu^*(C_{g_i})$ denotes the cyclotomic coset in G corresponding to the cyclotomic coset $\{\mu^*(\chi_g) | g \in C_{g_i}\}$ in $\widehat{G}$.

We can be more precise on the definition of $\mu^*(C_{g_i})$ by using the isomorphism

$\eta : G \to \widehat{G}$. Define $\bar{\mu} : G \to G$ such that $\mu^*(\chi_g) = \chi_{\bar{\mu}(g)}$.[1] More precisely, $\bar{\mu}$ is defined such that $\mu^*(\eta(g)) = \eta(\bar{\mu}(g))$. Hence, $\bar{\mu}(g) = \eta^{-1}(\mu^*(\eta(g)))$. Clearly, $\mu^*(C_{g_i})$ is $\bar{\mu}(C_{g_i}) = C_{\bar{\mu}(g_i)}$ by definition, therefore, $\mu \cdot d_{g_i} = d_{\bar{\mu}(g_i)}$.

Thus, $\mu \cdot d_{g_i} = d_{\bar{\mu}(g_i)}$ is a primitive idempotent and this shows that μ acts on the primitive idempotents the same way $\bar{\mu}$ acts on the cyclotomic cosets. One can show that the map $\mu \to \bar{\mu}$ is an isomorphism of $Aut(G)$ of order two. So, given $\sigma \in Aut(G)$, there is a unique $\tau \in Aut(G)$ such that $\sigma = \bar{\tau}$. Also, the action of μ on the primitive idempotents is the same as the action of $\bar{\mu}$ on the cyclotomic cosets via the correspondence established by η.

We will define $X = \{d_{g_0}, d_{g_1}, \ldots, d_{g_r}\}$ as the set of all the primitive idempotents of $\mathbb{F}_q[G]$. Also, for given $Y \subset X$, we will define $e_Y = \sum_{d_g \in Y} d_g$ as the idempotent of $\mathbb{F}_q[G]$ that corresponds to Y. We note that the previous definition is exhaustive. That is, given an idempotent e of $\mathbb{F}_q[G]$ there is $Y \subset X$ such that $e = e_Y$.

Using the previous notation, one can show:

$$\begin{aligned} e_X &= 1, \\ e_\emptyset &= 0, \\ e_{X_1} * e_{X_2} &= e_{X_1 \cap X_2}, \qquad (2.1) \\ \langle e_{X_1}, e_{X_2} \rangle &= \langle e_{X_1 \cup X_2} \rangle, \qquad (2.2) \\ \mu \cdot e_{X_1} &= e_{\mu(X_1)}, \qquad (2.3) \end{aligned}$$

where $X_1 \subset X$, $X_2 \subset X$, and $\mu(X_1) = \{\mu \cdot d_g = d_{\bar{\mu}(g)} \mid d_g \in X_1\}$.

2.2 Abelian n-adic Codes

Definition 2.2.1. *We will assume that n is a prime. An n-*adic code *is a pair e, μ where e is an idempotent and $\mu \in Aut(G)$ satisfying $Stab_{\langle \mu \rangle}(e) = \{\mu^k | \mu^k \cdot e = e\} =$*

[1] Clearly, $\bar{\mu} \in Aut(G)$.

$\langle \mu^n \rangle$ *and*

$$\begin{aligned} \langle e_1, \ldots, e_n \rangle &= \mathbb{F}_q[G], && (2.4) \\ \langle e_1 \rangle \cap \langle e_2 \rangle \cap \cdots \cap \langle e_n \rangle &= \langle d_{g_0} \rangle && (2.5) \\ &= \langle \frac{1}{|G|} \sum_{g \in G} [g] \rangle, \end{aligned}$$

where $e_i = \mu^{i-1} \cdot e$. *We will call* μ *the splitter of the code.*

Definition 2.2.2. *We will say that an* n*-adic code* μ, e *is* "reduced" *if* $\langle e_i \rangle \cap \langle e_j \rangle = d_{g_0}$ *for all* i, j.

Examples of n-adic codes are given by the Q-codes of Rushanan in [22], which are n-adic codes where $n = 2$.

The main objective of this section is to solve the existence problem for abelian n-adic codes in $\mathbb{F}_q[G]$. This is is summarized by theorem 2.2.3.

Theorem 2.2.3. *The following are true:*

1. *There is an* n*-adic code in* $\mathbb{F}_q[G]$ *if and only if there is an* n*-adic code in* $\mathbb{F}_q[S]$ *for every sylow subgroup* S *of* G.

2. *There are no* n*-adic codes in* $\mathbb{F}_q[G]$ *when* G *is an* n*-group,*

3. *Let* G *be an* s*-group where* $(s, n) = 1$. *Let* $t_s(k) = |\mu_k|$ *in* $Aut(\mathbb{Z}/s\mathbb{Z})$. *Then,*

   (a) *Let* s *be an odd prime. Assume* n *divides* $\frac{s-1}{t_q(s)}$, *then there is an* n*-adic code in* $\mathbb{F}_q[G]$.

   (b) *Let* s *be an odd prime. Assume* n *does not divide* $\frac{s-1}{t_q(s)}$, *and* $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times (\mathbb{Z}/s^2\mathbb{Z})^{\pi_2} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$. *Then,*

      i. *If* $s = 1$ *modulo* n *there is an* n*-adic code in* $\mathbb{F}_q[G]$ *if and only if* $\pi_i = 0$ *modulo* n *for all* i.

      ii. *If* $s \neq 1$ *modulo* n *there is an* n*-adic code in* $\mathbb{F}_q[G]$ *if and only if* $t_s(n)$ *divides* π_i *for all* i.

(c) *Let $s = 2$ be such that $(2, n) = 1$. Let $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times (\mathbb{Z}/s^2\mathbb{Z})^{\pi_2} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$. There is an n-adic code in $\mathbb{F}_q[G]$ if and only if $t_n(2)$ divides π_i for all i.*

We proceed to show existence conditions for n-adic codes. The next subsections will take care of the individual cases of theorem 2.2.3.

2.2.1 Existence Criteria

We will show criteria for existence of n-adic codes that will be used in the proof of theorem 2.2.3.

A direct consequence of the n-adic code definition is that the order of the splitter $|\mu|$ in $Aut(G)$ is divisible by n. We can show this by contradiction. If $|\mu| = n * n' + l$ where $l \in \{1, \ldots, n-1\}$, then

$$\begin{aligned} e &= \mu^{|\mu|} \cdot e \\ &= \mu^{n*n'+l} \cdot e \\ &= \mu^{l} \cdot e, \end{aligned}$$

which contradicts the choice of n as the smallest power of μ such that $\mu^k \cdot e = e$.

Using equations (2.1) and (2.3), and the n-adic code definition, we can force set conditions. Let $e = e_Y$ for some $Y \subset X$ where e, μ give an n-adic code, then $e_i = \mu^{i-1} \cdot e = e_{\mu^{i-1}(Y)}$. Equations (2.1), (2.3), and (2.5) give the following:

$$\begin{aligned} d_{g_0} &= e_1 * \cdots * e_n \\ &= e_Y * e_{\mu(Y)} * \cdots * e_{\mu^{n-1}(Y)} \\ &= e_{Y \cap \mu(Y) \cap \cdots \cap \mu^{n-1}(Y)}. \end{aligned}$$

Thus,

$$Y \cap \mu(Y) \cap \cdots \cap \mu^{n-1}(Y) = \{d_{g_0}\}. \tag{2.6}$$

Similarly, equations (2.2) and (2.4) give:

$$Y \cup \mu(Y) \cup \cdots \cup \mu^{n-1}(Y) \;=\; X. \tag{2.7}$$

We can use the previous set conditions to deduce properties of the splitter μ.

Corollary 2.2.4. *Let, e, μ give an n-adic code in $\mathbb{F}_q[G]$, then:*

1. *If there is a primitive idempotent d such that $d * \mu = d$ then $d = d_{g_0} = \frac{1}{|G|}\sum_{g\in G}[g]$.*
2. *If there is a cyclotomic coset such that $\bar{\mu}(C_g) = C_g$ then $C_g = \{1\}$.*

Proof. Both conclusions are equivalent, as the action of μ on the primitive idempotents is the same as the action of $\bar{\mu}$ on the cyclotomic cosets and d_{g_0} corresponds to $C_1 = \{1\}$. Only the first statement will be shown.

Let d be a primitive idempotent; then Equation (2.7) says that $d \in \mu^k(Y)$ for some k. That is, $d = \mu^k \cdot d'$ for some $d' \in Y$. Suppose $\mu \cdot d = d$. Note that $\mu^{k+l} \cdot d' = \mu^l \cdot (\mu^k \cdot d') = \mu^l \cdot d = d$ which shows that $d \in \mu^{k+l}(Y)$ for all l. That is, $d \in \mu^l(Y)$ for all l. Equation (2.6) forces $d = d_{g_0}$. □

We define $m_q(G)$ as the number of cyclotomic q cosets of $\widetilde{G} = G\backslash\{1\}$.

Theorem 2.2.5. *Let e, μ give an n-adic code in $\mathbb{F}_q[G]$ then:*

1. *The orbits of the action of $\bar{\mu}$ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n.*
2. *The number of cyclotomic q-cosets of $\widetilde{G}$ is divisible by n. That is, $m_q(G) = 0$ modulo n.*

Proof. Clearly, part 2 is a consequence of part 1. Let e, μ give an n-adic code in $\mathbb{F}_q[G]$. Let Ω be an orbit of $\bar{\mu}$ on the cyclotomic cosets of $\widetilde{G}$. Let $|\mu| = n^l * n_1$ where $(n, n_1) = 1$.[2] Note that $\mu' = \mu^{n_1}$ has order n^l. Clearly, $\bar{(.)}$ is an isomorphism of

[2]This is possible since n is prime.

$Aut(G)$, and $|\bar{\mu'}| = |\mu'| = n^l$. Since $|\bar{\mu'}| = n^l$, all orbits of μ' on Ω have size a power of n.

It suffices to show that μ' has no fixed points in Ω because then all orbits of μ' on Ω have size n^l", where $l \geq 1$; that is, their length is divisible by n. Hence, Ω must have size divisible by n.

Suppose μ' has a fixed point in Ω, that is $\bar{\mu'}(C_g) = C_g$. We will show that e, μ' gives another n-adic code. Clearly, $(n, n_1) = 1$ implies

$$\{0, 1, \ldots, n-1\} \quad = \quad \{0, n_1, 2 * n_1, \ldots, (n-1) * n_1\},$$

where the above equation is modulo n. Therefore,

$$\{e, \mu \cdot e, \ldots, \mu^{n-1} \cdot e\} \quad = \quad \{e, \mu^{n_1} \cdot e, \ldots, \mu^{n_1 * (n-1)} \cdot e\}. \tag{2.8}$$

By using an arithmetic argument, we can show that n is the smallest power of μ' such that $(\mu')^n \cdot e = e$. Therefore,

$$Stab_{\langle \mu' \rangle}(e) \quad = \quad \langle (\mu')^n \rangle.$$

Equation (2.8) shows that

$$\begin{aligned} \mathbb{F}_q[G] &= \langle e, \mu \cdot e, \ldots, \mu^{n-1} \cdot e \rangle \\ &= \langle e, \mu' \cdot e, \ldots, (\mu')^{n-1} \cdot e \rangle, \\ \langle d_{g_0} \rangle &= \langle e \rangle \cap \langle \mu \cdot e \rangle \cap \cdots \cap \langle \mu^{n-1} \cdot e \rangle \\ &= \langle e \rangle \cap \langle \mu' \cdot e \rangle \cap \cdots \cap \langle (\mu')^{n-1} \cdot e \rangle. \end{aligned}$$

Hence, e, μ' gives an n-adic code.

By corollary 2.2.4, $C_g = C_1 = \{1\}$; however, this contradicts our choice of Ω which is made of cyclotomic cosets of $\widetilde{G}$ and $1 \notin \widetilde{G}$. □

Theorem 2.2.6. *There is an n-adic code in $\mathbb{F}_q[G]$ if and only if there is $\sigma \in Aut(G)$ such that the orbits of σ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n.*

Proof. Suppose there is an n-adic code in $\mathbb{F}_q[G]$ given by e, μ. By the proof of theorem 2.2.5, $\sigma = \bar{\mu'}$ has order n^l and the orbits of σ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n.

Conversely, let σ be such that the orbits of σ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n. Let $\Omega_1, \ldots, \Omega_N$ be the orbits of σ on the cyclotomic cosets of $\widetilde{G}$. Let $\Omega_i = \{C_{g_{j_{i,1}}}, \ldots, C_{g_{j_{i,N_i}}}\}$ where N_i is divisible by n and $\sigma(C_{g_{j_{i,k}}}) = C_{g_{j_{i,k+1}}}$ where k is taken modulo N_i. Let

$$\Omega_{j,k} \quad = \quad \{C_{j,k}, C_{j,k+n}, \ldots, C_{j,k+l*n}, \ldots, C_{j,k+(\frac{N_j}{n}-1)*n}\}$$

where $k + l * n$ is taken modulo N_j and $k \in \{1, \ldots, n\}$. Note that $\sigma(\Omega_{j,k}) = \Omega_{j,k+1}$ by construction, where k is taken modulo n.

Let $d_{g_i} = \sum_{g \in C_{g_i}} e_{\chi_g}$ be the primitive idempotent corresponding to the cyclotomic coset C_{g_i}. Choose $\mu \in Aut(G)$ such that $\bar{\mu} = \sigma$. Define $d_{j,k} = \sum_{C_g \in \Omega_{j,k}} d_g$. Since the action of μ on the primitive idempotents is the same as the action of σ on the cyclotomic cosets, and $\sigma(\Omega_{j,k}) = \Omega_{j,k+1}$, we have $\mu \cdot d_{j,k} = d_{j,k+1}$. Define $e_k = d_{g_0} + d_{1,k} + d_{2,k}, + \cdots + d_{N,k}$, then $\mu \cdot e_k = e_{k+1}$ and all $\{e_1, \ldots, e_n\}$ are distinct by construction.

Note that $d_{j,k} * d_{j',k'} = 0$, unless $j = j'$ and $k = k'$. Also, $d_{j,k} * d_{g_0} = 0$. Hence, $e_1 * e_2 * \cdots * e_n = d_{g_0}$.

Also note that $e_1 + \cdots + e_n - (n-1)e_1 * \cdots * e_n = 1$. Thus, $\langle e_1, \ldots, e_n \rangle = \langle 1 \rangle = \mathbb{F}_q[G]$, and $\langle e_1 \rangle \cap \cdots \cap \langle e_n \rangle = \langle d_{g_0} \rangle$; therefore, e_1, μ gives an n-adic code.

We observe that the constructed n-adic code e_1, μ is also "reduced." □

As a corollary, we deduce that the "reduced" condition does not modify the solution to the existence problem for n-adic codes.

Corollary 2.2.7. *$\mathbb{F}_q[G]$ allows an n-adic code if and only if $\mathbb{F}_q[G]$ allows a "reduced" n-adic code.*

Proof. ($\Rightarrow$). Let there be an n-adic code in $\mathbb{F}_q[G]$; then by theorem 2.2.6, there is $\sigma \in Aut(G)$ such that the orbits of σ on the cyclotomic cosets of $\widetilde{G}$ have length

divisible by n. Applying theorem 2.2.6, once again, we can construct an n-adic code in $\mathbb{F}_q[G]$ that is reduced.

($\Leftarrow$) This is clear. □

Theorem 2.2.8. *There is an n-adic code in $\mathbb{F}_q[G]$ if and only if there is $\sigma \in Aut(G)$ such that $|\sigma| = n^l$ and σ fixes no cyclotomic coset of $\widetilde{G}$.*

Proof. Suppose there is an n-adic code in $\mathbb{F}_q[G]$ given by e, μ. Then by the proof of theorem 2.2.5, $\sigma = \bar{\mu'}$ has order n^l and σ fixes no cyclotomic coset of $\widetilde{G}$.

Conversely, suppose $\sigma \in Aut(G)$ such that $|\sigma| = n^l$ and σ fixes no cyclotomic coset of $\widetilde{G}$. Then, the orbits of σ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n. Using the same construction of the second part of the proof of theorem 2.2.6, one can construct an n-adic code in $\mathbb{F}_q[G]$. □

For the next sections, $t_{k'}(k) = |\mu_k|$ in $Aut((\mathbb{Z}/k'\mathbb{Z}))$, will denote the multiplicative order of k modulo k'.

Corollary 2.2.9. *Let $G = (\mathbb{Z}/s\mathbb{Z}) \times \cdots \times (\mathbb{Z}/s\mathbb{Z}) \simeq (\mathbb{Z}/s\mathbb{Z})^r$. If there is an n-adic code in $\mathbb{F}_q[G]$, then $m_q(G) = \frac{s^r-1}{t_s(q)} = 0$ modulo n.*

Proof. By theorem 2.2.5, it suffices to show that $m_q(G) = \frac{s^r-1}{t_s(q)}$. This will be done by using the fundamental counting principle.

Define $N_i = |\{g \in \widetilde{G} | \mu_{q^i}(g) = \mu_q^i(g) = g\}|$. Let $t = t_s(q)$, then

$$m_q(G) \;=\; \frac{1}{t}\sum_{i=0}^{t-1} N_i.$$

Clearly, $N_0 = s^r - 1$. Note that $N_i = 0$ for $i \in \{1, \ldots, t-1\}$; because, if $\mu_{q^i}(g) = g$ then $(q^i - 1) * g = 0$ in G. Thus $q^i - 1 = 0$ modulo $|g| = s$. This contradicts the choice of i. Thus, no g exists such that $\mu_{q^i}(g) = g$. Therefore,

$$m_q(G) \;=\; \frac{1}{t}\{(s^r - 1) + 0 + \cdots + 0\}.$$

□

Theorem 2.2.10. *If there is an n-adic code in $\mathbb{F}_q[K]$ and in $\mathbb{F}_q[L]$ then there is an n-adic code in $\mathbb{F}_q[K \times L]$.*

Proof. By theorem 2.2.8, it suffices to show that there is $\gamma \in Aut(K \times L)$ of order $|\gamma| = n^l$, and γ fixes no cyclotomic coset of $\widetilde{K \times L}$. By theorem 2.2.8, there are $\sigma \in Aut(K)$ and $\tau \in Aut(L)$ of orders $|\sigma| = n^{l_1}$ and $|\tau| = n^{l_2}$, where σ fixes no cyclotomic coset of $\widetilde{K}$ and τ fixes no cyclotomic coset of $\widetilde{L}$. Consider $\gamma(k,l) = (\sigma(k), \tau(l))$. Clearly, $|\gamma| = lcm(|\sigma|, |\tau|) = lcm(n^{l_1}, n^{l_2}) = n^l$. Let $C_{(k,l)}$ denote the cyclotomic coset of $K \times L$ containing (k,l). Now, suppose $\gamma(C_{(k,l)}) = C_{(k,l)}$ where $C_{(k,l)}$ is a cyclotomic coset of $\widetilde{K \times L}$; then, $(\sigma(k), \tau(l)) = \gamma(k,l) = \mu_q^i(k,l) = \mu_{q^i}(k,l) = (\mu_{q^i}(k), \mu_{q^i}(l))$. Thus, $\sigma(k) = \mu_{q^i}(k)$ and $\tau(l) = \mu_{q^i}(l)$. Therefore, $\sigma(C_k) = C_k$ and $\tau(C_l) = C_l$. By the choice of σ and τ, $C_k = C_1$ and $C_l = C_1$. Thus, $C_{(k,l)} = C_{(1,1)}$ and this contradicts the choice of $C_{(k,l)}$ since $C_{(1,1)}$ is not a cyclotomic coset of $\widetilde{K \times L}$. Therefore, γ fixes no cyclotomic coset of $\widetilde{K \times L}$. □

Theorem 2.2.11. *Let e, μ give an n-adic code in $\mathbb{F}_q[G]$. Suppose $K \subset G$ is a subgroup such that $\mu(K) = K$. Then, there is an n-adic code in $\mathbb{F}_q[K]$ and $\mathbb{F}_q[G/K]$.*

Proof. By theorem 2.2.5, the orbits of $\sigma = \bar{\mu}$ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n. Consider the restriction of σ to K. Since $\mu(K) = K$, it can be shown that $\bar{\mu}(K) = K$. Thus, $\sigma \in Aut(K)$. Since $\sigma(K) = K$, the orbit of a cyclotomic coset C_k of K is made up of cyclotomic cosets of K. By assumption of σ, all orbits of σ on the cyclotomic cosets of $\widetilde{K}$ have length divisible by n. By theorem 2.2.6, there is an n-adic code in $\mathbb{F}_q[K]$.

To show the other result, consider the epimorphism $\rho : G \to G/K$ which can be extended to an algebra epimorphism $\rho : \mathbb{F}_q[G] \to \mathbb{F}_q[G/K]$. As $\mu(K) = K$, μ factors through K to give $\phi \in Aut(G/K)$ defined by $\phi(gK) = \mu(g)K$. Note that ϕ has the property $\rho(\mu \cdot e) = \phi \cdot \rho(e)$. Consider the pair $e' = \rho(e), \phi$; it will be shown that they give an n-adic code in $\mathbb{F}_q[G/K]$. As ρ is an epimorphisms of algebras, $e' = \rho(e)$ is

clearly an idempotent. Since $\rho(\mu^i \cdot e) = \phi^i \cdot \rho(e)$,

$$\begin{aligned}\mathbb{F}_q[G/K] &= \langle 1 \rangle \\ &= \langle \rho(e), \rho(\mu \cdot e), \ldots, \rho(\mu^{n-1} \cdot e) \rangle \\ &= \langle e', \phi \cdot e', \ldots, \phi^{n-1} \cdot e' \rangle.\end{aligned}$$

Also, note that:

$$\begin{aligned}e' * (\phi \cdot e') * \cdots * (\phi^{n-1} \cdot e') &= \rho(e) * (\rho(\mu \cdot e)) * \cdots * (\rho(\mu^{n-1} \cdot e)) \\ &= \rho(e * (\mu \cdot e) * \cdots * (\mu^{n-1} \cdot e)) \\ &= \rho(d_{g_0}) \\ &= d_{g_0}.\end{aligned}$$

Thus, $\langle e' \rangle \cap \langle \phi \cdot e' \rangle \cap \cdots \cap \langle \phi^{n-1} \cdot e' \rangle = \langle d_{g_0} \rangle$.

It suffices to show that the smallest power of ϕ that fixes e' is n. Clearly, $\mu^n \cdot e = e$, since $\phi^n \cdot e' = \phi^n \cdot \rho(e) = \rho(\mu^n \cdot e) = \rho(e) = e'$. Suppose that there is $1 \leq k \leq n-1$ such that $\phi^k \cdot e' = e'$. Note that, since n is prime, $(k, n) = 1$; thus by choosing k' such that $k * k' = n * n_1 + 1$, we have that $e' = \phi^{k*k'} \cdot e' = \phi^{n*n_1+1} \cdot e' = \phi \cdot e'$. In particular $\langle e' \rangle = \langle e', \phi \cdot e', \ldots, \phi^{n-1} \cdot e' \rangle = \langle 1 \rangle = \mathbb{F}_q[G/K]$. By uniqueness of idempotents generating ideals in $\mathbb{F}_q[G/K]$, we have that $e' = 1$ in $\mathbb{F}_q[G/K]$. Thus, $\rho(e) = 1$ in $\mathbb{F}_q[G/K]$ which forces e to be an idempotent of $\mathbb{F}_q[K]$ alone. Note that since $\mu(K) = K$, $\{e, \mu \cdot e, \ldots, \mu^{n-1} \cdot e\}$ are idempotents of $\mathbb{F}_q[K]$. Thus $\mathbb{F}_q[G] = \langle e, \mu \cdot e, \ldots, \mu^{n-1} \cdot e \rangle$ is a subideal of $\mathbb{F}_q[K]$. This is a contradiction; therefore, $\phi \cdot e'$ cannot equal e'. Thus, no such k exists. Therefore, n is the smallest power of ϕ that fixes e'. □

Theorem 2.2.11 can be applied to any characteristic subgroup. In particular, it can be applied to the sylow subgroups of G, since these are characteristic as G is abelian. Thus, theorems 2.2.10 and 2.2.11 yield the following corollary.

Corollary 2.2.12. *There is an n-adic code in $\mathbb{F}_q[G]$ if and only if there is an n-adic code in $\mathbb{F}_q[S]$ for every sylow subgroup S of G.*

And also,

Corollary 2.2.13. *Let s be a prime and let $(s,q)=1$. If there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s^r\mathbb{Z}]$, then there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s\mathbb{Z}]$.*

Proof. Let $G_{(1)} = \langle s \rangle \subset (\mathbb{Z}/s^r\mathbb{Z})$. Clearly, $G_{(1)}$ is a characteristic subgroup of $\mathbb{Z}/s^r\mathbb{Z}$. By applying theorem 2.2.10 to $L = (\mathbb{Z}/s^r\mathbb{Z})/G_{(1)} \simeq \mathbb{Z}/s\mathbb{Z}$, the conclusion follows. □

Corollary 2.2.12 reduces the existence problem to s-groups, where s is a prime. We will see that the existence problem in s-groups has different answers depending on s.

2.2.2 Existence in n-groups

For this section, we will let $G = (\mathbb{Z}/n\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/n^r\mathbb{Z})^{\pi_r}$ be an n-group. We will show that there are no n-adic codes in $\mathbb{F}_q[G]$.

Lemma 2.2.14. *If $G = (\mathbb{Z}/n\mathbb{Z})^{\pi_1}$, then there are no n-adic codes in $\mathbb{F}_q[G]$.*

Proof. By corollary 2.2.9, $m_q(G) = \frac{n^{\pi_1}-1}{t_n(q)} = 0$ modulo n. Note that modulo n we have:

$$\begin{aligned} \frac{n^{\pi_1}-1}{t_n(q)} &= \frac{n-1}{t_n(q)}\{1+n+\cdots+n^{\pi_1-1}\} \\ &= \frac{n-1}{t_n(q)} \\ &\neq 0. \end{aligned}$$

This is a contradiction. Thus, there cannot be an n-adic code in $\mathbb{F}_q[G]$. □

Theorem 2.2.15. *Let $G = (\mathbb{Z}/n\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/n^r\mathbb{Z})^{\pi_r}$ be an abelian n-group, then there are no n-adic codes in $\mathbb{F}_q[G]$.*

Proof. Define $G_{(i)} = \{g \in G \mid |g| \text{ divides } n^i\}$. Clearly, $G_{(i)}$ is a characteristic subgroup of G. Suppose there is an n-adic code in $\mathbb{F}_q[G]$. Consider $L = G/G_{(r-1)} \simeq (\mathbb{Z}/n\mathbb{Z})^{\pi_r}$. By theorem 2.2.11, there is an n-adic code in $\mathbb{F}_q[L]$. This contradicts lemma 2.2.14. □

2.2.3 Existence in s-groups with $(\mathbf{s}, \mathbf{n}) = \mathbf{1}$

The existence problem depends on the value of s modulo n and on the parity of s modulo 2. The parity of s modulo 2 is important, since $(\mathbb{Z}/s^r\mathbb{Z})^*$ is not cyclic when $s = 2$, whereas it is when s is an odd prime. Because of this, the proofs have to be modified. We note that by the previous section, we can assume that $s \neq n$.

2.2.3.1 Existence in s-groups, $(\mathbf{s}, \mathbf{2}) = \mathbf{1}$

First, we will consider $G = \mathbb{Z}/s\mathbb{Z}$. Let $t = t_s(q)$.

Theorem 2.2.16. *There is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s\mathbb{Z}]$ if and only if $\frac{s-1}{t} = m_q(\mathbb{Z}/s\mathbb{Z}) = 0$ modulo n.*

Proof. Suppose there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s\mathbb{Z}]$, then by theorem 2.2.5 we have $m_q(\mathbb{Z}/s\mathbb{Z}) = 0$ modulo n. Note that by corollary 2.2.9 we have $\frac{s-1}{t} = m_q(\mathbb{Z}/s\mathbb{Z})$.

Conversely, suppose $N = \frac{s-1}{t} = n * n_1$ is divisible by n. Let $\{C_{g_1}, \ldots, C_{g_N}\}$ be all the cyclotomic cosets of $\widetilde{G}$. By theorem 2.2.6, it suffices to find $\sigma \in Aut(G)$ such that the orbits of σ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n. It will be shown that $\sigma = \mu_l$, where $Aut(\mathbb{Z}/s\mathbb{Z}) = (\mathbb{Z}/s\mathbb{Z})^* = \langle \mu_l \rangle$ will do the job.

Consider, $H = \frac{\langle \mu_l \rangle}{\langle \mu_q \rangle} = \frac{(\mathbb{Z}/s\mathbb{Z})^*}{\langle q \rangle} = \frac{\langle l \rangle}{\langle q \rangle}$. Note that every coset of H is a cyclotomic coset. This can be seen by considering,[3]

$$\begin{aligned} C_g &= \{[g], [g * q], \ldots, [g * q^{t-1}]\} \\ &= \mu_g(\{[1], [q], \ldots, [q^{t-1}]\}) \\ &= \mu_g(\langle \mu_q \rangle). \end{aligned}$$

Since H is cyclic and generated by μ_l, this shows that μ_l acts transitively on the cosets of H. Thus, μ_l acts transitively on the cyclotomic cosets of $\widetilde{G}$. Therefore, the action of μ_l on the cyclotomic cosets of $\widetilde{G}$ is one orbit of length N. Since $N = 0$ modulo n, the conclusion follows. □

Now, we consider $G = \mathbb{Z}/s^r\mathbb{Z}$.

[3]We remind the reader that in $G = \mathbb{Z}/s\mathbb{Z}$, $1 = [0]$ since G is written additively and $1 \neq [1]$.

Theorem 2.2.17. *There is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s^r\mathbb{Z}]$ if and only if there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s\mathbb{Z}]$.*

Proof. Suppose there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s^r\mathbb{Z}]$, then by corollary 2.2.13 there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s\mathbb{Z}]$.

Conversely, suppose there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s\mathbb{Z}]$. Let $G = \mathbb{Z}/s^r\mathbb{Z}$. Since $s \neq 2$, $Aut(G) = \langle \mu_l \rangle$ is cyclic. Following the same construction as in the proof of theorem 2.2.16, we will show that the action of μ_l on the cyclotomic cosets of $\widetilde{G}$ has orbits of length divisible by n.

Define $S_i = \{g \in \widetilde{G} \mid g = s^{r-i} * g_1, (g_1, s) = 1\}$. Clearly, S_i is a characteristic subset of G. Thus, S_i is the union of cyclotomic cosets of $\widetilde{G}$. Also, $\widetilde{G} = S_1 \cup \cdots \cup S_r$.

Define N_i to be the number of cyclotomic cosets of S_i. First, we will calculate $N_i = \frac{s^{i-1}(s-1)}{t_{s^i}(q)}$. Second, we will show that μ_l acts transitively on the cyclotomic cosets of S_i and that N_i is divisible by n if and only if N_1 is divisible by n. By theorem 2.2.16, $N_1 = \frac{s-1}{t_s(q)}$ is divisible by n. Hence, this will show that the action of μ_l on the cyclotomic cosets $\widetilde{G}$ is made up of r orbits, each orbit of length N_i where all N_is are divisible by n. By theorem 2.2.6, the conclusion will follow.

Let $Aut(\mathbb{Z}_{s^i}) = (\mathbb{Z}/s^i\mathbb{Z})^*$ be the units of the ring $\mathbb{Z}/s^i\mathbb{Z}$. Define $H_i = \frac{(\mathbb{Z}/s^i\mathbb{Z})^*}{\langle \mu_q \rangle}$ and $K_i = (\mathbb{Z}/s^i\mathbb{Z})^*$. Consider C_g a cyclotomic coset of S_i. Then, $g = s^{r-i} * g_1$, where $(g_1, s) = 1$. Note that we think of g_1 as a unit in $\mathbb{Z}/s^i\mathbb{Z}$. Consider,

$$\begin{aligned} C_g &= \{[s^{r-i} * g_1], [s^{r-i} * g_1 * q], \ldots, [s^{r-i} * g_1 * q^{t_{s^i}(q)-1}]\} \\ &= \mu_{s^{r-i}}(\mu_{g_1}(\{[1], [q], \ldots, [q^{t_{s^i}(q)-1}]\})) \\ &= \mu_{s^{r-i}}(\mu_{g_1}\langle \mu_q \rangle). \end{aligned}$$

The above implies that C_g is the image under $\mu_{s^{r-i}}$ of a coset of H_i. This shows that the number of cyclotomic cosets of S_i is the order of H_i. The order of H_i can be

calculated directly as:

$$\begin{aligned} |H_i| &= \frac{|(\mathbb{Z}/s^i\mathbb{Z})^*|}{|\langle \mu_q \rangle|} \\ &= \frac{s^{i-1}(s-1)}{t_{s^i}(q)}. \end{aligned}$$

Since μ_l generates $(\mathbb{Z}/s^r\mathbb{Z})^*$, it also generates $(\mathbb{Z}/s^i\mathbb{Z})^*$ for every $1 \leq i \leq r$.[4] Thus, μ_l acts transitively on the cosets of H_i and therefore on the cyclotomic cosets of S_i.

Now we show that $|H_i|$ is divisible by n if and only if $|H_1|$ is divisible by n. This will show that N_i is divisible by n if and only if N_1 is divisible by n, and the proof will be finished.

Lemma 2.2.18. *q is an n-adic residue modulo s if and only if q is an n-adic residue modulo s^i for every i.*[5]

Proof. This is a result from Number Theory and can be shown in the following way. Clearly, if q is an n-adic residue modulo s^i, then it is an n-adic residue modulo s. Conversely, suppose q is an n-adic residue modulo s. Consider the equation:

$$X^n - q = 0, \tag{2.9}$$

in the s-adic numbers $\mathbb{Q}_s$, where s is a prime. Since q is an n-adic residue modulo s, Equation (2.9) has a solution in the residue field $\mathbb{Z}_s/(s\mathbb{Z}_s) = \mathbb{F}_s$ of $\mathbb{Q}_s$.[6] Note that $f(x) = x^n - q$ has no double roots in $\mathbb{F}_s$ as $f'(x) = n * x^{n-1}$ and $(f(x), f'(x)) = 1$ in $\mathbb{F}_s[x]$. Thus, $f(x) = (x - x_o)g(x)$, where $x_o \in \mathbb{F}_s$; and $g(x) \in \mathbb{F}_s[x]$, where $(g(x), x - x_o) = 1$ in $\mathbb{F}_s[x]$. By Hensel's lemma, this factorization can be lifted to a factorization in $\mathbb{Z}_s[x]$. That is, there is $X_o \in \mathbb{Z}_s$ and $h(x) \in \mathbb{Z}_s[x]$ such that: $f(x) = (x - X_0)h(x)$, $x - X_o = x - x_o \bmod s\mathbb{Z}_s[x]$; where, $h(x) = g(x) \bmod s\mathbb{Z}_s[x]$. Thus, $X^n = q$ has a solution in the s-adic integers, namely X_o. Through the canonical projection from $\mathbb{Z}_s \to \mathbb{Z}_s/(s^i\mathbb{Z}_s) = \mathbb{Z}/s^i\mathbb{Z}$, we find a solution of $X^n = q$ in $\mathbb{Z}/s^i\mathbb{Z}$.

[4] μ_l when viewed as an element of $(\mathbb{Z}/s^i\mathbb{Z})^*$ is basically μ_{l_o} where $l = l_o$ modulo s^i $(1 \leq l_o \leq s^i - 1)$.
[5] q is an n-adic residue modulo s^i if and only if there is $x \in \mathbb{Z}/s^i\mathbb{Z}$ such that $x^n = q \bmod s^i$.
[6] Here, $\mathbb{Z}_s$ denotes the s-adic integers.

Thus, q is an n-adic residue modulo s^i. □

Let $K_i = (\mathbb{Z}/s^i\mathbb{Z})^*$. Suppose that $|H_i| = \frac{s^{i-1}(s-1)}{t_{s^i}(q)}$ is divisible by n. Note that, since $(s,n) = 1$ and n divides $|H_i| = \frac{s^{i-1}(s-1)}{t_{s^i}(q)}$, we have that n divides $\frac{s-1}{t_{s^i}(q)}$. In particular, n divides $s-1$; therefore, n divides $|K_j| = s^{j-1}(s-1)$ for all j.

Since K_j is cyclic and n divides $|K_j|$, we have that $\frac{K_j}{K_j^n} = \mathbb{Z}/n\mathbb{Z}$, where $K_j^n = \{g \in K_j \mid x^n = g, \text{for some } x \in K_j\}$.[7] Therefore, we have the following lemma.

Lemma 2.2.19. *If n divides $|H_i|$ for some i, then n divides $|K_j|$ for all j and $\frac{K_i}{K_i^n} = \mathbb{Z}/n\mathbb{Z}$.*

Now we are ready to prove our final claim.

Lemma 2.2.20. *The order of H_i is divisible by n if and only if the order of H_1 is divisible by n.*

Proof. Suppose $|H_i|$ is divisible by n. By lemma 2.2.19, n divides $|K_j|$ and $\frac{K_j}{K_j^n} = \mathbb{Z}/n\mathbb{Z}$ for all j.

Since K_i is cyclic, we can apply the following claim to K_i that we include without proof.

Claim 2.2.21. *Suppose H, K are subgroups of a cyclic group G. If $|H|$ divides $|K|$ then $H \subset K$.*

Consider,

$$\begin{aligned} |\langle \mu_q \rangle| * |H_i| &= |K_i| \\ &= \left|\frac{K_i}{K_i^n}\right| * |K_i^n| \\ &= n * |K_i^n|. \end{aligned}$$

Since n divides $|H_i|$, this forces $|\langle \mu_q \rangle|$ to divide $|K_i^n|$. By claim 2.2.21, we have that $\langle \mu_q \rangle \subset K_i^n$. In particular, q is an n-adic residue modulo s^i.

[7] In general, if G is cyclic of order m, then $G/G^n = \mathbb{Z}/(n,m)\mathbb{Z}$.

By lemma 2.2.18, q is an n-adic residue modulo s. Thus $\mu_q \in K_1^n$. Consider:

$$\begin{aligned} |H_1| &= \left|\frac{K_1}{\langle \mu_q \rangle}\right| \\ &= \left|\frac{K_1}{K_1^n}\right| * \left|\frac{K_1^n}{\langle \mu_q \rangle}\right| \\ &= n * \left|\frac{K_1^n}{\langle \mu_q \rangle}\right|. \end{aligned}$$

Thus, n divides $|H_1|$.

Conversely, suppose n divides $|H_1|$. By lemma 2.2.19, we have that n divides K_j and $\frac{K_j}{K_j^n} = (\mathbb{Z}/n\mathbb{Z})$ for all j. By considering,

$$\begin{aligned} |\langle \mu_q \rangle| * |H_1| &= |K_1| \\ &= \left|\frac{K_1}{K_1^n}\right| * |K_1^n| \\ &= n * |K_1^n|, \end{aligned}$$

one can conclude that $|\langle \mu_q \rangle|$ divides $|K_1^n|$ since n divides $|H_1|$. Thus, q is an n-adic residue modulo s by claim 2.2.21 about cyclic groups. By lemma 2.2.18, q is an n-adic residue modulo s^i. Using the same argument as above, by considering the equation:

$$\begin{aligned} |H_i| &= \left|\frac{K_i}{\langle \mu_q \rangle}\right| \\ &= \left|\frac{K_i}{K_i^n}\right| * \left|\frac{K_i^n}{\langle \mu_q \rangle}\right| \\ &= n * \left|\frac{K_i^n}{\langle \mu_q \rangle}\right|, \end{aligned}$$

we conclude that n divides H_i. □

□

Now we consider general s-groups. Let $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$. Note that if $m_q(\mathbb{Z}/s\mathbb{Z}) = \frac{s-1}{t_s(q)} = 0$ modulo n, then by theorem 2.2.16 there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s\mathbb{Z}]$. By theorem 2.2.17, there is an n-adic code in $\mathbb{F}_q[\mathbb{Z}/s^r\mathbb{Z}]$, for all r. By theorem 2.2.10, there is an n-adic code in $\mathbb{F}_q[G]$. Thus we have:

Corollary 2.2.22. *If $m_q(\mathbb{Z}/s\mathbb{Z}) = 0$ modulo n and $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$ is an s-group with $(s,n) = 1$, s odd, then there is an n-adic code in $\mathbb{F}_q[G]$.*

However, what happens when $m_q(\mathbb{Z}/s\mathbb{Z}) \neq 0$ modulo n? This is answered partially by the following theorem.

Theorem 2.2.23. *Suppose $m_q(\mathbb{Z}/s\mathbb{Z}) \neq 0$ modulo n, $(s,n) = 1$, and s an odd prime. If there is an n-adic code in $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$, then either:*

1. *If $s = 1$ modulo n, then $\pi_k = 0$ modulo n for all k,*

2. *If $s \neq 1$ modulo n, then $t_n(s)$ divides π_k for all k.*

Proof. Consider the case $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1}$. Suppose there is an n-adic code in $\mathbb{F}_q[G]$. By theorem 2.2.5, $\frac{s^{\pi_1}-1}{t_s(q)} = m_q(G) = 0$ modulo n. Thus, $\frac{s-1}{t_s(q)}\{1 + s + \cdots + s^{\pi_1-1}\} = \frac{s^{\pi_1}-1}{t_s(q)} = 0$ modulo n. Since $\frac{s-1}{t_s(q)} \neq 0$ modulo n and n is a prime, we can divide by $\frac{s-1}{t_s(q)}$ in the previous equation to get $1 + s + \cdots + s^{\pi_1-1} = 0$ modulo n. Thus, if $s = 1$ modulo n, this implies $\pi_1 = 0$ modulo n. If $s \neq 1$ modulo n, this implies $\frac{s^{\pi_1}-1}{s-1} = 0$ modulo n forcing $s^{\pi_1} = 1$ modulo n. That is, $t_n(s)$ divides π_1.

Now consider the general case $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$, and suppose there is an n-adic code in $\mathbb{F}_q[G]$. Define the following groups:

$$\begin{aligned} G_{(i)} &= \{g \in G \mid |\, |g| \text{ divides } s^i\}, \\ G^{(i)} &= \{s^i * g \mid |g \in G\}. \end{aligned}$$

Clearly, $G_{(i)}, G^{(i)}$ are characteristic subgroups of G. Note that $L = \frac{G}{G_{(n-1)}} \simeq (\mathbb{Z}/s\mathbb{Z})^{\pi_r}$. By theorem 2.2.11, $\mathbb{F}_q[L]$ has an n-adic code. Thus, π_r satisfies one of the conclusions of the previous case.

Suppose that: $\pi_{i+1}, \ldots, \pi_r$ are known to be divisible by n, if $s = 1$ modulo n; or they are known to be divisible by $t_n(s)$, if $s \neq 1$ modulo n. Consider $K = \frac{G}{G_{(i-1)}} = (\mathbb{Z}/s\mathbb{Z})^{\pi_i} \times \cdots \times (\mathbb{Z}/s^{r-i+1}\mathbb{Z})^{\pi_r}$. By theorem 2.2.11, there is an n-adic code in $\mathbb{F}_q[K]$. Consider $H = \frac{K}{K^{(1)}} = (\mathbb{Z}/s\mathbb{Z})^{\pi_i + \cdots + \pi_r}$, by theorem 2.2.11, $\mathbb{F}_q[H]$ has an n-adic code. Thus, $\pi_i + \cdots + \pi_r$ is divisible by n, if $s = 1$ modulo n; or, it is divisible by $t_n(s)$, if

$s \neq 1$ modulo n. Clearly, this forces π_i to be divisible by n, if $s = 1$ modulo n; or, to be divisible by $t_n(s)$, if $s \neq 1$ modulo n.

Inductively, all π_i are divisible by n, if $s = 1$ modulo n; or, they are all divisible by $t_n(s)$, if $s \neq 1$ modulo n. □

The following results are the converse to the above.

Theorem 2.2.24. *Suppose $m_q(\mathbb{Z}/s\mathbb{Z}) \neq 0$ modulo n, $(s, n) = 1$, and s is an odd prime. Let $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$ where π_k is divisible by n for all k, and $s = 1$ modulo n. Then, there is an n-adic code in $\mathbb{F}_q[G]$.*

Proof. It suffices to show that: there is an n-adic code in $\mathbb{F}_q[G]$ where $G = (\mathbb{Z}/s^r\mathbb{Z}) \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z}) = (\mathbb{Z}/s^r\mathbb{Z})^n$, and r is arbitrary. The conclusion will follow by theorem 2.2.10.

So, let $G = (\mathbb{Z}/s^r\mathbb{Z})^n$. Consider $\tau \in Aut(G)$ defined by $\tau(a_1, \ldots, a_n) = (q * a_n, a_1, \ldots, a_{n-1})$. Note that $\tau^n = \mu_q$ in $Aut(G)$. It will be shown that the orbits of τ on the cyclotomic cosets of $\widetilde{G}$ have length n. The result will follow by theorem 2.2.6.

Since $\tau^n = \mu_q$, we have that for any cyclotomic coset $C_{(a_1,\ldots,a_n)}$:

$$\tau^n(C_{(a_1,\ldots,a_n)}) \;=\; C_{(a_1,\ldots,a_n)}.$$

If there is a cyclotomic coset $C_{(a_1,\ldots,a_n)}$ of $\widetilde{G}$ whose orbit under τ has length less than n, then there is $1 \leq k \leq n-1$ such that $\tau^k(C_{(a_1,\ldots,a_n)}) = C_{(a_1,\ldots,a_n)}$. Since n is prime, we can find $1 \leq k_1 \leq n-1$ such that $k * k_1 = 1 + n * n_1$. Thus, $\tau(C_{(a_1,\ldots,a_n)}) = \tau^{n*n_1+1}(C_{(a_1,\ldots,a_n)}) = \tau^{k*k_1}(C_{(a_1,\ldots,a_n)}) = C_{(a_1,\ldots,a_n)}$. Therefore, τ fixes $C_{(a_1,\ldots,a_n)}$. Hence, there is l such that $(q * a_n, a_1, \ldots, a_{n-1}) = \tau(a_1, \ldots, a_n) = \mu_{q^l}(a_1, \ldots, a_n)$. This forces the equations modulo s^r:

$$\begin{aligned} q * a_1 &= q^l * a_n, \\ a_2 &= q^l * a_1, \\ &\vdots \\ a_n &= q^l * a_{n-1}. \end{aligned}$$

From these, we can deduce $a_n = q^{l*n-1} * a_n$ modulo s^r. Note that if $a_n = 0$ modulo s^r, then by the above equations $a_i = 0$ modulo s^r for all i. Thus, we can assume $a_n = s^{r-i} * a'_n$, where $(a'_n, s) = 1$. Hence, we can deduce that $a'_n = q^{l*n-1} * a'_n$ modulo s^i which gives $1 = q^{l*n-1}$ modulo s^i. Thus, $t_{s^i}(q)$ divides $l * n - 1$ which forces $t_{s^i}(q) \neq 0$ modulo n.

However, we will deduce that $t_{s^i}(q) = 0$ modulo n, for all i, from our assumptions. This will show a contradiction and will show that n is the smallest power of τ that fixes $C_{(a_1,\ldots,a_n)}$. Therefore, the conclusion will follow.

Using the notation of the proof of theorem 2.2.17, $|H_1| = |\frac{(\mathbb{Z}/s\mathbb{Z})^*}{\langle \mu_q \rangle}| = \frac{s-1}{t_s(q)} \neq 0$ modulo n. The proof of theorem 2.2.17 shows that $|H_1| \neq 0$ modulo n if and only if $|H_i| \neq 0$ modulo n. Thus $|H_i| = \frac{s^{i-1}(s-1)}{t_{s^i}(q)} \neq 0$ modulo n. Since $s = 1$ modulo n, the following equation modulo n:

$$\begin{aligned} 0 &= s^{i-1}(s-1) \\ &= \frac{s^{i-1}(s-1)}{t_{s^i}(q)} t_{s^i}(q) \\ &= |H_i| t_{s^i}(q), \end{aligned}$$

forces $t_{s^i}(q) = 0$ modulo n.

□

Theorem 2.2.25. *Suppose $m_q(\mathbb{Z}/s\mathbb{Z}) \neq 0$ modulo n, $(s, n) = 1$, and s is an odd prime. Let $G = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z})^{\pi_r}$, where π_k is divisible by $t_n(s)$ for all k and $s \neq 1$ modulo n. Then, there is an n-adic code in $\mathbb{F}_q[G]$.*

Proof. It suffices to show that there is an n-adic code in $\mathbb{F}_q[G]$ where $G = (\mathbb{Z}/s^r\mathbb{Z}) \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z}) = (\mathbb{Z}/s^r\mathbb{Z})^{t_n(s)}$, and r is arbitrary. The conclusion will follow by theorem 2.2.10.

Let $k = t_n(s)$. Consider an unramified extension $K = \mathbb{Q}_s(\beta)$ of $\mathbb{Q}_s$ of degree k.[8] Let O_K be the ring of integers of K. As K is unramified, s is the uniformizer of O_K. By Hensel's Lemma, O_K has all the $(s^k - 1)$th roots of unity. In particular, O_K has an

[8] $\mathbb{Q}_s$ are the s-adic numbers.

nth root of unity, call it $\alpha \in O_K$. Note that $O_K/s^rO_K = (\mathbb{Z}/s^r\mathbb{Z}) \times \cdots \times (\mathbb{Z}/s^r\mathbb{Z}) = G$ as abelian groups under addition. If μ_q is a numerical multiplier of G, then μ_q acting on O_K/s^rO_K is given by $\mu_q(x + s^rO_K) = qx + s^rO_K$. Thus, a q-cyclotomic coset in O_K/s^rO_K is a set of the form $\{x + s^rO_K, qx + s^rO_K, q^2x + s^rO_K, \ldots, q^lx + s^rO_K\}$.

Consider the map $\mu(x + s^rO_K) = \alpha x + s^rO_K$, μ lifts to an automorphism of G. Note that μ has order n as α is an nth root of unity. We claim that μ fixes no cyclotomic coset of $(O_K/s^rO_K)\backslash s^rO_K = \widetilde{G}$. Since μ has prime order, it will follow that all orbits of μ on the cyclotomic cosets of $\widetilde{G}$ have length n. Hence, by theorem 2.2.6, there is an n-adic code in $\mathbb{F}_q[G]$.

Suppose there was $x + s^rO_K$ such that $\mu(x + s^rO_K) = q^lx + s^rO_K$. Then, $\alpha x = q^lx + s^ry$ for some $x, y \in O_K$. As $x + s^rO_K$ is non trivial, the s-valuation of x is $0 \leq v_s(x) \leq r-1$. Thus, $x = s^{v_s(x)}x'$, where x' is a unit. Therefore, $\alpha = q^l + s^{r-v_s(x)}y(x')^{-1}$. Since $1 \leq r - v_s(x)$, we have $\alpha = q^l \bmod sO_K$. Since α maps to a nontrivial nth root of unity in the residue field, we have that $t_s(q)$ does not divide l. However, $1 = \alpha^n = q^{ln} \bmod sO_K$. Thus, $t_s(q)$ divides ln. This forces n to divide $t_s(q)$.

Consider: $s - 1 = t_s(q)\frac{s-1}{t_s(q)} = 0 \bmod n$. This contradicts the assumption that $s \neq 1 \bmod n$. □

2.2.3.2 Existence in 2-groups with $(2, n) = 1$

Theorem 2.2.26. *There are no n-adic codes in $\mathbb{F}_q[\mathbb{Z}/2^r\mathbb{Z}]$.*

Proof. Note that $C = \{2^{r-1}\}$ is fixed by all $\mu \in Aut(\mathbb{Z}/2^r\mathbb{Z})$.[9] In particular, C is a cyclotomic coset of $\widetilde{\mathbb{Z}/2^r\mathbb{Z}}$ that is fixed by all $\mu \in Aut(\mathbb{Z}/2^r\mathbb{Z})$. Thus, for any μ, the orbit of C under μ has length 1. In particular, the length of the orbit of C under μ cannot be divisible by n, where n is an odd prime. This contradicts theorem 2.2.5. □

Theorem 2.2.27. *If there is an n-adic code in $G = (\mathbb{Z}/2\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/2^r\mathbb{Z})^{\pi_r}$, then $t_n(2)$ divides π_k for all k.*

Proof. This proof is similar to the proof of theorem 2.2.23. □

[9] $\mu \in Aut(\mathbb{Z}/2^r\mathbb{Z})$ if and only if $\mu = \mu_l$ where l is odd. That C is fixed by μ_l is a trivial calculation.

Theorem 2.2.28. *Let $G = (\mathbb{Z}/2\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/2^r\mathbb{Z})^{\pi_r}$ where π_k is divisible by $t_n(2)$ for all k. Then, there is an n-adic code in $\mathbb{F}_q[G]$.*

Proof. Proceed as in theorem 2.2.25. It suffices to show the theorem for $G = (\mathbb{Z}/2^r\mathbb{Z}) \times \cdots \times (\mathbb{Z}/2^r\mathbb{Z}) = (\mathbb{Z}/2^r\mathbb{Z})^{t_n(2)}$, where r is arbitrary. The result will follow by theorem 2.2.10.

Let $k = t_n(2)$, and consider an unramified extension $K = \mathbb{Q}_2(\beta)$ of $\mathbb{Q}_2$ of degree k.[10] Let O_K be the ring of integers of K. As K is unramified, 2 is the uniformizer of O_K. By Hensel's Lemma, O_K has all the $(2^k - 1)$th roots of unity. In particular, O_K has an nth root of unity, call it $\alpha \in O_K$. Note that $O_K/2^rO_K = (\mathbb{Z}/2^r\mathbb{Z}) \times \cdots \times (\mathbb{Z}/2^r\mathbb{Z}) \simeq G$ as abelian groups under addition. If μ_q is a numerical multiplier of G, then μ_q acting on O_K/s^rO_K is given by $\mu_q(x + 2^rO_K) = qx + 2^rO_K$. Thus, a q-cyclotomic coset in $O_K/2^rO_K$ is a set of the form $\{x + 2^rO_K, qx + 2^rO_K, q^2x + 2^rO_K, \ldots, q^lx + 2^rO_K\}$.

Consider the map $\mu(x + 2^rO_K) = \alpha x + 2^rO_K$, μ lifts to an automorphism of G. Note that μ has order n, as α is an nth root of unity. We claim that μ fixes no cyclotomic coset of $(O_K/2^rO_K)\backslash 2^rO_K = \widetilde{G}$. Since μ has prime order, it will follow that all orbits of μ on the cyclotomic cosets of $\widetilde{G}$ have length n. Hence, by theorem 2.2.6, there is an n-adic code in $\mathbb{F}_q[G]$.

Suppose there was $x + 2^rO_K$ such that $\alpha x + 2^rO_K = \mu(x + 2^rO_K) = q^lx + 2^rO_K$. Thus, there is $y \in O_K$ such that $\alpha x = q^lx + 2^ry$. Since $x + O_K$ is a nontrivial class, the 2 valuation of x is $0 \leq v_2(x) \leq r - 1$. Note that there is a unit x_o such that $x = 2^{v_2(x)}x_o$. Thus, $\alpha = q^l + 2^{r-v_2(x)}yx_o^{-1}$. Since $1 \leq r - v_2(x)$, we have that $\alpha = q^l \mod 2O_K$. Thus, $\alpha = q^l$ in the residue field. As q is an odd prime ($(q, |G|) = 1$), we have that $q = 1$ in $\mathbb{F}_{2^k}$. Thus, $\alpha = 1$ in the residue field. This is a contradiction since α maps to a nontrivial nth root of unity in the residue field.

□

[10] $\mathbb{Q}_2$ is the 2-adic numbers.

2.3 Duadic Code Generalizations and n-adic Codes

We will recall the definitions of the generalizations of Duadic Codes by previous authors and then show equivalence results between these and n-adic codes.

The history of Duadic Codes starts with a generalization of the cyclic Quadratic Residue Codes by Rushanan in [22], and by Pless and Rushanan in [21]; whom, introduced the notion of Generalized Q-Codes given by:

Definition 2.3.1. *Let e_1 and e_2 be two idempotents of $\mathbb{F}_q[G]$ and $\mu \in Aut(G)$ such that the following two equations hold:*

$$\begin{aligned} e_2 &= \mu \cdot e_1, \\ e_1 + e_2 - 1 &= \frac{1}{|G|} \sum_{g \in G} g. \end{aligned}$$

The four codes: $C_1 = \langle e_1 \rangle, C_1' = \langle 1 - e_2 \rangle, C_2 = \langle e_2 \rangle, C_2' = \langle 1 - e_1 \rangle$ are the Generalized Q-Codes *defined by e_1, e_2, and μ.*

Generalized Q-codes then became known as Duadic Codes in the literature. Duadic Codes were first studied in the cyclic binary case. Since their introduction there have been various generalizations with respect to:

1. parity of the characteristic of the field,
2. number of idempotents used,
3. the cyclic and noncyclic abelian case.

The following is a history of these generalizations:

The Duadic Even Characteristic, by Rushanan in [22]. These are codes in $\mathbb{F}_q[G]$ where G is an arbitrary abelian group, q is even, and 2 idempotents are used in its definition.

The Duadic Odd Characteristic, by Smid in [25]. These are codes in $\mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]$ where q is odd and 2 idempotents are used in its definition.

The Triadic Codes, by Pless and Rushanan in [21]. These are codes in $\mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]$ where q is even and 3 idempotents are used in its definition.

The Polyadic Codes, by Brualdi and Pless in [4]. These are codes in $\mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]$ and m idempotents are used in its definition.

The m-adic Polyadic Codes, by Ling and Xing in [18]. These are codes in $\mathbb{F}_q[G]$ where G is a general abelian group and m idempotents are used in its definition.

Cyclic Triadic Codes were introduced by Pless and Rushanan in [21] to generalize Duadic Codes with respect to the number of idempotents. The following is their definition.

Definition 2.3.2. *Let e_1, e_2, e_3 be three even-like idempotents in $\mathbb{F}_q[\mathbb{Z}/n\mathbb{Z}]$ where $(n, q) = 1$ and:*

1. *There is a coordinate permutation μ_b, where $\mu_b \in Aut(G)$, such that: $\mu_b \cdot e_1 = e_2, \mu_b \cdot e_2 = e_3, \mu_b \cdot e_3 = e_1$.*

2. *The idempotents satisfy*

$$e_1 + e_2 + e_3 - 2e_1e_2e_3 \;\; = \;\; 1 - \frac{1}{n}\sum_{g \in G} g.$$

Then, e_1, e_2 are called even-like Triadic Codes.

Definition 2.3.3. *A Triadic Code is called* "reduced" *if $e_ie_j = 0$ whenever $i \neq j$.*

Cyclic Triadic Codes were later generalized further by Brualdi and Pless in [4] by introducing the concept of Cyclic Polyadic Codes.

Definition 2.3.4. *Let m be an integer with $m \geq 2$. A* Cyclic Polyadic Code *or an m-*adic family of even-like codes of class I *(over $GF(q)$ of length n) is a family $C_0, C_1, \ldots, C_{m-1}$ of distinct cyclic even-like codes satisfying:*

1. *There exist an integer a, where $\gcd(a, n) = 1$, such that μ_a cyclically permutes:*

$$C_0, C_1, \ldots, C_{m-1}.$$

2. *There exist a cyclic code F of $V = (GF(q))^n$ such that $C_i \cap C_j = F$, for all $i \neq j$.*

3. *$\langle C_0, C_1, \ldots, C_{m-1} \rangle = \langle d_{g_0} \rangle$, where $d_{g_0} = \frac{1}{|G|} \sum_{g \in G} \rho(g)$, $G = (\mathbb{Z}/n\mathbb{Z})$, and ρ is the left regular representation of G onto $GL(V)$ with $V = (GF(q))^n$.*

Definition 2.3.5. *If $C_0, \ldots, C_{m-1}$ is an m-adic polyadic family of even-like cyclic codes of class I, then we will call this family* "reduced" *if $C_i \cap C_j = \{0\}$ for all i, j.*

Just recently, Ling and Xing in [18] have introduced a generalization of Cyclic Polyadic Codes from the cyclic case to the case of an arbitrary abelian group G. These new codes, called m-adic Polyadic Codes, are defined by first introducing the notion of an m-splitting.

Definition 2.3.6. *Let G be an abelian group and $X_\infty \neq \phi$ a subset of G. An* m-splitting of G over X_∞ *is an $(m+1)$-tuple $(X_\infty, X_0, \ldots, X_{m-1})$ such that:*

1. *Each X_i is a the union of q-cyclotomic cosets of G, where q is a power of a prime.*

2. *The sets $X_\infty, X_0, \ldots, X_{m-1}$ form a partition of G, i.e.,*

$$G \;=\; X_\infty \cup X_0 \cup \cdots \cup X_{m-1}.$$

3. *There exists $\mu_s \in Aut(G)$, i.e., there is an s with $\gcd(s, exp(G)) = 1$, such that $\mu_s(X_\infty) = X_\infty$ and $\mu_s(X_i) = X_{i+1}$ for all $0 \leq i \leq m-1$, where the subscripts are taken modulo m.*

Definition 2.3.7. *Let $(X_\infty, X_0, \ldots, X_{m-1})$ be an m-splitting of G over X_∞ and $X'_\infty = X_\infty \backslash \{0\}$. For any subset of X of G, define the* ideal in $\mathbb{F}_q[G]$ induced by X *as*

$$I_X \;=\; \{c \in \mathbb{F}_q[G] \mid \widehat{c_x} = 0, \forall x \in X\},$$

where

$$\begin{aligned} \widehat{c_x} &= \sum_{g \in G} \chi_x(g) c_g, \\ \chi_x &= \theta(x) \text{ where } \theta : G \to \widehat{G}, \end{aligned}$$

for some noncanonical isomorphism θ. Alternatively, using the language of primitive idempotents, we define I_X as

$$I_X = \langle e_{\sim X} \rangle.$$

Any of the following four families of codes given by the m-splitting are referred as an m-adic Polyadic Code in $\mathbb{F}_q[G]$*:*

1. *(Class I). $C_1, \ldots, C_{m-1}$ where $C_i = I_{\sim(X'_\infty \cup X_i)}$,*
2. *(Class II). $\widehat{C_1}, \ldots, \widehat{C_{m-1}}$ where $\widehat{C_i} = I_{X'_\infty \cup X_i}$,*
3. *(Class III). $D_1, \ldots, D_{m-1}$ where $D_i = I_{X_\infty \cup X_i}$,*
4. *(Class IV). $\widehat{D_1}, \ldots, \widehat{D_{m-1}}$ where $\widehat{D_i} = I_{\sim(X_\infty \cup X_i)}$.*

Definition 2.3.8. *We will call any m-adic Polyadic Code* "reduced" *if $X_\infty = \{0\}$.*

We proceed to show that the codes of Ling and Xing generalize all Duadic generalizations done by Brualdi, Rushanan and Pless.

Proposition 2.3.9. *The following hold:*

1. *A Cyclic Triadic Code is a 3-adic Polyadic Code of Class I in the sense of Ling and Xing.*
2. *A Cyclic Polyadic Code given by an m-adic family of even-like codes is an m-adic Polyadic Code of Class I in the sense of Ling and Xing.*

Proof. We recall a fact that can be found in the work of Pless and Rushanan in [21]. to prove the first assertion.

Claim 2.3.10. *If e_1, e_2, e_3 is a Triadic Code then $e_i e_j = e_1 e_2 e_3$ for all i, j.*

Using the notation of primitive idempotents, let $e_i = e_{Y_i}$. The equation $e_i e_j = e_1 e_2 e_3$ reduces to:

$$Y_i \cap Y_j \;=\; X'_\infty,$$

where X'_∞ is some fixed subset of G.

Let $X_i = Y_i \backslash X'_\infty$ and $X_\infty = X'_\infty \cup \{0\}$, then clearly

$$(X_\infty, X_1, X_2, X_3),$$

is a 3-splitting of G and the codes given by $I_{\sim(X'_\infty \cup X_i)} = \langle e_{X'_\infty \cup X_i} \rangle = \langle e_{Y_i} \rangle$ are a family of 3-adic Polyadic Codes of Class I in the sense of Ling and Xing.

The second assertion uses a similar construction. □

We will show that Abelian n-adic Codes generalize Duadic Codes and intersect the other Duadic Generalizations under the "reduced" condition. Before we state the equivalence result: we note that for an n-adic code e, μ to exist, it is necessary to assume that e be an oddlike idempotent. Otherwise, if $d_{g_0} e = 0$, we would have

$$\begin{aligned} 0 &= d_{g_0} e(\mu \cdot e)(\mu^2 \cdot e) \cdots (\mu^{n-1} \cdot e) \\ &= d_{g_0} d_{g_0} \\ &= d_{g_0}, \end{aligned}$$

which is a contradiction. Thus, we assume that all n-adic codes are given by oddlike idempotents.

Proposition 2.3.11. *The following equivalences are true:*

1. *An oddlike Duadic code is a 2-adic code.*
2. *A 2-adic code is an oddlike Duadic code.*
3. *If (μ, e) is a "reduced" Triadic Code, then $(\mu, e + d_{g_0})$ is a "reduced" 3-adic code.*

4. *If* (μ, e) *is a "reduced" 3-adic code, then* $(\mu, e - d_{g_0})$ *is a "reduced" Triadic Code.*

5. *If* $(\mu, \langle e_0\rangle, \ldots, \langle e_{m-1}\rangle)$ *is a "reduced" Cyclic Polyadic Code in the sense of Brualdi and Pless and* m *is a prime, then* $(\mu, \langle e_0 + d_{g_0}\rangle)$ *is a "reduced" m-adic code.*

6. *If* (μ, e_0) *is a "reduced" n-adic code and* $G = (\mathbb{Z}/n\mathbb{Z})$ *is cyclic, then*

$$(\mu, \langle e_0 - d_{g_0}\rangle, \ldots, \langle e_{n-1} - d_{g_0}\rangle)$$

   is a "reduced" Cyclic Polyadic Code in the sense of Brualdi and Pless.

7. *If* $(\mu, C_0 = \langle e_0\rangle, \ldots, C_{m-1} = \langle e_{m-1}\rangle)$ *is a "reduced" m-adic Polyadic Code of Class IV and* m *is a prime, then* $(\mu, \langle e_0\rangle, \ldots, \langle e_{m-1}\rangle)$ *is a "reduced" m-adic code.*

8. *If* (μ, e_0) *is a "reduced" m-adic code, where is* m *a prime, then* (μ, e_0) *is a "reduced" m-adic Polyadic Code of Class IV.*

Proof. We proceed to show each part separately.

Part 1. Let $e_1, e_2 = \mu \cdot e_1, \mu$ be a Duadic Code in $\mathbb{F}_q[G]$. Clearly, the following equations hold:

$$\begin{aligned} e_2 &= \mu \cdot e_1, \\ e_1 + e_2 - 1 &= d_{g_0}. \end{aligned}$$

To show that e_1, e_2, μ forms a 2-adic code, we must show that:

$$\begin{aligned} \langle e_1, e_2\rangle &= \mathbb{F}_q[G], \\ \langle e_1\rangle \cap \langle e_2\rangle &= \langle d_{g_0}\rangle. \end{aligned}$$

Suppose that $\mathbb{F}_q$ has odd characteristic. Consider:

$$\begin{aligned} 1 + 3d_{g_0} &= (1 + d_{g_0})^2 \\ &= (e_1 + e_2)^2 \\ &= e_1 + e_2 + 2e_1e_2 \\ &= (e_1 + e_2 - 1) + 1 + 2e_1e_2 \\ &= d_{g_0} + 1 + 2e_1e_2. \end{aligned}$$

Thus $2d_{g_0} = 2e_1e_2$. Hence, $e_1e_2 = d_{g_0}$. Therefore, it follows that e_1, e_2, μ is a 2-adic code.

Now, suppose that $\mathbb{F}_q$ has even characteristic. Let $e_1 = e_{X_1}$, $e_2 = e_{X_2}$ and $d_{g_0} = e_{\{0\}}$. Clearly, because the characteristic is even, $e_{X_1} + e_{X_2} = e_{X_1 \triangle X_2}$. Thus:

$$\begin{aligned} e_{X_1 \triangle X_2} &= e_{X_1} + e_{X_2} \\ &= 1 + d_{g_0} \\ &= e_X + e_{\{0\}}. \end{aligned}$$

Therefore, $X_1 \triangle X_2 = X \triangle \{0\}$. Hence, $X_1 \cap X_2 = \{0\}$; or, $X_1 \cap X_2 = \{\}$ and $\{0\} \subset\sim (X_1 \cup X_2)$.

If $X_1 \cap X_2 = \{0\}$ then $e_1e_2 = e_{X_1}e_{X_2} = e_{\{0\}} = d_{g_0}$; thus, it follows that e_1, e_2 form a 2-adic code.

If $\{0\} \subset\sim (X_1 \cup X_2)$; then, $d_{g_0}e_1 = 0$ and $d_{g_0}e_2 = 0$. Thus, contradicting the assumption that e_1 and e_2 are oddlike idempotents.

Part 2. Suppose that e_1, e_2, μ forms a 2-adic code, then:

$$\begin{aligned} e_1 + e_2 - e_1e_2 &= 1, \\ e_1e_2 &= d_{g_0}. \end{aligned}$$

Thus, $e_1 + e_2 = 1 + d_{g_0}$. Hence, e_1, e_2 forms a Duadic Code.

Part 3. This is a clear consequence of parts 7 and 8, and proposition 2.3.9.

Part 4. This is a clear consequence of parts 7 and 8, and proposition 2.3.9.

Part 5. This is a clear consequence of parts 7 and 8, and proposition 2.3.9.

Part 6. This is a clear consequence of parts 7 and 8, and proposition 2.3.9.

Part 7. Suppose $(\mu, \langle e_0\rangle, \ldots, \langle e_{m-1}\rangle)$ is a "reduced" m-adic Polyadic Code of Class IV and m is a prime. Define Y_i such that $e_i = e_{Y_i}$. Clearly, since $e_i e_j = d_{g_0}$, we have:

$$Y_i \cap Y_j \;=\; \{0\}.$$

By letting $X_i = Y_i \backslash \{0\}$ and $X_\infty = \{0\}$, the partition $(X_\infty, X_0, \ldots, X_{m-1})$ forms an m-splitting. Thus, $Y_0 \cup \cdots \cup Y_{m-1} = G$ and $Y_0 \cap \cdots \cap Y_{m-1} = Y_i \cap Y_j = \{0\}$. These equations guarantee that the idempotents e_i form a "reduced" m-adic code.

Part 8. Suppose (μ, e_0) is a "reduced" m-adic code, where m a prime. Let X_i be defined by $e_i = e_{X_i}$, where $e_i = \mu^i \cdot e_0$. By the reduced condition,

$$\begin{aligned} d_{\{0\}} &= d_{g_0} \\ &= e_i e_j \\ &= e_{X_i} e_{X_j} \\ &= e_{X_i \cap X_j}. \end{aligned}$$

Thus, $X_i \cap X_j = \{0\}$ for all i, j. Since $\langle e_0, \ldots, e_{m-1}\rangle = \mathbb{F}_q[G] = \langle 1\rangle$, we must have:

$$X_\infty \cup X_0 \cup \cdots \cup X_{m-1} \;=\; G.$$

Note that, by letting $Y_i = X_i \backslash \{0\}$ for $0 \leq i \leq m-1$, and $Y_\infty = \{0\}$, we can construct the m-splitting $(Y_\infty, Y_0, \ldots, Y_{m-1})$ of G. Using this m-splitting, the n-adic code becomes a "reduced" m-adic Polyadic Code of Class IV. $\square$

2.4 Abelian n-adic Groups

We will prove an analogous result to proposition 1.1.2 for abelian n-adic codes by introducing the concept of abelian n-adic groups.

The case when the splitter $\mu = \mu_l$ is a numerical multiplier, where $(l, |G|) = 1$, will be of interest to us. Since $Stab_{\langle\mu\rangle}(e) = \langle\mu^n\rangle$, it will be required that $|\mu|$ be divisible by n. Hence, we will consider numerical multipliers of order n; that is, nontrivial solutions to the equation $x^n = 1$ modulo $exp(G)$.

Because, the equation $x^n = 1$ modulo m will not always have nontrivial solutions, we will impose some conditions on G to guarantee a nontrivial solution. This is shown by the following theorem.

Proposition 2.4.1. *Let $m = p_0^{\alpha_0} * p_1^{\alpha_1} * \cdots * p_r^{\alpha_r}$ where $(p_i, p_j) = 1$ for $i \neq j$, $\alpha_i \geq 1$ for $i \geq 1$, $\alpha_0 \geq 0$, and $p_0 = n$. The equation $x^n = 1$ modulo m has a nontrivial solution modulo $p_i^{\alpha_i}$ for all $1 \leq i \leq r$ if and only if $p_i = 1$ modulo n for all $1 \leq i \leq r$ and either: $\alpha_0 = 0$; or, $\alpha_0 \geq 2$.*

Proof. This is a consequence of the fact that $x^n = 1$ has a nontrivial solution modulo p^α if and only if n divides $\phi(p^\alpha) = p^{\alpha-1}(p-1)$. □

Proposition 2.4.2. *Let $m = p_1^{\alpha_1} * \cdots * p_r^{\alpha_r}$, where n does not divide m.*

1. *If $p_i = 1$ mod n for all $1 \leq i \leq r$, then there is a nontrivial solution to $l^n = 1$ mod $p_i^{\alpha_i}$ for all $1 \leq i \leq r$ where:*
   (a) *The solution l satisfies $l \neq 1$ mod p_i for all $i = 1, \ldots, r$,*
   (b) *The solution l satisfies $l \neq 1$ mod p_i^f for all $1 \leq f \leq \alpha_i$ and for all $1 \leq i \leq r$.*
2. *If there is a nontrivial solution to $x^n = 1$ mod $p_i^{\alpha_i}$ where $x \neq 1$ mod p_i for all $1 \leq i \leq r$, then $p_i = 1$ mod n for all $1 \leq i \leq r$.*

Proof. We proceed to show each part separately.

Part 1. This is an application of the Chinese Remainder Theorem. As n divides $p_i - 1$, there is a nontrivial solution l_i to $x^n = 1 \bmod p_i$. Lift this solution to a

solution L_i of $x^n = 1$ in $\mathbb{Q}_{p_i}$ using Hensel's Lemma. Define $l_i' = L_i \bmod p_i^{\alpha_i}\mathbb{Z}_{p_i}$ as the projection onto $\mathbb{Z}_{p_i}/p_i^{\alpha_i}\mathbb{Z}_{p_i}$.

Note that this choice of l_i' has the property:

$$l_i' \neq 1 \bmod p_i^f,$$

for every $1 \leq f \leq \alpha_i$. We can deduce this by contradiction. If it $l_i' = 1 \bmod p_i^f$, then $l_i' = 1 \bmod p_i^f$ and $L_i = l_i' = 1 \bmod p_i$; but, $L_i = l_i \bmod p_i$ by construction, thus $l_i = L_i = l_i' = 1 \bmod p_i$. Hence, contradicting the choice of l_i.

Thus, we have a set of solutions $(l_1', \ldots, l_r')$ to $x^n = 1 \bmod (p_1^{\alpha_1}, \ldots, p_r^{\alpha_r})$. By the Chinese Remainder Theorem, we can find a solution to $x^n = 1 \bmod m = p_1^{\alpha_1} * \cdots p_r^{\alpha_r}$ with the desired properties.

Part 2. Under the assumptions, we must have n divide $\phi(p_i^{\alpha_i}) = p^{\alpha_i - 1}(p_i - 1)$ for all $1 \leq i \leq r$. Since n does not divide m, we must have n divide $p_i - 1$. Hence, the result follows. □

Thus, by proposition 2.4.2, it suffices to assume that all primes s that divide $|G|$ have the property $s = 1$ modulo n to guarantee the existence of a nontrivial $\mu_l \in Aut(G)$, numerical multiplier, with the properties: $\mu_l^n = 1$, and $l \neq 1 \bmod s^i$ for every prime power s dividing $exp(G)$; i.e., μ_{l-1} is a numerical multiplier of G. In this subsection, we will assume that G always has this property and call G an n-adic group.

Definition 2.4.3. *If G is an abelian group such that $s = 1$ mod n for every prime s dividing $exp(G)$, then G is an* n-adic group.

Corollary 2.4.4. *If G is an n-adic group, then there is a numerical multiplier μ_l such that:*

1. *The multiplier l satisfies $l^n = 1$ mod $exp(G)$,*
2. *The multiplier l satisfies $l \neq 1$ mod s^i for every prime power s^i dividing the $exp(G)$,*

3. *The map μ_{l-1} is a numerical multiplier of G; that is, $(l-1, exp(G)) = 1$,*

4. *The following holds $l^{n-1} + l^{n-2} + \cdots + l + 1 = 0 \ mod \ exp(G)$.*

Proof. Parts 1 and 2 are consequences of proposition 2.4.2. We show part 3 by noting: if s divides $exp(G)$ and $l-1$, then the choice of l in proposition 2.4.2 gives us a contradiction. Part 4 follows from the following identity modulo $exp(G)$:

$$\begin{aligned} 0 &= l^n - 1, \\ &= (l-1)(l^{n-1} + l^{n-2} + \cdots + l + 1). \end{aligned}$$

Hence, by part 3, $(l-1)$ is invertible modulo $exp(G)$. Therefore, part 4 follows. □

Definition 2.4.5. *We will define a splitter μ_l in G such that:*

1. *The splitter l is an nth root of unity, i.e. , $l^n = 1 \ mod \ exp(G)$,*

2. *The splitter satisfies $l \neq 1 \ mod \ s^i$ for every prime power s^i dividing $exp(G)$,*

a canonical splitter*.*

As a consequence we have the following.

Proposition 2.4.6. *An abelian group G allows a canonical splitter if and only if G is an n-adic group.*

Proof. This is a consequence of proposition 2.4.2. □

2.4.1 Canonical Splitters for n-adic Groups

Theorem 2.4.7. *Let G be an n-adic group. Let μ_l be a canonical splitter of order n in $Aut(G)$. Then, μ_l fixes a cyclotomic coset of $\widetilde{G} = G\backslash\{0\}$ if and only if $t_s(q) = 0$ modulo n for some prime s dividing $|G|$.*

Proof. ($\Rightarrow$). Let $G = S_{s_1} \times \cdots \times S_{s_r}$ be an n-adic group; where each $s_i = 1$ modulo n, and S_{s_i} are the s_i-sylow groups of G.

Suppose C_g, a cyclotomic coset of $\widetilde{G}$, is fixed by μ_l. Hence, $\mu_l(C_g) = C_g$; thus, $l * g = q^f * g$. In other words, $l = q^f$ modulo $|g|$. Without loss of generality, assume s_1^i is the highest power of s_1 that divides $|g|$. Thus, we have $l = q^f$ modulo s_1^i. Let $s = s_1$. Since $l^n = 1$ modulo $exp(G)$ and $|g|$ divides $exp(G)$, we have $1 = l^n = q^{fn}$ modulo s^i. In particular, $t_{s^i}(q)$ divides fn. Thus,

$$t_{s^i}(q)e \;=\; fn.$$

Since l is a canonical splitter, $l \neq 1$ modulo s^i. If n does not divide $t_{s^i}(q)$, then $t_{s^i}(q)$ divides f. Hence, modulo s^i:

$$\begin{aligned} l &= q^f \\ &= (q^{t_{s^i}(q)})^{\frac{f}{t_{s^i}(q)}} \\ &= 1^{\frac{f}{t_{s^i}(q)}} \\ &= 1, \end{aligned}$$

which is a contradiction. Thus, $t_{s^i}(q)$ does not divide f and therefore n divides $t_{s^i}(q)$.

Since $t_s(q)|t_{s^i}(q)|s^{i-1}t_s(q)$ and $(s, n) = 1$, we have that n divides $t_s(q)$ if and only if n divides $t_{s^i}(q)$. Thus, n divides $t_s(q)$ and the conclusion follows.

($\Leftarrow$). Conversely, suppose n divides $t_s(q)$ for some s dividing $|G|$. Then, n divides $t_{s^i}(q)$ for all i. Without loss of generality, assume $s = s_1$. Let $S_{s_1} = (\mathbb{Z}/s\mathbb{Z})^{\pi_1} \times \cdots \times (\mathbb{Z}/s^t\mathbb{Z})^{\pi_t}$, where s^t is the highest power of s that divides $exp(G)$. Consider,

$$g \;=\; (0, \ldots, 0) \times \cdots \times (s^{\pi_t - 1}, 0, \ldots, 0) \in S_{s_1} \subset G.$$

Clearly, g has order s. Let $f = \frac{t_s(q)}{n}$, then $(q^f)^n = 1$ modulo s. Note that, $l^n = 1$ modulo s. Since all the nontrivial solutions of $x^n = 1$ modulo s are powers of one another, because n is a prime and $(\mathbb{Z}/s\mathbb{Z})^*$ is cyclic; we have $l^{n_0} = q^f$ modulo s, where $1 \leq n_0 \leq n-1$. Thus, we have $\mu_l^{n_0}(C_g) = C_g$, where $1 \leq n_0 \leq n-1$. Since n is prime and $\mu_l^n = 1$, this implies $\mu_l(C_g) = C_g$. Hence, the conclusion follows. $\square$

Corollary 2.4.8. *Let G be an n-adic group. Let μ_l be a canonical splitter of order n in $Aut(G)$. Then, $\mathbb{F}_q[G]$ has an n-adic code with splitter given by μ_l if and only if $t_s(q) \neq 0$ modulo n, for every prime s dividing $|G|$.*

Proof. By theorem 2.2.10, μ_l is a splitter for an n-adic code in $\mathbb{F}_q[G]$ if and only if all orbits of $\bar{\mu_l}$ on the cyclotomic cosets of $\widetilde{G}$ have length divisible by n. Since μ_l has order n and n is a prime, this is equivalent to saying that $\bar{\mu_l}$ fixes no cyclotomic coset of $\widetilde{G}$. Note that $\bar{\mu_l} = \mu_l^{n-1} = \mu_{l'}$, where $(l')^n = 1$ modulo $exp(G)$. It can be shown that $l' = l^{n-1} = l^{-1}$ is also a canonical splitter. By theorem 2.2.5, $\mu_{l'}$ fixes no cyclotomic coset of $\widetilde{G}$ if and only if $t_s(q) \neq 0$ modulo n for every s dividing $|G|$. Hence, the result follows. □

We note that, if μ_l is a canonical splitter and e, μ give an n-adic code, then e, μ^{n_0}, $1 \leq n_0 \leq n-1$ gives the same n-adic code. Also, for the case $n = 2$, there is a unique canonical splitter given by μ_{-1}.

Definition 2.4.9. *In an n-adic Group, we call the n-adic codes e, μ_l given by canonical splitters* Margarita Codes.

For $n = 2$, Margarita codes are the almost self dual codes of Rushanan in [22] and Pless in [20].

2.4.2 Margarita Codes

A quick calculation using Equation (2.5) shows that the minimum distance d_0 of oddlike words[11] in an n-adic code satisfies the bound $d_0^n \geq |G|$. One can do better for Margarita codes; however, we will introduce some preliminaries before we show this result.

Proposition 2.4.10. *Let μ_l be a canonical splitter in the n-adic group G. Then, $(l-1, exp(G)) = 1$; that is, μ_{l-1} is a numerical multiplier.*

[11] an oddlike word is $w = \sum_{g \in G} w_g[g]$ where $\sum_{g \in G} w_g \neq 0$ in $\mathbb{F}_q$.

Proof. Let μ_l give a canonical splitter in $\mathbb{F}_q[G]$ and assume e, μ_l gives an n-adic code. Note that since G is an n-adic group, we have that for every prime s_i dividing $|G|$, $s_i = 1 \bmod n$. Also, since μ_l has order n, we must have $l^n = 1 \bmod exp(G)$.

Let s be a prime dividing $exp(G)$,[12] and $l-1$. Since $s - 1 = cn$ for some positive constant c, we must have $n \leq cn = s - 1$. Thus, $n - 1 \leq s$ and we deduce that $n \leq cn = s - 1$. Therefore, n does not divide $s - 1$. □

Theorem 2.4.11. *Let e, μ_l give a Margarita code in $\mathbb{F}_q[G]$ where G is an n-adic group and μ_l a canonical splitter of order n. Let d_0 be the minimum weight of all oddlike vectors of $\langle e \rangle$. Let $w \in \langle e \rangle$ be an oddlike vector of weight d_0. Let $w = \sum_{g \in B} \beta_g[g]$ where $B \subset G$ is the support of w. Let $\widetilde{B} = \sum_{g \in B}[g]$ be the characteristic function of the support of w. Define $r_{n,\mu_l,G} : G \to \mathbb{Z}$ as,*

$$r_{n,\mu_l,G}(g) \;=\; |H_g \cap (B \times \ldots \times B)|,$$

where

$$H_g \;=\; \{(g_1, \ldots, g_n) \in G \times \cdots \times G | g_1 + \mu_l(g_2) + \cdots + \mu_{l^{n-1}}(g_n) = g\}.$$

Then,

1. *The constant d_0 satisfies $d_0^n - r_{n,\mu_l,G}(1) + 1 \geq |G|$,*
2. *If $d_0^n - r_{n,\mu_l,G}(1) + 1 = |G|$, then:*
   (a) *The oddlike word satisfies $w = \alpha * \widetilde{B}$ for some $\alpha \in \mathbb{F}_q$,*
   (b) *The characteristic function of the support of w satisfies,*

$$\widetilde{B} * (\mu_l \cdot \widetilde{B}) * \cdots * (\mu_l^{n-1} \cdot \widetilde{B}) \;=\; (r_{n,\mu_l,G}(1) - 1)[1] + \sum_{g \in G}[g].$$

3. *The constant $r_{n,\mu_l,G}(1)$ satisfies $r_{n,\mu_l,G}(1) = d_0$ modulo n,*
4. *The constant $r_{n,\mu_l,G}(1)$ satisfies $r_{n,\mu_l,G}(1) \geq d_0$.*

[12] and therefore $|G|$.

Proof. We proceed to show each part separately.

Part 1. Define $F_l(x_1, \ldots, x_n) = x_1 + l * x_2 + \cdots + l^{n-1} * x_n$ where: $x_i \in G$, $l^i * x$ means $\mu_l^i(x)$, and $+$ is the group addition of G. Clearly, F_l is a group homeomorphism from $G \times \cdots \times G = G^n \to G$. We will show that this map is onto.

Let d_0 be the minimum weight among all oddlike words of $\langle e \rangle$. Let w be an oddlike vector of $\langle e \rangle$ of weight d_0. Define $B \subset G$ such that $w = \sum_{g \in B} \beta_g[g]$, $\beta_g \neq 0$. Let $B(x) = \sum_{g \in B}[g]$. By Equation (2.5), we conclude that there is an $\alpha \in \mathbb{F}_q$ such that:

$$\begin{aligned} \alpha * \sum_{g \in G}[g] &= \sum_{(g_1,\ldots,g_n) \in B \times \cdots \times B} \beta_{g_1}\beta_{g_2}\cdots\beta_{g_n}[F_l(g_1, \ldots, g_n)] \\ &= (\sum_{g \in B} \beta_g[g]) * (\sum_{g \in B} \beta_g[\mu_l(g)]) * \cdots * (\sum_{g \in G} \beta_g[\mu_l^{n-1}(g)]) \\ &= w * (\mu_l \cdot w) * \cdots * (\mu_l^{n-1} \cdot w). \end{aligned} \tag{2.10}$$

In particular, this shows that F_l is onto.

For the moment define,

$$\begin{aligned} H_g &= \{(g_1, \ldots, g_n) \in G \times \cdots \times G \mid F_l(g_1, \ldots, g_n) = g\}, \\ L_g &= H_g \cap (B \times \cdots \times B), \\ r_{n,\mu_l,G}(g) &= |L_g|. \end{aligned}$$

Clearly, $|L_g| \geq 1$.

Let 1 be the identity of G, a direct calculation shows that $r_{n,\mu_l,G}(1) \geq d_0$. This is because: $F_l(g, \ldots, g) = (1 + l + \cdots + l^{n-1}) * g = 0 * g = 1$, since l is a canonical splitter. Thus, $\{(g, \ldots, g) | g \in G\} \subset H_1$ and $\{(g, \ldots, g) | g \in B\} \subset L_1$. Therefore, $d_0 = |B| \leq |L_1| = r_{n,\mu_l,G}(1)$.

We note that for $n = 2$ we can calculate $r_{2,\mu_l,G}(1) = d_0$; however, we leave it as an exercise.

By considering Equation (2.10), we can deduce the bound

$$d_0^n - r_{n,\mu_l,G}(1) + 1 \geq |G|,$$

because,

$$\begin{aligned} d_0^n &= |L_1| + \sum_{g \neq 1} |L_g| \\ &= r_{n,\mu_l,G}(1) + \sum_{g \neq 1} |L_g| \\ &\geq r_{n,\mu_l,G}(1) + \sum_{g \neq 1} 1 \\ &= r_{n,\mu_l,G}(1) + |G| - 1. \end{aligned}$$

Part 2. Assume for now the following result that will be shown later.

Claim 2.4.12. *$|L_g| = 1$ for all $g \neq 1$ if and only if $d_0^n - r_{n,\mu_l,G}(1) + 1 = |G|$.*

Consider the subcases:

(a) Equation (2.10) shows that: if $F_l(g_1, \ldots, g_n) \neq 1$, then $\beta_{g_1} \cdots \beta_{g_n} = \alpha$, where α is defined by Equation (2.10).

Let $g, g' \in G$ and $g \neq g'$, consider $F_l(g, g', \ldots, g') = g(g')^{l+l^2+\cdots+l^{n-1}} = g(g')^{-1} \neq 1$; we must have $\beta_g(\beta_{g'})^{n-1} = \alpha$ for all $g, g' \in G$, where $g \neq g'$. Hence, $\beta_g = \beta_{g''}$ for all $g, g'' \in B$. Thus (2a) follows.

(b) Without loss of generality, we can assume that $\beta_g = 1$, then $w = \widetilde{B}$. Equation (2.10) gives:

$$\begin{aligned} \widetilde{B} * (\mu_l \cdot \widetilde{B}) * \cdots * (\mu_l^{n-1} \cdot \widetilde{B}) &= \sum_{g \in G} |L_g|[g] \\ &= (r_{n,\mu_l,G}(1) - 1)[1] + \sum_{g \in G} [g]. \end{aligned}$$

Thus, it suffices to show claim 2.4.12. Assume that $|L_g| = 1$ for $g \neq 1$, consider:

$$\begin{aligned} d_0^n &= |L_1| + \sum_{g \in G, g \neq 1} |L_g| \\ &= r_{n,\mu_l,G}(1) + |G| - 1. \end{aligned}$$

Conversely, if $d_0^n - r_{n,\mu_l,G}(1) + 1 = |G|$, then

$$\sum_{g \in G, g \neq 1} |L_g| \;=\; d_0^n - |L_1| = d_0^n - r_{n,\mu_l,G}(1) = |G| - 1.$$

Thus, $|L_g| = 1$ for all $g \neq 1$.

Part 3. Note that, if $(g_1, \ldots, g_n) \in H_1$, then $(g_n, g_1, \ldots, g_{n-1}) \in H_1$; because, if

$$g_1 (g_2)^l \cdots (g_n)^{l^{n-1}} \;=\; 1,$$

then,

$$\begin{aligned} 1 &= (1)^l \\ &= (g_1 (g_2)^l \cdots (g_n)^{l^{n-1}})^l \\ &= (g_1)^l (g_2)^{l^2} \cdots (g_{n-1})^{l^{n-1}} (g_n)^{l^n} \\ &= g_n (g_1)^l \cdots (g_{n-1})^{l^{n-1}}. \end{aligned}$$

Hence, $(g_n, g_1, \ldots, g_{n-1}) \in H_1$. Thus, we have shown that H_1 is invariant under the action of $\mathbb{Z}/n\mathbb{Z}$, where $[1] \in \mathbb{Z}/n\mathbb{Z}$ acts like $[1] * (g_1, g_2, \ldots, g_n) = (g_n, g_1, \ldots, g_{n-1})$. Note that since n is prime, all orbits of this action have length 1 or n. Also, note that: if $[1] * (g_1, \ldots, g_n) = (g_1, \ldots, g_n)$, then $(g_1, \ldots, g_n) = (g_1, \ldots, g_1)$. In addition, note that $B \times \cdots \times B$, where $B \subset G$, is also invariant under the action of $\mathbb{Z}/n\mathbb{Z}$. Thus, $L_1 = H_1 \cap B \times \cdots \times B$ is invariant under the action of $\mathbb{Z}/n\mathbb{Z}$, and the only fixed points of L_1 are points of the form $(g, \ldots, g)$ where $g \in B$. In particular, this shows that $r_{n,\mu_l,G}(1) = |L_1| = |B| + n * k = d_0 + n * k$. Hence, the conclusion follows.

Part 4. This is a clear consequence of part 3. □

Since for 2-adic codes the canonical splitter is given by μ_{-1}, and $r_{2,\mu_{-1},G}$ can be computed to be d_0; theorem 2.4.11 gives theorem 1.1.2 as a corollary.

Corollary 2.4.13. *Let e, μ_l give a 2-adic Margarita code in $\mathbb{F}_q[G]$. Let d_0 be the minimum weight of all oddlike vectors of $\langle e \rangle$. Let $w \in \langle e \rangle$ be an oddlike vector of*

weight d_0. *Let* $w = \sum_{g\in B} \beta_g[g]$ *where* $B \subset G$ *is the support of* w. *Let* $\widetilde{B} = \sum_{g\in B}[g]$. *Then,*

1. *The minimum oddlike weight satisfies* $d_0^2 - d_0 + 1 \geq |G|$.
2. *If* $d_0^2 - d_0 + 1 = |G|$, *then,*
   (a) *The oddlike vector* w *is constant, i.e. ,* $w = \alpha * \widetilde{B}$ *for some* $\alpha \in \mathbb{F}_q$,
   (b) *The shifts of* $\widetilde{B}$ *form the blocks of a projective plane of order* $(d_0 - 1)$. *That is,* $\widetilde{B} * (\widetilde{B}^{-1}) = (d_0 - 1)[1] + \sum_{g\in G}[g]$.

2.5 Conclusion

We have introduced the concept of n-adic codes and solved their existence problem. Additionally, we have introduced the concept of canonical splitters to define Margarita Codes, which are generalizations of Rushanan's Self-Dual Codes; and, we have shown the generalized minimal oddlike weight support theorem, theorem 1.1.5, for Margarita Codes.

We close this chapter with a few observations about n-adic codes:

1. We note that for Margarita n-adic codes with $n \neq 2$, $r_{n,\mu_l,G}$ depends also on the idempotent e and the oddlike word of minimal length.

   This is shown by the 3-adic code in $\mathbb{F}_{29}[\mathbb{Z}/7\mathbb{Z}]$ given by the canonical splitter $\mu = \mu_2$ and the idempotent $e = 9[0]+5[1]+2[2]+8[3]+18[4]+11[5]+6[6]$. This pair μ, e gives a code of minimal oddlike weight 3. Consider the two oddlike words of weight 3 given by $w_1 = 26[2]+9[3]+8[5]$ and $w_2 = 21[4]+10[5]+3[6]$. The values of $r_{3,\mu_2,G}$ that arise from w_1 is 6 and from w_2 is 3.

2. Theorem 2.2.16 has been proven for Duadic Codes by Pless and Rushanan in [21] for even Characteristic, and by Smid in [25] for odd characteristic.

3. Corollary 2.4.8 for the case $n = 2$, $q = 2^m$, and $G = \mathbb{Z}/s\mathbb{Z}$ where s is an odd prime has been proven by Rushanan in [22] in page 102; and also by Pless in [20] in theorem 2 of the cited paper.

4. Corollary 2.4.13 for the case $q = 2$ has been proven by Pless in [20] in theorem 4 and corollary 1 of the cited paper.

5. Theorem 1.1.5 has also been generalized to m-adic Polyadic Codes by Ling and Xing in [18]. This is given by theorem 2.5.1.

   Theorem 2.5.1. *Let* $C \in \{C_0, \ldots, C_{m-1}, \ldots, \widehat{D_0}, \ldots, \widehat{D_{m-1}}\}$ *be an* m*-adic Polyadic Code over* $\mathbb{F}_q$ *associated with the* m*-splitting*

   $$(X_\infty, X_0, \ldots, X_{m-1}),$$

   of the finite abelian group G *given by* μ_s*.*

   Let $n' = [G : \langle X_\infty \rangle]$*. Suppose that* $\mu_s(X_\infty) = \mu_{q^r}(X_\infty)$*, where* $r \geq 1$*. Then, for* $p > 1$ *dividing* m *the minimum weight* d *of the codewords in* $C \backslash \tilde{C}$*, also known as the oddlike words, satisfies:*

   $$n' \leq \begin{cases} d^m - d^{m/p} + 1 & \text{if } s_{m,p} = 0 \bmod exp(G), \\ d^m & \text{otherwise,} \end{cases}$$

   where

   $$\begin{aligned} s_{m,p} &= s^{\frac{m(p-1)}{p}} + s^{\frac{m(p-2)}{p}} + \cdots + s^{\frac{2m}{p}} + s^{\frac{m}{p}} + 1, \\ \tilde{C} &= I_{X_\infty} \cdot C. \end{aligned}$$

   The analogous result for m-adic Polyadic Codes, by Ling and Xing, gives a more general bound on the minimum distance of oddlike words. For the case when: m is a prime, s is given by a splitter of order m, and the additional assumption that the m-adic Polyadic Code is "reduced"; Ling and Xing's result reduces to a result about Margarita Codes by choosing $r = 1$ and $p = m$. This is illustrated by the following theorem.

   Theorem 2.5.2. *Let* m *be a prime. Let* C *be a "reduced" Class IV* m*-adic Polyadic Code, i.e.,* $X_\infty = \{0\}$*, in an* m*-adic group* G *where the splitting is*

given by a canonical splitter μ_s of order m. Then, $n' = [G : \langle X_\infty \rangle] = |G| = n$ and the minimum weight d of the codewords in $C \backslash \tilde{C}$, i.e., oddlike words, satisfy:

$$n \leq \begin{cases} d^m - d + 1 & \text{if } s_{m,m} = 0 \bmod exp(G), \\ d^m & \text{otherwise,} \end{cases}$$

where:

$$\begin{aligned} s_{m,m} &= s^{\frac{m(m-1)}{m}} + s^{\frac{m(m-2)}{m}} + \cdots + s^{\frac{2m}{m}} + s^{\frac{m}{m}} + 1 \\ &= s^{m-1} + s^{m-2} + \cdots + s^2 + s + 1. \end{aligned}$$

Since s is a canonical splitter, we always have $s_{m,m} = 0 \bmod exp(G)$; hence, we get a similar bound to that of theorem 1.1.5.

Chapter 3

Generalized Skew Hadamard Difference Sets

We will assume that G is an abelian group, and we will use the additive notation for its group operation. We will begin with the definition of generalized skew hadamard difference Sets, and then construct towards a generalization of proposition 1.2.1.

Definition 3.0.3. *A* generalized skew hadamard difference set *(GSHDS) is an element of the group algebra $D(x) \in \mathbb{Z}[G]$ such that:*

$$D(x)D(x^{n_o}) = (k_o - \lambda)[1] + \lambda G(x), \tag{3.1}$$

$$D(x) + D(x^{n_o}) = G(x) - [1], \tag{3.2}$$

where $[1] = x^0$ is the multiplicative unit of $\mathbb{Z}[G]$, $k_o = |D(x) \cap D(x^{-n_o})|$, and n_o is a Non-Quadratic Residue of $(\mathbb{Z}/exp(G)\mathbb{Z})^*$.

We will assume that n_0 is a Non-Quadratic Residue of $(\mathbb{Z}/exp(G)\mathbb{Z})^*$, and χ_0 is the principal character of G.

Lemma 3.0.4. *Let G admit a GSHDS, then $k_o = 0$ or $k_o = k$. Also:*

1. *If $k_o = 0$, then $k = \frac{v-1}{2}$, $\lambda = \frac{v-1}{4}$, and for any nonprincipal character χ*

$$\chi(D) = \frac{-1 + \epsilon_\chi \sqrt{v}}{2},$$

2. If $k_o = k$, then $k = \frac{v-1}{2}$, $\lambda = \frac{v-3}{4}$, and for any nonprincipal character χ

$$\chi(D) \quad = \quad \frac{-1 + \epsilon_\chi \sqrt{-v}}{2},$$

where in the above, $\epsilon_\chi \in \{1, -1\}$.

Proof. Let χ be a nonprincipal character of G. Equation (3.2) forces $k = |D(x)| = \frac{v-1}{2}$. Also, Equation (3.1) forces:

$$k_o + \lambda(v-1) \quad = \quad k^2,$$

hence,

$$k_o \quad = \quad \frac{v-1}{2}(\frac{v-1}{2} - 2\lambda), \tag{3.3}$$

thus, $k = \frac{v-1}{2}$ divides k_o.

By definition $k_o \leq k$. Therefore, either $k_o = 0$ or $k_o = k$. Clearly, by Equation (3.3), if $k_0 = 0$ then $\lambda = \frac{v-1}{4}$. Similarly, we can show: if $k_o = k$ then $\lambda = \frac{v-3}{4}$.

Note that equations (3.1) and (3.2) yield:

$$D(x)^2 + D(x) + [1](k_o - \lambda) \quad = \quad (k - \lambda)G(x). \tag{3.4}$$

Let us suppose that $k_o = 0$ and apply χ to Equation (3.4), we get:

$$\chi(D)^2 + \chi(D) - \frac{v-1}{4} \quad = \quad 0,$$

hence,

$$\chi(D) \quad = \quad \frac{-1 + \epsilon_\chi \sqrt{v}}{2},$$

where $\epsilon_\chi \in \{1, -1\}$.

Similarly, one can show that if $k_o = k$, then

$$\chi(D) = \frac{-1 + \epsilon_\chi \sqrt{-v}}{2}.$$

The proposition follows. □

Proposition 3.0.5. *Let G admit a GSHDS D, then $|G| = p^{2\alpha+1}$ and,*

(a) If $k_o = 0$, then $|G| = p^{2\alpha+1} = 1 \ mod\ 4$,

(b) If $k_o = k$, then $|G| = p^{2\alpha+1} = 3 \ mod\ 4$.

Proof. We proceed to show each part separately.

Part a. Let us assume $k_o = 0$. Also that, $v = |G|$ is composite and divisible by two distinct primes p and s. Let χ be a character of order p and ψ a character of order s. Lemma 3.0.4 shows that $\chi(D) = \frac{-1+\epsilon_\chi\sqrt{v}}{2}$. Since $\chi(D)$ is an algebraic integer in $\mathbb{Q}(\eta_p)$, where η_p a primitive pth root of unity, this shows that $\sqrt{v} \in \mathbb{Q}(\eta_p)$. Similarly, using ψ instead of χ one can show that $\sqrt{v} \in \mathbb{Q}(\eta_s)$. Thus, $\sqrt{v} \in \mathbb{Q}(\eta_p) \cap \mathbb{Q}(\eta_s) = \mathbb{Q}$. Hence, forcing v to be a square.

We claim that v cannot be square by showing a contradiction using Fourier inversion. So let us suppose v is a square and let χ be an arbitrary nonprincipal character. By lemma 3.0.4, $\chi(D)$ is a rational integer. Thus, it remains invariant under the action of any Galois automorphism of $\mathbb{Q}(\eta_{exp(G)})$. Since the $Gal(\mathbb{Q}(\eta_{exp(G)})|\mathbb{Q}) = (\mathbb{Z}/exp(G)\mathbb{Z})^*$, we can choose the Galois automorphism $\mu_{n_o} \in Gal(\mathbb{Q}(\eta_{exp(G)})|\mathbb{Q})$[1] to conclude that $\chi(D(x^{n_o})) = \mu_{n_o}(\chi(D(x))) = \chi(D(x))$. Thus,

$$\begin{aligned} \chi(D(x)D(x^{n_o})) &= \chi(D(x))\chi(D(x^{n_o})) \\ &= \chi(D)^2, \end{aligned}$$

hence, $\chi(D(x)D(x^{n_o})) = \chi(D)^2$ is always a nonnegative integer.

[1] n_0 is a Non-Quadratic Residue.

By calculating $D(x)D(x^{n_o})$ at [1] using Fourier inversion and applying the above equation we conclude:

$$D(x)D(x^{n_o})([1]) \quad = \quad \frac{k^2 + \sum_{\chi \neq 1} \chi(D)^2 \overline{\chi([1])}}{v}.$$

However, from Equation (3.1) and $k_o = 0$, we know $D(x)D(x^{n_o})([1]) = 0$. Thus, the previous equation gives:

$$0 \quad = \quad \frac{k^2 + \sum_{\chi \neq 1} \chi(D)^2}{v},$$

forcing k to be zero. Hence, $D(x) = 0$; giving a contradiction.

Therefore, v cannot be a square. Thus, v must be a prime power. Since $\lambda = \frac{v-1}{4}$, for this case, we have that $|G| = p^r = v = 1 \bmod 4$.

Similarly, we can show v is an odd prime power by using a similar argument as the one used to show that v cannot be a square. Hence, the conclusion follows

Part b. This case is very similar to the previous case. Let us suppose v is composite and divisible by at least two distinct primes p and s. Let χ be a character of order p and ψ a character of order s. By lemma 3.0.4, $\chi(D) = \frac{-1+\epsilon_\chi\sqrt{-v}}{2}$ is an algebraic integer in $\mathbb{Q}(\eta_p)$. Hence, $\sqrt{-v} \in \mathbb{Q}(\eta_p)$. Similarly, by using ψ instead of χ, we can show that $\sqrt{-v} \in \mathbb{Q}(\eta_s)$. Thus $\sqrt{-v} \in \mathbb{Q}(\eta_p) \cap \mathbb{Q}(\eta_s) = \mathbb{Q}$. This is a contradiction as $v > 1$. Hence, v is divisible by only one prime.

Since $v = 3 \bmod 4$ as $\lambda = \frac{v-3}{4}$, this forces v to an odd prime power. The conclusion follows. □

As a consequence of proposition 3.0.5, we will assume that G is an an abelian p-group, where $p \geq 3$ and $exp(G) = p^s$. We will also assume that $|G| = v = p^{2\alpha+1} = p^m$, where $m = 2\alpha + 1$, when G contains a GSHDS. We get the following result as a corollary to the the above results.

Corollary 3.0.6. *Let G be a p-group and D be a GSHDS. Let $p^s = exp(G)$, n be a Quadratic Residue mod p^s, and m a Non-Quadratic Residue mod p^s. Then,*

1. $|G| = v = p^{2\alpha+1}$,

2. $D(x^n) = D(x)$,

3. $k_o = |D(x) \cap D(x^{-m})|$.

Proof. Clearly, part 1 is a consequence of proposition 3.0.5. We proceed to show part 2. Clearly, if $\mu_n \in Gal(\mathbb{Q}(\eta_{p^s})|\mathbb{Q})$ is the Galois automorphism corresponding to $n \in (\mathbb{Z}/p^s\mathbb{Z})^*$ and $\chi \in \widehat{G}$, then

$$\begin{aligned} \chi(D(x^n)) &= \mu_n(\chi(D(x))) \\ &= \mu_n(\chi(D)). \end{aligned}$$

Note that,

$$\begin{aligned} \chi(D) &= \frac{-1 + \epsilon_\chi \sqrt{(\frac{-1}{p})v}}{2} \\ &= \frac{p^\alpha \epsilon_\chi - 1}{2} + p^\alpha \epsilon_\chi \omega, \end{aligned}$$

where $\omega = \frac{-1+\sqrt{(\frac{-1}{p})p}}{2}$. Hence, $\chi(D) \in \mathbb{Q}(\omega) \subset \mathbb{Q}(\eta_{p^s})$.

Note that $\mathbb{Q}(\omega)$ is the fixed field of the quadratic residues subgroup $(\mathbb{Z}/p^s\mathbb{Z})^{*2} \subset (\mathbb{Z}/p^s\mathbb{Z})^* = Gal(\mathbb{Q}(\eta_{p^s})|\mathbb{Q})$. Thus, $\mu_n(\chi(D)) = \chi(D)$, since n is a quadratic residue mod p^s. Hence, $\chi(D(x^n)) = \chi(D) = \chi(D(x))$ for any arbitrary character $\chi \in \widehat{G}$. By Fourier inversion, we must have $D(x^n) = D(x)$.

Now we show part 3. Clearly, there is n' such that $m = n_o n' \bmod p^s$ and n' is a quadratic residue mod p^s. Let $\phi_{n'}$ be the induced algebra isomorphism of $\mathbb{Z}[G]$ by the numerical multiplier $\mu_{n'} \in Aut(G)$ ($\mu_{n'}(g) = g + \cdots + g = n'g$).[2] By applying $\phi_{n'}$ to Equation (3.1) of the GSHDS condition, we get:

$$\phi_{n'}(D(x)D(x^{n_o})) = (k_o - \lambda)\phi_{n'}([1]) + \lambda\phi_{n'}(G(x)). \tag{3.5}$$

Note that $\phi_{n'}(D(x)) = D(x^{n'}) = D(x)$ by part 2. Also, $\phi_{n'}(D(x^{n_o})) = D(x^{n'n_o}) =$

[2]The algebra isomorphism is given by $\phi_{n'}(\sum_{g\in G} c_g[g]) = \sum_{g\in G} c_g[\mu_{n'}(g)] = \sum_{g\in G} c_g[n'g]$.

$D(x^m)$ and $\phi_{n'}(G(x)) = G(x^{n'}) = G(x)$. Hence, Equation (3.5) simplifies to:

$$D(x)D(x^m) \;=\; (k_o - \lambda)[1] + \lambda G(x).$$

Note that the value at [1] of the left-hand side of the above equation gives $|D(x) \cap D(x^{-m})|$, and the value of the right-hand side at [1] is k_o. Hence, $k_o = |D(x) \cap D(x^{-m})|$ and the result follows. □

The next lemma will be used in proposition 3.0.8.

Lemma 3.0.7. *Let G admit a GSHDS D. Then, a nonzero (nonidentity) element g can be at most $\frac{v-1}{4}$ times the difference of two elements of D.*

Proof. We will proceed by cases depending on the value of k_0.

Case $\mathbf{k_0 = 0}$. By using the GSHDS equations, we conclude:

$$D(x)D(x) \;=\; \frac{v-1}{2}[1] + \frac{v-5}{4}D(x) + \frac{v-1}{4}D(x^{n_o}).$$

Since in this case $v = p^{2\alpha+1} = 1(4)$, we must have that -1 is a quadratic residue mod p^s. Hence, $D(x^{-1}) = D(x)$ and:

$$D(x)D(x^{-1}) \;=\; \frac{v-1}{2}[1] + \frac{v-5}{4}D(x) + \frac{v-1}{4}D(x^{n_o}).$$

Thus, a nonzero element $g \in G$ is the difference of two elements of D: $\frac{v-5}{4}$ times, if $g \in D$; and $\frac{v-1}{4}$ times, if $g \in D(x^{n_o})$. In particular, g can be the difference of two elements of D at most $\frac{v-1}{4}$ times.

Case $\mathbf{k_0 = k}$. In this case, -1 is a nonquadratic residue mod p^s. Hence, $D(x^{-1}) = D(x^{n_o})$. Also, the GSHDS equations give the following:

$$D(x)D(x^{n_o}) \;=\; \frac{v-1}{2}[1] + \frac{v-3}{4}D(x) + \frac{v-3}{4}D(x^{n_o}),$$

hence,

$$D(x)D(x^{-1}) \;=\; \frac{v-1}{2}[1] + \frac{v-3}{4}D(x) + \frac{v-3}{4}D(x^{-1}).$$

Thus, a nonzero element of $g \in G$ is the is the difference of two elements of D exactly $\frac{v-3}{4}$ times. Since $\frac{v-3}{4} < \frac{v-1}{4}$, we can say that g is the difference of two elements of D at most $\frac{v-1}{4}$ times. □

The following result, shown for Skew Hadamard Difference Sets in [5], is due to Camion and Mann.

Proposition 3.0.8. *Let G admit a GSHDS D. Then, $G = \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^{a_3}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_l}\mathbb{Z}$ where $s \geq a_3 \geq \cdots \geq a_l$.*

Proof. Assume that $G = \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^{a_2}\mathbb{Z} \times \mathbb{Z}/p^{a_3}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_l}\mathbb{Z}$, where $s > a_2 \geq \cdots \geq a_l$. Let $S = \{(a_1, a_2, \ldots, a_l) \in G \mid a_1 \text{ is a unit in } \mathbb{Z}/p^s\mathbb{Z}\}$. Clearly, $|S| = v - \frac{v}{p}$. Also, by choosing $b = a_1^{-1} \bmod p$, $1 + bp^{s-1}$ is a quadratic residue mod p^s. Note that if $g \in S$ then $g - (1 + bp^{s-1})g = (p^{s-1}, 0, \ldots, 0)$.

Consider $S \cap D$, clearly this set is closed under the action of the quadratic residues mod p^s. Hence, the element $(p^{s-1}, 0, \ldots, 0)$ can be written as the difference of two elements $S \cap D$ at least $|S \cap D|$ times.

We proceed to calculate $|S \cap D|$ by observing that S is closed under the action of $G_1 = (\mathbb{Z}/p^s\mathbb{Z})^*$. Let $G_2 = (\mathbb{Z}/p^s\mathbb{Z})^{*2}$, then every G_1 orbit of S splits into two equally sized orbits of G_2. Since D is the sum of G_2 orbits where each G_2 orbit is picked from exactly one G_1 orbit;[3] we must have $|S \cap D| = \frac{|S|}{2} = \frac{v - \frac{v}{p}}{2}$.

Thus, the element $(p^{s-1}, 0, \ldots, 0)$ can be written as the difference of two elements of $S \cap D \subset D$ at least $\frac{v - \frac{v}{p}}{2}$ times. By the previous lemma, this number cannot exceed $\frac{v-1}{4}$. Therefore, we must have:

$$\frac{v - \frac{v}{p}}{2} \leq \frac{v-1}{4}.$$

Hence, we deduce $v(1 - \frac{2}{p}) \leq -1$. Thus, $1 - \frac{2}{p} < 0$, implying $p < 2$. Clearly a contradiction. □

In the next sections, we will build the necessary concepts to prove proposition 1.2.1 part 3b, which is known as Xiang's exponent bound.

[3] This deduction follows from the fact that D is invariant under the action of G_2, the quadratic residues, and the fact that $D(x) + D(x^{n_o}) = G(x) - [1]$.

3.1 Quadratic Residue Slices (QRS)

For the rest of the chapter, we will assume that G is an abelian p-group, and has $exp(G) = p^s$ with $|G| = v = p^m = p^{2\alpha+1}$. We will embed $G_1 = (\mathbb{Z}/p^s\mathbb{Z})^* \subset Aut(G)$ and $G_2 = (\mathbb{Z}/p^s\mathbb{Z})^{*2} \subset Aut(G)$; where, $a \in G_1 \rightarrow \mu_a \in Aut(G)$ and $\mu_a(g) = g + \cdots + g = a * g$. We will also assume a natural action of: $\mu \in Aut(G)$ on $g \in G$ given by $\mu \cdot g = \mu(g)$; and of $\mu \in Aut(G)$ on $\chi \in \widehat{G}$ given by $\mu \cdot \chi = \chi \circ \mu^{-1}$.

The results of the last section showed that: if G admits a GSHDS D, then $G_2 = (\mathbb{Z}/p^s\mathbb{Z})^{*2}$ are numerical multipliers of D. We will introduce the concept of Quadratic Residue Slices to simplify the study of GSHDSs.

Definition 3.1.1. *Let D be a subset of G such that:*

1. *$D(x^n) = D(x)$, for all $n \in G_2$,*
2. *$D(x) + D(x^{n_o}) = G(x) - [1]$, where n_o is a nonquadratic residue mod p^s,*

then, we say D is a Quadratic Residue Slice *(QRS).*

We will also assume that $\{g_1, \ldots, g_r\}$ is a full set of orbit representatives of the action of G_1 on $\widetilde{G} = G\backslash\{0\}$, and similarly, $\{\chi_1, \ldots, \chi_r\}$ as a full set of representatives of the action of G_1 on $\widehat{G}\backslash\{1\}$. Hence, will assume that $r = r(G)$ is the number of orbits of $G_1 = (\mathbb{Z}/exp(G)\mathbb{Z})^*$ on $G\backslash\{0\}$.

We will denote by O_{g_i} as the G_2 class of g_i and by Ω_{g_i} as the G_1 class of g_i. Clearly,

$$\Omega_{g_i} \;=\; O_{g_i} + O_{g_i}^{(n_0)}.$$

We will define Ω_{χ_i} and O_{χ_i} similarly.

We will represent QRSs in 4 useful ways:

1. Define $X = \bigoplus_{i=1}^{r} \mathbb{C}\Omega_{g_i}$ as the space of G_1 classes on $G\backslash\{0\}$. A QRS D of G is any vector $d = \sum_{i=1}^{r} d_i\Omega_{g_i}$ of ± 1s of X where:

$$D \cap \Omega_{g_i} \;=\; \begin{cases} O_{g_i} & \text{if } d_i = 1, \\ O_{g_i}^{(n_0)} & \text{if } d_i = -1. \end{cases}$$

As short-hand notation, we will write sometimes $D = \sum_{i=1}^{r} O_{\beta_i \cdot g_i}$ where $\beta_i \in (\mathbb{Z}/p^s\mathbb{Z})^*$ and:

$$D \cap \Omega_{g_i} = \begin{cases} O_{g_i} & \text{if } \left(\frac{\beta_i}{p}\right) = 1, \\ O_{g_i}^{(n_0)} & \text{if } \left(\frac{\beta_i}{p}\right) = -1. \end{cases}$$

2. Define $Y = \bigoplus_{i=1}^{r} \mathbb{C}\Omega_{\chi_i}$ as the space of G_1 classes on $\widehat{G}\backslash\{1\}$. A QRS D of $\widehat{G}$ is any vector $d = \sum_{i=1}^{r} d_i \Omega_{\chi_i}$ of ± 1s of X where:

$$D \cap \Omega_{\chi_i} = \begin{cases} O_{\chi_i} & \text{if } d_i = 1, \\ O_{\chi_i}^{(n_0)} & \text{if } d_i = -1. \end{cases}$$

3. Define $W = \bigoplus_{i=1}^{r} \mathbb{C}(O_{g_i} - O_{g_i}^{(n_0)})$ as the space of Compact QRSs of G. A QRS D of G is any vector of $d = \sum_{i=1}^{r} d_i (O_{g_i} - O_{g_i}^{(n_0)})$ of ± 1s where:

$$D \cap \Omega_{g_i} = \begin{cases} O_{g_i} & \text{if } d_i = 1, \\ O_{g_i}^{(n_0)} & \text{if } d_i = -1. \end{cases}$$

4. Define $V = \bigoplus_{i=1}^{r} \mathbb{C}(\Omega_{\chi_i} - \Omega_{\chi_i}^{(n_0)})$ as the space of Compact QRSs of $\widehat{G}$. A QRS D of $\widehat{G}$ is any vector of $d = \sum_{i=1}^{r} d_i (O_{\chi_i} - O_{\chi_i}^{(n_0)})$ of ± 1s where:

$$D \cap \Omega_{\chi_i} = \begin{cases} O_{\chi_i} & \text{if } d_i = 1, \\ O_{\chi_i}^{(n_0)} & \text{if } d_i = -1. \end{cases}$$

3.1.1 The Aut(G) Action

We will introduce an action of $Aut(G)$ on the set of QRSs of G and on the set of QRSs of $\widehat{G}$. Before we proceed to show this action, we will introduce the spaces where the actions will be defined.

Definition 3.1.2. *(**Action of G on QRSs**). Let $X = \bigoplus_{i=1}^{r} \mathbb{C}\Omega_{g_i}$ be the space of G_1 classes in $G\backslash\{0\}$. Clearly, a QRS of G is a vector of ± 1s in X. The action of*

Aut(G) on X is defined as:

$$\rho_{\mathrm{X}}(\sigma)\Omega_{\mathrm{g_i}} \quad = \quad \left(\frac{n}{p}\right)\Omega_{g_j},$$

where $n \in (\mathbb{Z}/p^s\mathbb{Z})^*$ *such that* $\sigma(g_i) = \mu_n \cdot g_j$.

Definition 3.1.3. *(***Action of $\widehat{\mathbf{G}}$ on QRSs***). Let* $Y = \bigoplus_{i=1}^{r} \mathbb{C}\Omega_{\chi_i}$ *be the space of* G_1 *classes in* $\widehat{G}\backslash\{1\}$ *Clearly, a QRS of* $\widehat{G}$ *is a vector of* ± 1*s in* Y*. The action of Aut(G) on Y is defined as:*

$$\rho_{\mathrm{Y}}(\sigma)\Omega_{\chi_{\mathrm{i}}} \quad = \quad \left(\frac{n}{p}\right)\Omega_{\chi_j},$$

where $n \in (\mathbb{Z}/p^s\mathbb{Z})^*$ *such that* $\sigma \cdot \chi_i = \mu_n \cdot \chi_j$.

For technical reasons that will be clear later, we will require the notion of a "commutative" pairing.

Definition 3.1.4. *A bijection* $\theta : G \to \widehat{G}$ *is a* commutative pairing *if:*

1. θ *is an isomorphism of abelian groups.*
2. $\theta(g)(g') = \theta(g')(g)$ *for all* $g, g' \in G$.

We will use θ to relate the χ_is to the g_is by $\chi_i = \theta(g_i)$.

From the definition of a commutative pairing, we can construct a "bilinear" map α as it is shown in the following proposition.

Proposition 3.1.5. *Let* $\theta : G \to \widehat{G}$ *be a commutative pairing and* $\mu_n \in (\mathbb{Z}/p^s\mathbb{Z})^* \subset$ *Aut(G). Fix a* p^s*th primitive root of unity* η_{p^s}*. Define* $\alpha(g, g')$ *such that* $\theta(g)(g') = (\eta_{p^s})^{\alpha(g,g')}$*. Then:*

1. $\alpha(g, g') = \alpha(g', g) \ mod\ p^s$.
2. $n\alpha(g, g') = \alpha(\mu_n \cdot g, g') \ mod\ p^s$.
3. $\alpha(\mu_n \cdot g, g') = \alpha(g, \mu_n \cdot g') \ mod\ p^s$.

4. $\alpha(g_1 + g_2, g') = \alpha(g_1, g') + \alpha(g_2, g') \ mod\ p^s$.

5. $\alpha(g, g'_1 + g'_2) = \alpha(g, g'_1) + \alpha(g, g'_2) \ mod\ p^s$.

Proof. We will show part 2 and 3. The remaining parts are trivial calculations.

To show part 2, consider:

$$\begin{aligned}(\eta_{p^s})^{\alpha(\mu_n \cdot g, g')} &= \theta(\mu_n \cdot g)(g') \\ &= (\theta(g)(g'))^n \\ &= ((\eta_{p^s})^{\alpha(g,g')})^n \\ &= (\eta_{p^s})^{n\alpha(g,g')}.\end{aligned}$$

Clearly, part 2 follows from the above equations.

To show part 3, consider the following mod p^s:

$$\begin{aligned}\alpha(\mu_n \cdot g, g') &= n\alpha(g, g') \\ &= n\alpha(g', g) \\ &= \alpha(\mu_n \cdot g', g) \\ &= \alpha(g, \mu_n \cdot g').\end{aligned}$$

□

We note that θ induces an involution $(\cdot)^* : Aut(G) \to Aut(G)$. The following proposition constructs $(\cdot)^*$.

Proposition 3.1.6. *Let $\sigma \in Aut(G)$ and θ a commutative pairing, then there is a unique $\gamma \in Aut(G)$ such that:*

$$\theta(\gamma(g))(g') = \theta(g)(\sigma(g)).$$

Proof. Let $g \in G$, clearly $\theta(g) \circ \sigma \in \widehat{G}$. Since θ is an isomorphism, there is g'' such that $\theta(g'') = \theta(g) \circ \sigma$. Define $\gamma(g) = g''$.

We proceed to show $\gamma(g)$ is a bijection. It suffices to show $\gamma(g)$ is injective, surjectivity will follow from G being finite. Let $g_1, g_2 \in G$ such that $\gamma(g_1) = \gamma(g_2)$. That is,

$$\begin{aligned} \theta(g_1) \circ \sigma &= \gamma(g_1) \\ &= \gamma(g_2) \\ &= \theta(g_2) \circ \sigma. \end{aligned}$$

Clearly, since θ is an isomorphism of abelian groups, $\theta(g_1 - g_2) \circ \sigma = \chi_0$. Thus, $G = Im(\sigma) \subset Ker(\theta(g_1 - g_2))$. Therefore, $\theta(g_1 - g_2) = \chi_0$. Hence, $g_1 - g_2 = 0$, since θ has trivial kernel. Therefore, γ is injective.

Now, we proceed to show $\mathbb{Z}$-linearity and uniqueness. It suffices to show $\mathbb{Z}$-linearly for γ, since uniqueness follows from θ having trivial kernel.

Note that $\gamma(g_1 + g_2)$ is defined as the unique g_3' such that $\theta(g_3') = \theta(g_1 + g_2) \circ \sigma$. Consider,

$$\begin{aligned} \theta(\gamma(g_1 + g_2)) &= \theta(g_3') \\ &= \theta(g_1 + g_2) \circ \sigma \\ &= (\theta(g_1) \circ \sigma)(\theta(g_2) \circ \sigma) \\ &= (\theta(\gamma(g_1)))(\theta(\gamma(g_2))) \\ &= \theta(\gamma(g_1) + \gamma(g_2)). \end{aligned}$$

Thus, $\gamma(g_1 + g_2) = \gamma(g_1) + \gamma(g_2)$. □

Definition 3.1.7. *Let $\sigma \in Aut(G)$ and θ a commutative pairing, then $(\sigma)^*$ is defined as the unique $\gamma \in Aut(G)$ such that for all $g, g' \in G$:*

$$\theta(\gamma(g))(g') = \theta(g)(\sigma(g)).$$

We note some properties of the $(\cdot)^*$ operation that we leave as exercises.

Proposition 3.1.8. *Let $\sigma, \beta \in Aut(G)$.*

1. $(\sigma\beta)^* = (\beta)^*(\sigma)^*$.

2. $((\sigma)^*)^* = \sigma$.

3. $(\sigma^{-1})^* = (\sigma^*)^{-1}$.

We can calculate the action of $Aut(G)$ on Y in terms of the action of $Aut(G)$ on X when the pairing θ is used. Proposition 3.1.9 shows this result.

Proposition 3.1.9. *Identify each χ_i with g_i via a commutative pairing θ. The action of ρ_Y on Y is given by:*

$$\rho_Y(\sigma) \;=\; \rho_X((\sigma^{-1})^*).$$

Proof. Clearly,

$$\rho_Y(\sigma)(\Omega_{\chi_i}) \;=\; \left(\frac{n}{p}\right)\Omega_{\chi_j},$$

where $\sigma \cdot \chi_i = \mu_n \cdot \chi_j$ and $n \in (\mathbb{Z}/p^s\mathbb{Z})^*$. By using the pairing θ we can deduce:

$$\begin{aligned}
\theta((\sigma^{-1})^*(g_i))(g) &= \theta(g_i)(\sigma^{-1}(g)) \\
&= \sigma \cdot \chi_i \\
&= n \cdot \chi_j \\
&= n \cdot \theta(g_j)(g) \\
&= \theta(g_j)(n^{-1} \cdot g) \\
&= \theta(n^{-1} \cdot g_j)(g).
\end{aligned}$$

Thus, $(\sigma^{-1})^*(g_i) = n^{-1} \cdot g_j$. Clearly this shows that $\rho_Y(\sigma) = \rho_X((\sigma^{-1})^*)$. □

3.1.2 Character Values of QRS

Quadratic Residue Slices have special character values; these are given by the following proposition, which was originally drafted by Chen, Sehgal, and Xiang in [6].

Proposition 3.1.10. *Let D be a QRS in G, $|G| = p^m$, $\chi \in \widehat{G}$, and let $\omega = \frac{-1+\sqrt{(\frac{-1}{p})p}}{2}$. Then, the following are true:*

1. *$\chi(D) = a_\chi + (2a_\chi + 1)\omega$, for some integer a_χ.*
2. *If $m = 2\alpha$, then $\exists \chi \ni p^\alpha \not| (2a_\chi + 1)$.*
3. *If $m = 2\alpha + 1$, then $\exists \chi \ni p^{\alpha+1} \not| (2a_\chi + 1)$.*
4. *If $m = 2\alpha + 1$ and $\forall \chi \in \widehat{G}$ $p^\alpha | (2a_\chi + 1)$, then D is a GSHDS.*

Proof. Note that, if D is a QRS, then $D(x^n) = D(x)$ for all $n \in (\mathbb{Z}/p^s\mathbb{Z})^{*2} = G_2$. Since $\chi(D(x^n)) = \mu_n(\chi(D))$, where $\mu_n \in Gal(\mathbb{Q}_{\eta_{p^s}}|\mathbb{Q}) = (\mathbb{Z}/p^s\mathbb{Z})^* = G_1$ is the Galois Automorphism corresponding to n, we must have $\mu_n(\chi(D)) = \chi(D)$ for all $\mu_n \in G_2$. Thus, $\chi(D)$ belongs to the fixed field of G_2 in $\mathbb{Q}(\eta_{p^s})$. Since this fixed field is $\mathbb{Q}(\omega)$, we must have $\chi(D) \in \mathbb{Q}(\omega)$. Also, note that $\chi(D)$ is an algebraic integer, hence, $\chi(D)$ belongs to $O_{\mathbb{Q}(\omega)} = \mathbb{Z} \bigoplus \mathbb{Z}\omega$. Thus, $\chi(D) = a_\chi + b_\chi\omega$.

Since $D(x) + D(x^{n_o}) = G(x) - [1]$, we deduce that $\chi(D) + \mu_{n_o}(\chi(D)) = -1$. Note that $\mu_{n_o}(\chi(D)) = \mu_{n_o}(a_\chi + b_\chi\omega) = a_\chi + b_\chi\mu_{n_o}(\omega)$. Since n_o is a nonquadratic residue, it is a nontrivial coset of $G_1/G_2 = Gal(\mathbb{Q}(\omega)|\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$. Thus, μ_{n_o} is the nontrivial Galois automorphism of $\mathbb{Q}(\omega)$, i.e., conjugation. Hence, $\mu_{n_0}(\omega) = \overline{\omega} = \frac{-1-\sqrt{(\frac{-1}{p})p}}{2} = -1 - \omega$.

Thus, $\mu_{n_o}(\chi(D)) = a_\chi + b_\chi(-1 - \omega) = (a_\chi - b_\chi) - b_\chi\omega$. Hence,

$$\begin{aligned} -1 &= \chi(D) + \mu_{n_o}(\chi(D)) \\ &= a_\chi + b_\chi\omega + (a_\chi - b_\chi) - b_\chi\omega \\ &= 2a_\chi - b_\chi. \end{aligned}$$

Thus, we deduce that $b_\chi = 2a_\chi + 1$. This shows part 1.

Now, we show part 2. Let n_0 be a fixed nonquadratic residue, first note that $\chi(D) = a_\chi + (2a_\chi + 1)\omega = \frac{-1+(2a_\chi+1)\sqrt{(\frac{-1}{p})p}}{2}$ and $\mu_{n_o}(\chi(D)) = a_\chi + (2a_\chi + 1)\overline{\omega} =$

$\frac{-1-(2a_\chi+1)\sqrt{(\frac{-1}{p})p}}{2}$. Hence,

$$\chi(D(x)D(x^{n_o})) = \frac{1-(2a_\chi+1)^2(\frac{-1}{p})p}{4}.$$

Let us assume otherwise, that is, $\forall\chi \in \widehat{G}$, $p^\alpha \mid 2a_\chi + 1$. Let, $2a_\chi + 1 = p^\alpha c_\chi$ for some integer c_χ. The previous analysis calculates the nontrivial character values of the element $D(x)D(x^{n_o})$ in $\mathbb{C}[G]$. These character values are given by:

$$\chi(D(x)D(x^{n_o})) = \frac{1-p^{2\alpha+1}(\frac{-1}{p})}{4}c_\chi^2.$$

Now we proceed by cases. First assume that $p = 1 \bmod 4$. Then -1 is a quadratic residue mod p^s. Hence $D(x^{-1}) = D(x)$ and

$$\begin{aligned} D(x^{-n_o}) &= \phi_{n_o}(\phi_{-1}(D(x))) \\ &= \phi_{n_o}(D(x^{-1})) \\ &= \phi_{n_o}(D(x)) \\ &= D(x^{n_o}). \end{aligned}$$

Note that $D(x)D(x^{n_o})$ evaluated at $[1]$ is $|D(x) \cap D(x^{-n_o})| = |D(x) \cap D(x^{n_o})| = 0$, since $D(x) + D(x^{n_o}) = G(x) - [1]$. Now, we proceed to calculate $D(x)D(x^{n_o})$ at $[1]$ using Fourier inversion:

$$D(x)D(x^{n_o})([1]) = \frac{1}{v}\sum_{g\in G}\chi(D(x)D(x^{n_o}))\overline{\chi([1])}.$$

Hence,

$$0 = \frac{1}{p^{2\alpha}}\{\frac{(p^{2\alpha}-1)^2}{4} + \sum_{\chi\neq\chi_0}\frac{1-p^{2\alpha+1}c_\chi^2}{4}\},$$

where χ_0 is the trivial character of G. From the above equation we deduce that:

$$p^{2\alpha}(p^{2\alpha}-1) \;=\; p^{2\alpha+1}\sum_{\chi\neq\chi_0} c_\chi^2,$$

which implies that $p \mid (p^{2\alpha}-1)$. Clearly a contradiction.

Now, we assume that $p = 3 \bmod 4$. Under this assumption -1 is nonquadratic residue, hence $-n_o$ is a quadratic residue. Thus, $D(x^{-n_o}) = D(x)$ and $|D(x) \cap D(x^{-n_o})| = |D(x)| = \frac{v-1}{2}$. Clearly, $D(x)D(x^{n_o})$ evaluated at $[1]$ is $|D(x) \cap D(x^{n_o})| = \frac{v-1}{2}$. We proceed as the previous case and we calculate $D(x)D(x^{n_o})$ at $[1]$ using Fourier inversion to get:

$$\frac{p^{2\alpha}-1}{2} \;=\; \frac{1}{p^{2\alpha}}\{\frac{(p^{2\alpha}-1)^2}{4} + \sum_{\chi\neq\chi_0}\frac{1+p^{2\alpha+1}c_\chi^2}{4}\}.$$

From the above equation we deduce once again:

$$p^{2\alpha}(p^{2\alpha}-1) \;=\; p^{2\alpha+1}\sum_{\chi\neq\chi_0} c_\chi^2$$

Hence, $p \mid (p^{2\alpha}-1)$, clearly a contradiction.

For part 3, we can use similar proof to one used in part 2.

We proceed to show part 4. We assume that $|G| = v = p^{2\alpha+1}$ and $2a_\chi + 1 = p^\alpha c_\chi$ for some integer c_χ. If we perform a similar analysis as in the proof of parts 2 and 3, that is we calculate the value of $D(x)D(x^{n_o})$ at $[1]$ using Fourier inversion; we get an equation that simplifies in both cases $p = 1$ or $p = 3 \bmod 4$ to:

$$p^{2\alpha+1}(p^{2\alpha+1}-1) \;=\; p^{2\alpha+1}\sum_{\chi\neq\chi_0} c_\chi^2.$$

Hence, $\sum_{\chi\neq\chi_0} c_\chi^2 = p^{2\alpha+1}-1$. Thus, $c_\chi^2 = 1$, since we have a sum of $p^{2\alpha+1}-1$ nonnegative integers adding up to $p^{2\alpha+1}-1$. Therefore, $2a_\chi+1 = \pm p^\alpha$ and $\chi(D(x)D(x^{n_o})) = \frac{1-(\frac{-1}{p})p^{2\alpha+1}}{4}$.

Using Fourier inversion once again, one can show that $D(x)D(x^{n_o}) = (k_o-\lambda)[1]+$

$\lambda G(x)$.[4] We proceed and show this. Let $g \in G$ be nonzero, then

$$\begin{aligned} D(x)D(x^{n_o})([g]) &= \frac{1}{v}\{(\frac{v-1}{2})^2 + \sum_{\chi \neq \chi_0} \chi(D(x)D(x^{n_o}))\overline{\chi(g)}\} \\ &= \frac{1}{v}\{\frac{(v-1)^2}{4} + \frac{1-v(\frac{-1}{p})}{4}\sum_{\chi \neq \chi_0} \overline{\chi(g)}\} \\ &= \frac{1}{4v}\{(v-1)^2 - (1-v(\frac{-1}{p})\} \\ &= \frac{v-2+(\frac{-1}{p})}{4} \\ &= \lambda. \end{aligned}$$

□

Definition 3.1.11. *Let D be a QRS in G and $\chi \in \widehat{G}$. By the previous proposition, $\chi(D) = a_\chi + (2a_\chi + 1)\omega$. We will call $d_G(\chi, D) = 2a_\chi + 1$ the* difference coefficient of D in G at χ.

Definition 3.1.12. *Let D be a QRS. The* dual of D, *denoted by $\overline{D}$ is defined in $\widehat{G}$ as*

$$\overline{D} = \{\chi \in \widehat{G}\backslash\{1\} \mid d_G(\chi, D) > 0\}.$$

Note that $\overline{D}$ is a QRS whenever D is a QRS. This is nontrivial to show, but it follows from the definition of QRSs and the following equation that we leave as an exercise.

$$d_G(\mu_n \cdot \chi, D) = (\frac{n^{-1}}{p}) d_G(\chi, D) \text{ when } n \in G_1.$$

Also, direct calculations show that in general $\overline{\overline{D}} \neq D$; however, this is true when D is a GSHDS, we will show this later.

We will prove proposition 3.1.15 as a start at calculating the character value of a general QRS D; we first prove a few lemmas that will aid in its proof.

[4] This equation will be different depending on the parity of p mod 4.

Lemma 3.1.13. *Let* $\tau = \sum_{i=1}^{p-1}(\frac{i}{p})\eta_p^i$, *where* η_p *is any primitive pth root of unity, then* $\tau^2 = (\frac{-1}{p})p$.

Proof. This is a straight-forward calculation. Consider

$$\begin{aligned}
\tau^2 &= \sum_{a,b=1,\ldots,p-1} \left(\frac{ab}{p}\right)\eta_p^{a+b} \\
&= \sum_{a,b=1,\ldots,p-1} \left(\frac{-ab}{p}\right)\eta_p^{a-b} \\
&= \sum_{a,b=1,\ldots,p-1} \left(\frac{-ab^{-1}}{p}\right)\left(\frac{b^2}{p}\right)\eta_p^{a-b} \\
&= \sum_{a,b=1,\ldots,p-1} \left(\frac{-ab^{-1}}{p}\right)\eta_p^{a-b},
\end{aligned}$$

where in the above, b^{-1} is the multiplicative inverse of b mod p. In the last equation, let $c = ab^{-1}$ and $a = bc$; these substitutions give:

$$\begin{aligned}
\tau^2 &= \sum_{b,c=1,\ldots,p-1} \left(\frac{-c}{p}\right)\eta_p^{b(c-1)} \\
&= \sum_{c=2}^{p-1}\{\left(\frac{-c}{p}\right)\sum_{b=1}^{p-1}\eta_p^{b(c-1)}\} + \sum_{b=1}^{p-1}\left(\frac{-1}{p}\right).
\end{aligned}$$

Note that $\eta_p' = \eta_p^{c-1}$ is again a primitive pth root of unity and thus a conjugate of η_p. Therefore, both η_p and η_p' are roots of the same irreducible polynomial $\phi_p(x)$ over the $\mathbb{Q}$. Hence, $1 + \eta_p' + \eta_p'^2 + \cdots \eta_p'^{p-1} = 0$ since $\phi_p(x) = 1 + x + \cdots + x^{p-1}$. Thus, $\sum_{b=1}^{p-1}(\eta_p^{c-1})^b = \sum_{b=1}^{p-1}(\eta_p')^b = -1$. Therefore, our calculation of τ^2 simplifies to:

$$\begin{aligned}
\tau^2 &= -\sum_{c=2}^{p-1}\left(\frac{-c}{p}\right) + (p-1)\left(\frac{-1}{p}\right) \\
&= p\left(\frac{-1}{p}\right) - \sum_{c=1}^{p-1}\left(\frac{-c}{p}\right) \\
&= p\left(\frac{-1}{p}\right) - \left(\frac{-1}{p}\right)\sum_{c=1}^{p-1}\left(\frac{c}{p}\right).
\end{aligned}$$

Consider,

$$\begin{aligned}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right) &= \sum_{c\in(\mathbb{Z}/p\mathbb{Z})^*}\psi(c)\\ &= \psi((\mathbb{Z}/p\mathbb{Z})^*),\end{aligned}$$

where ψ is a the Quadratic Residue symbol that is viewed as a multiplicative character of the group $(\mathbb{Z}/p\mathbb{Z})^*$. Since ψ is nontrivial on $(\mathbb{Z}/p\mathbb{Z})^*$, we must have $\psi((\mathbb{Z}/p\mathbb{Z})^*) = 0$. Thus, the calculation of τ^2 simplifies to:

$$\begin{aligned}\tau^2 &= \left(\frac{-1}{p}\right)p - \left(\frac{-1}{p}\right)\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\\ &= \left(\frac{-1}{p}\right)p - \left(\frac{-1}{p}\right)\psi((\mathbb{Z}/p\mathbb{Z})^*)\\ &= \left(\frac{-1}{p}\right)p,\end{aligned}$$

hence, the result follows. □

Lemma 3.1.14. *Let p be an odd prime and η_p a pth root of unity. Let $\omega = \sum\{\eta_p^n \mid \left(\frac{n}{p}\right) = 1$ and $1 \le n \le p-1\}$ and $\overline{\omega} = \sum\{\eta_p^n \mid \left(\frac{n}{p}\right) = -1$ and $1 \le n \le p-1\}$. Then,*

1. $\omega + \overline{\omega} = -1$,
2. $\omega = \frac{-1\pm\sqrt{(\frac{-1}{p})p}}{2}$,
3. $\overline{\omega} = \frac{-1\mp\sqrt{(\frac{-1}{p})p}}{2}$.

Proof. Note that, the irreducible polynomial $\phi_p(x)$ of η_p over the rationals $\mathbb{Q}$ is $\phi_p(x) = 1 + x + \cdots + x^{p-1}$. Hence, $0 = 1 + \sum_{i=1}^{p-1}\eta_p^i = 1 + \omega + \overline{\omega}$. This shows part 1.

To show part 2 and part 3, we will make use of the Gauss sum $\tau = \sum_{i=1}^{p-1}(\frac{i}{p})\eta_p^i$. For the following, let $\omega_0 = \omega$ and $\omega_1 = \overline{\omega}$. Note that $\tau = \omega_0 - \omega_1 = 1 + 2\omega_0$. Thus, by lemma 3.1.13, we have $(\frac{-1}{p})p = (1+2\omega_0)^2$. Hence, $\omega_0 = \frac{-1\pm\sqrt{(\frac{-1}{p})p}}{2}$ and parts 2 and 3 follow. □

For the rest of the chapter, we will choose η_p such that $\omega = \frac{-1+\sqrt{(\frac{-1}{p})p}}{2}$ and $\overline{\omega} = \frac{-1-\sqrt{(\frac{-1}{p})p}}{2}$.

Proposition 3.1.15. *Let O_g be the G_2 orbit of $g \in G$ and $\chi \in \widehat{G}$. Then*

$$\chi(O_g) = \begin{cases} \omega o(p \cdot g) & \text{if } \chi(g) = \eta_p^n, (\frac{n}{p}) = 1, \\ \overline{\omega} o(p \cdot g) & \text{if } \chi(g) = \eta_p^n, (\frac{n}{p}) = -1, \\ |O_g| & \text{if } \chi(g) = 1, \\ 0 & \text{else,} \end{cases}$$

where $o(p \cdot g)$ is the order of the element $p \cdot g = g + \cdots + g$, i.e., g summed p times, $\omega = \frac{-1+\sqrt{(\frac{-1}{p})p}}{2}$ and $\overline{\omega} = \frac{-1-\sqrt{(\frac{-1}{p})p}}{2}$.

Proof. Note that $G_1 = K \times H = (\mathbb{Z}/(p-1)\mathbb{Z}) \times (\mathbb{Z}/p^{s-1}\mathbb{Z})$ via the decomposition $n = n_0(1 + pb_1 + p^2b_2 + \cdots + p^{s-1}b_{s-1})$, where $n_0 \in (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/(p-1)\mathbb{Z} = K$ and $1 + pb_1 + \cdots + p^{s-1}b_{s-1} \in H$ with $b_i \in \{0, \ldots, p-1\}$. Another form of H is $\{n \in G_1 | n = 1 \bmod p\}$. From this decomposition of G_1, a decomposition of G_2 follows as $G_2 = K^2 \times H = (\mathbb{Z}/p\mathbb{Z})^{*2} \times H$. Hence, $O_g = \sum_{1 \le i \le p-1, (\frac{i}{p})=1} [i \cdot g]\langle p \cdot g \rangle$ where: $i \cdot g = g + \cdots + g$, g summed i times; $p \cdot g = g + \cdots + g$, g summed p times; and $\langle p \cdot g \rangle$ is the group generated by $p \cdot g$. Thus,

$$\chi(O_g) = \sum_{1 \le i \le p-1, (\frac{i}{p})=1} \chi(i \cdot g))\chi(\langle p \cdot g \rangle).$$

Since G is an abelian group, $\chi(\langle p \cdot g \rangle)$ changes values depending on the restriction of χ to $\langle p \cdot g \rangle$. That is,

$$\chi(\langle p \cdot g \rangle) = \begin{cases} o(p \cdot g) & \text{if } \chi(p \cdot g) = 1, \\ 0 & \text{if } \chi(p \cdot g) \neq 1. \end{cases}$$

Also note that when $\chi(p \cdot g) = 1$, we must have $\chi(g) = \eta_p^n$ for some $n \in \{0, \ldots, p-1\}$ depending on g and χ. Let us assume, $n \neq 0$, then

$$\begin{aligned}\sum_{1\le i\le p-1,\left(\frac{i}{p}\right)=1}\chi(i\cdot g) &= \sum_{1\le i\le p-1,\left(\frac{i}{p}\right)=1}\eta_p^{in}\\ &= \begin{cases}\omega_0=\omega & \text{if } \left(\frac{n}{p}\right)=1,\\ \omega_1=\overline{\omega} & \text{if } \left(\frac{n}{p}\right)=-1,\end{cases}\end{aligned}$$

where we use the notation and results of lemma 3.1.14 in the above equation.

Combining the deductions of the above paragraphs gives the conclusion of the proposition. □

Corollary 3.1.16. *Let $m \in G_1$, then*

$$\chi(O_{m\cdot g}) = \begin{cases}\omega o(p\cdot g) & \text{if } \chi(g)=\eta_p^n, \left(\frac{mn}{p}\right)=1,\\ \overline{\omega} o(p\cdot g) & \text{if } \chi(g)=\eta_p^n, \left(\frac{mn}{p}\right)=-1,\\ |O_g| & \chi(g)=1,\\ 0 & \text{else.}\end{cases}$$

Proof. This is a consequence of the previous proposition and the fact that: if $\chi(g) = \eta_p^n$, then $\chi(m\cdot g)=\eta_p^{mn}$. □

Now, we are ready to calculate the character value an arbitrary QRS D.

Proposition 3.1.17. *Let $D=\sum_{i=1}^r O_{\beta_i\cdot g_i}$ be a general QRS, where $\beta_i \in \{1, n_0\}$. Let $\chi \in \widehat{G}$, then $\chi(D) = a_\chi + d_G(\chi, D)\omega$ where:*

$$\begin{aligned} d_G(\chi,D) &= \sum\left\{\left(\frac{n\beta_i}{p}\right)o(p\cdot g_i) \mid \chi(g_i)=\eta_p^n\right\},\\ a_\chi &= \sum\{|O_{g_i}| \mid \chi(g_i)=1\} - \sum\left\{o(p\cdot g_i) \mid \chi(g_i)=\eta_p^n, \left(\frac{n\beta_i}{p}\right)=-1\right\},\\ a_\chi &= \frac{d_G(\chi,D)-1}{2},\end{aligned}$$

where η_p is a fixed primitive pth root of unity such that,

$$\begin{aligned}\omega &= \sum\left\{\eta_p^n \mid \left(\frac{n}{p}\right) = 1, 1 \leq n \leq p-1\right\} \\ &= \frac{-1+\sqrt{\left(\frac{-1}{p}\right)p}}{2}.\end{aligned}$$

Proof. From corollary 3.1.16, we have:

$$\begin{aligned}\chi(D) &= \sum_{i=1}^{r}\chi(O_{\beta_i\cdot g_i}) \\ &= f_\chi + g_\chi\omega + h_\chi\overline{\omega} \\ &= (f_\chi - h_\chi) + (g_\chi - h_\chi)\omega,\end{aligned}$$

where,

$$\begin{aligned}f_\chi &= \sum\left\{|O_{g_i}| \mid \chi(g_i) = 1\right\}, \\ g_\chi &= \sum\left\{o(p\cdot g_i) \mid \chi(g_i) = \eta_p^n, \left(\frac{n\beta_i}{p}\right) = 1\right\}, \\ h_\chi &= \sum\left\{o(p\cdot g_i) \mid \chi(g_i) = \eta_p^n, \left(\frac{n\beta_i}{p}\right) = -1\right\}.\end{aligned}$$

The result follows from the above equations. □

3.1.3 The QRS Incidence Structure $\mathbf{A_{G,G_1}}$

Proposition 3.1.17 motivates the definition of an incidence structure that will prove helpful when determining the character values of a general QRS D.

Definition 3.1.18. *Let $g_1, \ldots, g_r$ be the orbit representatives of the action of G_1 on $G\backslash\{0\}$. Let $\theta : G \to \widehat{G}$ be any commutative pairing. Let $\chi_i = \theta(g_i)$. Clearly, $\chi_1, \ldots, \chi_r$ are orbit representatives of the action of G_1 on $\widehat{G}\backslash\{1\}$. The G_1* QRS incidence structure on G, *called A_{G,G_1}, is defined by:*

$$A_{G,G_1}(\Omega_{\chi_i}, \Omega_{g_j}) = \left(\frac{f_0(\alpha(g_i, g_j))}{p}\right)o(p\cdot g_j),$$

where $\alpha(g_i, g_j)$ is defined by proposition 3.1.5 by:

$$\theta(g_i)(g_j) \;=\; \eta_{p^s}^{\alpha(g_i,g_j)},$$

where $\eta_p = (\eta_{p^s})^{p^{s-1}}$ satisfies the assumptions of proposition 3.1.17; and, $f_0(x) : (\mathbb{Z}/p^s\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})$ is a function defined by:

$$f_0(x) \;=\; \begin{cases} y & \text{if } x = p^{s-1}y \bmod p^s, \\ 0 & \text{else.} \end{cases}$$

For the rest of the chapter, we will assume that g_is and χ_is are chosen as in definition 3.1.18. That is, they are paired via a noncanonical isomorphism $\theta : G \to \widehat{G}$ such that $\theta(g)(g') = \theta(g')(g)$.

The definition of A_{G,G_1} motivates the introduction of the function $\alpha'(g, g') = f_0(\alpha(g, g'))$ that is understood as a function $\alpha' : G \times G \to (\mathbb{Z}/p\mathbb{Z})$. Clearly, α' is no longer "bilinear," however, α' inherets some properties of α. This is summarized by the following proposition.

Proposition 3.1.19. *Let $g, g' \in G$, $\sigma \in Aut(G)$, and $n \in (\mathbb{Z}/n\mathbb{Z})^*$, then modulo p:*

1. $\alpha'(g, g') = \alpha'(g', g)$,
2. $n\alpha'(g, g') = \alpha'(\mu_n \cdot g, g')$,
3. $\alpha'(\mu_n \cdot g, g') = \alpha'(g, \mu_n \cdot g')$,
4. $\alpha'((\sigma)^* \cdot g, g') = \alpha'(g, \sigma \cdot g')$.

Proof. Clearly, these are trivial calculations. □

The following result on A_{G,G_1} and the difference coefficients of an arbitrary QRS D paraphrases proposition 3.1.17.

Proposition 3.1.20. *If D is a QRS such that $D = \sum_{i=1}^{r} O_{\beta_i \cdot g_i}$, then the difference*

coefficients of D are given by:

$$A_{G,G_1}\begin{pmatrix} d_1 \\ \vdots \\ d_r \end{pmatrix} = \begin{pmatrix} d_G(\chi_1, D) \\ \vdots \\ d_G(\chi_r, D) \end{pmatrix},$$

where $d_i = \left(\frac{\beta_i}{p}\right)$.

The following proposition shows that A_{G,G_1} is indeed an $Aut(G)$ map from X, the QRS space of G, to Y,the QRS space of $\widehat{G}$.

Proposition 3.1.21. *The matrix A_{G,G_1} is an $Aut(G)$ map from X to Y. More precisely, for any $\sigma \in Aut(G)$:*

$$\rho_X(((\sigma)^*)^{-1})A_{G,G_1} = A_{G,G_1}\rho_X(\sigma),$$

where we view A_{G,G_1} as a matrix on $X \times X$ by defining it as:

$$A_{G,G_1}(\Omega_{g_i}, \Omega_{g_j}) = A_{G,G_1}(\Omega_{\theta(g_i)}, \Omega_{g_j}).$$

Proof. Let $A = A_{G,G_1}$ and $\sigma \in Aut(G)$. Clearly,

$$\begin{aligned} A(\Omega_{g_i}, \Omega_{g_j}) &= A(\Omega_{\chi_i}, \Omega_{g_j}) \\ &= \left(\frac{\alpha'(g_i, g_j)}{p}\right) o(p \cdot g_j). \end{aligned}$$

Note that,

$$\begin{aligned} A(\Omega_{\chi_i}, \Omega_{\sigma(g_j)}) &= \left(\frac{\alpha'(g_i, \sigma(g_j))}{p}\right) o(p \cdot g_j) \\ &= \left(\frac{\alpha'((\sigma)^*(g_i), g_j)}{p}\right) o(p \cdot g_j). \end{aligned}$$

Let $\sigma(g_j) = \mu_n \cdot g'_j$, where $n \in (\mathbb{Z}/p^s\mathbb{Z})^*$. Identify $\Omega_{\sigma(g_j)}$ with $\Omega_{g'_j}$. Consider:

$$\begin{aligned}
A\rho_X(\sigma)\Omega_{g_j} &= \left(\frac{n}{p}\right) A\Omega_{g'_j} \\
&= \left(\frac{n}{p}\right) \sum_{i=1}^{r} A(\Omega_{g_i}, \Omega_{g'_j})\Omega_{g_i} \\
&= \left(\frac{n}{p}\right) \sum_{i=1}^{r} \left(\frac{\alpha'(g_i, g'_j)}{p}\right) o(p \cdot g'_j)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{n\alpha'(g_i, g'_j)}{p}\right) o(p \cdot g'_j)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{\alpha'(g_i, \mu_n \cdot g'_j)}{p}\right) o(p \cdot g'_j)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{\alpha'(g_i, \sigma(g_j))}{p}\right) o(p \cdot g'_j)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{\alpha'((\sigma)^*(g_i), g_j)}{p}\right) o(p \cdot g_j)\Omega_{g_i}.
\end{aligned}$$

Define $n_i \in (\mathbb{Z}/p^s\mathbb{Z})^*$ be such that $(\sigma)^* \cdot g_i = \mu_{n_i} \cdot g'_i$ then:

$$\begin{aligned}
A\rho_X(\sigma)\Omega_{g_j} &= \sum_{i=1}^{r} \left(\frac{\alpha'((\sigma)^*(g_i), g_j)}{p}\right) o(p \cdot g_j)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{\alpha'(\mu_{n_i} \cdot g'_i, g_j)}{p}\right) o(p \cdot g_j)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{n_i}{p}\right)\left(\frac{\alpha'(g'_i, g_j)}{p}\right) o(p \cdot g_j)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{\alpha'(g'_i, g_j)}{p}\right) o(p \cdot g_j)\left(\frac{n_i}{p}\right)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{\alpha'(g'_i, g_j)}{p}\right) o(p \cdot g_j)\left(\frac{n_i^{-1}}{p}\right)\Omega_{g_i} \\
&= \sum_{i=1}^{r} \left(\frac{\alpha'(g'_i, g_j)}{p}\right) o(p \cdot g_j)\rho_X(((\sigma)^*)^{-1})\Omega_{g'_i} \\
&= \rho_X(((\sigma)^*)^{-1})A\Omega_{g_j}.
\end{aligned}$$

□

In addition to being an $Aut(G)$-map, the matrix A_{G,G_1} also satisfies a simple equation that will be shown later.

Proposition 3.1.22. *The matrix A_{G,G_1} satisfies:*

$$A_{G,G_1}^2 = \frac{|G|}{p} I.$$

The equation of proposition 3.1.22 will prove to be an useful tool in studying GSHDS. The following corollary is an example of its usefulness.

Corollary 3.1.23. *Let D be a GSHDS and $\overline{D}$ its dual. Then,*

1. *$\overline{D}$ is a GSHDS.*
2. *$\overline{\overline{D}} = D$.*

Proof. Let $|G| = v = p^{2\alpha+1}$. Let $D = \sum_{i=1}^{r} O_{\beta_i \cdot g_i}$ and d be the $r \times 1$ vector in the QRS space X, where $d_i = (\frac{\beta_i}{p})$. Clearly, $A_{G,G_1} d = (d_G(\chi_1, D), \ldots, d_G(\chi_r, D))^T$ is the vector of distinct difference coefficients of D. Since D is a GSHDS, by proposition 3.1.10 part 4 we have $d_G(\chi_i, D) = p^\alpha \epsilon_i$, where $\epsilon_i \in \{1, -1\}$. Hence,

$$A_{G,G_1} d = p^\alpha \overline{d},$$

where $\overline{d}$ is the $r \times 1$ vector given by

$$\overline{d_i} = \begin{cases} 1 & \text{if } d_G(\chi_i, D) > 0, \\ -1 & \text{if } d_G(\chi_i, D) < 0. \end{cases}$$

Clearly, if the dual of D is given by $\overline{D} = \sum_{i=1}^{r} O_{\gamma_i \cdot \chi_i}$, where $\gamma_i \in \{1, n_0\}$; then $\left(\frac{\gamma_i}{p}\right) = \overline{d_i}$ by construction. Hence, $\overline{d}$ is a representation of $\overline{D}$.

Multiplying the above equation by A_{G,G_1} and using proposition 3.1.22, we deduce:

$$A_{G,G_1} \overline{d} = p^\alpha d,$$

hence, $\overline{D}$ is a GSHDS by proposition 3.1.10 part 4. In particular, we also deduce $\overline{\overline{d}} = d$.

Since $\overline{d}$ is the representation of $\overline{D}$ and $\overline{\overline{d}} = d$, we must have $\overline{\overline{D}} = D$. □

As a closing remark, we note that A_{G,G_1} appears in the calculation of the character values of elements of the space of Compact QRSs of G.

Proposition 3.1.24. *Let* $W = \bigoplus_{i=1}^{r} \mathbb{C}(O_{g_i} - O_{g_i}^{(n_0)})$ *and* $a = \sum_{i=1}^{r} a_i(O_{g_i} - O_{g_i}^{(n_0)})$ *where* $a_i \in \mathbb{C}$*, then:*

1. *Let* $\chi_j = \theta(g_j) \in \widehat{G}$*, then:*

$$\begin{aligned} \chi_j(O_{g_i} - O_{g_i}^{(n_0)}) &= \left(\frac{\alpha'(g_j, g_i)}{p}\right) o(p \cdot g_i) \sqrt{\left(\frac{-1}{p}\right) p} \\ &= A_{G,G_1}(O_{\chi_j}, O_{g_i}) \sqrt{\left(\frac{-1}{p}\right) p}. \end{aligned}$$

2. *Let* $\chi_j = \theta(g_j) \in \widehat{G}$*, then:*

$$\chi_j(a) = \left(\sum_{i=1}^{r} A_{G,G_1}(O_{\chi_j}, O_{g_i}) a_i\right) \sqrt{\left(\frac{-1}{p}\right) p}.$$

Proof. Part 1 is a clear application of proposition 3.1.15 and the definition of A_{G,G_1}. Part 2 is an application of part 1. □

3.2 Difference Coefficients

In this section, we will study properties of the difference coefficients that arise from an arbitrary QRS D in an abelian p-group G. We will work toward stablishing the generalized version of Xiang's exponent bound, i.e., proposition 1.2.1 part 4b. We will use the notation and assumptions of the previous sections.

We start with a reduction formula that is due to Chen, Sehgal, and Xiang in the language of Skew Hadamard Differenc Sets.

Proposition 3.2.1. *Let D be a QRS in G, $G' \subset G$, and $D' = G' \cap D$. Let $\chi' \in \widehat{G'}$ and $L^G_{G'}(\chi') = \{\chi \in \widehat{G} \mid \chi|_{G'} = \chi'\}$. Then:*

1. *$G'^T \simeq \widehat{(\frac{G}{G'})}$, where $G'^T = \{\chi \in \widehat{G} \mid \chi|_{G'} = 1\}$.*

2. *Every character $\chi' \in \widehat{G'}$ can be extended into a character χ_1 of G exactly $|G'^T| = [G : G']$ times. That is, the set $L^G_{G'}(\chi') = \chi_1 G'^T$ where χ_1 is any extension of χ' from G' to G.*

3. *The difference coefficients obey the formula:*

$$d_{G'}(\chi', D') \;=\; \frac{1}{[G : G']} \sum_{\chi \in L^G_{G'}(\chi')} d_G(\chi, D).$$

Proof. To show part 1, note that one can define a map $\kappa : G'^T \to \widehat{(\frac{G}{G'})}$ by $\kappa(\chi)(gG') = \chi(g)$ for a given $\chi \in G'^T$. If $g = g_1 g'$ for some $g' \in G'$, then $\chi(g) = \chi(g_1 g') = \chi(g_1)\chi(g') = \chi(g_1)$. Thus, $\kappa(\chi) \in \widehat{(\frac{G}{G'})}$ is well defined. Note that, if $\kappa(\chi_1) = \kappa(\chi_2)$, then $\chi_1 = \chi_2$ by definition. Hence, κ is injective. To show surjectivity, let $\widehat{\chi} \in \widehat{(\frac{G}{G'})}$. Consider the character $\chi = \widehat{\chi} \circ \pi$, where $\pi : G \to \frac{G}{G'}$ is the canonical projection of G onto the factor group $\frac{G}{G'}$. Clearly, $\kappa(\chi) = \widehat{\chi}$. This shows part 1.

To show part 2, consider the restriction map $\theta : \widehat{G} \to \widehat{G'}$ by $\theta(\chi) = \chi\,|_{G'}$. We show that θ is onto. Let $ker(\theta) = G'^T = \{\chi \in \widehat{G} \mid \chi\,|_{G'} = 1\}$. Note that $\chi \in Ker(\theta)$ if and only if $\widehat{\chi} \in \widehat{(\frac{G}{G'})}$.[5] Hence, $|Ker(\theta)| = \frac{|G|}{|G'|}$. Thus, the image of θ, which is isomorphic to $\frac{\widehat{G}}{Ker(\theta)}$, has order $\frac{|\widehat{G}|}{|Ker(\theta)|} = |G'|$ and must be all of G'. Thus, θ is onto.

Note that $L^G_{G'}(\chi') = \theta^{-1}(\chi') = \chi_1 G'^T$, where χ_1 is any fixed extension of χ' to all of G. By the above, $|L^G_{G'}(\chi')| = |Ker(\theta)| = [G : G']$. This shows part 2.

To show part 3, let $G = (g_1 + G') \cup (g_2 + G') \cup \cdots \cup (g_r + G')$, where $g_1 = 0$ and $r = [G : G']$. Note that $D = D' \cup (g_2 + D_2) \cup \cdots \cup (g_r + D_r)$, where $D_i \subset G'$ such that $D \cap (g_i + G') = g_i + D_i$.

[5] where $\widehat{\chi}(gG') = \chi(g)$.

Consider the sum:

$$\begin{aligned}
\sum_{\chi\in L^G_{G'}(\chi')}\chi(D) &= \sum_{\chi\in G'^T}(\chi_1\chi)(D)\\
&= \sum_{\chi\in G'^T}\{(\chi_1\chi)(D')+(\chi\chi_1)(g_2+D_2)+\cdots+(\chi\chi_1)(g_r+D_r)\}\\
&= \sum_{\chi\in G'^T}\{\chi_1(D')+\chi(g_2)\chi_1(g_2)\chi_1(D_2)+\cdots+\chi(g_r)\chi_1(g_r)\chi_1(D_r)\}\\
&= [G:G']\chi'(D')+\chi_1(g_2)\chi_1(D_2)\sum_{\chi\in G'^T}\chi(g_2)+\cdots+\\
&\quad +\chi_1(g_r)\chi_1(D_r)\sum_{\chi\in G'^T}\chi(g_r).
\end{aligned}$$

Since $G'^T\simeq\frac{\widehat{G}}{G'}$ via the pairing $\chi\in G'^T$ with $\widehat{\chi}\in\widehat{(\frac{G}{G'})}$; we have, whenever $g_i\notin G'$, by the second orthogonality relation:

$$\begin{aligned}
\sum_{\chi\in G'^T}\chi(g_i) &= \sum_{\widehat{\chi}\in\widehat{(\frac{G}{G'})}}\widehat{\chi}(g_iG')\\
&= 0.
\end{aligned}$$

Hence,

$$\sum_{\chi\in L^G_{G'}(\chi')}\chi(D) = [G:G']\chi'(D').$$

Clearly, D' is a QRS as D is a QRS. Thus,

$$[G:G'](a_{\chi'}+d_{G'}(\chi',D')\omega) = \sum_{\chi\in L^G_{G'}(\chi')}\{a_\chi+d_G(\chi,D)\omega\}.$$

By equating the ω-coordinate on both sides of the above equation we get the conclusion. □

The next result is an application of the previous proposition.

Corollary 3.2.2. *Let D be GSHDS in G and $G'\subset G$ a subgroup with $D'=D\cap G'$.*

Let $p^{2\alpha+1} = |G|$ *and* $\chi' \in \widehat{G'}$*. Then,*

$$d_{G'}(\chi', D') = \frac{|G'|}{p^{\alpha+1}}\{|\overline{D} \cap \chi_1 G'^T| - |\overline{D}^{(n_0)} \cap \chi_1 G'^T|\},$$

where n_0 *is a Non-Quadratic Residue in* $(\mathbb{Z}/p^s\mathbb{Z})^*$*,* $p^s = exp(G)$*; and* $\overline{D}$ *is the dual QRS of* D *in* G*.*

Proof. Clearly, since D is a GSHDS, $d_G(\chi, D) = p^\alpha \epsilon_\chi$; where $\epsilon_\chi \in \{1, -1\}$. Hence, by proposition 3.2.1 part 3, we have:

$$d_{G'}(\chi', D') = \frac{|G'|}{p^{\alpha+1}} \sum_{\chi \in \chi_1 G'^T} \epsilon_\chi,$$

where we have chosen a fixed arbitrary extension χ_1 of χ' to G. Note that by definition of $\overline{D}$,

$$\sum_{\chi \in \chi_1 G'^T} \epsilon_\chi = |\overline{D} \cap \chi_1 G'^T| - |\overline{D}^{(n_0)} \cap \chi_1 G'^T|.$$

Thus, the result follows. □

The right-hand side of corollary 3.2.2 motivates the definition of the difference intersection numbers.

Definition 3.2.3. *Let* D *be a QRS in* G*,* $L \subset G$ *be a subgroup,* $\frac{G}{L} = \{g'_1 L, \ldots, g'_s L\}$*. The* difference intersection numbers of D with respect to L in G *are defined as:*

$$\nu_{G,L}(D, g'_i) = |D \cap g'_i L| - |D^{(n_0)} \cap g'_i L|.$$

The difference intersection numbers will occur in some calculations that will follow. We will show a relationship of the difference intersection numbers to the difference coefficients at the end of the section. For now, we point out the the G_2-invariance of the $\nu_{G,L}(D, g')$s.

Proposition 3.2.4. *Let $l \in G$ and $L \subset G$ a subgroup. Assume $n \in (\mathbb{Z}/p^s\mathbb{Z})^* = G_1$, then:*

$$\nu_{G,L}(D, \mu_n \cdot l_i) = \left(\frac{n}{p}\right)\nu_{G,L}(D, l_i).$$

Proof. Clearly, μ_n is a bijection of G and hence of $\frac{G}{L}$. Also, since D is a QRS,

$$\mu_n \cdot D = \begin{cases} D & \text{if } \left(\frac{n}{p}\right) = 1, \\ D^{(n_0)} & \text{if } \left(\frac{n}{p}\right) = -1, \end{cases}$$

$$\mu_n \cdot D^{(n_0)} = \begin{cases} D & \text{if } \left(\frac{n}{p}\right) = -1, \\ D^{(n_0)} & \text{if } \left(\frac{n}{p}\right) = 1. \end{cases}$$

Consider,

$$\begin{aligned} \nu_{G,L}(D, \mu_n \cdot l_i) &= |D \cap (\mu_n \cdot l_i L)| - |D^{(n_0)} \cap (\mu_n \cdot l_i L)| \\ &= |(\mu_n^{-1} \cdot D) \cap l_i L| - |(\mu_n^{-1} \cdot D^{(n_0)}) \cap l_i L| \\ &= \begin{cases} \nu_{G,L}(D, l_i) & \text{if } \left(\frac{n}{p}\right) = 1, \\ -\nu_{G,L}(D, l_i) & \text{if } \left(\frac{n}{p}\right) = -1. \end{cases} \end{aligned}$$

Hence, the conclusion follows. □

The next result has been shown by Chen, Sehgal, and Xiang for Skew Hadamard Difference Sets [6]. This result will be used in the proof Xiang's exponent bound.

Proposition 3.2.5. *Let G be an abelian p-group and $|G| = p^m$. Let $K_l = \{g \mid p^l \cdot g = 0\}$, D be a QRS, and $|K_l| = p^{l'}$. If $l \geq \lfloor \frac{l'+1}{2} \rfloor$, then there are at least $|K_l^T| = p^{m-l'}$ characters χ such that $p^l \not| d_G(\chi, D)$.*

Proof. Define $\phi : G \to G$ by $\phi(g) = p^l \cdot g$. Let $K = Ker(\phi) = K_l$ and $D_{K_l} = D \cap K_l$, $D_0 = D \backslash D_{K_l}$. Clearly, both D_{K_l} and D_0 are invariant under the action of the quadratic residues. Also, note that if $D = \sum_{i=1}^{r} O_{\beta_i \cdot g_i}$, then $D_0 = \sum\{O_{\beta_i \cdot g_i} \mid o(g_i) > p^l\}$ and $D_{K_l} = \sum\{O_{\beta_i \cdot g_i} \mid o(g_i) \leq p^l\}$.

Consider,

$$\begin{aligned} d_G(\chi, D) &= \sum \left\{ \left(\frac{n\beta_i}{p} \right) o(p \cdot g_i) \mid \chi(g_i) = \eta_p^n \right\} \qquad (3.6) \\ &= \sum \left\{ \left(\frac{n\beta_i}{p} \right) o(p \cdot g_i) \mid \chi(g_i) = \eta_p^n, o(g_i) \leq p^l \right\} \\ &\quad + \sum \left\{ \left(\frac{n\beta_i}{p} \right) o(p \cdot g_i) \mid \chi(g_i) = \eta_p^n, o(g_i) > p^l \right\} \\ &= \sum \left\{ \left(\frac{n\beta_i}{p} \right) o(p \cdot g_i) \mid \chi(g_i) = \eta_p^n, o(g_i) \leq p^l \right\} \bmod p^l \\ &= d_{K_l}(\chi|_{K_l}, D_{K_l}) \bmod p^l. \end{aligned}$$

By proposition 3.1.10 parts 2 and 3, there is $\chi' \in \widehat{K_l}$ such that $p^{\lfloor \frac{l'+1}{2} \rfloor}$ does not divide $d_{K_l}(\chi', D_{K_l})$. Since $\lfloor \frac{l'+1}{2} \rfloor \leq l$, we must have p^l does not divide $d_{K_l}(\chi', D_{K_l})$.

By Equation (3.6), we have that any extension of χ of χ' to G has the property $d_G(\chi, D) = d_{K_l}(\chi', D_{K_l}) \bmod p^l$. Since p^l does not divide $d_{K_l}(\chi', D_{K_l})$, we must have p^l not divide $d_G(\chi, D)$. Since there are $|K_l^T| = [G : K_l] = p^{m-l'}$ extensions of χ' to a character χ of G, we must have at least $p^{m-l'}$ characters χ such that p^l does not divide $d_G(\chi, D)$. □

Corollary 3.2.6. *Let $G = \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z}$, then for any D, a QRS, there are at least $p^{2(s-1)}$ characters $\chi \in \widehat{G}$ such that p does not divide $d_G(\chi, D)$.*

Proof. We will use proposition 3.2.5 by letting $l = 1$. A direct calculation gives $K_1 = \langle (p^{s-1}, 0), (0, p^{s-1}) \rangle$. Thus, $|K_1| = p^2$ and $|K_1^T| = p^{2(s-1)}$. Since $1 \geq \lfloor \frac{2+1}{2} \rfloor = 1$, we can apply proposition 3.2.5 and conclude that there $p^{2(s-1)}$ characters $\chi \in \widehat{G}$ such that p does not divide $d_G(\chi, D)$. □

The next result is the generalization of Xiang's exponent bound. It can be found in [6] in the context for Skew Hadamard Difference Sets.

Proposition 3.2.7. *Let D be GSHDS in G where $|G| = p^{2\alpha+1}$ and $p^s = exp(G)$. Then,*

$$s \leq \frac{\alpha + 1}{2}.$$

Proof. Note that, if G is elementary abelian, then the result follows. So let us assume that G is not elementary abelian. By proposition 3.0.8, we have that $G = \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^{a_3}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_l}\mathbb{Z}$ where $s \geq a_3 \geq \cdots \geq a_l$. Let $G' = \mathbb{Z}/p^s\mathbb{Z} \times \mathbb{Z}/p^s\mathbb{Z} \subset G$ and $D' = D \cap G'$. By corollary 3.2.6, there is $\chi' \in \widehat{G'}$ such that p does not divide $d_{G'}(\chi', D')$. Let χ_1 be an extension of χ' from G' to G. By corollary 3.2.2, we deduce the following.

$$\begin{aligned} d_{G'}(\chi', D') &= \frac{|G'|}{p^{\alpha+1}}\{|\overline{D} \cap \chi_1 G'^T| - |\overline{D}^{(n_0)} \cap \chi_1 G'^T|\} \\ &= p^{2s-(\alpha+1)}\{|\overline{D} \cap \chi_1 G'^T| - |\overline{D}^{(n_0)} \cap \chi_1 G'^T|\}. \end{aligned}$$

By the choice of χ', we must have p not dividing $d_{G'}(\chi', D')$. This forces the exponent of p in the above equation to be negative. Hence, giving the result. □

We close this section with a result that shows a relationship between the difference intersection numbers and the difference coefficients.

Proposition 3.2.8. *Let $\pi : G \to H$ be a group homeomorphsim that is surjective with kernel $Ker(\pi) = L$. Let θ_G be a commutative pairing of G and choose the restriction of θ to H as the commutative pairing of H. That is, $\theta_H = \theta_G \mid_H$.*

Let $h_1, \ldots, h_s$ be a complete set of H_1-representatives of $H\backslash\{0\}$ and define $\chi_i = \theta_H(h_i)$ as the corresponding complete set of H_1-representatives of $\widehat{H}\backslash\{1\}$. Choose g_i' to be any lift of h_i under π, i.e., g_i' is chosen so that $\pi(g_i') = h_i$. Extend each χ_i to a character of G by letting $\chi_i' = \chi_i \circ \pi$. Then,

$$A_{H,H_1}\begin{pmatrix} \nu_{G,L}(D, g_1') \\ \vdots \\ \nu_{G,L}(D, g_s') \end{pmatrix} = \begin{pmatrix} d_G(D, \chi_1') \\ \vdots \\ d_G(D, \chi_s') \end{pmatrix}.$$

Proof. We will consider $D(x) - D(x^{n_0})$ in $\mathbb{Z}[G]$. By applying the projection π, we

will deduce:

$$\pi(D - D^{(n_0)}) \;=\; \sum_{i=1}^{s} \nu_{G,L}(D, g_i')(O_{h_i} - O_{h_i}^{(n_0)}). \tag{3.7}$$

By applying χ_j to Equation (3.7), we can deduce by use of proposition 3.1.24:

$$d_G(D, \chi_j')\sqrt{\left(\frac{-1}{p}\right)p} \;=\; \sum_{i=1}^{s} \nu_{G,L}(D, g_i')A_{H,H_1}(O_{\chi_j}, O_{h_i})\sqrt{\left(\frac{-1}{p}\right)p}.$$

From the above equation, the conclusion follows.

Thus, it suffices to show Equation (3.7). Let G decompose into:

$$G \;=\; \cup_{i=1}^{t}(l_i L).$$

Clearly, as sets:

$$\begin{aligned} D &= \cup_{i=1}^{t}(D \cap l_i L), \\ D^{(n_0)} &= \cup_{i=1}^{t}(D^{(n_0)} \cap l_i L). \end{aligned}$$

Hence, as elements in $\mathbb{Z}[G]$:

$$\begin{aligned} \pi(D) &= \sum_{i=1}^{t} |D \cap l_i L| h_i, \\ \pi(D^{(n_0)}) &= \sum_{i=1}^{t} |D^{(n_0)} \cap l_i L| h_i. \end{aligned}$$

Thus,

$$\begin{aligned} \pi(D - D^{(n_0)}) &= \sum_{i=1}^{t} \nu_{G,L}(D, l_i) h_i \\ &= \sum_{h \in H} \nu_{G,L}(D, \pi^{-1}(h)) h, \end{aligned} \tag{3.8}$$

where $\pi^{-1}(h)$ is any preimage in G of h under π.

We can deduce Equation (3.7) by applying the G_2-invariance property of the difference intersection numbers to Equation (3.8), i.e., proposition 3.2.4. □

3.3 The G_2 Association Scheme

In this section, we will prove proposition 3.1.22 by using the character table of a special Association Scheme.

We will assume a noncanonical isomorphism $\theta : G \to \widehat{G}$ such that $\theta(g)(g') = \theta(g')(g)$. We will let $g_1, \ldots, g_r$ be the G_1-orbit representatives of the action of G_1 on $G\backslash\{0\}$. From the representatives $g_1, \ldots, g_r$ and θ, we will get $\chi_i = \theta(g_i)$ that will be the corresponding G_1-orbit representatives of the action of G_1 on $\widehat{G}\backslash\{1\}$.

First, we introduce the algebra $H(G, K)$ where $K \subset Aut(G)$, which we will call the S-ring algebra of G with respect to K.

Definition 3.3.1. *Let $K \subset Aut(G)$ and define the* action of K on $\mathbb{C}[G]$ *by $\sigma \cdot [x^g] = [x^{\sigma(g)}]$. Let $H(G, K) = \mathbb{C}[G]^H = \{z \in \mathbb{C}[G] \mid \sigma \cdot z = z, \forall \sigma \in K\}$. $H(G, K)$ will be called the* S-ring algebra of G with respect to K.

Proposition 3.3.2. *The set $H(G, K)$ is a subalgebra of $\mathbb{C}[G]$.*

Proof. It suffices to show $H(G, K)$ is closed under the convolution product of $\mathbb{C}[G]$. Note that for general $z, z' \in \mathbb{C}[G]$ and $\sigma \in Aut(G)$, $\sigma \cdot (z * z') = (\sigma \cdot z) * (\sigma \cdot z')$,[6] because G is abelian and σ is an autormorphism of G.

Let $z, z' \in H(G, K)$ and $\sigma \in K$, then $\sigma \cdot (z * z') = (\sigma \cdot z) * (\sigma \cdot z') = z * z'$. Hence, $z * z' \in H(G, K)$. □

The algebras $H(G, K)$ are examples of S-rings, and are studied in detail by Bannai and Ito in [2]. In the following, we will show that $H(G, K)$ has a character table, and we will calculate it for general K.

Standard character theory shows that the primitive idempotents of $\mathbb{C}[G]$ are given

[6] where $*$ is the convolution product of $\mathbb{C}[G]$.

by:

$$e_\chi = \frac{1}{|G|}\sum_{g\in G}\overline{\chi(g)}[x^g].$$

Note that if $\sigma \in Aut(G)$, then one can define an action on the primitive idempotents of $\mathbb{C}[G]$ by:

$$\begin{aligned}\sigma \cdot e_\chi &= \frac{1}{|G|}\sum_{g\in G}\overline{\chi(g)}[x^{\sigma(g)}] \\ &= \frac{1}{|G|}\sum_{g\in G}\overline{\chi(\sigma^{-1}(g))}[x^g] \\ &= \frac{1}{|G|}\sum_{g\in G}\overline{(\sigma\cdot\chi)(g)}[x^g] \\ &= e_{\sigma\cdot\chi},\end{aligned}$$

where we have defined the action of $\sigma \in Aut(G)$ on $\chi \in \widehat{G}$ by $(\sigma\cdot\chi)(g) = \chi(\sigma^{-1}(g))$. The action of $K \subset Aut(G)$ on the primitive idempotents of $\mathbb{C}[G]$ give us a formula for the linearly independent idempotents of $H(G,K)$.

In the following, we will assume that $h_0 = 0, h_1, \ldots, h_l$ are the distinct orbit representatives of the action of K on G; and we will let $\chi'_0 = \theta(h_0), , \chi_1 = \theta(h_1), \ldots, \chi'_l = \theta(h_l)$ be the distinct orbit representatives of the action of K on $\widehat{G}$, where χ'_0 is the trivial character. We will also let l be the number of orbits of the action of K on G.

Proposition 3.3.3. *Let $O_{\chi'_i}$ be the orbit of χ'_i under the action of K on $\widehat{G}$. Let O_{h_i} be the orbit of h_i under the action of K on G. Let $d_{\chi'_i} = \sum_{\chi\in O_{\chi'_i}} e_\chi$. Then,*

1. *The dimension of $H(G,K)$ is given by $dim_{\mathbb{C}}(H(G,K)) = l+1$.*
2. *The set $\{O_{h'_0}, O_{h'_1}, \ldots, O_{h'_l}\}$ is a basis of $H(G,K)$.*
3. *The set $\{d_{\chi'_0}, d_{\chi'_1}, \ldots, d_{\chi'_l}\}$ is a basis of idempotents of $H(G,K)$.*

4. *Given* $z \in H(G,K)$,

$$\begin{aligned} z &= \sum_{i=0}^{l} \chi_i'(z) d_{\chi_i'}, \\ z &= \sum_{i=0}^{l} z_{h_i} O_{h_i}, \end{aligned}$$

where z_{h_i} *is the value of* z *on* $[x^{h_i}]$.

5. *The basis change from* $\{d_{\chi_i}\}$ *to* $\{O_{h_i}\}$ *is given by* $O_{h_i} = \sum_{j=0}^{l} \chi_j'(O_{h_i}) d_{\chi_i}$.

6. *The basis change from* $\{O_{h_i}\}$ *to* $\{d_{\chi_i}\}$ *is given by* $d_{\chi_i'} = \frac{1}{|G|} \sum_{j=0}^{l} \overline{O_{\chi_i'}(h_j)} O_{h_j}$, *where* $O_{\chi_i'}(h_j) = \sum_{\chi \in O_{\chi_i'}} \chi(h_j)$.

7. *Let* $C_{G,K}$ *be the* $(l+1) \times (l+1)$ *matrix given by* $C_{G,K}(\chi_i', h_j) = \chi_i'(O_{h_j})$, *and* $B_{G,K}$ *be the* $(l+1) \times (l+1)$ *matrix given by* $B_{G,K}(h_i, \chi_j') = \overline{O_{\chi_j'}(h_i)}$. *Then,*

$$\begin{aligned} B_{G,K} C_{G,K} &= |G| I_{l+1,l+1}, \\ C_{G,K} B_{G,K} &= |G| I_{l+1,l+1}, \\ B_{G,K} &= \overline{C_{G,K}}, \end{aligned}$$

where $I_{l+1,l+1}$ *is the* $(l+1) \times (l+1)$ *identity matrix.*

Proof. First, we will show part 1 and part 2. Note that if $z \in H(G,K)$ then $z = \sum_{g \in G} z_g [x^g]$; and given $\sigma \in K$,

$$\begin{aligned} z &= \sigma \cdot z \\ &= \sum_{g \in G} z_g [x^{\sigma(g)}] \\ &= \sum_{g \in G} z_{\sigma^{-1}(g)} [x^g]. \end{aligned}$$

Hence, $z_g = z_{\sigma^{-1}(g)}$, i.e., z is constant on the orbits of K on G. This shows part 1 and 2.

Clearly, the number of orbits of the action of K on G is the same as the number

of orbits of the action of K on $\widehat{G}$. To show part 3, it suffices to show that: the vectors $d_{\chi_i'}$ are linearly independent, they belong to $H(G,K)$, and they are idempotents themselves. Clearly, each $d_{\chi_i'}$ is an idempotent, as each $d_{\chi_i'}$ is a sum of distinct orthogonal primitive idempotents. Consider,

$$\begin{aligned} 0 &= \sum_{j=0}^{l} c_j d_{\chi_j'} \\ &= \sum_{j=0}^{l} c_j \{ \sum_{\chi \in O_{\chi_j'}} e_\chi \} \\ &= \sum_{\chi \in \widehat{G}} c_\chi' e_\chi, \end{aligned}$$

where in the last equation, c_χ's are paired with the c_js. Since, the e_χ are linearly independent as they form another basis of $\mathbb{C}[G]$ because G is abelian; we must have $c_j = c_\chi' = 0$. This shows linearly independence of the $d_{\chi_i'}$.

To show that each $d_{\chi_i'} \in H(G,K)$, suffices to show that $\sigma \cdot d_{\chi_i'} = d_{\chi_i'}$ for $\sigma \in K$. Consider,

$$\begin{aligned} \sigma \cdot d_{\chi_i'} &= \sum_{\chi \in O_{\chi_i'}} \sigma \cdot e_\chi \\ &= \sum_{\chi \in O_{\chi_i'}} e_{\sigma \cdot \chi} \\ &= \sum_{\chi \in O_{\chi_i'}} e_\chi \\ &= d_{\chi_i'}. \end{aligned}$$

This shows part 3.

Now we show part 4. Clearly, if $z \in H(G,K)$, then z is constant on the orbits of the action of K on G. That is, $z = \sum_{i=0}^{l} z_{h_i} O_{h_i}$. Also, note that $z * e_\chi = \chi(z) e_\chi$;[7]

[7] We are using G is abelian.

hence, for $\sigma \in K$:

$$\begin{aligned}
\chi(z)e_\chi &= z * e_\chi \\
&= (\sigma \cdot z) * e_\chi \\
&= \sigma \cdot (z * (\sigma^{-1} \cdot e_\chi)) \\
&= \sigma \cdot (z * e_{\sigma^{-1}\cdot\chi}) \\
&= \sigma \cdot ((\sigma^{-1} \cdot \chi)(z) e_{\sigma^{-1}\cdot\chi}) \\
&= (\sigma^{-1} \cdot \chi)(z) e_\chi \\
&= \chi(\sigma(z)) e_\chi.
\end{aligned}$$

Hence, for $\sigma \in K$, $\chi \in \widehat{G}$ and $z \in H(G,K)$, $\chi(z) = \chi(\sigma(z))$. In particular, we have that:

$$\begin{aligned}
z * d_{\chi'_j} &= \sum_{\chi \in O_{\chi'_j}} z * e_\chi \\
&= \sum_{\chi \in O_{\chi'_j}} \chi(z) e_\chi \\
&= \chi'_j(z) \sum_{\chi \in O_{\chi'_j}} e_\chi \\
&= \chi'_j(z) d_{\chi'_j}.
\end{aligned}$$

Since

$$\begin{aligned}
[1] &= [x^0] \\
&= \sum_{\chi \in \widehat{G}} e_\chi \\
&= \sum_{j=0}^{l} d_{\chi'_j},
\end{aligned}$$

we have that $z = \sum_{j=0}^{l} z * d_{\chi'_j} = \sum_{j=0}^{l} \chi'_j(z) d_{\chi'_j}$. This shows part 4.

To show part 5, note that $[x^g] = \sum_{\chi \in \widehat{G}} \chi(g) e_\chi$. Hence, $O_{h_i} = \sum_{\chi \in \widehat{G}} \chi(O_{h_i}) e_\chi$.

Note that, if $\sigma \in K$, then

$$\begin{aligned}(\sigma \cdot \chi)(O_{h_i}) &= (\sigma \cdot \chi)(\sum_{g \in O_{h_i}} [x^g]) \\ &= \sum_{g \in O_{h_i}} (\sigma \cdot \chi)(g) \\ &= \sum_{g \in O_{h_i}} \chi(\sigma^{-1}(g)) \\ &= \sum_{g \in O_{h_i}} \chi(g) \\ &= \chi(O_{h_i}).\end{aligned}$$

Thus, $\chi(O_{h_i}) = \chi'(O_{h_i})$ whenever $\chi, \chi' \in O_\chi$. Therefore,

$$\begin{aligned}O_{h_i} &= \sum_{\chi \in \widehat{G}} \chi(O_{h_i}) e_\chi \\ &= \sum_{j=0}^{l} \chi'_j(O_{h_i}) d_{\chi'_j}.\end{aligned}$$

This shows part 5.

Part 6 is shown similarly. Note that $e_\chi = \frac{1}{|G|} \sum_{g \in G} \overline{\chi(g)}[x^g]$, hence

$$\begin{aligned}d_{\chi'_i} &= \frac{1}{|G|} \sum_{g \in G} \{ \overline{\sum_{\chi \in O_{\chi'_i}} \chi(g)} \}[x^g] \\ &= \frac{1}{|G|} \sum_{g \in G} \overline{O_{\chi'_i}(g)}[x^g].\end{aligned}$$

Similarly as in the previous part, we can show that:

$$\begin{aligned} O_{\chi_i'}(g) &= \sum_{\chi \in O_{\chi_i'}} \chi(g) \\ &= \sum_{\chi \in O_{\chi_i'}} (\sigma^{-1} \cdot \chi)(g) \\ &= \sum_{\chi \in O_{\chi_i'}} \chi(\sigma(g)) \\ &= O_{\chi_i'}(\sigma(g)). \end{aligned}$$

Thus,

$$\begin{aligned} d_{\chi_i'} &= \frac{1}{|G|} \sum_{g \in G} \overline{O_{\chi_i'}(g)}[x^g] \\ &= \frac{1}{|G|} \sum_{j=0}^{l} \overline{O_{\chi_i'}(h_j)} O_{h_j}, \end{aligned}$$

hence showing part 6.

Part 7's first two equations are clearly a consequence of parts 5 and 6. We show the last equation. Note that, $O_{\chi_i'} = \theta(O_{h_i})$ by the choice of θ and χ_i'. Thus,

$$\begin{aligned} O_{\chi_i'}(h_j) &= \sum_{\chi \in O_{\chi_i'}} \chi(h_j) \\ &= \sum_{h \in O_{h_i}} \theta(h)(h_j) \\ &= \sum_{h \in O_{h_i}} \theta(h_j)(h) \\ &= \sum_{h \in O_{h_i}} \chi_j'(h) \\ &= \chi_j'(O_{h_i}). \end{aligned}$$

Thus, by the choice of θ and χ'_i, we have that

$$\begin{aligned} B_{G,K}(h_i, \chi'_j) &= \overline{O_{\chi'_j}(h_i)} \\ &= \overline{\chi'_i(O_{h_j})} \\ &= \overline{C_{G,K}(\chi'_i, h_j)}. \end{aligned}$$

Therefore, $B(G,K) = \overline{C_{G,K}}$. □

Parts 5 and 6 of proposition 3.3.3 gives the basis change between two basis of $H(G,K)$. Although not needed here, one can show that the $d_{\chi'_i}$s are the primitive idempotents of $H(G,K)$, and that $H(G,K)$ is a semisimple algebra. Thus, parts 5 and 6 of proposition 3.3.3 gives the character table and the inverse character table of $H(G,K)$. Also, one can show that $H(G,K)$ is itself an Association Scheme, as it is an S-ring in the sense of Bannai and Ito in [2]; and also a Hecke Algebra. However, we will not use this structure.

To prove proposition 3.1.22, we will consider the case when G is an abelian p-group with $K = G_2$, and we will exploit the identity of part 7 of proposition 3.3.3.

Proposition 3.3.4. *Let G be a an abelian p-group. Then,*

$$A^2_{G,G_1} = \frac{|G|}{p} I_{r,r},$$

where r is the number of G_1 orbits in $G\backslash\{0\}$, $I_{r,r}$ is the identity $r \times r$ matrix, and $r = r(G)$ is the number of G_1 orbits of $\widetilde{G} = G\backslash\{0\}$.

Proof. Let $g_1, \ldots, g_r$ be the distinct orbit representatives of the action of G_1 on $G\backslash\{0\}$. Let $g_0 = 0$, and $g_{r+i} = n_0 \cdot g_i$ for $i = 1, \ldots, r$; where n_0 is a Non-Quadratic Residue mod $p^s = exp(G)$. Clearly, $g_0, g_1, \ldots, g_r, g_{r+1}, \ldots, g_{2r}$ are orbit representatives of the action of G_2 on G. Let $\chi_i = \theta(g_i)$. With the choices of g_i and χ_i and using proposition

3.3.3 and corollary 3.1.16, we have that a matrix representation of C_{G,G_2} is:

$$\begin{pmatrix} 1 & |O_{g_1}|\cdots|O_{g_r}| & |O_{g_1}|\cdots|O_{g_r}| \\ \underline{1} & A_0 & \widetilde{A_0} \\ \underline{1} & \widetilde{A_0} & A_0 \end{pmatrix},$$

where $A_0 = B_1 + \omega A_{G,G_1}$, $\widetilde{A_0} = B_1 + \overline{\omega} A_{G,G_1}$,[8] $\underline{1}$ is the $r \times 1$ vector of all 1s, and B_1 is given by:

$$B_1(\chi_i, g_j) = \begin{cases} |O_{g_j}| & \text{if } \chi_i(g_j) = 1, \\ -o(p \cdot g_j) & \text{if } \chi_i(g_j) = \eta_p^n \text{ and } (\frac{n}{p}) = -1, \\ 0 & \text{else.} \end{cases}$$

Now, we proceed by cases. First let $p = 3 \bmod 4$. Clearly, -1 is a Non-Quadratic Residue mod $p^s = exp(G)$. Also, $\overline{\omega}$ is the complex conjugate of ω, thus:

$$C_{G,G_2} = \begin{pmatrix} 1 & |O_{g_1}|\cdots|O_{g_r}| & |O_{g_1}|\cdots|O_{g_r}| \\ \underline{1} & A_0 & \overline{A_0} \\ \underline{1} & \overline{A_0} & A_0 \end{pmatrix}.$$

By proposition 3.3.3 part 7, we get that $\overline{C_{G,G_2}} C_{G,G_2} = |G|I$. Thus:

$$\begin{pmatrix} 1 & |O_{g_1}|\cdots|O_{g_r}| & |O_{g_1}|\cdots|O_{g_r}| \\ \underline{1} & \overline{A_0} & A_0 \\ \underline{1} & A_0 & \overline{A_0} \end{pmatrix} \begin{pmatrix} 1 & |O_{g_1}|\cdots|O_{g_r}| & |O_{g_1}|\cdots|O_{g_r}| \\ \underline{1} & A_0 & \overline{A_0} \\ \underline{1} & \overline{A_0} & A_0 \end{pmatrix}$$

$$= |G|I.$$

[8]Note that $\overline{\omega}$ is not necessarily the complex conjugate of ω but it is instead the Galois conjugate of ω in $\mathbb{Q}(\omega)$.

From the above equation, we can deduce the following equations:

$$J_0 + \overline{A_0}A_0 + A_0\overline{A_0} = |G|I, \tag{3.9}$$

$$J_0 + A_0^2 + \overline{A_0}^2 = 0, \tag{3.10}$$

where $J_0 = JDiag(|O_{g_1}|, \ldots, |O_{g_r}|)$ and J is the $r \times r$ matrix of all 1s. Substracting Equation (3.10) from Equation (3.9), we get:

$$\begin{aligned} |G|I &= \overline{A_0}A_0 + A_0\overline{A_0} - A_0^2 - \overline{A_0}^2 \\ &= -(A_0 - \overline{A_0})(A_0 - \overline{A_0}). \end{aligned}$$

Note that $A_0 - \overline{A_0} = (\omega - \overline{\omega})A_{G,G_1} = \sqrt{-p}A_{G,G_1}$. Thus,

$$\begin{aligned} |G|I &= -(\sqrt{-p}A_{G,G_1})(\sqrt{-p}A_{G,G_1}) \\ &= pA_{G,G_1}^2, \end{aligned}$$

hence, the result follows.

Now, we proceed to prove the case when $p = 1 \bmod 4$. Under this case, -1 is a Quadratic Residue and ω is a real number; thus, A_0 is a real matrix and $\overline{A_0} = A_0$, $\overline{\widetilde{A_0}} = \widetilde{A_0}$. Therefore, the equation $\overline{C_{G,G_2}}C_{G,G_2} = |G|I$ reduces to:

$$\begin{pmatrix} 1 & |O_{g_1}| \cdots |O_{g_r}| & |O_{g_1}| \cdots |O_{g_r}| \\ \underline{1} & A_0 & \widetilde{A_0} \\ \underline{1} & \widetilde{A_0} & A_0 \end{pmatrix} \begin{pmatrix} 1 & |O_{g_1}| \cdots |O_{g_r}| & |O_{g_1}| \cdots |O_{g_r}| \\ \underline{1} & A_0 & \widetilde{A_0} \\ \underline{1} & \widetilde{A_0} & A_0 \end{pmatrix}$$

$$= |G|I.$$

Hence, we deduce the following equations:

$$|G|I = A_0^2 + \widetilde{A_0}^2 + J_0, \tag{3.11}$$

$$0 = A_0\widetilde{A_0} + \widetilde{A_0}A_0 + J_0. \tag{3.12}$$

Substracting Equation (3.12) from Equation (3.11), we get:

$$\begin{aligned} |G|I &= A_0^2 + \widetilde{A_0}^2 - A_0\widetilde{A_0} - \widetilde{A_0}A_0 \\ &= (A_0 - \widetilde{A_0})(A_0 - \widetilde{A_0}). \end{aligned}$$

Under the assumption that $p = 1 \bmod 4$, $A_0 - \widetilde{A_0} = \sqrt{p}A_{G,G_1}$. Thus,

$$\begin{aligned} |G|I &= (\sqrt{p}A_{G,G_1})(\sqrt{p}A_{G,G1}) \\ &= pA_{G,G_1}^2. \end{aligned}$$

Hence, the result follows. □

As a corollary we get a relationship in the Smith Normal Form of A_{G,G_1}.

Corollary 3.3.5. *Let S_G be the Smith Normal Form of A_{G,G_1} and $|G| = p^m$. Then*

1. *The matrix A_{G,G_1} has Smith Normal Form,*

$$S_G = Diag((1)^{a_0}, (p)^{a_1}, \ldots, (p^{m-1})^{a_{m-1}}).$$

2. *The exponents of part 1 satisfy $a_{m-1-i} = a_i$ for all $i \in \{0, \ldots, m-1\}$.*

Proof. Let $S = S_G$ be the SNF of $A = A_{G,G_1}$, then there are unimodular matrices E, F such that $EAF = S$. Thus, $A^{-1} = FS^{-1}E$. Since $A^2 = p^{m-1}I$, we must have $A = p^{m-1}A^{-1} \in M_r(\mathbb{Z})$ is an $r \times r$ matrix of integers. Therefore, as $A = p^{m-1}A^{-1} = p^{m-1}FS^{-1}E$, we have that $p^{m-1}S^{-1} = F^{-1}AE^{-1}$ must be integral since E, F are unimodular. Let $S = Diag(s_1, \ldots, s_r)$, then:

$$p^{m-1}S^{-1} = p^{m-1}\begin{pmatrix} s_1^{-1} & 0 & \cdots & 0 \\ 0 & s_2^{-1} & \cdots & 0 \\ 0 & \vdots & \cdots & 0 \\ 0 & 0 & 0 & s_r^{-1}, \end{pmatrix}.$$

Hence, p^{m-1} is divisible by s_i. Thus, s_i must be a pth power. Therefore, all invariant factors of A are powers of p.

If $s_r < p^{m-1}$, then $s_r A^{-1} = F(s_r S^{-1})E \in M_r(\mathbb{Z})$ is an integral matrix; but, $s_r A^{-1} = \frac{s_r}{p^{m-1}} A \notin M_r(\mathbb{Z})$ as A has entries that are ± 1 given by columns that correspond to Ω_{g_i} where g_i has order p^{s-1}. Thus, $s_r \geq p^{m-1}$. By using a similar argument, we can show that $s_r > p^{m-1}$ gives a contradiction. Hence, $s_r = p^{m-1}$ and part 1 follows.

To show part 2, note that $A = p^{m-1}A^{-1} = p^{m-1}FS^{-1}E$. Thus, if,

$$S = Diag((1)^{a_0}, \ldots, (p^{m-1})^{a_{m-1}}),$$

then

$$\begin{aligned} A &= FDiag((p^{m-1})^{a_0}, \ldots, (1)^{a_{m-1}})E \\ &= F'Diag((1)^{a_{m-1}}, \ldots, (p^{m-1})^{a_0})E', \end{aligned}$$

where $F' = FP_0$ and $E = E'P_0$, for some permutation matrix P_0. By uniqueness of the SNF, we have that $a_0 = a_{m-1}, a_1 = a_{m-2}, \ldots, a_{m-1} = a_0$. Hence, the result follows. □

Corollary 3.3.6. *Let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, then A_{G,G_1} has SNF $Diag((1)^{\frac{p+1}{2}}, (p)^{\frac{p+1}{2}})$.*

Proof. By the previous corollary, $S = Diag((1)^{a_0}, (p)^{a_1})$ and $a_0 = a_1$. Since $a_0 + a_1 = r = p + 1$, the result follows. □

We calculate A_{G,G_1} for $G = (\mathbb{Z}/p^s\mathbb{Z})$ as an illustrative example and leave the proof as an exercise.

Proposition 3.3.7. *Let $G = (\mathbb{Z}/p^s\mathbb{Z})$, then:*

1. *A full set of G_1 orbit representatives of $\widetilde{G}$ is given by $X_1 = \{1, p, \cdot, p^{s-1}\}$.*

2. *A commutative pairing for G is given by:*

$$\theta(a)(b) = \eta_{p^s}^{ab}.$$

3. *By using,*

$$\begin{aligned} X &= \mathbb{C}\Omega_{p^{s-1}} \oplus \mathbb{C}\Omega_{p^{s-2}} \oplus \cdots \oplus \Omega_1, \\ Y &= \mathbb{C}\Omega_{\chi_{p^{s-1}}} \oplus \mathbb{C}\Omega_{\chi_{p^{s-2}}} \oplus \cdots \oplus \Omega_{\chi_1}, \end{aligned}$$

where $\chi_{p^i} = \theta(p_i)$*, we can calculate* A_{G,G_1} *as:*

$$A_{G,G_1} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & p^{s-1} \\ 0 & 0 & 0 & \cdots & p^{s-2} & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & p^2 & \cdots & 0 & 0 \\ 0 & p & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

3.4 Results for Special Groups

We will give two examples of the map $\theta : G \to \widehat{G}$ such that $\theta(g)(g') = \theta(g')(g)$; then, we will use these θs to state GSHDS existence conditions for the special groups $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^\alpha$.

Our results will make use of Galois Rings, which are defined in proposition 3.4.1. Proposition 3.4.1 can be shown using standard local algebraic number theory.

Proposition 3.4.1. *Let* $K = \mathbb{Q}_p(\eta)$ *be an umramified extension of* $\mathbb{Q}_p$ *of degree* α*. Let* O_K *be the ring of integers of* K*. Define* $R(p^k, \alpha) = \frac{O_K}{p^k O_K}$*. Let* $q = p^\alpha$*, then:*

1. $R(p^k, \alpha) = (\mathbb{Z}/p^k\mathbb{Z})(\eta)$ *is the Galois extension of the ring* $(\mathbb{Z}/p^k\mathbb{Z})$ *of degree* α *and exponent* p^k*.*

2. *There is a set of "Teichmüller Units,"* $\tau = \{1, \eta, \ldots, \eta^{q-2}\} \subset (O_K)^*$*, of* $(q-1)$*th primitive roots of unity in* O_K *that are distinct mod* pO_K*.*

3. *Every element* $\gamma \in R(p^k, \alpha)$ *decomposes into:*

$$\gamma = r_0(\gamma) + r_1(\gamma)p + \cdots + r_{k-1}(\gamma)p^{k-1},$$

where the $r_i(\gamma) \in \tau \cup \{0\}$ *are unique.*

4. *The* $Gal(K \mid \mathbb{Q}_p) = \langle Fr \rangle$*; where* Fr*, the "Frobenious" map, is defined by* $Fr(\eta) = \eta^p$*.*

5. *The* $Gal(K \mid \mathbb{Q}_p)$ *induces a group of automorphisms of* $R(p^k, \alpha)$ *that leaves* $(\mathbb{Z}/p^k\mathbb{Z})$ *invariant and is defined by* $Fr(\gamma) = r_0(\gamma)^p + r_1(\gamma)^p p + \cdots + r_{k-1}(\gamma)^p p^{k-1}$*.*

6. *The Trace map* $Tr : K \to \mathbb{Q}_p$ *defined by:*

$$Tr(x) \;=\; \sum_{j=0}^{n-1} Fr^i(x),$$

induces a Trace map $Tr : R(p^k, \alpha) \to (\mathbb{Z}/p^k\mathbb{Z})$*.*

By using Galois Rings, we give a list of H_1 orbit representatives for $H = (\mathbb{Z}/p^2\mathbb{Z})^\alpha$ that will prove useful.

Proposition 3.4.2. *Let* $H = (\mathbb{Z}/p^2\mathbb{Z})^\alpha$ *and* $L = \{g \in H \mid o(g) = p\} = p \cdot H$*.*

1. *H can be viewed as Galois Ring* $R(p^2, \alpha)$ *by using any isomorphism of additive groups* $\kappa : H \to R(p^2, \alpha)$*. That is, we can define the corresponding multiplication on H as:*

$$g * g' \;=\; \kappa^{-1}(\kappa(g) * \kappa(g')).$$

2. *Let* r' *be number of orbits of the action of* $L_1 = (\mathbb{Z}/p\mathbb{Z})^*$ *on* $L \backslash \{0\}$*, then* $r' = p^{\alpha-1} + p^{\alpha-2} + \cdots + p + 1$*.*

3. *Let* $q = p^\alpha$*. There is a set* $\mu_{q-1} = \{k_1, \ldots, k_{q-1}\}$ *of elements of H of order* p^2*, called the "Teichmüller Units," such that:*

$$\begin{aligned} p \cdot \mu_{q-1} &= \{p \cdot k_1, \ldots, p \cdot k_{p^\alpha - 1}\} \\ &= L \backslash \{0\}. \end{aligned}$$

4. *There are sets* $\{l_1, \ldots, l_{r'}\} \subset \mu_{q-1}$ *and* $\{l'_1, \ldots, l'_{p^{\alpha-1}}\} \subset \mu_{q-1} \cup \{0\}$*, such that,*

   (a) *The elements* $\{p \cdot l_1, \ldots, p \cdot l_{r'}\}$ *are orbit representatives of the action of* L_1 *on* $\widetilde{L} = L \backslash \{0\}$*.*

   (b) *The elements* $\{p \cdot l'_1, \ldots, p \cdot l'_{p^{\alpha-1}}\}$ *are orbit representatives of the action of* $((\mathbb{Z}/p\mathbb{Z}), +)$ *on* $(L, +)$*.*

   (c) *The elements* $h_{i,j} = l_i + p \cdot l'_{i,j} = l_i * (1 + pl'_j)$ *, where* $i = 1, \ldots, r'$ *and* $j = 1, \ldots, p^{\alpha-1}$*, form a set of orbit representatives of the action of* H_1 *on the elements of order* p^2 *in* H*.*

Proof. Part 1 is clear. We show part 2 by observing that L_1 has order $p-1$ and is acting on, $L\backslash\{0\}$, a set of size $p^\alpha - 1$. Since this action has no fixed points, a direct use of Burnside's formula for group actions gives the number of orbits as $\frac{p^\alpha - 1}{p-1} = p^{\alpha-1} + p^{\alpha-2} + \cdots + p + 1$. Hence, part 2 follows.

To show parts 3 and 4, we will view H as a Galois Ring; the extra operation of multiplication will help us construct the desired H_1 orbit representatives.

Let $K = \mathbb{Q}_p(\beta)$ be an unramified extension of $\mathbb{Q}_p$, the p-adic numbers, of degree α. Denote by O_K the ring of integers in K. Let τ be the Teichm*ü*ller Units of proposition 3.4.1.

Define $\mu_{q-1} = \tau \mod p^2 O_K$. Since $R(p^2, \alpha)$ is a local ring with maximal ideal given by $pR(p^2, \alpha)$, it follows that all units have order p^2. Hence, every element of μ_{q-1} has order p^2. To show part 3, let $k_1 \neq k_2$ both in μ_{q-1} such that $p \cdot k_1 = p \cdot k_2$ in $L \subset H$. By construction, there are $\eta_1 \neq \eta_2$ both in τ such that $p \cdot \eta_1 = p \cdot \eta_2 \mod p^2 O_K$. Thus, $p \cdot (\eta_1 - \eta_2) = 0 \mod p^2 O_K$. Since K is an unramified discrete valuation ring with prime p, it follows that p divides $\eta_1 - \eta_2$, i.e., $\eta_1 = \eta_2 \mod pO_K$. This contradicts proposition 3.4.1 part 2. Hence, $p \cdot \mu_{q-1} \subset L\backslash\{0\}$ has $q-1$ elements. Since $|L\backslash\{0\}| = q - 1$, it must be the case that $p \cdot \mu_{q-1} = L\backslash\{0\}$.

Now, we proceed to show part 4. By using standard local algebraic number theory, we know that $K^* = \langle p \rangle \times \mu_{q-1} \times U^{(1)}$; where $\langle p \rangle = \{p^i \mid i \in \mathbb{Z}\}$ and $U^{(1)} = \{x \in O_K \mid x = 1 + pz \text{ where } z \in O_K\}$. Thus, we can deduce that $R(p^2, \alpha)^*$ can be parameterized

by tuples in the following form:

$$R(p^2,\alpha)^* \;=\; \{(a_0,a_1) \mid a_0 \in \mu_{q-1}, a_1 \in \mu_{q-1}\cup\{0\}\}, \tag{3.13}$$

where $(a_0,a_1) = a_0(1+pa_1) \in R_p(2,\alpha)$. We note that the parametrization in Equation (3.13) is more of a multiplicative decomposition instead of an additive decomposition. That is, $(a_0,0)(0,a_1) = (a_0,a_1)$ but $(a_0,0)+(0,a_1) \neq (a_0,a_1)$.

Note that $(\mathbb{Z}/p^2\mathbb{Z}) = \mathbb{Z}_p/p^2\mathbb{Z}_p \subset O_K/p^2O_K = R_p(2,\alpha)$. A direct calculation shows that:

$$(\mathbb{Z}/p^2\mathbb{Z})^* \;=\; \{(b_0,b_1) \mid b_0 \in \mu_{p-1}, b_1 \in \mu_{p-1}\cup\{0\}\},$$

where μ_{p-1} is the subset of μ_{q-1} consisting of the $(p-1)$th roots of unity. Note that the action of $(\mathbb{Z}/p^2\mathbb{Z})^*$ on H is given by multiplication of $(\mathbb{Z}/p^2\mathbb{Z})$ on $R_p(2,\alpha)$. Also, note that multiplication of tuples has a nice formula since:

$$\begin{aligned}(b_0,b_1)(a_0,a_1) &= b_0(1+pb_1)a_0(1+pa_1) \\ &= b_0a_0(1+p(b_1+a_1)) \bmod p^2O_K \\ &= (b_0a_0, b_1+a_1),\end{aligned} \tag{3.14}$$

where the addition in the second coordinate is taken as addition in $\mathbb{F}_q$, and multiplication in the first coordinate is taken as multiplication in $(\mathbb{F}_q)^*$.

Clearly, if we are considering elements of order p^2, then we are considering the elements of $R(p^2,\alpha)^*$. Also, the action of $(\mathbb{Z}/p^2\mathbb{Z})^* = H_1$ on $R(p^2,\alpha)^* = H$ "decomposes" via the use of Equation (3.14) onto the action of $\mathbb{F}_p^*$ on $\mathbb{F}_q^*$ on the first coordinate and the action of $(\mathbb{F}_p,+)$ on $(\mathbb{F}_q,+)$ on the second coordinate.

Let $m_1,\ldots,m_{r'}$ be orbit representatives of the action of μ_{p-1} on μ_{q-1}. Also, let $n_1,\ldots,n_{p^{\alpha-1}}$ be orbit representatives of the action of $(\mathbb{F}_p,+) = \mu_{p-1}\cup\{0\}$ on $(\mathbb{F}_q,+) = \mu_{q-1}\cup\{0\}$.

We claim that the set of tuples $(m_i,n_j) = m_i(1+pn_j)$ form a set of orbit representatives of the action of $(\mathbb{Z}/p^2\mathbb{Z})^*$ on $R(p^2,\alpha)^*$. This will show part 4.

Let $(m,n) \in R(p^2,\alpha)^*$. Clearly, m belongs to the orbit of some m_{i_0}. That is, there is $b_0 \in \mu_{p-1}$ such that $m = b_0 m_{i_0}$. Also, n belongs to the orbit of some n_{j_0}. That is, there is $b_1 \in (\mathbb{F}_p, +) = \mu_{p-1} \cup \{0\}$ such that $n = b_1 + n_{j_0}$. Note that this means $(m,n) = (b_0,b_1)(m_{i_0}, n_{j_0})$, where $(b_0,b_1) \in (\mathbb{Z}/p^2\mathbb{Z})^*$. Hence, the list (m_i, n_j) is exahustive.

It suffices to show that each orbit is represented by at most one (m_i, n_j). Suppose that (m_i, n_j) and $(m_{i'}, n_{j'})$ represent the same orbit H_1 orbit of $H\backslash\{0\}$. Clearly, there is $b \in H_1 = (\mathbb{Z}/p^2\mathbb{Z})^*$ such that:

$$m_i(1+pn_j) \;\; = \;\; b * m_{i'}(1+pn_{j'}).$$

Since, we can decompose b into (b_0,b_1), clearly, $(m_{i'}, n_{j'}) = (b_0,b_1)(m_i,n_j) = (b_0 m_i, b_1 + n_j)$. Thus $m_{i'} = b_0 m_i$ and $n_{j'} = b_1 + n_j$. Hence, forcing $i = i'$ and $j = j'$ by the choice of the m_is and n_js. □

We note that the $l'_{i,j}$s of proposition 3.4.2 may repeat themselves; but, the l_is and l'_js do not.

3.4.1 Examples of $\Theta : G \to \widehat{G}$

Our first example are θs induced by Invariant Factor Inner Products.

Definition 3.4.3. *Let G be an abelian p-group with invariant factor decomposition $G = (\mathbb{Z}/p^{a_1}\mathbb{Z}) \times (\mathbb{Z}/p^{a_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z})$, where $a_1 \geq a_2 \geq \cdots \geq a_r \geq 1$. Given $g, g' \in G$, let $g = (g_1, \ldots, g_r), g' = (g'_1, \cdots, g'_r)$, where $g_i, g'_i \in \mathbb{Z}/p^{a_i}\mathbb{Z}$. The* invariant factor inner product *is defined as:*

$$\langle g', g \rangle_G \;\; = \;\; \sum_{i=1}^{r} g'_i g_i p^{a_1 - a_i} \;\; mod\; p^{a_1}.$$

The following proposition justifies the definition of $\langle g', g \rangle_G$.

Proposition 3.4.4. *Let $\chi \in \widehat{G}$, there is a unique $g' = (b_1, \ldots, b_r) \in G$ such that for*

any $g = (c_1, \ldots, c_r) \in G$,

$$\chi(g) \;=\; \eta_{p^{a_1}}^{\langle g', g\rangle_G},$$

where $\langle g', g\rangle_G = \sum_{i=1}^{r} b_i c_i p^{a_1 - a_i} \mod p^{a_1}$, *and* $\eta_{p^{a_1}}$ *is a fixed primitive* p^{a_1}*th root of unity.*

Proof. Clearly, to know the values of χ on G, we only need to know χ on a set of minimal generators of G. Using the notation of definition 3.4.3, $f_1 = (1, 0, \ldots, 0)$, $f_2 = (0, 1, \ldots, 0), \ldots, f_r = (0, 0, \ldots, 1)$ are canonical generators of G; hence, it suffices to know χ at the f_is.

Let $\chi(f_i) = \eta_{p^{a_i}}^{b_i}$. Since $\eta_{p^{a_i}} = \eta_{p^{a_1}}^{p^{a_1 - a_i}}$, we have that $\chi(f_i) = \eta_{p^{a_1}}^{p^{a_1 - a_i} b_i}$. Given $g = (c_1, \ldots, c_r) = c_1 \cdot f_1 + \cdots + c_r \cdot f_r$, we have that:

$$\begin{aligned}
\chi(g) &= \chi(c_1 \cdot f_1 + \cdots + c_r \cdot f_r) \\
&= \chi(f_1)^{c_1} \cdots \chi(f_r)^{c_r} \\
&= \eta_{p^{a_1}}^{p^{a_1 - a_1} b_1 c_1} \cdots \eta_{p^{a_1}}^{p^{a_1 - a_r} b_r c_r} \\
&= \eta_{p^{a_1}}^{p^{a_1 - a_1} b_1 c_1 + \cdots + p^{a_1 - a_r} b_r c_r} \\
&= \eta_{p^{a_1}}^{\langle g', g\rangle_G}.
\end{aligned}$$

It suffices to show that $g' = (b_1, \ldots, b_r)$ is unique when χ is fixed. This follows by construction, as the b_is determine χ once we fix the basis f_is. □

Note that in the above proof, the choice of $g' = (b_1, \ldots, b_r)$ depends on the choice of the f_is and of the root $\eta_{p^{a_1}}$. Thus, the choice of g' is noncanonical. However, the above proposition gives a way of defining θ.

Corollary 3.4.5. *Let* $\theta(g')(g) = \eta_{p^{a_1}}^{\langle g', g\rangle_G}$, *then* $\theta : G \to \widehat{G}$ *is an isomorphism and* $\theta(g')(g) = \theta(g)(g')$.

Hence, we can define A_{G,G_1} in terms of $\langle g', g\rangle_G$ by:

$$A_{G,G_1}(O_{\theta(g')}, O_g) = \begin{cases} \left(\frac{n}{p}\right) o(p \cdot g) & \text{if } \langle g', g\rangle_G = np^{a_1-1} \bmod p^{a_1}, \\ 0 & \text{else.} \end{cases} \quad (3.15)$$

Definition 3.4.6. *When A_{G,G_1} is defined using an invariant factor inner product $\langle , \rangle_G$, we will say that A_{G,G_1} is induced by an invariant factor inner product.*

The second example for θ is uses the multiplication and trace function in a Galois Ring. The following proposition will justify our example for θ.

Proposition 3.4.7. *Let $H = R(p^k, \alpha) \simeq (\mathbb{Z}/p^k\mathbb{Z})^\alpha$ be a Galois Ring of degree α and exponent p^k. Let $Tr : R(p^k, \alpha) \to (\mathbb{Z}/p^k\mathbb{Z})$ be the trace function of proposition 3.4.1, then the following map $\theta : H \to \widehat{H}$ is a commutative pairing:*[9]

$$\theta(g')(g) = \eta_{p^k}^{Tr(g'*g)},$$

where η_{p^k} is a fixed p^kth primitive root of unity in $\mathbb{C}$, and $g, g' \in H$.

Definition 3.4.8. *Let $G = (\mathbb{Z}/p^k\mathbb{Z})^\alpha$. We will say that A_{G,G_1} is induced by a* Galois ring structure *when A_{G,G_1} is of the form:*

$$\theta(g')(g) = \eta_{p^k}^{Tr(g'*g)},$$

where $*$ is multiplication in the Galois Ring $G = R(p^k, \alpha)$, and Tr is the trace function of proposition 3.4.1.

We note that the choice of $Tr()$ depends on the embedding of $H = (\mathbb{Z}/p^k\mathbb{Z})^\alpha$ in the Galois Group $R(p^k, \alpha)$, and the choice of η_{p^k}.

[9] where H is viewed as an abelian group under $+$.

3.4.2 Results for Θs Induced by Invariant Factor Inner Products

As an application of A_{G,G_1}, using $\langle g', g\rangle_G$, we will show a result that gives some algebraic conditions whenever there is a GSHDS in $G = \mathbb{Z}/p\mathbb{Z} \times (\mathbb{Z}/p^2\mathbb{Z})^3$.

Corollary 3.4.9. *Let $H = (\mathbb{Z}/p^2\mathbb{Z})^\alpha$ and $L = p \cdot H = (\mathbb{Z}/p\mathbb{Z})^\alpha$. Then, there is an ordering of the orbits of the action of H_1 on $H\backslash\{0\}$, such that:*

$$A_{H,H_1} = \begin{pmatrix} 0 & pA_{L,L_1} & \cdots & pA_{L,L_1} \\ A_{L,L_1} & pJ_{H,1,1} & \cdots & pJ_{H,1,p^{\alpha-1}} \\ \vdots & \vdots & \cdots & \vdots \\ A_{L,L_1} & pJ_{H,p^{\alpha-1},1} & \cdots & pJ_{H,p^{\alpha-1},p^{\alpha-1}} \end{pmatrix} \begin{matrix} \} & m_{\alpha,p} \\ \} & p^{\alpha-1}m_{\alpha,p} \end{matrix},$$

where $J_{H,i,j}$ has nonzero support on the zero pattern of A_{L,L_1}, and $m_{\alpha,p} = p^{\alpha-1} + p^{\alpha-1} + \cdots + p + 1$.

Proof. We will organize the orbit H_1 orbit representatives according to the parametrization of proposition 3.4.2. Using the notation of proposition 3.4.2, consider the following enumeration of the orbits:

$$\begin{array}{ll} \{p \cdot l_1, \ldots, p \cdot l_{r'}\} & \text{for elements of order } p, \\ \{l_1 + p \cdot l'_{1,1}, \ldots, l_{r'} + p \cdot l_{r',1}, l_1 + p \cdot l'_{1,2}, \ldots, & \text{for elements of order } p^2. \\ l_{r'} + p \cdot l_{r',2}, \ldots, l_1 + p \cdot l'_{1,p^{\alpha-1}}, \ldots, l_{r'} + p \cdot l_{r',p^{\alpha-1}}\} & \end{array}$$

Using the above enumeration, we can calculate A_{H,H_1} as the following:

$$A_{H,H_1} = \begin{pmatrix} A_{0,0} & pA_{0,1} & \cdots & pA_{0,p^{\alpha-1}} \\ A_{1,0} & pA_{1,1} & \cdots & pA_{1,p^{\alpha-1}} \\ \vdots & \vdots & \cdots & \vdots \\ A_{p^{\alpha-1},0} & pA_{p^{\alpha-1},1} & \cdots & pA_{p^{\alpha-1},p^{\alpha-1}} \end{pmatrix},$$

where the $A_{i,j}$s are all $r' \times r'$ matrices; $A_{0,j}$, where $1 \leq j$, is defined on tuples of the

form $(p \cdot l_k, l_t + p \cdot l'_{t,j})$; $A_{i,0}$, where $1 \leq i$, is defined on tuples of the form $(l_k + p \cdot l'_{k,i}, l_t)$; $A_{0,0}$ is defined on tuples of the form $(p \cdot l_k, p \cdot l_t)$; and $A_{i,j}$, where $1 \leq i, 1 \leq j$, is defined on tuples of the form $(l_k + p \cdot l'_{k,i}, l_t + p \cdot l'_{t,j})$.

We proceed to calculate the $A_{i,j}$s using Equation (3.15). First note that:

$$\langle (a_1, \ldots, a_\alpha), (b_1, \ldots, b_\alpha) \rangle_H = \sum_{i=1}^{\alpha} a_i b_i,$$

hence, $\langle g, g' \rangle_H$ is the regular inner product.

We calculate $A_{0,0}$. Since $A_{0,0}$ is valued on tuples of the form $(p \cdot l_k, p \cdot l_t)$ and

$$\begin{aligned} \langle p \cdot l_k, p \cdot l_t \rangle_H &= p^2 \langle l_k, l_t \rangle_H \\ &= 0 \bmod p^2. \end{aligned}$$

By Equation (3.15), $A_{0,0} = 0$.

Now, we calculate $A_{i,0}$ $(1 \leq i)$. Since $A_{i,0}$ is valued on tuples of the form $(l_k + p \cdot l'_{k,i}, p \cdot l_t)$ and

$$\begin{aligned} \langle l_k + p \cdot l'_{k,i}, p \cdot l_t \rangle_H &= p \langle l_k, l_t \rangle_H + p^2 \langle l'_{k,i}, l_t \rangle_H \\ &= p \langle l_k, l_t \rangle_H \bmod p^2 \\ &= p \langle \overline{l_k}, \overline{l_t} \rangle_L \bmod p^2, \end{aligned}$$

where $\overline{l_k}$ is the result of taking all the coordinates of l_k mod p. Hence, by using Equation (3.15), we have $A_{i,0} = A_{L,L_1}$. The proof that $A_{0,j} = A_{L,L_1}$ is similar to this case.

It suffices to show that $A_{i,j}$, where $1 \leq i, 1 \leq j$, has nonzero support on the zero pattern of A_{L,L_1}. Clearly, $A_{i,j}$ is valued on the tuples of the form $(l_k + p \cdot l'_{k,i}, l_t + p \cdot l'_{t,j})$

and

$$\begin{aligned}\langle l_k + p\cdot l'_{k,i}, l_t + p\cdot l'_{t,j}\rangle_H &= \langle l_k, l_t\rangle_H + p(\langle l'_{k,i}, l_t\rangle_H + \langle l_t, l'_{t,j}\rangle_H) \\ &\quad + p^2\langle l'_{k,i}, l'_{t,j}\rangle_H \\ &= \langle l_k, l_t\rangle_H \\ &\quad + p(\langle l'_{k,i}, l_t\rangle_H + \langle l_t, l'_{t,j}\rangle_H) \bmod p^2.\end{aligned}$$

Hence, if $A_{i,j}(l_k + p\cdot l'_{k,i}, l_t + p\cdot l'_{t,j}) \neq 0$, then $\langle l_k + p\cdot l'_{k,i}, l_t + p\cdot l'_{t,j}\rangle_H = pf \bmod p^2$ where $f \in \{1,\ldots,p-1\}$. Thus,

$$\begin{aligned}pf &= \langle l_k + p\cdot l'_{k,i}, l_t + p\cdot l'_{t,j}\rangle_H \\ &= \langle l_k, l_t\rangle_H + p(\langle l'_{k,i}, l_t\rangle_H + \langle l_t, l'_{t,j}\rangle_H) \bmod p^2,\end{aligned}$$

hence, $\langle l_k, l_t\rangle_H = 0 \bmod p$. But $\langle l_k, l_t\rangle_H = \langle \overline{l_k}, \overline{l_t}\rangle_L \bmod p$. Thus, if $A_{i,j}(l_k + p\cdot l'_{k,i}, l_t + p\cdot l'_{t,j}) \neq 0$, then $\langle \overline{l_k}, \overline{l_t}\rangle_L = 0 \bmod p$. That is, $A_{i,j}$ is nonzero on a subset of the zero pattern of A_{L,L_1}. □

Corollary 3.4.10. *Let H and A_{H,H_1} be given as they are in corollary 3.4.9. Let*

$$B'_H = \begin{pmatrix} J_{H,1,1} & \cdots & J_{H,1,p^{\alpha-1}} \\ \vdots & \cdots & \vdots \\ J_{H,p^{\alpha-1},1} & \cdots & J_{H,p^{\alpha-1},p^{\alpha-1}} \end{pmatrix},$$

and $B_H = pB'_H$. Then,

1. *The matrix B'_H has zero row sums, i.e., $B'_H J = 0$; and, $\sum_{j=1}^{p^{\alpha-1}} J_{H,i,j} = 0$.*
2. *The matrix B'_H has zero column sums, i.e., $JB'_H = 0$; and, $\sum_{i=1}^{p^{\alpha-1}} J_{H,i,j} = 0$.*
3. *The matrix B_H satisfies $B_H^3 = \frac{|H|}{p}B_H = p^{2\alpha-1}B_H$.*
4. *The matrix B_H satisfies $B_H^2 = p^{2\alpha-1}I - p^{\alpha}J_{p^{\alpha-1},p^{\alpha-1}} \otimes I_{r'}$.*

Proof. This is a consequence of $A_{H,H_1}^2 = p^{2\alpha-1}I$. Consider:

$$p^{2\alpha-1}I \quad = \tag{3.16}$$

$$\begin{pmatrix} 0 & pA_{L,L_1} & \cdots & pA_{L,L_1} \\ A_{L,L_1} & pJ_{H,1,1} & \cdots & pJ_{H,1,p^{\alpha-1}} \\ \vdots & \vdots & \cdots & \vdots \\ A_{L,L_1} & pJ_{H,p^{\alpha-1},1} & \cdots & pJ_{H,p^{\alpha-1},p^{\alpha-1}} \end{pmatrix} \begin{pmatrix} 0 & pA_{L,L_1} & \cdots & pA_{L,L_1} \\ A_{L,L_1} & pJ_{H,1,1} & \cdots & pJ_{H,1,p^{\alpha-1}} \\ \vdots & \vdots & \cdots & \vdots \\ A_{L,L_1} & pJ_{H,p^{\alpha-1},1} & \cdots & pJ_{H,p^{\alpha-1},p^{\alpha-1}} \end{pmatrix},$$

Equation (3.16) gives:

$$\begin{aligned} p(\sum_{j=1}^{p^{\alpha-1}} J_{H,i,j})A_{L,L_1} &= 0, \\ pA_{L,L_1}(\sum_{i=1}^{p^{\alpha-1}} J_{H,i,j}) &= 0. \end{aligned}$$

From which parts 1 and 2 follow.

Note that Equation (3.16) also gives the following equation.

$$pA_{L,L_1}^2 + \sum_{k=1}^{p^{\alpha-1}} (pJ_{H,i,k})(pJ_{H,k,j}) \quad = \quad \delta_{i,j}p^{2\alpha-1}I.$$

Since $A_{L,L_1}^2 = p^{\alpha-1}I$, we get that

$$\sum_{k=1}^{p^{\alpha-1}} (pJ_{H,i,k})(pJ_{H,k,j}) \quad = \quad \delta_{i,j}p^{2\alpha-1}I - p^{\alpha}I. \tag{3.17}$$

From which part 3 follows.

To show part 4, apply B_H to Equation (3.17),

$$\begin{aligned}
\sum_{k=1,j=1}^{p^{\alpha-1}} (pJ_{H,i,k})(pJ_{H,k,j})(pJ_{H,j,l}) &= \sum_{j=1}^{p^{\alpha-1}} (\delta_{i,j}p^{2\alpha-1}I - p^{\alpha}I)(pJ_{H,j,l}) \\
&= \sum_{j=1}^{p^{\alpha-1}} \delta_{i,j}p^{2\alpha-1}(pJ_{H,j,l}) - p^{\alpha}\sum_{j=1}^{p^{\alpha-1}}(pJ_{H,j,l}) \\
&= \sum_{j=1}^{p^{\alpha-1}} \delta_{i,j}p^{2\alpha-1}(pJ_{H,j,l}) \\
&= p^{2\alpha-1}(pJ_{H,i,l}),
\end{aligned}$$

from which part 4 follows. □

Corollary 3.4.11. *Let $D \subset H = (\mathbb{Z}/p^2\mathbb{Z})^{\alpha}$ be a QRS, such that $d = (d_0^T, d_1^T, \ldots, d_{p^{\alpha-1}}^T)$ is the representation of D with respect to the choice of H_1 orbit representatives of corollary 3.4.9. Let $L = p \cdot H \simeq (\mathbb{Z}/p\mathbb{Z})^{\alpha}$. Assume that $A_{H,H_1}d = p^{\alpha-1}\tilde{d}$, where $p^{\alpha-1}\tilde{d}$ is the difference coefficient vector of D. Then,*

1. *The following holds for $\tilde{d}$, $A_{H,H_1}\tilde{d} = p^{\alpha}d$.*
2. *The following holds, $A_{L,L_1}d_0 + p\sum_{j=1}^{p^{\alpha-1}} J_{H,i,j}d_j = p^{\alpha-1}\tilde{d}_i$; where $1 \le i \le p^{\alpha-1}$.*
3. *The following holds, $A_{L,L_1}\tilde{d}_0 + p\sum_{j=1}^{p^{\alpha-1}} J_{H,i,j}\tilde{d}_j = p^{\alpha}d_i$; where $1 \le i \le p^{\alpha-1}$.*
4. *All the entries of $A_{L,L_1}d_0$ are divisible by p.*
5. *All the entries of $A_{L,L_1}\tilde{d}_0$ are divisible by p.*
6. *The difference coefficients of d_0 in L satisfy $A_{L,L_1}d_0 = \sum_{i=1}^{p^{\alpha-1}} \tilde{d}_i$.*
7. *The following holds for $\tilde{d}_0$, $A_{L,L_1}\tilde{d}_0 = p\sum_{i=1}^{p^{\alpha-1}} d_i$.*

Proof. Part 1 is a consequence of the equation $A_{H,H_1}^2 = \frac{|H|}{p}I$. Parts 2 and 3 are consequences of the equations $A_{H,H_1}d = p^{\alpha-1}\tilde{d}$ and $A_{H,H_1}\tilde{d} = p^{\alpha}d$. Parts 4 and 5 are consequences of parts 2 and 3. To conclude part 6, sum the equation of part 2 over the distinct values of i and use the identity $\sum_{j=1}^{p^{\alpha-1}} J_{H,i,j} = 0$ from corollary 3.4.10

part 1. To conclude part 7, sum the equation of part 3 over the distinct values of i and use the identity $\sum_{j=1}^{p^{\alpha-1}} J_{H,i,j} = 0$ from corollary 3.4.10 part 2. □

Now we prove some results for the group $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^\alpha$.

Proposition 3.4.12. *Let $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^\alpha$ and $D \subset G$ a GSHDS. Let $H = \{0\} \times (\mathbb{Z}/p^2\mathbb{Z})^\alpha \subset G$ and $L = p \cdot H \simeq (\mathbb{Z}/p\mathbb{Z})^\alpha$. Let $D' = H \cap D$ and $D'' = L \cap D$. Let d' be the vector of ± 1s representing D' using the orbit representatives of H in corollary 3.4.9. Hence, $d' = (d_0'^T, d_1'^T, \ldots, d_{p^{\alpha-1}}'^T)$ where d_i' is a $(p^{\alpha-1} + \cdots + p + 1) \times 1$ vector of ± 1s. Also, let $\tilde{d_i}'$ be the difference coefficients corresponding to H_1 classes in d_i'. Then,*

1. *The following holds, $A_{H,H_1} d' = p^{\alpha-1} \tilde{d}'$ and $A_{H,H_1} \tilde{d}' = p^\alpha d'$.*
2. *The following holds, $A_{L,L_1} d_0' + p \sum_{j=1}^{p^{\alpha-1}} J_{H,i,j} d_j' = p^{\alpha-1} \tilde{d_i}'$; where $1 \le i \le p^{\alpha-1}$.*
3. *The following holds, $A_{L,L_1} \tilde{d_0}' + p \sum_{j=1}^{p^{\alpha-1}} J_{H,i,j} \tilde{d_j}' = p^\alpha d_i'$; where $1 \le i \le p^{\alpha-1}$.*
4. *All the entries of $A_{L,L_1} d_0'$ are divisible by p.*
5. *All the entries of $A_{L,L_1} \tilde{d_0}'$ are divisible by p.*
6. *The difference coefficients of d_0' in L satisfy $A_{L,L_1} d_0' = \sum_{i=1}^{p^{\alpha-1}} \tilde{d_i}'$.*
7. *The following holds, $A_{L,L_1} \tilde{d_0}' = p \sum_{i=1}^{p^{\alpha-1}} d_i'$.*

Proof. We use the same technique as in proposition 3.2.7. Let χ' be any nonprincipal character of H; let χ_1 be an extension of χ' from H to G. Let D be a GSHDS of G. By corollary 3.2.2,

$$\begin{aligned} d_H(\chi', D') &= \frac{p^{\frac{(2\alpha+1)-1}{2}}}{[G:H]} \{ |\overline{D} \cap \chi_1 H^T| - |\overline{D}^{(n_0)} \cap \chi_1 H^T| \} \\ &= \frac{p^\alpha}{p} \{ |\overline{D} \cap \chi_1 H^T| - |\overline{D}^{(n_0)} \cap \chi_1 H^T| \} \\ &= p^{\alpha-1} \{ |\overline{D} \cap \chi_1 H^T| - |\overline{D}^{(n_0)} \cap \chi_1 H^T| \}, \end{aligned}$$

hence, all difference coefficients of D' are divisible by $p^{\alpha-1}$. Thus, parts 1 through 7 follow by corollary 3.4.11. □

Proposition 3.4.13. *Under the assumptions of proposition 3.4.12, let $\alpha = 3$; then,*

1. *The set D'' is a GSHDS in L.*

2. *Let $\mu_p : G \to G$ be defined as $\mu_p(x) = p \cdot x$. Clearly, $\mu_p(G) = L$. Let $H' = ker(\mu_p)$. Clearly, $H' = \{x \in G \mid p \cdot x = 0\}$. Let $d_{D\cap L}$ be the QRS space representation of ± 1 of $D'' = D \cap L$ in L. Let $\nu_{G,H'}$ be the vector of difference intersection numbers of D with respect to H' in G. Then,*

$$\nu_{G,H'} \quad = \quad p^2 d_{D\cap L}.$$

3. *The difference coefficients of d'_0 in L are divisible by p. That is, $A_{L,L_1} d'_0 = p\overline{d_0}'$, where $\overline{d_0}'$ is a $p^2 + p + 1 \times 1$ vector of ± 1s.*

4. *The difference coefficients of d' in H are divisible by p^2. That is, $A_{H,H_1} d' = p^2 \tilde{d}'$ for some integral vector $\tilde{d}'$.*

5. *The following holds, $A_{L,L_1} \tilde{d_0}' = p\overline{\tilde{d}_0}'$ for some integral vector $\overline{\tilde{d}_0}'$.*

6. *The following holds, $\overline{\tilde{d}_0}' = \sum_{i=1}^{p^2} d_i$.*

7. *The following holds, $p\overline{d_0}' = \sum_{i=1}^{p^2} \tilde{d_i}'$.*

Proof. Clearly, d'_0 is a representation of D''. Hence, by part 4 of proposition 3.4.12 $A_{L,L_1} d'_0$ a multiple of p at least. That is, all the difference coefficients of D'' in L are multiples of p. By proposition 3.1.10 part 4, we conclude that D'' must be a GSHDS.

Now we proceed to show the second part. Clearly, by proposition 3.2.8,

$$p^3 d_{\overline{D}\cap L} \quad = \quad A_{L,L_1} \nu_{G,H'}.$$

Consider,

$$\begin{aligned} p^2\nu_{G,H'} &= A^2_{L,L_1}\nu_{G,H'} \\ &= p^3 A_{L,L_1} d_{\overline{D}\cap L} \\ &= p^3 p d_{D\cap L} \text{ because } D\cap L \text{ is a GSHDS} \\ &= p^4 d_{D\cap L}, \end{aligned}$$

hence, the second part follows.

The remaining parts follow from parts 1, 2, 3, 4, 5, 6, and 7 of proposition 3.4.12.

□

3.4.3 Results for Θs Induced by Galois Group Structures

In the following we will let $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^{2\beta+1} = (\mathbb{Z}/p\mathbb{Z}) \times H$, where $H = (\mathbb{Z}/p^2\mathbb{Z})^{2\beta+1}$ and $L = pH \simeq (\mathbb{Z}/p\mathbb{Z})^{2\beta+1}$.

In the construction of the H_1 orbit representatives of proposition 3.4.2, we will pick the set $\{l_1, \ldots, l_{r'}\} \subset \mu_{q-1}$ to be any slice of $\frac{\mu^2_{q-1}}{\mu^2_{p-1}}$ consisting of Quadratic Residues of μ_{q-1}. We will do this to deduce group algebra equations. The following proposition justifies the choice of the l_is.

Proposition 3.4.14. *Let $q = p^{2\beta+1}$ then any slice of $\frac{\mu^2_{q-1}}{\mu^2_{p-1}}$ is also an slice of $\frac{\mu_{q-1}}{\mu_{p-1}}$.*

Proof. Clearly, the number representatives in a slice of $\frac{\mu^2_{q-1}}{\mu^2_{p-1}}$ is the same as the number of representatives in a slice of $\frac{\mu_{q-1}}{\mu_{p-1}}$. It suffices to show that: if $x, y \in \mu^2_{q-1}$ are inequivalent mod μ^2_{p-1}, then they are inequivalent mod μ_{p-1}.[10] Thus, suppose otherwise; i.e., x, y are inequivalent mod μ^2_{p-1} but they are equivalent mod μ_{p-1}. Let $x = y\psi$, where $\psi \in \mu_{p-1}\backslash\mu^2_{p-1}$. Clearly, the quadratic residue symbol $\left(\frac{\cdot}{p}\right)$ is a multiplicative

[10] in the multiplicative sense.

character of μ_{q-1}. Hence,

$$\begin{aligned} 1 &= \left(\frac{x}{p}\right) \\ &= \left(\frac{y}{p}\right)\left(\frac{\psi}{p}\right) \\ &= \left(\frac{\psi}{p}\right). \end{aligned}$$

Therefore, ψ is a quadratic residue in μ_{q-1}. Thus, $\mu_{p-1} \subset \mu_{q-1}^2$. The following claim will give us a contradiction.

Claim 3.4.15. *Let p be a prime and $q = p^\beta$, then: $\mathbb{F}_p^* \subset (\mathbb{F}_q^*)^2$ if and only if $q = p^{2\alpha}$ is an even power of p.*

Proof. ($\Rightarrow$) If $\psi \in (\mathbb{F}_p^*) \backslash (\mathbb{F}_p^*)^2$, then the splitting field of ψ over $\mathbb{F}_p$ must be contained in $\mathbb{F}_q$; Hence, $\mathbb{Z}/2\mathbb{Z}$ must be a subgroup of $G(\mathbb{F}_q \mid \mathbb{F}_p)$, the Galois Group of $\mathbb{F}_q$ over $\mathbb{F}_p$. Note that $G(\mathbb{F}_q, \mathbb{F}_p) = (\mathbb{Z}/\beta\mathbb{Z})$; thus, 2 must divide β since $(\mathbb{Z}/2\mathbb{Z}) \subset (\mathbb{Z}/\beta\mathbb{Z})$.

($\Leftarrow$) Let $\psi \in (\mathbb{F}_p^*) \backslash (\mathbb{F}_p^*)^2$, then the splitting field of ψ over $\mathbb{F}_p$ has degree 2; hence, it has Galois Group $(\mathbb{Z}/2\mathbb{Z})$ and order p^2. Note that the Galois Group of $\mathbb{F}_q$ over $\mathbb{F}_p$ is $(\mathbb{Z}/2\alpha\mathbb{Z})$. Hence, $\mathbb{F}_q$ has a subfield $\mathbb{F}$ with Galois Group $(\mathbb{Z}/2\mathbb{Z})$ and order p^2. Since, the field of p^2 elements is unique modulo field isomorphisms, it must follow that $\mathbb{F}$ is the splitting field of ψ. Thus, $\psi \in (\mathbb{F}_q^*)^2$ and the conclusion follows. □

By the previous claim, we arrive at a contradiction. □

We note that our choice of l_is is also a multiplicative group since $\frac{\mu_{q-1}^2}{\mu_{p-1}^2}$ is naturally a multiplicative group. This property will prove useful. Also, instead of using the pairing θ of corollary 3.4.5 to calculate A_{H,H_1}, we will use another pairing that is induced by the Galois Ring structure of $H = GR(p^2, 2\beta + 1)$. The pairing θ that we will use is:

$$\theta(g')(g) = \eta_{p^2}^{f_0(Tr(g' * g))},$$

where Tr is the trace map of the Galois Ring $GR(p^2, 2\beta+1) = H$, $*$ is the product operation of the Galois Ring, and $f_0()$ is defined in definition 3.1.18.

Under the choice of the l_is and θ, we can prove similar results as those deduced for the case when θ is induced by $\langle , \rangle_H$.

Proposition 3.4.16. *Let $H = (\mathbb{Z}/p^2\mathbb{Z})^{2\beta+1}$ and $L = p \cdot H \simeq (\mathbb{Z}/p\mathbb{Z})^{2\beta+1}$. Then, there is an ordering of the orbits of the action of H_1 on $H\backslash\{0\}$, such that:*

$$A_{H,H_1} = \begin{pmatrix} 0 & pA_{L,L_1} & \cdots & pA_{L,L_1} \\ A_{L,L_1} & pJ_{H,1,1} & \cdots & pJ_{H,1,p^{2\beta}} \\ \vdots & \vdots & \cdots & \vdots \\ A_{L,L_1} & pJ_{H,p^{2\beta},1} & \cdots & pJ_{H,p^{2\beta},p^{2\beta}} \end{pmatrix} \begin{matrix} \} & m_{2\beta+1,p} \\ \} & p^{2\beta}m_{2\beta+1,p} \end{matrix},$$

where $m_{2\beta+1,p} = p^{2\beta} + p^{2\beta-1} + \cdots + p + 1$.

Proof. The same proof of corollary 3.4.9 will hold since Tr is a bilinear function. □

Proposition 3.4.17. *Let H and A_{H,H_1} be given as they are in proposition 3.4.16. Let*

$$B'_H = \begin{pmatrix} J_{H,1,1} & \cdots & J_{H,1,p^{2\beta}} \\ \vdots & \cdots & \vdots \\ J_{H,p^{2\beta},1} & \cdots & J_{H,p^{2\beta},p^{2\beta}} \end{pmatrix},$$

and $B_H = pB'_H$. Then,

1. *The matrix B'_H has zero row sums, i.e., $B'_H J = 0$; and, $\sum_{j=1}^{p^{\alpha-1}} J_{H,i,j} = 0$.*
2. *The matrix B'_H has zero column sums, i.e., $JB'_H = 0$; and, $\sum_{i=1}^{p^{\alpha-1}} J_{H,i,j} = 0$.*
3. *The matrix B_H satisfies $B_H^3 = \frac{|H|}{p} B_H = p^{2\alpha-1} B_H$.*
4. *The matrix B_H satisfies $B_H^2 = p^{2\alpha-1} I - p^{\alpha} J_{p^{\alpha-1},p^{\alpha-1}} \otimes I_{r'}$.*

Proof. The proof is similar to corollary 3.4.10. □

Proposition 3.4.18. *Let $\underline{j}$ be the vector all 1s. Using the assumptions on the l_is and the results and notation of propositions 3.4.16 and 3.4.17, where $H = (\mathbb{Z}/p\mathbb{Z})^{2\beta+1}$ and $L = p \cdot H \simeq (\mathbb{Z}/p\mathbb{Z})^{2\beta+1}$, the following hold:*

1. *The matrix $J_{H,s,t}$ has constant row sum. That is, $J_{H,s,t}\underline{j} = \lambda_{s,t}\underline{j}$ for some integer $\lambda_{s,t}$. More percisely,*

$$\lambda_{s,t} \;=\; \sum_{j=1}^{p^{2\beta}} \left(\frac{Tr'(l_j(1+p(l'_s+l'_t)))}{p} \right),$$

   where $Tr'(x) : GR(p^2, 2\beta+1) \to (\mathbb{Z}/p\mathbb{Z})$ is given by $f_0(Tr(x))$.

2. *The matrix A_{L,L_1} has constant row sum. That is, $A_{L,L_1}\underline{j} = \epsilon_0 p^{\beta}\underline{j}$ where $\epsilon_0 \in \{1, -1\}$.*

3. *Let $L = [[\lambda_{s,t}]]$, the matrix formed by the $\lambda_{s,t}$s. Then,*

$$L^2 \;=\; p^{2\beta-1}(p^{2\beta}I - J).$$

4. *The matrix L of part 3 is self transposed. That is, $L^T = L$.*

Proof. Part 1 is a direct consequence of our choice of l_is, they form a group under Galois Ring multiplication, and the choice of $\theta(g)(g')$. Clearly, $J_{H,s,t}$ is a matrix on the tuples $(l_i(1+pl'_s), l_j(1+pl'_t))$; hence, the ith coordinate of $J_{H,s,t}\underline{j}$ is equal to:

$$\sum_{j=1}^{p^{2\beta}} \left(\frac{Tr'(l_i(1+pl'_s)l_j(1+pl'_t))}{p} \right) \;=\; \sum_{t=1}^{p^{2\beta}} \left(\frac{Tr'(l_i l_j(1+p(l'_s+l'_t)))}{p} \right).$$

Note that $(1+p(l'_s+l'_t))$ is fixed in the above sum. Also, $l_i l_j = l_{\sigma(j)}\alpha_{i,j}$ where: σ is the induced permutation action of l_i on $\frac{\mu_{q-1}^2}{\mu_{p-1}^2}$, and $\alpha_{i,j} \in \mu_{p-1}^2$ is some quadratic residue

mod p. Clearly,

$$\begin{aligned}\left(\frac{Tr'(l_i l_j(1+p(l'_s+l'_t)))}{p}\right) &= \left(\frac{Tr'(l_{\sigma(j)}\alpha_{i,j}(1+p(l'_s+l'_t)))}{p}\right)\\ &= \left(\frac{\alpha_{i,j}}{p}\right)\left(\frac{Tr'(l_{\sigma(j)}(1+p(l'_s+l'_t)))}{p}\right)\\ &= \left(\frac{Tr'(l_{\sigma(j)}(1+p(l'_s+l'_t)))}{p}\right)\\ &= \left(\frac{Tr'(l_{\sigma(j)}l''_{s,t})}{p}\right),\end{aligned}$$

where $l''_{s,t} = 1 + p(l'_s + l'_t)$. Hence, the ith coordinate of $J_{H,s,t}\underline{j}$ is equal to:

$$\begin{aligned}\sum_{j=1}^{p^{2\beta}}\left(\frac{Tr'(l_i l_j(1+p(l'_s+l'_t)))}{p}\right) &= \sum_{j=1}^{p^{2\beta}}\left(\frac{Tr'(l_{\sigma(j)}l''_{s,t})}{p}\right)\\ &= \sum_{j=1}^{p^{2\beta}}\left(\frac{Tr'(l_j l''_{s,t})}{p}\right),\end{aligned}$$

which is a value that is independent of i but dependent on s, t. This shows part 1.

Now, we proceed to show part 2. Note that by the choice of the l_is, the vector of all 1s ,$\underline{j}$, represents the Quadratic Residues $(\mathbb{F}^*_{p^{2\beta+1}})^2$ of $L \simeq (\mathbb{F}_{p^{2\beta+1}}, +)$. Hence $A_{L,L_1}\underline{j} = p^\beta \overline{d}$ for some vector $\overline{d}$ of $\pm$1s, since $\underline{j}$ is a GSHDS in L. Clearly, the ith coordinate of $A_{L,L_1}\underline{j}$ is given by:

$$\sum_{j=1}^{r'}\left(\frac{Tr'(\overline{l_i l_j})}{p}\right),$$

where $\overline{l_i} = l_i \bmod p$ and $\overline{l_j} = l_j \bmod p$. Clearly, $\{\overline{l_1}, \cdots, \overline{l_{r'}}\} = \frac{(\mathbb{F}^*_{p^{2\beta+1}})^2}{(\mathbb{F}^*_p)^2}$ is a group; and, by using a similar reasoning as part 1, we can deduce that the ith coordinate of

$A_{L,L_1}\underline{j}$ is given by:

$$\begin{aligned}\sum_{j=1}^{r'}\left(\frac{Tr'(\overline{l_i l_j})}{p}\right) &= \sum_{j=1}^{r'}\left(\frac{Tr'(\overline{l_{\sigma(j)}})}{p}\right)\\ &= \sum_{j=1}^{r'}\left(\frac{Tr'(\overline{l_j})}{p}\right)\\ &= \epsilon_0 p^{\beta},\end{aligned}$$

where $\epsilon_0 = \pm 1$. Thus, the ith coordinate $A_{L,L_1}\underline{j}$ is independent of i and the second part follows.

To show part 3, consider the following equation from proposition 3.4.17.

$$\sum_{k=1}^{p^{2\beta}}(pJ_{H,i,k})(pJ_{H,k,j}) = \delta_{i,j}p^{4\beta+1}I - p^{2\beta+1}I \tag{3.18}$$

By multiplying(3.18) by $\underline{j}$ and simplyfing, we get part 3.

Part 4 follows from $J_{H,s,t} = J_{H,t,s}$. □

We will identify each block $J_{H,i,j}$ of A_{H,H_1} with the element $l'_j \in \frac{\mu_{q-1}\cup\{0\}}{\mu_{p-1}\cup\{0\}} \simeq \frac{(\mathbb{F}_q,+)}{(\mathbb{F}_p,+)} \simeq (\mathbb{Z}/p\mathbb{Z})^{2\beta}$. Under this identification, the matrix L of proposition 3.4.18 can be thought as a matrix over entries indexed by the elements of $(\mathbb{F}_{p^{2\beta+1}},+)$ mod $(\mathbb{F}_p,+)$. Hence, the matrix L can be viewed as indexed by elements in $(\mathbb{F}_{p^{2\beta}},+) \simeq (\mathbb{Z}/p\mathbb{Z})^{2\beta} = K$. Thus, for each l'_j denote k_j the corresponding element in K. We will assume an ordering of the l'_js such that l_1 corresponds to the 0 element of K.

Let us introduce the following element of $\mathbb{Z}[K]$.

$$L_0 = \sum_{k_i\in K}\lambda_{1,i}x^{k_i}$$

We will show some properties of L_0, and we will use L_0 to stablish an existence condition for GSHDS in G.

Proposition 3.4.19. *Let ρ_K be the regular representation of K with action on $Z = \bigoplus_{i=1}^{p^{2\beta}}\mathbb{C}e_{k_i}$. Then,*

1. *For $g \in K$, $\rho_K(g^{-1})L = L\rho_K(g)$, as matrices.*

2. *For $\chi \in \widehat{K}$, $Le_\chi = \overline{\chi}(L_0)e_{\overline{\chi}}$ where:*

$$e_\chi = \frac{1}{p^{2\beta}} \sum_{k \in K} \overline{\chi}(k) e_k.$$

3. *For $\chi \in \widehat{K}$, χ non principal. $\chi(L_0)\overline{\chi}(L_0) = p^{4\beta-1}$.*

4. *Let χ_0 be the principal character of K, then $\chi_0(L_0) = 0$.*

5. *The following holds for L_0 in the group algebra of K,*

$$L_0 * L_0^{(-1)} = p^{4\beta-1}[x^0] - p^{2\beta-1}K(x).$$

Proof. We proceed to show part 1. Let $k_j \in K$ and l'_j the corresponding element to k_j. Consider $\sigma = 1 + pl'_j \in H$, clearly, $(\sigma)^* = \sigma$; since,

$$\begin{aligned} Tr(g\sigma(g')) &= Tr(g(1+pl'_j)g') \\ &= Tr((1+pl'_j)gg') \\ &= Tr(\sigma(g)g'). \end{aligned}$$

Hence, $((\sigma)^*)^{-1} = (\sigma)^{-1} = 1 - pl'_j$.

By proposition 3.1.21, it follows that:

$$\rho_X(1-pl'_j)A_{H,H_1} = A_{H,H_1}\rho_X(1+pl'_j). \tag{3.19}$$

We note that $\rho_X(1+pl'_j)$ permutes the blocks $J_{H,s,t}$, and it acts like $\rho_K(k_j)$ when we identify the blocks $J_{H,s,t}$ with their corresponding elements of K. Similarly, $\rho_X(1-pl'_j)$ acts like $\rho_K(k_j^{-1})$ on the blocks $J_{H,s,t}$.

We will show

$$\rho_K(k_j^{-1})L = L\rho_K(k_j), \tag{3.20}$$

by showing that the columns of the left-hand side equal the columns of the right-hand side. Thus, consider the column of the left-hand side of Equation (3.20) that corresponds to k_s. Clearly, this equals to

$$\rho_K(k_j^{-1}) \begin{pmatrix} \lambda_{1,s} \\ \vdots \\ \lambda_{p^{2\beta},s} \end{pmatrix}.$$

Clearly, this is equal to the left-hand side of Equation (3.19) after we multiply it on the right with the vector:

$$e_{k_s} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

where the 1s corresponds to the block $\{l_1(1+pl'_s), \ldots, l_{r'}(1+pl'_s)\}$.

Note that when we multiply the right-hand side of Equation (3.19) by e_{k_s} on the right, we get the column that corresponds to k_s in the right-hand side of Equation (3.20). This establishes part 1.

For part 2, consider the matrices:

$$P_\chi = \frac{1}{p^{2\beta}} \sum_{k \in K} \overline{\chi}(k) \rho_K(k),$$

where $\chi \in \widehat{K}$. Clearly, the set of P_χ forms a complete set of orthogonal projections.

That is, $\sum_{\chi \in \widehat{K}} P_\chi = I$ and $P_\chi P_{\chi'} = \delta_{\chi,\chi'} P_{\chi'}$. Also, one can calculate $P_\chi e_{\chi'} = \delta_{\chi,\chi'} e_{\chi'}$.

By part 1, we can show $P_{\overline{\chi'}} L = L P_{\chi'}$ for all χ'. Hence,

$$\begin{aligned} P_{\chi'} L e_\chi &= L P_{\overline{\chi'}} e_\chi \\ &= \begin{cases} L e_\chi & \text{if } \chi' = \overline{\chi}, \\ 0 & \text{else.} \end{cases} \end{aligned}$$

Thus, $L e_\chi$ belongs to $Im(P_{\overline{\chi}}) = \langle e_{\overline{\chi}} \rangle$. Hence,

$$L e_\chi = \alpha e_{\overline{\chi}},$$

for some complex number $\alpha \in \mathbb{C}$. We can calculate the number α by considering the first row of $L e_\chi$. Clearly, this row has value:

$$\begin{aligned} L_0^T e_\chi &= \langle L_0, e_{\overline{\chi}} \rangle \\ &= \frac{\overline{\chi}(L_0)}{p^{2\beta}}. \end{aligned}$$

On the other hand the first row of $\alpha e_{\overline{\chi}}$ has value $\frac{\alpha}{p^{2\beta}}$. Thus, $\alpha = \overline{\chi}(L_0)$. Hence, part 2 follows.

Now, we proceed to show part 3. Note that by part 2:

$$\begin{aligned} L e_\chi &= \overline{\chi}(L_0) e_{\overline{\chi}}, \\ L e_{\overline{\chi}} &= \chi(L_0) e_\chi, \end{aligned}$$

hence,

$$\begin{aligned}
\chi(L_0)\overline{\chi}(L_0) &= \chi(L_0)\overline{\chi}(L_0)e_{\chi}^{T}e_{\overline{\chi}} \\
&= (Le_{\overline{\chi}})^{T}(Le_{\chi}) \\
&= e_{\overline{\chi}}^{T}L^{T}Le_{\chi} \\
&= e_{\overline{\chi}}^{T}L^{2}e_{\chi} \\
&= e_{\overline{\chi}}^{T}(p^{2\beta-1}(p^{2\beta}I - J))e_{\chi} \\
&= p^{4\beta-1}e_{\overline{\chi}}^{T}e_{\chi} \\
&= p^{4\beta-1}.
\end{aligned}$$

Thus, part 3 follows.

Clearly, part 4 follows from proposition 3.4.17, since the row sums of B'_H are zero. This forces the row sums of L to be zero. In particular, the sum of all the entries of L_0 are zero.

Part 5 follows from parts 3 and 4 by using Fourier inversion. □

The next result, gives a solution to an equation in the group algebra of K whenever there is a GSHDS in $(\mathbb{Z}/p\mathbb{Z}) \times H$.

Proposition 3.4.20. *Let D be a GSHDS in $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^{2\beta+1}$. Then, there are elements A and B in $\mathbb{Z}[K]$ such that:*

1. *The following holds, $p^{2\beta}A = \chi_0(A)K(x) + L_0 * B^{(-1)}$; where χ_0 is the principal character of K.*

2. *The following holds, $p^{2\beta}B = \chi_0(B)K(x) + pL_0 * A^{(-1)}$; where χ_0 is the principal character of K.*

3. *The principal character of A is given by $\chi_0(A) = p^{\beta-1}\epsilon_0 b_0$, where ϵ_0 is ± 1 and b_0 is an integer.*

4. *The principal character of B is given by $\chi_0(B) = p^{\beta}\epsilon_0 a_0$; where ϵ_0 is ± 1, and equal to the ϵ_0 of part 3; and, a_0 is an integer.*

5. *All the coefficients of A are odd, and $\chi_0(A)$ is odd.*

6. *All the coefficients of B are odd, and $\chi_0(B)$ is odd.*

7. *The integers a_0 and b_0 are odd integers.*

Proof. We will proceed using the same analysis as proposition 3.4.11 and proposition 3.4.12. Let us assume that there is a GSHDS D in $G = (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p^2\mathbb{Z})^{2\beta+1}$. Let $H = \{0\} \times (\mathbb{Z}/p^2\mathbb{Z})^{2\beta+1}$, $L = p \cdot H$ and $K = \frac{L}{(\mathbb{Z}/p\mathbb{Z})}$. Let $D' = H \cap D$ and $D'' = L \cap D$. Let d' be the vector of ± 1s representing D' using the H_1 orbit representatives of $\widetilde{H}$ in proposition 3.4.16. Clearly, $d' = (d_0'^T, d_1'^T, \ldots, d_{p^{2\beta}}'^T)$, where d_i' is a $(p^{2\beta} + \cdots + p + 1) \times 1$ vector of ± 1s. Also, let $\tilde{d_i}'$ be the difference coefficients corresponding to the H_1 classes in d_i'. Using the same technique as in proposition 3.2.7, for $\chi' \in \widehat{H}$ a nonprincipal character, and χ_1 any extension of χ' to G, we have by corollary 3.2.2:

$$d_H(\chi', D') \;=\; p^{2\beta}\{|\overline{D} \cap \chi_1 H^T| - |\overline{D}^{(n_0)} \cap \chi_1 H^T|\}, \tag{3.21}$$

where $H^T = (\mathbb{Z}/p\mathbb{Z}) \times \{0\}$. Thus, we have:

$$A_{H,H_1} d' \;=\; p^{2\beta}\nu',$$

where $\nu' = (\nu_0'^T, \nu_1'^T, \ldots, \nu_{p^{2\beta}}'^T)$ is a vector of odd integers between $-p$ and p whose entries are defined by the right-hand side of Equation (3.21).

Using the form of A_{H,H_1} given by proposition 3.4.16, we get the following equations:

$$p \sum_{j=1}^{p^{2\beta}} A_{L,L_1} d_j' \;=\; p^{2\beta}\nu_0', \tag{3.22}$$

$$A_{L,L_1} d_0' + p \sum_{j=1}^{p^{2\beta}} J_{H,i,j} d_j' \;=\; p^{2\beta}\nu_i'. \tag{3.23}$$

By taking the inner product of Equation (3.22) with $\underline{j}$ and using the fact that $A_{L,L_1}^T =$

A_{L,L_1}, we get

$$\sum_{j=1}^{p^{2\beta}} p^{\beta+1}\epsilon_0\langle d'_j, \underline{j}\rangle \;=\; p^{2\beta}\langle \nu'_0, \underline{j}\rangle,$$

thus,

$$\sum_{j=1}^{p^{2\beta}} \langle d'_j, \underline{j}\rangle \;=\; p^{\beta-1}\epsilon_0\langle \nu'_0, \underline{j}\rangle.$$

Let $a = (a_1, \ldots, a_{p^{2\beta}})^T$, where $a_i = \langle d'_i, \underline{j}\rangle$, and let $b = (b_1, \ldots, b_{p^{2\beta}})^T$, where $b_i = \langle \nu'_i, \underline{j}\rangle$. Also, let $a_0 = \langle d'_0, \underline{j}\rangle$ and $b_0 = \langle \nu'_0, \underline{j}\rangle$.

We have shown that

$$\langle a, \underline{j}\rangle \;=\; p^{\beta-1}\epsilon_0 b_0. \tag{3.24}$$

Now, we will take the inner product of Equation (3.23) with $\underline{j}$, we get:

$$\langle A_{L,L_1} d'_0, \underline{j}\rangle + p\sum_{j=1}^{p^{2\beta}} \langle J_{H,i,j} d'_j, \underline{j}\rangle \;=\; p^{2\beta}\langle \nu'_i, \underline{j}\rangle,$$

where we used $J^T_{H,i,j} = J_{H,i,j}$. Hence, we have the following simplification:

$$\epsilon_0 p^{\beta}\langle d'_0, \underline{j}\rangle + p\sum_{j=1}^{p^{2\beta}} \lambda_{i,j}\langle d'_j, \underline{j}\rangle \;=\; p^{2\beta}\langle \nu'_i, \underline{j}\rangle,$$

or,

$$\epsilon_0 p^{\beta} a_0 + p\sum_{j=1}^{p^{2\beta}} \lambda_{i,j} a_j \;=\; p^{2\beta} b_i,$$

thus, we can deduce the following matrix equation:

$$p^{2\beta-1} b \;=\; p^{\beta-1}\epsilon_0 a_0 \underline{j} + La. \tag{3.25}$$

Performing the same analysis but starting with the equation $A_{H,H_1}\nu' = p^{2\beta+1}d'$, we get the following equations:

$$\begin{aligned} \langle b, \underline{j}\rangle &= p^{\beta}\epsilon_0 a_0, && (3.26)\\ p^{2\beta}a &= \epsilon_0 p^{\beta-1} b_0 \underline{j} + Lb. && (3.27) \end{aligned}$$

Let A be the element of $\mathbb{Z}[K]$ that has value a_i at k_i, and B be the element of $\mathbb{Z}[K]$ that has value b_i at k_i. We will use Equation (3.25) to establish a condition on the character values of A and B.

Let χ be a nonprincipal character of K. Equation (3.25) gives:

$$p^{2\beta-1}\langle b, e_\chi\rangle = \epsilon_0 a_0 p^{\beta-1}\langle \underline{j}, e_\chi\rangle + \langle La, e_\chi\rangle.$$

Since χ is nonprincipal, we have $\langle \underline{j}, e_\chi\rangle = 0$. Thus,

$$\begin{aligned} p^{2\beta-1}\langle e_\chi, b\rangle &= \langle e_\chi, La\rangle \\ &= \langle Le_\chi, a\rangle \\ &= \langle \overline{\chi}(L_0)e_{\overline{\chi}}, a\rangle \\ &= \overline{\chi}(L_0)\langle e_{\overline{\chi}}, a\rangle. \end{aligned}$$

Since, for any a, $\langle e_\chi, a\rangle = \frac{1}{p^{2\beta}}\overline{\chi}(a)$, we have:

$$\begin{aligned} p^{2\beta-1}\overline{\chi}(B) &= \overline{\chi}(L_0)\chi(A), \\ p^{2\beta-1}\chi(B) &= \chi(L_0)\overline{\chi}(A). && (3.28) \end{aligned}$$

Similarly, using Equation (3.27), we get:

$$p^{2\beta}\chi(A) = \chi(L_0)\overline{\chi}(B). \quad (3.29)$$

To show part 1, suffices to show that the left-hand side of part 1 and right-hand side of part 1 have the same character values; the equation will follow by Fourier

inversion in K. Note that for any nonprincipal character, Equation (3.29) shows that the left-hand side of part 1 and the right-hand side of part 1, do indeed, have the same character values. It suffices to show that the same holds for the principal character.

The principal character of the left-hand side of part 1 is $p^{2\beta}\chi_0(A)$. On the other hand, the principal character of the right-hand side is:

$$\begin{aligned}\chi_0(\chi_0(A)K(x) + L_0 * B^{(-1)}) &= \chi_0(A)p^{2\beta} + \chi_0(L_0)\overline{\chi}(B) \\ &= \chi_0(A)p^{2\beta},\end{aligned}$$

where we used $\chi_0(L_0) = 0$. This shows that part 1, does indeed, agree on both sides at the principal character. Thus, part 1 follows.

To show part 2, we use a similar analysis. By using Equation (3.28), we can deduce that the left-hand side of part 2 has the same character value as the right-hand side whenever the character used is nonprincipal. Thus, it suffices to show the same for the principal character χ_0. Clearly, the principal character of the left-hand side of part 2 is $p^{2\beta}\chi_0(B)$. On the other hand, the principal character of the right-hand side is:

$$\begin{aligned}\chi_0(\chi_0(B)K(x) + pL_0 * A^{(-1)}) &= \chi_0(B)p^{2\beta} + p\chi_0(L_0)\overline{\chi}(A) \\ &= \chi_0(B)p^{2\beta}.\end{aligned}$$

Thus, part 2 follows.

Clearly, part 3 is Equation (3.24) and part 4 is Equation (3.26).

We will show parts 5, 6, and 7 together. First, we will show that a_i is odd for $i = 0, \ldots, r'$. This will show that: all the coefficients of A are odd; a_0 is odd; $\chi_0(B)$ is odd, by part 4; $\chi_0(A)$ is odd, since it is the sum of an odd number of odd numbers; and b_0 is odd, by part 3. Finally, we will show that b_i is odd for $i = 1, \ldots, r'$.

Consider $a_i = \langle d'_i, \underline{j} \rangle$. Clearly, d'_i is a vector of ± 1s of length $r' = p^{2\beta} + \cdots + p + 1$. Let x be the number of entries in d'_i that are $+1$, and let y be the number of entries

of d'_i that are -1. Clearly,

$$\begin{aligned} x - y &= a_i, \\ x + y &= r'. \end{aligned}$$

Note that $r' = 1 \bmod 2$. Hence, the above equations mod 2 give $a_i = x - y = x + y = r' = 1$. Thus, a_i is odd.

It suffices to show b_i is odd for $i = 1, \ldots, r'$. By manipulating Equation (3.27) algebraically we can deduce:

$$p^{2\beta}a - \epsilon_0 p^{\beta-1} b_0 \underline{j} = Lb.$$

By multiplying the above equation by L on both sides, and simplyfing L^2 by using proposition 3.4.18; we deduce.

$$L(p^{2\beta}a - \epsilon_0 p^{\beta-1} b_0 \underline{j}) = p^{2\beta-1}(p^{2\beta}I - J)b. \tag{3.30}$$

Note that mod 2,

$$\begin{aligned} p^{2\beta}a - \epsilon_0 p^{\beta-1} b_0 \underline{j} &= \underline{j} - \underline{j} \\ &= 0, \end{aligned}$$

hence, Equation (3.30) mod 2 implies:

$$\begin{aligned} 0 &= (I - J)b \\ &= b - \chi_0(B)\underline{j} \\ &= b - \underline{j}. \end{aligned}$$

Thus, all the entries of b are odd. □

We leave as open problem to determine the feasibility of the elements $A, B \in \mathbb{Z}[K]$ derived in proposition 3.4.20. We note that the element L_0 can be nontrivial to

calculate.

3.5 Results for General G

We close this chapter by showing two existence conditions for a general abelian p-group G. The first result, due to Johnsen in [11], is the first exponent bound known for Skew Hadamard Difference Sets. The second result is a relation between the difference intersection numbers $\nu_{G,H}(D,h)$ and the difference coefficients $d_G(\chi,D)$, where we use a special subgroup $H \subset G$.

3.5.1 Johnsen's Exponent Bound

We show Johnsen's exponent bound, which is a special case of Xiang's exponent bound, to demonstrate the usefulness of the incidence structures A_{G,G_1}.

Proposition 3.5.1. *Let $D \subset D$ be a GSHDS, where $|G| = v = p^{2\alpha+1}$ and $exp(G) = p^s$. Then, $s \leq \alpha + 1$.*

Proof. Let,

$$\begin{aligned} G &= (\mathbb{Z}/p^s\mathbb{Z}) \times (\mathbb{Z}/p^{a_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p^{a_r}\mathbb{Z}) \\ &= (\mathbb{Z}/p^s\mathbb{Z}) \times L, \end{aligned}$$

where $s \geq a_2 \geq \cdots \geq a_r$. Consider the projection:

$$\pi : G \to (\mathbb{Z}/p^s\mathbb{Z}) = H,$$

where, $ker(\pi) = L$. By proposition 3.2.8, we have:

$$A_{H,H_1}\nu_{G,L}(D) = d_G(D,H),$$

where $\nu_{G,L}(D)$ are the difference intersection numbers of D with respect to L in G, and $d_G(D,H)$ are the difference coefficients of D with respect to the characters of H

extended to G. Since D is a GSHDS, we must have:

$$A_{H,H_1}\nu_{G,L}(D) \;=\; p^{\alpha}d_{\overline{D}\cap\widehat{H}},$$

where $\widehat{H} \hookrightarrow \widehat{G}$ by mapping $\chi \in \widehat{H} \to \chi \circ \pi \in \widehat{G}$. By multiplying by A_{H,H_1} on both sides and using proposition 3.1.22, we have

$$p^{s-1}\nu_{G,L}(D) \;=\; p^{\alpha}A_{H,H_1}d_{\overline{D}\cap\widehat{H}},$$

hence,

$$p^{s-1-\alpha}\nu_{G,L}(D) \;=\; A_{H,H_1}d_{\overline{D}\cap\widehat{H}}.$$

By proposition 3.3.7, we deduce

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & p^{s-1} \\ 0 & 0 & 0 & \cdots & p^{s-2} & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & p^2 & \cdots & 0 & 0 \\ 0 & p & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} d_{\overline{D}\cap\widehat{H}} \;=\; p^{s-1-\alpha}\nu_{G,L}(D).$$

By looking at the last row of the previous matrix equation, we deduce

$$\pm 1 \;=\; p^{s-1-\alpha}\nu_{G,L}(D,\chi_1),$$

hence, $p^{1+\alpha-s}$ is integral and the conclusion follows. □

3.5.2 A Special Condition

We will assume a general abelian p-group G that admits a GSHDS D. We will consider the map $\mu_p : G \to p\cdot G = H \subset G$ given by $\mu_p(x) = p\cdot x$. We will denote the $ker(\mu_p)$ by L.

We will work toward showing the following proposition:

Proposition 3.5.2. *Let $d_{D\cap H}$ be the QRS representation of ± 1s of $D\cap H$ and $\nu_{G,L}$ be the difference intersection numbers of D with respect to L in G. There is an integral vector c such that:*

$$pc \;=\; (a_p - b_p)d_{D\cap H} - \nu_{G,L},$$

where a_p, b_p are integer constants depending on p and α.

We start by introducing the definition of the constants a_p, b_p. For this, we will need the algebra A_D induced by D in $\mathbb{Z}[G]$.

3.5.2.1 The Algebra Induced by D

Proposition 3.5.3. *Let $D \subset G$ be a GSHDS. Then, $A_D = \langle D, D^{(n_0)}, [1]\rangle \subset \mathbb{Z}[G]$ is a three-dimensional subalgebra of the group algebra.*

Proof. The GSHDS conditions give:

$$\begin{aligned} DD^{(n_0)} &= k_0[1] + \lambda D + \lambda D^{(n_0)}, \\ DD &= (k-k_0)[1] + (k-\lambda-1)D + (k-\lambda)D^{(n_0)}, \\ D^{(n_0)}D^{(n_0)} &= (k-k_0)[1] + (k-\lambda-1)D^{(n_0)} + (k-\lambda)D, \end{aligned}$$

hence, the algebra $\langle D, D^{(n_0)}, [0]\rangle$ is three-dimensional. □

Definition 3.5.4. *Let $D \subset G$ be a GSHDS. The constants $\mathrm{a_p(G)}, \mathrm{b_p(G)}$ are defined by:*

$$D^p \;=\; c_p(G)[1] + a_p(G)D + b_p(G)D^{(n_0)}.$$

The next proposition shows that the constants $a_p(G), b_p(G)$ do not depend on the structure of G; but, rather on the order of G.

Proposition 3.5.5. *Let G, G' be an abelian groups such that $|G| = p^{2\alpha+1} = |G'|$. If there are GSHDS $D \subset G$ and $D' \subset G'$, then:*

$$\begin{aligned} a_p(G) &= a_p(G'), \\ b_p(G) &= b_p(G'). \end{aligned}$$

Proof. It is sufficient to show that the algebras A_D and $A_{D'}$ are isomorphic. Clearly, the structures of these algebras depend on the parameters of D and D'; hence, it suffices to show that D and D' have the same parameters. Note that D and D' indeed have the same parameters since $|G| = |G'|$. □

By proposition 3.5.5, we can drop the G in the notation of the structure constants $a_p(G), b_p(G)$. The simplest example of the structure constants a_p, b_p is for the prime $p = 3$. For this case, $a_3 = \frac{v-3}{4}\frac{v-1}{2}$ and $b_3 = \frac{v-3}{4}\frac{v+1}{2}$.

By considering $G = (\mathbb{F}_{p^{2\alpha+1}}, +)$, we can show a divisibility property of the structures constants a_p, b_p.

Proposition 3.5.6. *Let $D \subset G$ be a GSHDS, where G is a p-group. Then,*

$$p \mid (a_p - b_p).$$

Proof. Let $G = (\mathbb{F}_{p^{2\alpha+1}}, +)$, D be the GSHDS given by the Quadratic Residues of $\mathbb{F}_{p^{2\alpha+1}}$. By definition,

$$\begin{aligned} D^p &= c_p[1] + a_p D + b_p D^{(n_0)}, \\ (D^{(n_0)})^p &= c_p[1] + a_p D^{(n_0)} + b_p D, \end{aligned}$$

hence,

$$D^p - (D^{(n_0)})^p = (a_p - b_p)(D - D^{(n_0)}). \tag{3.31}$$

Also, by using the binomial theorem, there is $C \in \mathbb{Z}[G]$ such that:

$$\begin{aligned} D^p &= \mu_p \cdot D + pC, \\ (D^{(n_0)})^p &= \mu_p \cdot D^{(n_0)} + pC^{(n_0)}. \end{aligned}$$

Since, G is elementary p-abelian, we must have $\mu_p \cdot D = k[1]$ and $\mu_p \cdot D^{(n_0)} = k[1]$. Hence,

$$D^p - (D^{(n_0)})^p = p(C - C^{(n_0)}). \tag{3.32}$$

By equating equations (3.32) and (3.31), we deduce

$$(a_p - b_p)(D - D^{(n_0)}) = p(C - C^{(n_0)}),$$

hence, the conclusion follows. □

3.5.2.2 The Result

Proposition 3.5.7. *Let $d_{D\cap H}$ be the QRS representation of ± 1s of $D \cap H$ and $\nu_{G,L}$ be the difference intersection numbers of D with respect to L in G. There is an integral vector c such that:*

$$pc = (a_p - b_p)d_{D\cap H} - \nu_{G,L},$$

where a_p, b_p are integer constants depending on p and α.

Proof. We apply the same technique of proposition 3.5.6. Let $H = \mu_p \cdot G \subset G$, and $L = ker(\mu_p)$. Clearly, a similar reasoning as proposition 3.5.6 gives:

$$\begin{aligned} (a_p - b_p)(D - D^{(n_0)}) &= D^p - (D^{(n_0)})^p \\ &= \mu_p \cdot (D - D^{(n_0)}) + p(C - C^{(n_0)}). \end{aligned}$$

We restrict the previous equation to H. Thus, we deduce a similar equation in $\mathbb{Z}[H]$:

$$(a_p - b_p)(D_H - D_H^{(n_0)}) \quad = \quad \mu_p \cdot (D - D^{(n_0)}) + p(C_H - C_H^{(n_0)}).$$

We view the previous equation as an equation of Compact QRSs. Hence, we deduce:

$$(a_p - b_p)d_{H\cap D} \quad = \quad \nu_{G,L}(D) + pc,$$

where c is the integral vector corresponding to the Compact QRS: $C_H - C_H^{(n_0)}$. Clearly, the conclusion follows from the previous equation. □

Chapter 4

Equivariant Incidence Structures

In this chapter, we will study the inclusion matrices $W_{t,k}$ of t-subsets vs. k-subsets and their corresponding versions when the action of a permutation group is present.

In the first section, we will go over preliminary material about the space:

$$Hom_G(N, M) \;=\; \{T \mid T : N \to M \text{ , } T \text{ is a } G\text{-map}\},$$

where N, M are G-modules; also, the Smith Group of integral matrices, and the Johnson Scheme $J(v, k)$. These results will provide background for the sections that will follow.

In the second section, we will consider G-modules N, M when the G-action is given by a permutation action. We will study the Johnson Scheme that arises from the action of G, and we will show results analogous to the results given for the Johnson Scheme $J(v, k)$ in the section of preliminaries.

In the third section, we study the analogous matrices, $M_{t,k}$ and $M'_{t,k}$, of $W_{t,k}$ when the G-action is given by a permutation action. We show bounds on the exponent of the Smith Group of $M_{t,k}$ and $M'_{t,k}$, and we demonstrate that $M_{t,k}$ and $M'_{t,k}$ have full rank. Also, we give a partial answer to the integral preimage problem for $M_{t,k}$ and $M'_{t,k}$, and we give a brief study of the kernel of $M_{t,k}$ and $M'_{t,k}$.

In the fourth section, we introduce the concept of a "positive equivariant G-signing," and give some conditions on the existence of such signings.

In the fifth section, we consider the case when $G = Stab(\Omega)$, where Ω is a partition

of $\{1, \ldots, v\}$. We give examples of (t, k)-bases that admit a stabilizer group of the form $Stab(\Omega)$. We provide reduction results for showing that sets $\beta_{t,k}$ of columns of $W_{t,k}$ form a (t, k)-basis, and admit a positive equivariant G-signing. We formulate a conjecture about positive equivariant G-signings for special (t, k)-bases.

In the sixth section, we study the case when $G = (\mathbb{Z}/n\mathbb{Z})$. We find a $(2, 3)$ and $(2, 4)$-basis by introducing a partition of the orbits of G on the k-subsets. We use these bases to calculate the Smith Groups of $M_{2,3}, M'_{2,3}, M_{2,4}, M'_{2,4}$, and we give some partial results for the case $(3, 4)$.

4.1 Preliminaries

4.1.1 G-maps and G-spaces

Most of the results of this section are elemental, however, we include them for completeness. We will assume that $T : V \to W$ is a G-map of G-spaces where the vector spaces are taken over the complex numbers $\mathbb{C}$. We will also assume that G has $r + 1$ irreducible representations $M_0, M_1, \ldots, M_r$ over the complex numbers, and $\chi_0, \chi_1, \ldots, \chi_r$ are their corresponding irreducible characters; where χ_0 is the trivial character and M_0 is the trivial representation.

We will build machinery toward:

1. understanding the spaces $Hom_G(N, L)$ and $Hom_G(N, N)$, where N and L are G-spaces,

2. providing for a canonical form for $T \in Hom_G(N, L)$,

3. proving necessary and sufficient conditions when $T \in Hom_G(N, L)$ has full rank.

Our first result is well-known in the theory of finite group representations as "Masche's theorem."

Proposition 4.1.1. *Let*

1. *The space V be a G-module with representation $\rho_V : G \to GL(V)$.*

2. *The subspace $W \subset V$ be a G-submodule.*

3. *Define $\langle v, w \rangle_G$ be defined as,*

$$\begin{aligned} \langle v, w \rangle_G &= \frac{1}{|G|} \sum_{g \in G} \langle \rho_V(g)v, \rho_V(g)w \rangle \\ &= \overline{v}^T A_G w, \end{aligned}$$

where $A_G = \frac{\sum_{g \in G} \overline{\rho(g)}^t \rho(g)}{|G|}$ and $\langle , \rangle$ is the standard Hermitian inner product.

Then,

1. *The space V decomposes as $V = W \bigoplus W^T$, where $W^T = \{v \in V | \langle v, w \rangle_G = 0 \ \forall w \in W\}$ is a G-module.*

2. *For all $g_0 \in G$, $A_{G,V} \rho(g_0) = \overline{\rho(g_0^{-1})}^t A_G$.*

Proof. Note that,

$$\begin{aligned} \langle v, v \rangle_g &= \overline{v}^T \overline{\rho(g)}^T \rho(g) v \\ &= \langle \rho_V(g)v, \rho_V(g)v \rangle \\ &\geq 0, \end{aligned}$$

is a positive semidefinite inner product. Thus,

$$A_g = \overline{\rho(g)}^T \rho(g),$$

is a positive semidefinite Hermitian matrix. Therefore,

$$A_G = \frac{1}{|G|} \sum_{g \in G} \overline{\rho(g)}^T \rho(g),$$

is positive definite Hermitian as it is the sum of positive semidefinite Hermitian matrices and a positive definite Hermitian matrix, namely $A_1 = \frac{1}{|G|} I$. Thus,

$$\langle v, w \rangle_G = \overline{v}^T A_G w,$$

is a positive definite Hermitian inner product.

By looking at a basis of W extended to a basis of V and then applying Gram-Schmidt, one can show that $V = W \bigoplus W^T$,[1] where $W^T = \{v \in V | \langle v, w \rangle_G = 0 \ \forall w \in W\}$.

It suffices to show that W^T is G-invariant. Note that $\langle , \rangle_G$ is G-invariant in the following sense:

$$\langle v, w \rangle_G \ = \ \langle \rho_V(g)v, \rho_V(g)w \rangle_G \ \forall v, w \in V \ , \forall g \in G.$$

Let $w \in W$ and $w' \in W^T$, as W is G-invariant, $\rho(g^{-1})w \in W$, hence:

$$\begin{aligned} 0 &= \langle \rho(g^{-1})w, w' \rangle_G \\ &= \langle \rho(g)\rho(g^{-1})w, \rho(g)w' \rangle_G \\ &= \langle w, \rho(g)w' \rangle_G, \end{aligned}$$

therefore, $\rho(g)w' \in W^T$. Thus, W^T is G-invariant.

We leave part 2 as an exercise. □

As a direct corrollary, we deduce that V is completely reducible. That is, if $W \subset V$ is G-submodule, then W "splits"; more precisely, there is a G-invariant submodule W_1, say W^T from above, such that $V = W \bigoplus W_1$. Applying the splitting procedure, we get that V is the direct sum of irreducible G-modules. Hence, $V = N_1 \bigoplus N_2 \bigoplus \cdots \bigoplus N_k$ where each N_k cannot be decomposed further and has no proper G-submodule. Under this decomposition of V, we will get some of the N_ks isomorphic to each other. Thus, we can group the N_k according to their isomorphism class. Let $V_i = \bigoplus_{N_k \simeq M_i} N_k \simeq M_i \bigoplus \cdots \bigoplus M_i \simeq a_i M_i$, where a_i = number of N_ks in the decomposition of V that are isomorphic to M_i. The next proposition tells us how to calculate these V_i.

[1] Since $\langle , \rangle_G$ is a positive definite Hermitian inner product, Gram-Schmidt works. If we did not show $\langle , \rangle_G$ is positive definite, we could have an "isotropic" inner product that may cause Gram-Schmidt to fail.

Proposition 4.1.2. *Let V be a $\mathbb{C}[G]$ space with $\rho_V : G \to GL_v(\mathbb{C})$ its representation, where $v = dim_{\mathbb{C}}(V)$. Also, let $P_{i,V} = \frac{\chi_i(1)}{|G|}\sum_{g\in G}\overline{\chi_i(g)}\rho_V(g)$, where χ_i is the ith irreducible complex character of G. Then,*

1. *The maps $P_{i,V}$ are G-maps.*
2. *The maps $P_{i,V}$ form a system of orthogonal projections. That is,*

$$\begin{aligned} P_{i,V}P_{j,V} &= \delta_{i,j}P_{i,V}, \\ \sum_{i=0}^{r} P_{i,V} &= I_V. \end{aligned}$$

3. *The space V decomposes into $V = \bigoplus_{i=0}^{r} Im(P_{i,V})$ as G-spaces.*
4. *The space $Im(P_{i,V})$ decomposes into $Im(P_{i,V}) \simeq M_i \bigoplus \cdots \bigoplus M_i \simeq a_i M_i$; where a_i is the multiplicity of the ith irreducible in V, and χ_V is the character of V.*

We will denote the spaces $Im(P_{i,V})$ as the distinct "Isotypes" of G in V.

Proof. This is a consequence of a result that can be found in [7] in Chapter 18, Proposition 13. □

As a remark, we note that $a_i = \langle \chi_V, \chi_i \rangle_G$ where $\langle , \rangle_G$ is the inner product on the "class function" space defined by:

$$\langle \chi_V, \chi_i \rangle_G = \frac{1}{|G|}\sum_{g\in G}\overline{\chi_V}(g)\chi_i(g).$$

Proposition 4.1.3. *Let $e_i \in \mathbb{C}[G]$,*

$$e_i = \frac{\chi_i(1)}{|G|}\sum_{g\in G}\overline{\chi_i(g)}g.$$

Then, the e_is are the central primitive idempotents *of $\mathbb{C}[G]$. Also, $e_0 + \cdots + e_r = 1$, $e_i e_j = \delta_{i,j}e_i$.*

Proof. This follows as $\rho_V(e_i) = P_{i,V}$ acts as identity on isomorphic copies of M_i in V and it acts as zero on isomorphic copies of M_j, $i \neq j$, in V. □

Using the inner product $\langle , \rangle_G$, one can define the adjoin of a G-map. Let $T : V \to W$ be a G-map between the G spaces V and W. Let $\langle , \rangle_{G,W}$ be the G-invariant inner product of W of proposition 4.1.1 constructed using the standard euclidean inner product of W. Similarly, define $\langle , \rangle_{G,V}$. Then, the Adjoin T^* of T is defined via the relation:

$$\langle Tv, w \rangle_{G,W} = \langle v, T^* w \rangle_{G,V}.$$

Clearly, a consequence of the definition is $T^* : W \to V$. We will proceed to calculate T^*.

Proposition 4.1.4. *Let $T : V \to W$ be a G-map. Then,*

1. *$T^* = A_{G,V}^{-1} \overline{T}^T A_{G,W}$ is a G-map.*

2a. *$Im(T^*) = (Ker(T))^T$.*

2b. *$Im(T^*)^T = Ker(T)$.*

3. *$V = Ker(T) \bigoplus Im(T^*)$.*

4. *$W = Ker(T^*) \bigoplus Im(T)$.*

5. *$(T^*)^* = T$.*

Where the orthogonal complement $(\cdot)^T$ is taken using the inner products $\langle , \rangle_{G,V}$ and $\langle , \rangle_{G,W}$.

Proof. We show part 1. A direct calculation shows $T^* = A_{G,V}^{-1} \overline{T}^t A_{G,W}$. We proceed to show that T^* is a G-map using this formula. In what follows, we will be using:

$$\begin{aligned} A_{G,V} \rho_V(g) &= \overline{\rho_V(g^{-1})}^T A_{G,V}, \\ \rho_V(g) A_{G,V}^{-1} &= A_{G,V}^{-1} \overline{\rho_V(g^{-1})}^T, \\ A_{G,W} \rho_W(g) &= \overline{\rho_W(g^{-1})}^T A_{G,W}, \\ \rho_W(g) A_{G,W}^{-1} &= A_{G,W}^{-1} \overline{\rho_W(g^{-1})}^T, \end{aligned}$$

which are consequences of proposition 4.1.1. Consider,

$$\begin{aligned} T^*\rho_W(g) &= A_{G,V}^{-1}\overline{T}^T A_{G,W}\rho_W(g) \\ &= A_{G,V}^{-1}\overline{T}^T\overline{\rho_W(g^{-1})}^T A_{G,W} \\ &= A_{G,V}^{-1}\overline{\rho_W(g^{-1})T}^T A_{G,W} \\ &= A_{G,V}^{-1}\overline{T\rho_V(g^{-1})}^T A_{G,W} \\ &= A_{G,V}^{-1}\overline{\rho_V(g^{-1})}^T\overline{T}^T A_{G,W} \\ &= \rho_V(g)A_{G,V}^{-1}\overline{T}^T A_{G,W} \\ &= \rho_V(g)T^*. \end{aligned}$$

Hence, part 1 follows.

Now we show parts 2a and 2b. We will show $Im(T^*) \subset (Ker(T))^T$. Let $v \in Ker(T)$ and $w \in W$, then:

$$\begin{aligned} \langle v, T^*w\rangle_{G,V} &= \langle Tv, w\rangle_{G,w} \\ &= \langle 0, w\rangle_{G,W} \\ &= 0, \end{aligned}$$

thus, $T^*w \in (Ker(T))^T$. Therefore, $Im(T^*) \subset (Ker(T))^T$.

Similarly, we will show $Im(T)^T \subset Ker(T^*)$. Let $w \in Im(T)^T$ and $v \in V$, then

$$\begin{aligned} 0 &= \langle w, Tv\rangle_{G,W} \\ &= \langle T^*w, v\rangle_{G,V}. \end{aligned}$$

Since, $\langle T^*w, v\rangle_{G,V} = 0$ for arbitrary $v \in V$, and $\langle , \rangle_{G,V}$ is positive definite, we must have $T^*w = 0$. Thus, $w \in Ker(T^*)$.

Note that T^* is also a G-map and $(T^*)^* = T$. By letting $T = T^*$ in the above argument, we can deduce $Im(T^*)^T \subset Ker(T)$. Thus, using the containments $Im(T^*)^T \subset Ker(T)$ and $Im(T^*) \subset (Ker(T))^T$ and proposition 4.1.1, we have $V = Im(T^*) \bigoplus Im(T^*)^T \subset Ker(T) \bigoplus Ker(T)^T = V$. Therefore, by applying a di-

mension argument we must have $Im(T^*)^T = Ker(T)$ and $Im(T^*) = Ker(T)^T$. This shows part 2.

Parts 3 and 4 are a consequence of part 2 and proposition 4.1.1.

Part 5 follows from part 1 by a direct calculation. □

Corollary 4.1.5. *The following are consequences of proposition 4.1.4.*

1. *T is injective if and only if T^* is surjective.*

2. *T is surjective if and only if T^* is injective.*

3. *T is an isomorphism if and only if T^* is an isomorphism.*

Proof. Clearly, part 3 is a consequence of parts 2 and 3. Also, part 1 is a consequence of proposition 4.1.4 part 3. Part 2 is a consequence of proposition 4.1.4 part 4. □

We will state a result that gives a description of G-maps between two G-spaces. The five results that follow are standard facts taught in a Graduate Course on Algebra, however, we include them for completeness. The following result, known as Schur's theorem, will prove to be essential for the next propositions.

Proposition 4.1.6. *Let M and N be two complex irreducible complex G spaces, and let $T \in Hom_G(M, N)$ be a G-map. Then,*

1. *If M is G-isomorphic to N, then $Hom_G(M, N) = \mathbb{C}I_{M,N}$, where, $I_{M,N}$ is any fixed G-space isomorphism between M and N. That is, if $T \in Hom_G(M, N)$, then $T = \lambda I_{M,N}$, where $\lambda \in \mathbb{C}$. Also, if we choose a different vector space isomorphism, say $I'_{M,N}$, the λ changes accordingly to λ' by finding γ such that $I'_{M,N} = \gamma I_{M,N}$ and $T = \lambda' I'_{M,N} = \lambda'\gamma I_{M,N} = \lambda I_{M,N}$. Hence, $\lambda = \lambda'\gamma$.*

2. *If M is nonisomorphic to N, then $Hom_G(M, N) = 0$.*

Proof. Let us consider the first case and assume M and N be G-isomorphic. Let $I_{M,N} : M \to N$ a fixed G-isomorphism between M and N. Consider, $T * I^{-1}_{M,N} : N \to N$. It is clearly a G-map of N to N. Consider $E_\lambda = T * I^{-1}_{M,N} - \lambda I_N$, is clearly again a G-map, where I_N is the identity map of N. By noting that $det(E_\lambda)$ is a polynomial

of degree $dim_{\mathbb{C}}(N)$, there is a λ for which E_λ is singular. That is, E_λ has nontrivial kernel $Ker(E_\lambda)$. Clearly, the kernel of E_λ is a G-submodule of N. Hence, by using the irreducibility and idecomposability of N, either: $ker(E_\lambda) = N$, or $ker(E_\lambda) = 0$. Since we assume $ker(E_\lambda) \neq 0$, we deduce $E_\lambda = 0$. Thus, $T * I_{M,N}^{-1} - \lambda I_N = 0$ and therefore $T = \lambda I_{M,N}$. This, shows the first assertion.

To show the second assertion, let us assume otherwise. That is, there is a nonzero $T \in Hom_G(M, N)$. Since M is irreducible and idecomposable, we deduce $ker(T) = 0$. Therefore, T is an injection, and $T(M)$ is a nontrivial G-submodule of N. By the irreducibility and idecomposability of N, we deduce $T(M) = N$. Therefore, T is a G-isomorphism between M and N. This is a contradiction. □

Proposition 4.1.7. *Let N, M be G-spaces that decompose into irreducibles as $N = V_1 \bigoplus \cdots \bigoplus V_k$ and $M = W_1 \bigoplus \cdots \bigoplus W_l$, where all V_is and W_is are G-isomorphic. Let $T \in Hom_G(N, M)$, and $U_{i,j} : V_j \to W_i$ be a fixed set of G-isomorphisms. Let $v \in N$ and $Tv = w \in M$. Clearly, these vectors decompose uniquely into $v = v_1 + \cdots + v_k$ and $w = w_1 + \cdots + w_l$, where $v_i \in V_i$ and $w_i \in W_i$. Using this decomposition, we can describe T as:*

$$T = \begin{pmatrix} \lambda_{1,1}U_{1,1} & \lambda_{1,2}U_{1,2} & \cdots & \lambda_{1,k}U_{1,k} \\ \lambda_{2,1}U_{2,1} & \lambda_{2,2}U_{2,2} & \cdots & \lambda_{2,k}U_{2,k} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{l,1}U_{l,1} & \lambda_{l,2}U_{l,2} & \cdots & \lambda_{l,k}U_{l,k} \end{pmatrix},$$

where the $\lambda_{i,j}$s depend on T and the choice of $U_{i,j}$s.

Proof. Let P_i be a projection on V_i and Q_i a projection on W_i. Without loss of generality, we can assume P_i and Q_i are G-maps by substituting P_i by P_i^G and Q_i by Q_i^G, where in general T^G is defined as:

$$T^G = \frac{1}{|G|} \sum_{g \in G} \rho(g) T \rho(g^{-1}).$$

By construction,

$$\begin{aligned} P_1 + \cdots + P_k &= I_N, \\ Q_1 + \cdots + Q_l &= I_M, \end{aligned}$$

where I_N is the identity on N and I_M the identity on M. Consider,

$$\begin{aligned} T &= (\sum_{i=1}^{l} Q_i) T (\sum_{j=1}^{k} P_j) \\ &= \sum_{i=1,j=1}^{i=l,j=k} Q_i T P_j \\ &= \sum_{i=1,j=1}^{i=l,j=k} T_{i,j}, \end{aligned}$$

where the map $T_{i,j} = Q_i T P_j$ takes $N \to W_i$ and has kernel $\sum_{s=0}^{j} V_s$. Essentially, it is a G-map from $V_j \to W_i$. By Schur's theorem, $T_{i,j} = \lambda_{i,j} U_{i,j}$ when $T_{i,j}$ is restricted to V_j. If we extend $U_{i,j}$ to all of N, by letting $U_{i,j}$ be zero on V_s for $s \neq j$, we get the following decomposition of T:

$$T = \sum_{i=1,j=1}^{i=1,j=k} \lambda_{i,j} U_{i,j}.$$

The result follows. □

Now, we consider the case when the W_is are not G-isomorphic to the V_is.

Proposition 4.1.8. *Let N and M be G-spaces where $N = V_1 \bigoplus \cdots \bigoplus V_k$ and $M = W_1 \bigoplus \cdots \bigoplus W_l$ are the corresponding decompositions into irreducibles, and $V_i \simeq V_j$, $W_i \simeq W_j$ as G-spaces. Suppose that $V_i \not\simeq W_j$, i.e., they are nonisomorphic G-spaces. Then, $Hom_G(N, M) = 0$.*

Proof. We proceed similarly to proposition 4.1.7. Let P_i be a projection on V_i, and Q_i a projection on W_i. Without loss of generality, assume P_i and Q_i are G-maps. By

construction,

$$\begin{aligned} P_1 + \cdots + P_k &= I_N, \\ Q_1 + \cdots + Q_l &= I_M, \end{aligned}$$

where I_N is the identity on N, and I_M the identity on M. Also, one has:

$$\begin{aligned} T &= (\sum_{i=1}^{l} Q_i) T (\sum_{j=1}^{k} P_j) \\ &= \sum_{i=1,j=1}^{i=l,j=k} Q_i T P_j \\ &= \sum_{i=1,j=1}^{i=l,j=k} T_{i,j}, \end{aligned}$$

where the map $T_{i,j} = Q_i T P_j$ takes $N \to W_i$ and has kernel $\sum_{s=0}^{j} V_s$. Essentially, it is a G-map from $V_j \to W_i$. By Schur's theorem, $T_{i,j} = 0$ when $T_{i,j}$ is restricted to V_j. In particular, $T_{i,j} = 0$ on all of N. The result follows. □

Corollary 4.1.9. *Let N be a G-space that decomposes into irreducibles of the same isomorphism type. That is, $N = V_1 \bigoplus \cdots \bigoplus V_k$ where $V_i \simeq V_j$ as G-spaces. Any basis of V_1 can be extended to a basis of N so that for any map $T \in Hom_G(N, N)$ the $U_{i,j}s$ in proposition 4.1.7 become the identity. That is,*

$$\begin{aligned} T &= \begin{pmatrix} \lambda_{1,1} I & \lambda_{1,2} I & \cdots & \lambda_{1,k} I \\ \lambda_{2,1} I & \lambda_{2,2} & \cdots & \lambda_{2,k} I \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{k,1} I & \lambda_{k,2} I & \cdots & \lambda_{k,k} I \end{pmatrix} \\ &= \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,k} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,k} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{k,1} & \lambda_{k,2} & \cdots & \lambda_{k,k} \end{pmatrix} \otimes I \\ &= M_{k,k} \otimes I, \end{aligned}$$

where I is the $s \times s$ identity matrix and $s = dim_{\mathbb{C}}(V_1)$.

Proof. Let $\{v_1^1, \ldots, v_s^1\}$ be a basis of V_1. Choose G-isomorphisms,

$$\begin{aligned} U_{1,1} = I_{V_1} &: V_1 \to V_1, \\ U_{2,1} &: V_1 \to V_2, \\ &\cdots \\ U_{k,1} &: V_1 \to V_k, \end{aligned}$$

where $U_{1,1}$ is the identity map. Define, $U_{i,j} = U_{i,1} * U_{j,1}^{-1}$, and choose the basis $\{v_1^i = U_{i,1}v_1^1, \ldots, v_s^i = U_{i,1}v_s^1\}$ for V_i. Clearly,

$$\begin{aligned} U_{i,j}v_l^j &= (U_{i,1} * U_{j,1}^{-1})(U_{j,1}v_l^1) \\ &= U_{i,1}v_l^1 \\ &= v_l^i. \end{aligned}$$

Therefore, with respect to the basis $\{v_1^j, \ldots, v_s^j\}$ of V_j and the basis $\{v_1^i, \ldots, v_s^i\}$ of V_i, the G-isomorphism $U_{i,j}$ has matrix representation the identity matrix.

Note that each of the $U_{i,j}$s are G-maps. Thus, under the bases $\{v_j^1\}_{j=1}^s, \ldots, \{v_j^k\}_{j=1}^s$ and our chosen G-isomorphisms $U_{i,j}$, the map T has the desired representation via an application of proposition 4.1.7.

We note that the choice of the bases $\{v_i^1\}, \ldots, \{v_i^k\}$ depend on the V_is chosen, the G-structure of N, and the particular choice of $\{v_i^1\}$. Hence, it suffices pick a basis $\{v_i^1\}$ to decompose any $T \in Hom_G(N, N)$ into $M_{k,k} \otimes I_s$, for some $k \times k$ matrix of complex numbers $M_{k,k}$. □

Using a similar proof, we can generalize the previous corollary.

Corollary 4.1.10. *Let N and M be G-spaces that decompose into irreducibles of the same isomorphism type. That is, $N = V_1 \bigoplus \cdots \bigoplus V_k$ where $V_i \simeq V_j$ as G-spaces, and $M = W_1 \bigoplus \cdots \bigoplus M_l$ where $W_i \simeq W_j$ as G-spaces. Choose a G-isomorphism $U_{1,1} : V_1 \to W_1$. Let $\beta = \{v_1, \ldots, v_s\}$ be a basis of V_1. Define $\gamma = \{w_1, \ldots, w_s\} = U_{1,1}\beta$*

as a basis of W_1. *Then, one can extended* β *to a basis of* N, γ *to a basis of* M, *and choose* $U_{i,j}s$ *in proposition 4.1.7 such that for any map* $T \in Hom_G(N, M)$ *the* $U_{i,j}s$ *in proposition 4.1.7 become the identity. That is,*

$$\begin{aligned} T &= \begin{pmatrix} \lambda_{1,1}I & \lambda_{1,2}I & \cdots & \lambda_{1,k}I \\ \lambda_{2,1}I & \lambda_{2,2} & \cdots & \lambda_{2,k}I \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{l,1}I & \lambda_{l,2}I & \cdots & \lambda_{l,k}I \end{pmatrix} \\ &= \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,k} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,k} \\ \cdots & \cdots & \cdots & \cdots \\ \lambda_{l,1} & \lambda_{k,2} & \cdots & \lambda_{l,k} \end{pmatrix} \otimes I \\ &= M_{l,k} \otimes I, \end{aligned}$$

where I *is the* $s \times s$ *identity matrix and* $s = dim_{\mathbb{C}}(V_1)$.

Let N, M, L be G-spaces where

$$\begin{aligned} N &\simeq N_1 \oplus \cdots \oplus N_n,\ N_i \simeq N_j, \\ M &\simeq M_1 \oplus \cdots \oplus M_m,\ M_i \simeq M_j, \\ L &\simeq L_1 \oplus \cdots \oplus L_l,\ L_i \simeq L_j, \end{aligned}$$

and $N_i \simeq M_i \simeq L_i$. As a remark, we observe that the proof of corollary 4.1.10 gives bases of N, M, L such that for any $T \in Hom_G(N, M), K \in Hom_G(M, L)$,

$$\begin{aligned} T &= M_{m,n} \otimes I_s, \\ K &= M_{l,m} \otimes I_s, \\ KT &= (M_{l,m}M_{m,n}) \otimes I_s, \end{aligned}$$

where $s = dim_{\mathbb{C}}(N_1)$.

We proceed to find a canonical form for $T \in Hom_G(N, L)$, however, we introduce

some notation before we state our result. Let,

$$\begin{aligned} N &= R_1 \bigoplus \cdots \bigoplus R_r, \\ L &= S_1 \bigoplus \cdots \bigoplus S_s, \end{aligned}$$

be the decomposition of N and L into irreducible G-modules. Let

$$\begin{aligned} X_1 &= \{i \mid \exists j \ni S_j \simeq R_i\}, \\ X_2 &= \{1, \ldots, r\} \backslash X_1, \\ Y_1 &= \{j \mid \exists i \ni S_j \simeq R_i\}, \\ Y_2 &= \{1, \ldots, s\} \backslash Y_1. \end{aligned}$$

Clearly, X_1 and Y_1 constitute up to G-isomorphism the irreducible components that are common to N and L, and X_2, Y_2 constitute up to G-isomorphism the irreducible components that are not common to both N and L. Let

$$\begin{aligned} N_1' &= \bigoplus_{i \in X_1} R_i, \\ N_2' &= \bigoplus_{j \in X_2} R_j, \\ L_1' &= \bigoplus_{i \in Y_1} S_i, \\ L_2' &= \bigoplus_{j \in Y_2} S_j. \end{aligned}$$

Let $\{M_{t_1}, \ldots, M_{t_k}\}$ be the distinct isomorphism classes of irreducibles among $\{R_i | i \in X_1\}$, let $\{M_{r_1}, \ldots, M_{r_n}\}$ be the distinct isomorphism classes of irreducibles among $\{R_j | j \in X_2\}$, and let $\{M_{s_1}, \ldots, M_{s_l}\}$ be the distinct isomorphism classes of irreducibles among $\{S_j | j \in Y_2\}$. Clearly, by construction, the distinct isomorphism classes of irreducibles among the $\{S_i | i \in X_1\}$ is given by $\{M_{t_1}, \ldots, M_{t_k}\}$. Also, by

construction,

$$\begin{aligned}\{M_{t_1},\ldots,M_{t_k}\}\cap\{M_{r_1},\ldots,M_{r_n}\} &= \phi,\\ \{M_{t_1},\ldots,M_{t_k}\}\cap\{M_{s_1},\ldots,M_{s_l}\} &= \phi,\\ \{M_{r_1},\ldots,M_{r_n}\}\cap\{M_{s_1},\ldots,M_{s_l}\} &= \phi.\end{aligned}$$

and

$$\begin{aligned}L &= L_1'\bigoplus L_2',\\ N &= N_1'\bigoplus N_2'.\end{aligned}$$

Let

$$\begin{aligned}N_1' &= N_{t_1}\bigoplus\cdots\bigoplus N_{t_k},\\ N_{t_i} &= N_{t_i,1}\bigoplus\cdots\bigoplus N_{t_i,a_i},\\ N_{t_i,j} &\simeq M_{t_i},\end{aligned}$$

and let

$$\begin{aligned}L_1' &= L_{t_1}\bigoplus\cdots\bigoplus L_{t_k},\\ L_{t_i} &= L_{t_i,1}\bigoplus\cdots\bigoplus L_{t_i,b_i},\\ L_{t_i,j} &\simeq M_{t_i}.\end{aligned}$$

Using the notation introduced above, we find a canonical for any $T\in Hom_G(N,L)$.

Proposition 4.1.11. *Let N and L be defined as above. Given a basis of,*

$$N_{t_1,1},N_{t_2,1},\ldots,N_{t_k,1},$$

one can extend these bases to a basis of N, and choose a basis of L such that for any $T\in Hom_G(N,L)$,

1. $L_2' \subset coker(T)$.

2. $N_2' \subset Ker(T)$.

3. *T has matrix representation:*

$$\begin{pmatrix} M_{b_1,a_1} \bigotimes I_{s_{t_1}} & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & M_{b_k,a_k} \bigotimes I_{s_{t_k}} & 0 \\ 0 & \cdots & 0 & 0_{dim_{\mathbb{C}}(L_2'),dim_{\mathbb{C}}(N_2')} \end{pmatrix}.$$

Where,

1. *The matrices M_{b_i,a_i} are complex $b_i \times a_i$ matrices that depend on T and the chosen basis of N and L.*

2. *The matrix $0_{dim_{\mathbb{C}}(L_2'),dim_{\mathbb{C}}(N_2')}$ is the $dim_{\mathbb{C}}(L_2') \times dim_{\mathbb{C}}(N_2')$ zero matrix.*

3. *The dimension of M_{t_i} is given by $s_{t_i} = dim_{\mathbb{C}}(M_{t_i})$.*

4. *The matrix $I_{s_{t_i}}$ is the $s_{t_i} \times s_{t_i}$ identity matrix.*

5. *The cokernel of T is the orthogonal complement of $Im(T)$ by using the inner product $\langle , \rangle_{G,L}$. That is, $coker(T) = Im(T)^T$.*

Proof. Let $T \in Hom_G(N, L)$ and fix a basis for the spaces N_{t_i} and L_{t_i}. We begin by recalling proposition 4.1.2 from which we deduce that $L_i = Im(P_{i,L})$ and $N_i = Im(P_{i,N})$. Clearly, $P_{s,N} = 0$ when M_s does not occur in N. Similary, $P_{s,L} = 0$ when

M_s does not occur in L. Therefore,

$$\begin{aligned} I_N &= \sum_{i=0}^{r} P_{i,N} \\ &= \sum_{i=1}^{k} P_{t_i,N} + \sum_{j=1}^{n} P_{r_j,N}, \\ I_L &= \sum_{i=0}^{r} P_{i,L} \\ &= \sum_{i=1}^{k} P_{t_i,L} + \sum_{j=1}^{l} P_{s_j,L}. \end{aligned} \tag{4.1}$$

Consider,

$$\begin{aligned} T &= (\sum_{i=0}^{r} P_{i,L}) T (\sum_{j=0}^{r} P_{j,N}) \\ &= \sum_{i=0,j=0}^{i=r,j=r} P_{i,L} T P_{j,N} \\ &= \sum_{i=0,j=0}^{i=r,j=r} T_{i,j}, \end{aligned}$$

where $T_{i,j} = P_{i,L} T P_{j,N}$. Note that $T_{i,j}$ is a map from $N \to L_i$ that is zero on N_ss for $s \neq j$. Therefore, $T_{i,j}$ can be viewed as a G-map from $N_j \to L_i$. By proposition 4.1.8, $T_{i,j} = 0$ whenever N_j and L_i are not of the same isomorphism type. Thus,

$$T = \sum_{i=0}^{r} T_{i,i},$$

where the above sum is over all irreducible representations of G. Using Equation (4.1), we deduce $P_{s,N} = 0$, whenever $s \neq t_1, \ldots, t_k$ and $s \neq r_1, \ldots, r_n$. Similarly, $P_{s,L} = 0$, whenever $s \neq t_1, \ldots, t_k$ and $s \neq s_1, \ldots, s_l$. Therefore,

$$T = \sum_{i=1}^{k} T_{t_i,t_i} + \sum_{j=1}^{n} T_{r_j,r_j} + \sum_{l=1}^{l} T_{s_l,s_l}.$$

Note that $P_{s_l,N} = 0$ and $P_{r_j,L} = 0$. Thus,

$$T = \sum_{i=1}^{k} T_{t_i,t_i}, \tag{4.2}$$

hence, we deduce that $T(N) \subset L_1'$ by considering,

$$\begin{aligned} P_{s_j,L}T &= \sum_{i=1}^{k} P_{s_j,L}T_{t_i,t_i} \\ &= 0. \end{aligned}$$

Since, $L = L_1' \bigoplus L_2'$, $L_2' = (L_1')^T$, and $T(N) \subset L_1'$; we deduce $L_2' = (L_1')^T \subset (T(N))^T = coker(T)$.

Also, we deduce that $N_2' \subset Ker(T)$ by considering

$$\begin{aligned} TP_{r_j,N} &= \sum_{i=1}^{k} T_{t_i,t_i}P_{r_j,N} \\ &= 0. \end{aligned}$$

Equation (4.2), shows that $T(N_{t_i}) \subset L_{t_i}$ and $T(N_2') = 0$. Thus, with respect to the decomposition of $N = N_{t_1} \bigoplus \cdots \bigoplus N_{t_k} \bigoplus N_2'$ and $L = L_{t_1} \bigoplus \cdots \bigoplus L_{t_k} \bigoplus L_2'$, we conclude that T has the matrix representation:

$$\begin{pmatrix} T_{t_1,t_1} & 0 & \cdots & 0 & 0 \\ 0 & T_{t_2,t_2} & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & 0 & \cdots \\ 0 & 0 & \cdots & T_{t_k,t_k} & 0 \\ 0 & 0 & \cdots & 0 & 0_{dim_{\mathbb{C}}(L_2'),dim_{\mathbb{C}}(N_2')} \end{pmatrix},$$

where T_{t_i,t_i} is the matrix representation of the map T_{t_i,t_i} with the domain restricted to N_{t_i} and the range restricted to L_{t_i}.

In general, we cannot deduce that the matrices T_{t_i,t_i} have matrix representation $M_{b_i,a_i} \bigotimes I_{\dim_{\mathbb{C}}(M_{t_i})}$. However, by applying Corrollary(4.1.10) to T_{t_i,t_i}, we can choose

a basis of N_{t_i} and L_{t_i} such that T_{t_i,t_i} has matrix representation $M_{b_i,a_i} \bigotimes I_{dim_{\mathbb{C}}(M_{t_i})}$. Hence, the result follows by choosing the bases provided by corollary 4.1.10. □

Using the notation of the previous proposition, we can show that the maps T_{t_i,t_i} inherit some of the properties of the map T. This is illustrated by the next proposition.

Proposition 4.1.12. *Let T, N, and L be given as in proposition 4.1.11, so that:*

$$T = \sum_{i=1}^{k} T_{t_i,t_i}.$$

Then,

1. *T is injective if and only if $N_2' = 0$ and for all $i = 1, \ldots, k$, T_{t_i,t_i} is injective when restricted to N_{t_i}.*

2. *T is surjective if and only if $L_2' = 0$ and for all $i = 1, \ldots, k$, T_{t_i,t_i} is surjective when its image is restricted to L_{t_i}.*

Proof. **Part 1**. ($\Rightarrow$) We show the contrapositive. Suppose that there is $v \in N_{t_m}$ such that $T_{t_m,t_m} v = 0$ for some t_m, and $v \neq 0$. By assumption, $v = P_{t_m,N} v$, and $P_{t_i,N} v = 0$ for $t_i \neq t_m$. Consider,

$$\begin{aligned} Tv &= \sum_{i=1}^{k} T_{t_i,t_i} v \\ &= \sum_{i=1}^{k} P_{t_i,L} T P_{t_i,N} v \\ &= P_{t_m,L} T P_{t_m,N} v \\ &= T_{t_m,t_m} v \\ &= 0, \end{aligned}$$

hence, T is not injective.

($\Leftarrow$) Conversely, suppose there was $v \in N$ such that $Tv = 0$. By supposition, we can assume $v \in N_1'$. Hence, v decomposes as $v = v_{t_1} + \cdots + v_{t_k}$, where $v_{t_i} \in N_{t_i}$.

Clearly,

$$\begin{aligned} Tv_{t_i} &= TP_{t_i,N}v_{t_i} \\ &= TP_{t_i,N}P_{t_i,N}v_{t_i} \\ &= P_{t_i,L}TP_{t_i,N}v_{t_i} \\ &= T_{t_i,t_i}v_{t_i}. \end{aligned}$$

Let $w_{t_i} = T_{t_i,t_i}v_{t_i}$. Clearly, $w_{t_i} \in L_{t_i}$. Consider

$$\begin{aligned} 0 &= Tv \\ &= \sum_{i=1}^{k} Tv_{t_i} \\ &= \sum_{i=1}^{k} TP_{t_i,N}v_{t_i} \\ &= \sum_{i=1}^{k} T_{t_i,t_i}v_{t_i} \\ &= \sum_{i=1}^{k} w_{t_i}. \end{aligned}$$

Since $L = L_{t_1} \bigoplus \cdots \bigoplus L_{t_k} \bigoplus L'_2$, the previous equation above forces $w_{t_i} = 0$ for all i.

Therefore, $T_{t_i,t_i}v_{t_i} = w_{t_i} = 0$ for all i. By the injectivity of T_{t_i,t_i}, we deduce $v_{t_i} = 0$. Clearly, this forces $v = 0$. Thus, we have shown that T is injective.

Part 2. ($\Rightarrow$) Without loss of generality, it suffices to show T_{t_1,t_1} is surjective. Let $w_{t_1} \in L_{t_1}$. Since T is surjective, there is a $v \in N$ such that $Tv = w_{t_1}$. Let $v_{t_1} = P_{t_1,N}v$ and consider,

$$\begin{aligned} w_{t_1} &= P_{t_1,L}w_{t_1} \\ &= P_{t_1,L}Tv_{t_1} \\ &= P_{t_1,L}TP_{t_1,N}P_{t_1,N}v \\ &= T_{t_1,t_1}v_{t_1}, \end{aligned}$$

hence, w_{t_1} has a preimage under T_{t_1,t_1}.

($\Leftarrow$) Conversely, let $w \in L$. By supposition, we can assume $w \in L_1'$. Hence, $w = \sum_{i=1}^{k} w_{t_i}$ where $w_{t_i} = P_{t_i,L} w$. Since each T_{t_i,t_i} is surjective, we can find $v_{t_i} \in N_{t_i}$ such that $w_{t_i} = T_{t_i,t_i} v_{t_i}$. Define $v = \sum_{i=1}^{k} v_{t_i}$, a direct calculation shows $w = Tv$. Hence, T is surjective. □

The next proposition shows that the operation $(\cdot)_{t_i,t_i}$ preserves algebraic operations.

Proposition 4.1.13. *Let N, L and K be G spaces. Let $T_i : N \to L$, $S_i : L \to K$, and $R : N \to K$ be G-maps. Define $R_{t_1,t_1} = P_{t_1,K} R P_{t_1,N}$, $(T_i)_{t_1,t_1} = P_{t_1,L} T_i P_{t_1,N}$, and $(S_i)_{t_1,t_1} = P_{t_1,K} T_i P_{t_1,L}$. Then, if*

$$R = \sum_{i=1}^{m} S_i T_i. \tag{4.3}$$

Then,

$$R_{t_1,t_1} = \sum_{i=1}^{m} (S_i)_{t_1,t_1} (T_i)_{t_1,t_1}.$$

Proof. Consider

$$\begin{aligned} R P_{t_1,N} &= R P_{t_1,N} P_{t_1,N} \text{ because } P_{t_1,N} \text{ is a projection,} \\ &= P_{t_1,K} R P_{t_1,L} \text{ because } R \text{ is a } G\text{-map,} \\ &= R_{t_1,t_1}. \end{aligned}$$

Similarly, we can show that $S_i T_i P_{t_1,N} = (S_i)_{t_1,t_1} (T_i)_{t_1,t_1}$.

We can deduce the conclusion by multiply Equation (4.3) on the right by $P_{t_1,N}$ and substituting the previous deductions. □

Definition 4.1.14. *Let $T \in Hom_G(N, L)$. Denote T_{t_1,t_1} by,*

$$T_{t_1,t_1} = P_{t_1,L} T P_{t_1,L}.$$

We will refer to T_{t_1,t_1} *as the* projection of T on the M_{t_1} type of N and L.

Proposition 4.1.15. *Let:*

1. *The function* $f(x_1, x_2, \ldots, x_n)$ *be a multivariable complex polynomial of* n *variables.*
2. *The maps* $T_1, \ldots, T_n$ *be* G*-maps from* N *to* L.
3. *Assume* $f(T_1, \ldots, T_n) = 0$.
4. *Define* S_i *as* $S_i = (T_i)_{t_1,t_1}$.

Then, $f(S_1, \ldots, S_n) = 0$.

Proof. This is a consequence of proposition 4.1.13. □

We close this section with a structure result about the spaces $Hom_G(N, N)$ that will be of importance in later sections. We will view $Hom_G(N, N)$ as a ring with multiplication given by function composition. The spaces $Hom_G(N, N)$ are known in the literature as the Hecke Rings, and we will denote them by $H(G, N)$.

Proposition 4.1.16. *Let* N *be* G*-space over the complex numbers* $\mathbb{C}$. *Let* $N \simeq a_0M_0 \bigoplus \cdots \bigoplus a_rM_r$, *where the* M_i*s are the irreducible complex representations of* G. *Then,*

1. *The space* $H(G, N)$ *decomposes as* $H(G, N) = M_{a_0,a_0}(\mathbb{C}) \times \cdots \times M_{a_r,a_r}(\mathbb{C})$.
2. *The space* $H(G, N)$ *is a semisimple ring.*
3. *The space* $H(G, N)$ *is commutative if and only if all* $a_i = 1$ *or* 0. *That is,* N *is "multiplicity free."*

Proof. Part 1 is a consequence of proposition 4.1.11. Part 2 is a consequence of part 1 and the Artin-Weddenburn theorem for semisimple rings. Part 3 is a clear consequence of part 1. □

4.1.2 General Results for Smith Groups

In this section, we will first study short exact sequences of $\mathbb{Z}$-modules to provide necessary background, then we will prove general results about smith groups.

We start with a few definitions.

Definition 4.1.17. *Given an integral matrix $M : \mathbb{Q}^n \to \mathbb{Q}^m$.*

1. *The* general smith group *$S(M)$ is defined as $\frac{\mathbb{Z}^m}{Col_{\mathbb{Z}}(M)}$.*
2. *The* finite part *or* torsion part *of the smith group of M is denoted as $\overline{S}(M) = \frac{Col_{\mathbb{Q}}(M) \cap \mathbb{Z}^m}{Col_{\mathbb{Z}}(M)}$.*
3. *The* free part *of $S(M)$ is denoted as $\mathbb{F}(M) = \frac{S(M)}{\overline{S}(M)}$.*
4. *The* abelian rank *$r(M)$ of M is the rank of $\mathbb{F}(M)$ as a free $\mathbb{Z}$-module. In general $r(M) = null(M) + cork(M)$, where:*

$$cork(M) \quad = \quad \begin{cases} m - n & \text{if } m > n, \\ 0 & \text{else.} \end{cases}$$

5. *The* rank *of M is defined as $rk(M) = dim_{\mathbb{Q}}(Col_{\mathbb{Q}}(A)) = dim_{\mathbb{Q}}(Row_{\mathbb{Q}}(A))$.*

Definition 4.1.18. *In general, given a finitely generated abelian group H, the* torsion part *will be denoted as $\overline{H}$ and the* free part *as $\mathbb{F}(H)$. All abelian groups will be assumed to be finitely generated.*

Definition 4.1.19. *Given a finite abelian group A, we will define by $\mathrm{A_p}$ its p-sylow subgroup. Assume $A_p = (\mathbb{Z}/p^f\mathbb{Z})^{a_f} \oplus \cdots \oplus (\mathbb{Z}/p\mathbb{Z})^{a_1}$, where $a_i \geq 0$ and $p^f = exp(A_p)$. Then,*

1. *Define $(\mathrm{A})^{(\mathrm{p^k})} = \mathrm{Ker}(\mathrm{A_p} \overset{\mu_{\mathrm{p^k}}}{\to} \mathrm{A_p})$ where $\mu_{p^k}(g) = p^k \cdot g$ in additive notation. It can be shown that:*

$$(\mathrm{A})^{(\mathrm{p^k})} \quad = \quad (\mathbb{Z}/p^k\mathbb{Z})^{a_f} \oplus \cdots \oplus (\mathbb{Z}/p^k\mathbb{Z})^{a_k} \oplus (\mathbb{Z}/p^{k-1}\mathbb{Z})^{a_{k-1}} \oplus \cdots \oplus (\mathbb{Z}/p\mathbb{Z})^{a_1}.$$

2. *Define* $\mathrm{f_p}$ *by* $\sum_{i=1}^{f} a_i$. *That is,* $\mathrm{f_p}$ *is the number of idecomposable cyclic components of* A_p.

3. *Define* $\mathrm{a_{k;p}}$ *and* $\mathrm{b_{k;p}}$ *such that* $\mathrm{b_{k;p}} = \mathrm{p^{a_{k;p}}} = |(\mathrm{A_p})^{(\mathrm{p^k})}|$. *Note that,*

$$\mathrm{a_{k:p}} \quad = \quad \sum_{i=1}^{k-1} i a_i + k(\sum_{i=k}^{f} a_i).$$

4. *Define* $\mathrm{f_{k;p}}$ *as the number of idecomposible cyclic components that contain* $(\mathbb{Z}/p^k\mathbb{Z})$. *Note that* $\mathrm{f_{1;p}} = \mathrm{f_p}$.

5. *Define* $\mathrm{g_{k;p}} = \mathrm{f_p} - \mathrm{f_{k+1,p}}$ *as the number of idemcomposable componets of order* $\leq p^k$.

Definition 4.1.20. *Given an integral matrix* M, *we will denote the order of the torsion part of the smith group of* M *by* $|\mathrm{M}|$. *That is,* $|\mathrm{M}| = |\overline{\mathrm{S}}(\mathrm{M})|$. *Also, by* $|\mathrm{M}|_\mathrm{p} = \mathrm{p^{v_p(|M|)}}$, *we will denote the p-norm of* $|M|$, *where* $v_p(\cdot)$ *is the p-valuation function.*

4.1.2.1 Short Exact Sequences of Z-Modules

We will use the standard algebraic operations of the Torsion functor, Tensor functor, Ext functor and Hom functor to generate exact sequences of $\mathbb{Z}$-modules from known short exact sequences of $\mathbb{Z}$-modules. We will do this to deduce results about short exact sequences of $\mathbb{Z}$-modules that will be used in our study of the smith group of integral matrices. We note that results concerning the quantities defined in definition 4.1.19 will not be used in later sections; however, we include them to provide a complete study of short exact sequence of $\mathbb{Z}$-modules.

We start with a result about finitely generated abelian groups.

Proposition 4.1.21. *Let* A *be a free abelian group and* B *a subgroup. Then* $r(\frac{A}{B}) = r(A) - r(B)$.

Proof. Since A is free abelian, B is also free abelian and $r(A) \geq r(B)$. Clearly, there is a $\mathbb{Z}$-isomorphism ϕ such that:

$$\begin{array}{ccc} A & \xrightarrow{\phi} & \mathbb{Z}^{r(A)} \\ \cup & & \cup \\ B & \xrightarrow{\phi} & L \end{array},$$

where L is a free submodule of $\mathbb{Z}^{r(A)}$ isomorphic to B and of abelian rank $r(B)$.

Let $v_1, \ldots, v_{r(B)}$ be a $\mathbb{Z}$-basis of L. Define $M = [v_1, \ldots, v_{r(B)}]$. Clearly, since the v_is form a $\mathbb{Z}$-basis, M must have full rank. Thus, $rk(M) = r(B)$ and $r(M) = r(A) - r(B)$. Note that, $\frac{A}{B} \simeq S(M)$. Hence, $r(\frac{A}{B}) = r(M) = r(A) - r(B)$. □

We recall two results can be found in Munkres' book in [19].

Proposition 4.1.22. *Let A_1, A_2, A_3 and D be finitely generated $\mathbb{Z}$-modules or abelian groups. Assume,*

$$0 \to A_1 \to A_2 \to A_3 \to 0.$$

And,

1. *Let $*$ be the Torsion product of $\mathbb{Z}$-modules.*
2. *Let $\otimes$ be the tensor product of $\mathbb{Z}$-modules.*
3. *Let $Hom(A, B)$ the space of all $\mathbb{Z}$-maps from A to B.*
4. *Let $Ext(A, B) = Ext^1(A, B)$ be the first chain group that arises from a $\mathbb{Z}$-projective resolution of A and of B.*

Then, there are exact sequences such that:

$$\begin{array}{ccccccccc} 0 & \to & A_1 * D & \to & A_2 * D & \to & A_3 * D & \to & \\ & & A_1 \otimes D & \to & A_2 \otimes D & \to & A_3 \otimes D & \to & 0, \end{array} \tag{4.4}$$

$$\begin{array}{ccccccccc} 0 & \to & Hom(D,A_1) & \to & Hom(D,A_2) & \to & Hom(D,A_3) & \to & \\ & & Ext(D,A_1) & \to & Ext(D,A_2) & \to & Ext(D,A_3) & \to & 0, \end{array}$$

$$\begin{array}{ccccccccc} 0 & \to & Hom(A_3,D) & \to & Hom(A_2,D) & \to & Hom(A_1,D) & \to & \\ & & Ext(A_3,D) & \to & Ext(A_2,D) & \to & Ext(A_1,D) & \to & 0. \end{array} \tag{4.5}$$

Proposition 4.1.23. *Let G be a finitely generated $\mathbb{Z}$-module. Then,*

1. *The isomorphisms of figure 4.1 hold.*

2. *The following are isomorphic:*

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z}) \otimes (\mathbb{Z}/n\mathbb{Z}) &\simeq (\mathbb{Z}/m\mathbb{Z}) * (\mathbb{Z}/n\mathbb{Z}) \\ &\simeq (\mathbb{Z}/d\mathbb{Z}), \\ Hom((\mathbb{Z}/m\mathbb{Z}),(\mathbb{Z}/n\mathbb{Z})) &\simeq Ext((\mathbb{Z}/m\mathbb{Z}),(\mathbb{Z}/n\mathbb{Z})) \\ &\simeq (\mathbb{Z}/d\mathbb{Z}), \end{aligned}$$

   where $d = \gcd(n,m)$.

As a corollary, we show:

Corollary 4.1.24. *Let A be finitely generated abelian group, i.e., $\mathbb{Z}$-module, and let p be a prime. Then,*

1. *$Hom(\mathbb{Z},A) \simeq A \otimes \mathbb{Z} \simeq A$.*

2. *$Hom(A,\mathbb{Z}) \simeq \mathbb{F}(A)$.*

3. *$Ext(A,\mathbb{Z}) \simeq \overline{A}$.*

4. *$Ext(\mathbb{Z},A) \simeq A * \mathbb{Z} \simeq 0$.*

$\mathbb{Z} \otimes G \simeq G$	$Hom(\mathbb{Z}, G) \simeq G$
$(\mathbb{Z}/m\mathbb{Z}) \otimes G \simeq \frac{G}{mG}$	$Hom((\mathbb{Z}/m\mathbb{Z}), G) \simeq ker(G \stackrel{\mu_m}{\to} G)$
$Z * G \simeq 0$	$Ext(\mathbb{Z}, G) \simeq 0$
$(\mathbb{Z}/m\mathbb{Z}) * G \simeq ker(G \stackrel{\mu_m}{\to} G)$	$Ext((\mathbb{Z}/m\mathbb{Z}), G) \simeq \frac{G}{mG}$
$(\mathbb{Z}/m\mathbb{Z}) \otimes \mathbb{Z} \simeq (\mathbb{Z}/m\mathbb{Z})$	$(\mathbb{Z}/m\mathbb{Z}) * \mathbb{Z} \simeq 0$
$Ext((\mathbb{Z}/m\mathbb{Z}), \mathbb{Z}) \simeq (\mathbb{Z}/m\mathbb{Z})$	$Hom((\mathbb{Z}/m\mathbb{Z}), \mathbb{Z}) \simeq 0$
$Hom(\oplus A_i, B) \simeq \oplus Hom(A_i, B)$	$Hom(B, \oplus A_i) \simeq \oplus Hom(B, A_i)$
$Ext(\oplus A_i, B) \simeq \oplus Ext(A_i, B)$	$Ext(B, \oplus A_i) \simeq \oplus Ext(B, A_i)$
$(\oplus A_i) \otimes B \simeq \oplus(A_i \otimes B)$	$B \otimes (\oplus A_i) \simeq \oplus(B \otimes A_i)$
$(\oplus A_i) * B \simeq \oplus(A_i * B)$	$B * (\oplus A_i) \simeq \oplus(B * A_i)$

Figure 4.1. Algebraic isomorphisms.

5. The following are isomorphic,

$$\begin{aligned} Hom((\mathbb{Z}/p^k\mathbb{Z}), A) \simeq Ext(A, (\mathbb{Z}/p^k\mathbb{Z})) &\simeq A * (\mathbb{Z}/p^k\mathbb{Z}) \simeq (A_p)^{(p^k)}, \\ Hom(A, (\mathbb{Z}/p^k\mathbb{Z})) \simeq Ext((\mathbb{Z}/p^k\mathbb{Z}), A) &\simeq \\ A \otimes (\mathbb{Z}/p^k\mathbb{Z}) &\simeq (A_p)^{(p^k)} \oplus (\mathbb{Z}/p^k\mathbb{Z})^{r(A)}. \end{aligned}$$

6. Let $exp(A)$ divide d, then the following are isomorphic,

$$\begin{aligned} Hom((\mathbb{Z}/d\mathbb{Z}), A) \simeq Ext(A, (\mathbb{Z}/d\mathbb{Z})) \simeq A * (\mathbb{Z}/d\mathbb{Z}) &\simeq \overline{A}, \\ Hom(A, (\mathbb{Z}/d\mathbb{Z})) \simeq Ext((\mathbb{Z}/d\mathbb{Z}), A) \simeq A \otimes (\mathbb{Z}/d\mathbb{Z}) &\simeq \overline{A} \oplus (\mathbb{Z}/d\mathbb{Z})^{r(A)}. \end{aligned}$$

As a corollary to the previously shown algebraic isomorphisms, we have:

Corollary 4.1.25. *Let A,B,C be $\mathbb{Z}$-modules such that,*

$$0 \to A \to B \to C \to 0.$$

Then,

1. *The abelian rank of B is given by $r(B) = r(A) + r(C)$.*
2. *If $r(A) = 0$, then there is an exact sequence such that,*

$$0 \to \overline{C} \to \overline{B} \to \overline{A} \to 0.$$

Proof. We proceed to show part 2. Choose $D = \mathbb{Z}$ in the exact sequence 4.5 of proposition 4.1.22. We have,

$$0 \to \mathbb{F}(C) \to \mathbb{F}(B) \to \mathbb{F}(A) \to \overline{C} \to \overline{B} \to \overline{A} \to 0.$$

Hence, we can deduce part 2 whenever $r(A) = 0$ since $\mathbb{F}(A) = 0$.

We show part 1. Note that the previous exact sequence gives $\frac{\mathbb{F}(B)}{\mathbb{F}(C)} \simeq H \subset \mathbb{F}(A)$, where H is also free. By proposition 4.1.21, $r(H) = r(B) - r(C)$. Also, note that $\frac{\mathbb{F}(A)}{H} \simeq K \subset \overline{C}$, where K is a torsion. Hence, $r(K) = 0$. By proposition 4.1.21, $r(K) = r(A) - r(H) = r(A) - r(B) + r(C)$ and the result follows. □

In general, when given an exact sequence of finitely generated abelian groups:

$$0 \to A_1 \to A_2 \to A_3 \to 0.$$

We cannot deduce the same about the torsion part of the A_is. That is, we cannot deduce that:

$$0 \to \overline{A_1} \to \overline{A_2} \to \overline{A_3} \to 0.$$

However, we can whenever A_1 has zero abelian rank.

Proposition 4.1.26. *Let A, B, C be $\mathbb{Z}$-modules such that,*

$$0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0.$$

Then, there is a $\mathbb{Z}$-module H such that:

1. *The following holds:*

$$\frac{\overline{B}}{\overline{A}} \oplus \overline{H} \oplus \mathbb{F}(H) \simeq \overline{C} \oplus \mathbb{F}(C).$$

2. *The following are isomorphic:*

$$\begin{aligned} \mathbb{F}(H) &\simeq \mathbb{F}(C), \\ \overline{H} &\simeq C_1 \subset \overline{C}, \\ \frac{\overline{B}}{\overline{A}} \oplus \overline{H} &\simeq \overline{C}, \end{aligned}$$

   where C_1 is a subgroup of $\overline{C}$.

3. *If $\overline{B}$ is injected to $\overline{C}$ by ψ, then $\overline{A} = \{0\}$ and,*

$$\overline{B} \oplus \overline{H} \simeq \overline{C}.$$

4. *If $r(A) = 0$, then $\overline{H}$ is trivial and there is an exact sequence such that:*

$$0 \to \overline{A} \to \overline{B} \to \overline{C} \to 0.$$

Proof. We show part 1. Since A is injected into B, we must have:

$$\begin{aligned} \frac{\overline{B}}{\overline{A}} \oplus \frac{\mathbb{F}(B)}{\mathbb{F}(A)} &\simeq \frac{\overline{B} \oplus \mathbb{F}(B)}{\overline{A} \oplus \mathbb{F}(A)} \\ &\simeq \frac{B}{A} \\ &\simeq C \\ &\simeq \overline{C} \oplus \mathbb{F}(C). \end{aligned}$$

Let $H = \frac{\mathbb{F}(B)}{\mathbb{F}(A)}$. Clearly, proposition 4.1.21 and corollary 4.1.25, we have $r(H) = r(B) - r(A) = r(C)$. Clearly, we can decompose H as $\overline{H} \oplus \mathbb{F}(H)$ to get the desired isomorphism.

Part 2 follows from the isomorphism of part 1.

We show part 3. We will show that $\overline{A} = 0$. Let $g \in \phi(\overline{A}) \subset \overline{B}$. Clearly, $\psi(g) = 0$ by exactness. Since $\overline{B}$ is injected into $\overline{C}$, it follows that $g = 0$. Hence, $\phi(\overline{A}) = 0$. Since ϕ is an injection, it follows that $\overline{A} = \{0\}$ and the result follows from part 2.

We show part 4. Since $r(A) = 0$, $A = \overline{A}$ is a torsion group. Thus, $\mathbb{F}(A) = \{0\}$. By part 2, we have $\frac{\overline{B}}{\overline{A}} \simeq \overline{C}$. Consider the following exact sequence:

$$0 \to \overline{A} \xrightarrow{\iota} \overline{B} \xrightarrow{\pi} \overline{C} \to 0,$$

where π is the canonical projection and ι is the inclusion. Hence, the result follows. □

Corollary 4.1.27. *Let A,B, C be finitely generated $\mathbb{Z}$-modules. Assume, $r(A) = 0$ and*

$$0 \to A \to B \to C \to 0.$$

Then, there are exact sequences:

$$0 \to \overline{A} \to \overline{B} \to \overline{C} \to 0,$$
$$0 \to \overline{C} \to \overline{B} \to \overline{A} \to 0.$$

Proof. The first exact sequence is given in proposition 4.1.26. The second exact sequence is given by corollary 4.1.25. □

The previous corollary gives a result that is not true for finite nonabelian groups.

Corollary 4.1.28. *Let A,B, and C be finite abelian groups such that $\frac{A}{B} \simeq C$, then there is a subgroup $C_1 \subset A$ such that $\frac{A}{C_1} \simeq B$ and $C_1 \simeq C$.*

Proof. Since $\frac{A}{B} \simeq C$, we can construct the following exact sequence of $\mathbb{Z}$-modules,

$$0 \to A \to B \to C \to 0.$$

Since all groups are torsion, corollary 4.1.27 applies and there is an exact sequence such that:

$$0 \to C \to B \to A \to 0.$$

Let C_1 be the injected image of C in the above sequence. Clearly, C_1 satisfies the conclusion. □

We close this section with two results on divisibility conditions of short exact sequence of $\mathbb{Z}$-modules. We will use the exact sequences of proposition 4.1.22, when $D = (\mathbb{Z}/p^k\mathbb{Z})$ and $D = (\mathbb{Z}/d\mathbb{Z})$, to deduce these conditions.

Proposition 4.1.29. *Let A_1, A_2, and A_3 be finitely generated abelian groups such that:*

$$0 \to A_1 \to A_2 \to A_3 \to 0.$$

Let p^k be a prime power , $d = lcm(exp(A_1), exp(A_2), exp(A_3))$ and $a_i = |\overline{A_i}|$. Then,

1. *The number $b_{k;p}(A_1)$ divides $b_{k;p}(A_2)$.*
2. *The number $b_{k;p}(A_3)$ divides $b_{k;p}(A_2)p^{kr(A_1)}$.*
3. *The number $b_{k;p}(A_2)$ divides $b_{k;p}(A_1)b_{k;p}(A_3)$.*
4. *The number a_1 divides a_2.*
5. *The number a_3 divides $a_2 d^{r(A_1)}$.*
6. *The number a_2 divides $a_1 a_3$.*

Proof. Consider the exact sequence 4.4 of proposition 4.1.22 when $D = (\mathbb{Z}/p^k\mathbb{Z})$,

$$\begin{aligned} 0 \to ((A_1)_p)^{(p^k)} \xrightarrow{\phi_1} ((A_2)_p)^{(p^k)} &\xrightarrow{\phi_2} ((A_3)_p)^{(p^k)} \xrightarrow{\phi_3} \\ ((A_1)_p)^{(p^k)} \oplus (\mathbb{Z}/p^k)^{r(A_1)} &\xrightarrow{\phi_4} ((A_2)_p)^{(p^k)} \oplus (\mathbb{Z}/p^k)^{r(A_2)} \xrightarrow{\phi_5} \cdots . \end{aligned}$$

We show parts 1, 2, and 3. By using the exactness condition, we construct a table of integral conditions shown in figure 4.2.

ϕ_i	$\lvert Domain(\phi_i)\rvert$	$\lvert Range(\phi_i)$	$\lvert Ker(\phi_i)\rvert$	$\lvert Im(\phi_i)\rvert$
1	$b_{k;p}(A_1)$	$b_{k;p}(A_2)$	1	$\frac{b_{k;p}(A_2)}{b_{k;p}(A_1)}$
2	$b_{k;p}(A_2)$	$b_{k;p}(A_3)$	$\frac{b_{k;p}(A_2)}{b_{k;p}(A_1)}$	$\frac{b_{k;p}(A_1)b_{k;p}(A_3)}{b_{k;p}(A_2)}$
3	$b_{k;p}(A_3)$	$b_{k;p}(A_1)p^{kr(A_1)}$	$\frac{b_{k;p}(A_1)b_{k;p}(A_3)}{b_{k;p}(A_2)}$	$\frac{b_{k;p}(A_2)p^{kr(A_1)}}{b_{k;p}(A_3)}$

Figure 4.2. Exact sequence integral conditions.

Clearly, parts 1, 2, and 3 follow from the integral conditions of figure 4.2.

We show parts 4, 5, and 6. Consider the exact sequence 4.4 of proposition 4.1.22 when $D = (\mathbb{Z}/d\mathbb{Z})$ and d is the $lcm(exp(\overline{A_1}), exp(\overline{A_1}), exp(\overline{A_2}))$.

$$0 \to \overline{A_1} \xrightarrow{\phi_1} \overline{A_2} \xrightarrow{\phi_2} \overline{A_3} \xrightarrow{\phi_3} \overline{A_1} \oplus (\mathbb{Z}/d)^{r(A_1)} \xrightarrow{\phi_4} \overline{A_2} \oplus (\mathbb{Z}/d)^{r(A_2)} \xrightarrow{\phi_5} \cdots .$$

By using the exactness condition, we construct the table of integral conditions shown in figure 4.3.

Clearly, parts 4, 5, and 6 follow from the integral conditions of figure 4.3. □

4.1.2.2 The Results

We will start with a proposition that we will generalize later.

Proposition 4.1.30. *Let $C = AB$ where $Ker(A) \cap Im(B) = \{0\}$, then $\overline{S}(B) \subset \overline{S}(C)$.*

ϕ_i	$\lvert Domain(\phi_i)\rvert$	$\lvert Range(\phi_i)$	$\lvert Ker(\phi_i)\rvert$	$\lvert Im(\phi_i)\rvert$
1	a_1	a_2	1	$\frac{a_2}{a_1}$
2	a_2	a_3	$\frac{a_2}{a_1}$	$\frac{a_1 a_3}{a_2}$
3	a_3	$a_1 d^{r(A_1)}$	$\frac{a_1 a_3}{a_2}$	$\frac{a_2 d^{r(A_1)}}{a_3}$

Figure 4.3. Exact sequence integral conditions.

Proof. Assume, B is $k \times n$ matrix. Let $e_1, \ldots, e_k, e_{k+1}, \ldots, e_n$ be a primitive integral basis of the domain of B such that,

$$Be_i = \begin{cases} d_i f_i & \text{for } i = 1, \ldots, k, \\ 0 & \text{for } i = k+1, \ldots, n. \end{cases}$$

where $f_1, \ldots, f_k$ is a primitive integral basis of the range of B, and the invariant factors of B are given by $\{d_i\}$.

Clearly $Ce_i = ABe_i = d_i Af_i$. Thus, $v_i = Af_i = C(\frac{e_i}{d_i})$ is in $Im_{\mathbb{Q}}(C)$. We claim that $Af_1, \ldots, Af_k$ forms a subgroup of $\overline{S}(C)$ that is isomorphic to $\overline{S}(B)$.

It suffices to show that whenever $\sum_{i=1}^{k} n_i Af_i = Cz$ for some $z \in \mathbb{Z}$, then $d_i | n_i$. Because $\{e_i\}$ is a primitive integral basis, there are integral z_i such that $z = \sum_{i=1}^{k} z_i e_i + \sum_{i=k+1}^{n} z_i e_i$. Hence,

$$\begin{aligned} \sum_{i=1}^{k} z_i d_i Af_i &= Cz \\ &= \sum_{i=1}^{k} n_i Af_i. \end{aligned}$$

Thus,

$$\sum_{i=1} (z_i d_i - n_i) f_i \in Ker(A) \cap Im(B) = \{0\}.$$

Because the f_is are linearly independent, we must have $z_i d_i = n_i$. □

We generalize proposition 4.1.30 in the next proposition.

Proposition 4.1.31. *Let $C = AB$, where A is $n \times r$, B is $r \times k$. Assume $Ker(A) \cap Im(B) = \{0\}$. Then,*

1. *There is a finitely generated abelian group H such that:*

$$0 \to H \to S(C) \to S(A) \to 0.$$

2. *The abelian rank $r(H)$ of H is $rk(A) - rk(C)$.*

3. *The torsion part of the Smith Group of B is contained in H, i.e. ,$\overline{S}(B) \subset H$. Hence, $\overline{S}(B) \subset \overline{H}$.*

4. *There is a finitely generated abelian group K such that:*

$$0 \to K \to S(B) \to H \to 0,$$

   where $r(K) = r(B) - r(H)$.

5. *If $r(H) = 0$, i.e., $rk(A) = rk(C)$, then there is a finite abelian group $\overline{H_1}$ such that $H \simeq \overline{S}(B) \oplus \overline{H_1}$.*

Proof. Consider the following inclusion of free abelian groups:

$$Col_{\mathbb{Z}}(AB) \subset Col_{\mathbb{Z}}(A) \subset \mathbb{Z}^n.$$

We can deduce the following short exact sequence of $\mathbb{Z}$-modules.

$$0 \to \frac{Col_{\mathbb{Z}}(A)}{Col_{\mathbb{Z}}(AB)} \to \frac{\mathbb{Z}^n}{Col_{\mathbb{Z}}(AB)} \to \frac{\mathbb{Z}^n}{Col_{\mathbb{Z}}(A)} \to 0,$$

Therefore,

$$0 \to H \to S(AB) \to S(A) \to 0,$$

where $H = \frac{Col_{\mathbb{Z}}(A)}{Col_{\mathbb{Z}}(AB)}$. Clearly, as H is the quotient of free abelian groups, we have $r(H) = rk(A) - rk(AB)$. Hence, parts 1 and 2 follow.

Clearly, we can view A as a map of $\mathbb{Z}$-modules. Consider,

$$\begin{array}{ccc} & & \mathbb{Z}^n \\ & & \cup \\ \mathbb{Z}^r & \stackrel{A}{\rightarrow} & Col_{\mathbb{Z}}(A) \\ \cup & & \cup \\ Col_{\mathbb{Q}}(B) \cap \mathbb{Z}^r & \stackrel{A}{\rightarrow} & L \\ \cup & & \cup \\ Col_{\mathbb{Z}}(B) & \stackrel{A}{\rightarrow} & Col_{\mathbb{Z}}(AB) \ , \end{array}$$

where A restricted to $Col_{\mathbb{Z}}(B)$ and $Col_{\mathbb{Q}}(B) \cap \mathbb{Z}^r$ is injective since $Ker(A) \cap Im(B) = \{0\}$. Thus, A factors through $Col_{\mathbb{Z}}(B)$ to give a surjective map:

$$\frac{\mathbb{Z}^r}{Col_{\mathbb{Z}}(B)} \stackrel{A}{\rightarrow} \frac{Col_{\mathbb{Z}}(A)}{Col_{\mathbb{Z}}(AB)} \rightarrow 0,$$

and an injective map:

$$0 \rightarrow \frac{Col_{\mathbb{Q}}(B) \cap \mathbb{Z}^r}{Col_{\mathbb{Z}}(B)} \stackrel{A}{\rightarrow} \frac{Col_{\mathbb{Z}}(A)}{Col_{\mathbb{Z}}(AB)}.$$

Thus,

$$S(B) \stackrel{A}{\rightarrow} H \rightarrow 0,$$
$$0 \rightarrow \overline{S}(B) \stackrel{A}{\rightarrow} H.$$

Let K denote the kernel of the map induced by A, then clearly:

$$0 \rightarrow K \rightarrow S(B) \stackrel{A}{\rightarrow} H \rightarrow 0, \tag{4.6}$$

where $r(H) = r(\frac{S(B)}{K}) = r(B) - r(K)$. Thus, $r(K) = r(B) - r(H)$. Hence, parts 3 and 4 follow.

We show part 5. Clearly, $\overline{S}(B)$ is injected into H in the exact sequence 4.6. Therefore, by proposition 4.1.26, $H \simeq \overline{S}(B) \oplus \overline{H_1}$ for some finite abelian group $\overline{H_1}$. Hence, part 5 follows.

□

We can deduce more in proposition 4.1.31 when A is injective.

Proposition 4.1.32. *Let $C = AB$, where A is an $n \times r$ matrix and B is an $r \times k$ matrix.*

1. *If A is injective, then there is an exact sequence such that:*

$$0 \to S(B) \to S(C) \to S(A) \to 0.$$

2. *If B is onto, then there is an exact sequence such that:*

$$0 \to S(A^T) \to S(C^T) \to S(B^T) \to 0.$$

Proof. We show part 1. Consider the following inclusions of free abelian groups:

$$Col_{\mathbb{Z}}(AB) \subset Col_{\mathbb{Z}}(A) \subset \mathbb{Z}^n.$$

We can conclude the following exact sequence:

$$0 \to \frac{Col_{\mathbb{Z}}(A)}{Col_{\mathbb{Z}}(AB)} \to \frac{\mathbb{Z}^n}{Col_{\mathbb{Z}}(AB)} \to \frac{\mathbb{Z}^n}{Col_{\mathbb{Z}}(A)} \to 0.$$

Thus,

$$0 \to M \to S(AB) \to S(A) \to 0,$$

where $M = \frac{Col_{\mathbb{Z}}(A)}{Col_{\mathbb{Z}}(AB)}$. It suffices to show that $M \simeq S(B)$.

Because A is injective, we can view A as an injective map of $\mathbb{Z}$-modules. Consider,

$$\begin{array}{ccc} & & \mathbb{Z}^n \\ & & \cup \\ \mathbb{Z}^r & \stackrel{A}{\rightarrow} & Col_{\mathbb{Z}}(A) \\ \cup & & \cup \\ Col_{\mathbb{Z}}(B) & \stackrel{A}{\rightarrow} & Col_{\mathbb{Z}}(AB) \end{array},$$

hence, $S(B) = \frac{\mathbb{Z}^r}{Col_{\mathbb{Z}}(B)}$ is isomorphic to $\frac{Col_{\mathbb{Z}}(A)}{Col_{\mathbb{Z}}(AB)} = M$ via the map A.

We show part 2. By using the trivial action in proposition 4.1.4 parts 2a and 2b, B is onto if and only if B^T is injective. Part 2 will follow by applyng part 1 to $C^T = B^T A^T$. □

As a corollary, we deduce the following.

Corollary 4.1.33. *Let $C = AB$ where A is injective, then $\overline{S}(B) \subset \overline{S}(C)$.*

Proof. This can be viewed as a corollary to proposition 4.1.30 or proposition 4.1.31. □

We close the section with a result that can be found partly as theorem 2 in the work of Pless and Rushanan in [24], and in several sections of Rushanan's paper in [22].

Proposition 4.1.34. *(Rushanan) Let C be a nonsingular matrix with eigenvalues $\lambda_1, \ldots, \lambda_r$ with respective multiplicities $m_1, \ldots, m_r$. Then,*

1. *If λ_i is an integer, then λ_i divides $exp(\overline{S}(C))$.*
2. *If all $\lambda_i s$ are integral, then $lcm(\lambda_1, \ldots, \lambda_r)$ divides $\overline{S}(C)$.*
3. *If C diagonalizes with respect to $\lambda_i \in \mathbb{Z}$. That is, the algebraic multiplicity equals the geometric multiplicity. Then, $(\mathbb{Z}/\lambda_i\mathbb{Z})^{m_i}$ is a subgroup of $\overline{S}(C)$.*
4. *If C is diagonalizable with all eigenvalues integral. That is, every eigenvalue has its geometric multiplicity equal its algebraic multiplicity. Then, $exp(\overline{S}(C))$ divides $\lambda_1\lambda_2 \cdots \lambda_s$.*

4.1.3 The Johnson Scheme $\mathbf{J(v,k)}$

We will show results that are well-known for the Johnson Scheme $J(v,k)$. We start with a few general definitions about permutation actions that will be used for the rest of the chapter.

Definition 4.1.35. *Let $G \subset S_v$, where S_v is the symmetric group on v letters. Assume that S_v acts on $X = \{1, \ldots, v\}$.*

1. *Define* $\mathrm{C_k(X)} = \bigoplus_{\mathrm{K \subset X, |K|=k}} \mathbb{C}\mathrm{e_K}$. *That is, the* vector space of all k-subsets of X.

2. *We view $C_k(X)$ as a G-module with action given by,*

$$\rho(\sigma)e_K \quad = \quad e_{\sigma(K)} \ \sigma \in G \subset S_v,$$

where $\sigma(K) = \sigma(\{a_1, \ldots, a_k\}) = \{\sigma(a_1), \ldots, \sigma(a_k)\}$.

Definition 4.1.36. *The* Johnson Scheme $J(v,k)$ *is the Hecke Ring $H(S_v, C_k(X))$.*

For the rest of the section, we will define for k_0, k_1 as $k_0 = \min(k, v-k)$ and $k_1 = \max(k, v-k)$ where $0 \leq kv$.

Proposition 4.1.37. *The Johnson Scheme $J(v,k)$ admits a canonical basis given by the matrices A_i defined as,*

$$A_i^k(e_{K_1}, e_{K_2}) \quad = \quad \begin{cases} 1 & \text{if } |K_1 \cap K_2| = k - i, \\ 0 & \text{else,} \end{cases}$$

where $i = 0, \ldots, k_0$. In particular, $dim_{\mathbb{C}}(J(v,k)) = k_0 + 1$.

Proof. Clearly, if $A \in Hom_G(N,N)$, then $\rho(\sigma)A = A\rho(\sigma)$. Hence, for all $\sigma \in G$, we have

$$\rho(\sigma)A\rho(\sigma^{-1}) \quad = \quad A.$$

The previous equation forces A to be constant on the orbits of G on the set $C_k(X) \times C_k(X)$. Thus, we can assume A to be a linear combination of A_is where the A_is are the characteristic functions of the orbits of G on $C_k(X) \times C_k(X)$. It suffices to calculate these A_is for $G = S_v$. Clearly, each orbit Ω of S_v on $C_k(X) \times C_k(X)$ has a unique value for $|K_1 \cup K_2|$. That is, for any $(e_{K_1}, e_{K_2}) \in \Omega$, the value $|K_1 \cup K_2|$ is constant. It suffices to show that possible values of $|K_1 \cap K_2|$ are $k, k-1, \ldots, k-k_0$. We will do this by cases.

Case 2k $\leq$ v. Clearly, $k = k_0$. Also, $|K_1 \cap K_2| \geq k - k_0 = 0$ since one can find disjoint K_1, K_2. Obviously, $0 \leq |K_1 \cap K_2| \leq k$ and $|K_1 \cap K_2|$ takes on the values $0, \ldots, k$.

Case 2k > v. Clearly, $k = k_1$. Also, one cannot longer find K_1, K_2 that are disjoint. However, one can find K_1, K_2 such that $|K_1 \cup K_2| = v$. Therefore, $|K_1 \cup K_2| \leq v$ and $|K_1 \cap K_2| = 2k - |K_1 \cup K_2| \geq 2k - v = k - k_0$. Thus, clearly, $k \geq |K_1 \cap K_2| \geq k - k_0$. Obviously, $|K_1 \cap K_2|$ takes on every value between k and $k - k_0$. □

Proposition 4.1.38. *Let $C_k(X)$ be viewed as an S_v-module. Then, $C_k(X)$ has decomposition into irreducibles $C_k(X) = N_{0,k} \bigoplus N_{1,k} \bigoplus \cdots \bigoplus N_{k_0,k}$, where $N_{i,k}$ is the irreducible S_v-module with character*

$$\chi_i = \begin{cases} \pi_i - \pi_{i-1} & \text{for } 0 < i \leq \frac{v}{2}, \\ \chi_0 & \text{for } i = 0, \end{cases}$$

where χ_0 is the trivial character, and π_i is the permutation character of $C_i(X)$. In particular, $\pi_k = \chi_0 + \cdots + \chi_k$, where each χ_i is an irreducible complex character of S_v.

Proof. We proceed by cases.

Case k $\leq \frac{\mathbf{v}}{\mathbf{2}}$. The result can be found in [2] in chapter III, section 2, theorem 2.5.

Case k $> \frac{\mathbf{v}}{\mathbf{2}}$. Consider the S_v-map $P_k : C_k(X) \to C_{v-k}(X)$ defined by $P_k(e_K) = P_{v-k}(e_{\sim K})$. Clearly, by using P_k, we can show that $C_k(X)$ and $C_{v-k}(X)$ are isomorphic S_v-modules. Hence, the result follows by the previous case. □

Corollary 4.1.39. *Let $W \in J(v,k)$ and $P_{i,N_{i,k}} \in J(v,k)$ be the ith projection on the $N_{i,k}$ irreducible component of $C_k(X)$. Then,*

1. *The following holds, $I_{C_k(X)} = P_{0,N_{0,k}} + \cdots + P_{k_0,N_{k_0,k}}$.*
2. *The map W decomposes as $W = \lambda_0 P_{0,N_{0,k}} + \cdots + \lambda_{k_0} P_{k_0,N_{k_0,k}}$.*
3. *The space $N_{i,k}$ is an eigenspace of W with eigenvalue λ_i.*
4. *The matrices $P_{0,N_{0,k}}, \ldots, P_{k_0,N_{k_0,k}}$ form another basis of $J(v,k)$.*

Proof. Clearly, part 1 is a consequence of proposition 4.1.2.

We show part 2. By proposition 4.1.12, $W = \sum_{i=0}^{k_0} W_{i,i}$ where $W_{i,i} = P_{i,N_{i,k}} W P_{i,N_{i,k}}$. By proposition 4.1.9, $W_{i,i} = M_{a_i,a_i} \otimes I_{N_{i,k}}$ when restricted to $N_{i,k}$; where a_i is the multiplicity of $N_{i,k}$ in $C_k(X)$. Since $N_{i,k}$ has multiplicity 1, we must have $W_{i,i} = \lambda_i I_{N_{i,k}}$ when $W_{i,i}$ is restricted to $N_{i,k}$. Since $W_{i,i}$ is zero on $N_{j,k}$ for $i \neq j$, we must have $W_{i,i} = \lambda_i P_{i,N_{i,k}}$. Therefore, part 2 follows.

Clearly, part 3 follows from part 2 by recalling that the $P_{i,N_{i,k}}$ are projection operators.

Finally, part 2 shows that the matrices $P_{i,N_{i,k}}$ span $J(v,k)$. Hence, $\{P_{i,N_{i,k}}\}_{i=0}^{k_0}$ is a spanning set for $J(v,k)$. Since $J(v,k)$ has dimension k_0+1, it follows that $\{P_{i,N_{i,k}}\}_{i=0}^{k_0}$ form a basis. Hence, part 4 follows. □

We will denote the S_v projections $P_{s,N_{s,k}}$ by $E_{s,k}$ as short-hand notation. Now, we proceed to define another basis $H_{i,k} = W_{i,k}^T W_{i,k}$ for the Johnson Scheme $J(v,k)$. First, we quote a result that is theorem 1 in [14].

Proposition 4.1.40. *Let $0 \leq i \leq k_0 = \min(k, v-k)$. Then,*

$$H_{i,k} = \sum_{s=0}^{k_0} \binom{k-s}{i-s} \binom{v-i-s}{k-i} E_{s,k}.$$

Corollary 4.1.41. *The matrices $\{H_{i,k} = W_{i,k}^T W_{i,k}\}_{i=0}^{k_0}$ form a basis of $J(v,k)$.*

Proof. Clearly, by proposition 4.1.40, the matrix $M = [[m_{i,s}]] = [[\binom{k-s}{i-s}\binom{v-i-s}{k-i}]]$ is a change of coordinates between the $H_{i,k}$s and the $E_{s,k}$s. It suffices to show that M is nonsingular since this will show that M is a change of basis.

Note that M is lower triangular with diagonal entries of the form $\binom{v-2i}{k-i}$. Since $k+i \leq k+k_0 \leq v$, we must have $k-i \leq v-2i$. Thus, $\binom{v-2i}{k-i} \neq 0$. Since the determinant of an lower triangular matrix is the multiplication of the diagonal entries, and none of the diagonal entries of M are zero; we must have the determinant of M nonzero. Hence, M is nonsingular. □

Clearly, $H_{i,k}$ has nontrivial kernel when $i < k$ as the coefficients of $E_{s,k}$ for $i < s \leq k$ are zero. However, for the matrices $I_{i,k} = W_{i,k}W_{i,k}^T$, we will see otherwise.

Proposition 4.1.42. *Let* $0 \leq i \leq k_0 = \min(k, v-k)$ *and* $i_0 = \min(i, v-i)$. *Then,*

$$I_{i,k} = \sum_{s=0}^{i_0} \binom{k-s}{i-s}\binom{v-i-s}{k-i} E_{s,i}.$$

Proof. Clearly, $I_{i,k} \in J(v,i)$. Thus, $I_{i,k} = \sum_{s=0}^{i_0} \lambda_s E_{s,i}$ for some λ_ss. Let $H_{i,k} \in J(v,k)$ have expansion $H_{i,k} = \sum_{s=0}^{i_0} \beta_s E_{s,k}$ where β_s is given by proposition 4.1.40. We will show $\lambda_s = \beta_s$.

Consider,

$$\begin{aligned}
\sum_{s=0}^{i_0} \beta_s^2 E_{s,k} &= (\sum_{s=0}^{i_0} \beta_s^2 E_{s,k})(\sum_{s=0}^{i_0} \beta_s^2 E_{s,k}) \\
&= H_{i,k}H_{i,k} \\
&= W_{i,k}^T(W_{i,k}W_{i,k}^T)W_{i,k} \\
&= W_{i,k}^T(\sum_{s=0}^{i_0} \lambda_s E_{s,i})W_{i,k} \\
&= (\sum_{s=0}^{i_0} \lambda_s E_{s,k})W_{i,k}^T W_{i,k} \\
&= (\sum_{s=0}^{i_0} \lambda_s E_{s,k})(\sum_{s=0}^{i_0} \beta_s E_{s,k}) \\
&= \sum_{s=0}^{i_0} \lambda_s \beta_s E_{s,k},
\end{aligned}$$

where we have used the property $W_{t,k}^T E_{s,t} = E_{s,k} W_{t,k}^T$, which is justified since $E_{s,k}$ is the projection onto the sth isotopic S_v-irreducible and $W_{t,k}$ is an S_v-map.

Thus, by the above equations, we must have $\beta_s \lambda_s = \beta_s^2$. As $\beta_s \neq 0$, we deduce that $\lambda_s = \beta_s$. □

As a corollary, we calculate the determinant of $I_{i,k}$.

Corollary 4.1.43. *Let $t \leq \min(k, v-k) = k_0$ and $t_0 = \min(t, v-t)$. Then,*

$$\det(I_{t,k}) \;=\; \Pi_{s=0}^{t_0} \left(\binom{k-s}{t-s} \binom{v-t-s}{k-t} \right)^{\binom{v}{s} - \binom{v}{s-1}}.$$

Proof. Recall that the determinant of a square matrix is the multiplication of all its eigenvalues, counting multiplicities; the formula will follow by showing that $\binom{k-s}{t-s}\binom{v-t-s}{k-t}$ is an eigenvalue with multiplicity $\binom{v}{s} - \binom{v}{s-1}$. Clearly, this follows since $\binom{k-s}{t-s}\binom{v-t-s}{k-t}$ is the eigenvalue corresponding to the eigenspace $N_{s,k}$ by proposition 4.1.40, and $N_{s,k}$ has dimension $\binom{v}{s} - \binom{v}{s-1}$ by proposition 4.1.38. □

We proceed to calculate the eigenspace decomposition $W_{t,v-k}$.

Proposition 4.1.44. *Let $2t \leq v$, and $P_t : C_t(X) \to C_{v-t}(X)$ defined by $P_t(e_T) = e_{\sim T}$. Let $A_t = W_{t,v-t} P_t$. Then, A_t has eigenspace decomposition:*

$$A_t \;=\; \sum_{s=0}^{t} \kappa_s \binom{v-t-s}{t-s} E_{s,t},$$

where $\kappa_s \in \{\pm 1\}$.

Proof. Clearly, $A_t : C_t(X) \to C_t(X)$ is an S_v-map. Hence, $A_t \in J(v,t)$. By corollary 4.1.39, A_t must have an Eigenspace decomposition:

$$A_t \;=\; \sum_{s=0}^{t} \gamma_s E_{s,t},$$

for some constants γ_ss. Note that any $T \in J(v,k)$ is symmetric since the basis of proposition 4.1.37 consists of symmentric matrices. Hence, A_t is symmetric and $A_t^T = A_t$.

Consider the product,

$$\begin{aligned}\sum_{s=0}^{t}\gamma_s^2 E_{s,t} &= A_t A_t^T \\ &= W_{t,v-t}P_t(W_{t,v-t}P_t)^T \\ &= W_{t,v-t}P_tP_t^TW_{t,v-t}^T \\ &= W_{t,v-t}W_{t,v-t}^T \\ &= \sum_{s=0}^{t}\binom{v-t-s}{t-s}^2 E_{s,t},\end{aligned}$$

where we have used $P_t^T = P_t$, $P_tP_t = I$ and proposition 4.1.42.

Therefore, $\gamma_s^2 = \binom{v-t-s}{t-s}^2$ and the result follows. □

We will show some identities for the matrices A_t. But first, we will introduce the matrices $\overline{W_{k,i}}$.

Definition 4.1.45. *Let $\overline{W_{k,i}} : C_i(X) \to C_k(X)$ be defined by,*

$$\overline{W_{k,i}}(e_K, e_I) = \begin{cases} 1 & \text{if } |K \cap I| = 0, \\ 0 & \text{else.} \end{cases}$$

Proposition 4.1.46. *Assume $t \le k \le v-k$. Let $A_t = W_{t,v-t}P_t$, and $\lambda_{t,k} = \binom{v-t-k}{k-t}$. Then,*

1. $A_t = \overline{W_{t,t}}$.
2. $W_{k,v-t}P_t = \overline{W_{k,t}}$.
3. $W_{t,k}\overline{W_{k,t}} = \lambda_{t,k}A_t$.

Proof. By direct calculation, one can show

$$\begin{aligned}A_t(e_T) &= W_{t,v-t}P_t(e_T) \\ &= \sum_{T' \subset \sim T} e_{T'} \\ &= \overline{W_{t,t}}(e_T).\end{aligned}$$

Hence, part 1 follows.

Also, one can show

$$\begin{aligned} W_{k,v-t}P_t(e_T) &= \sum_{K' \subset \sim T} e_{K'} \\ &= \overline{W_{k,t}}(e_T). \end{aligned}$$

Hence, part 2 follows.

By considering the identity,

$$W_{t,k}W_{k,v-t} = \lambda_{t,k}W_{t,v-t},$$

we deduce

$$W_{t,k}W_{k,v-t}P_t = \lambda_{t,k}W_{t,v-t}P_t.$$

Hence, part 3 follows. □

Now, we proceed to study the more general function space $J(v,k,t)$.

Proposition 4.1.47. *Let W be a linear map of the vector space $J(v,k,t)$ where $J(v,k,t)$ is defined by*

$$J(v,k,t) = Hom_{S_v}(C_k(X), C_t(X)).$$

Let $W_i^{t,k} \in J(v,k,t)$ and be defined as

$$W_i^{t,k}(e_T, e_K) = \begin{cases} 1 & \text{if } |T \cap K| = min(t,k) - i, \\ 0 & \text{else.} \end{cases}$$

Let $t_0 = min(t, v-t)$, and $k_0 = min(k, v-k)$. Then,

1. *The space $J(v,k,t)$ decomposes into $J(v,k,t) = \mathbb{C}W_0^{t,k} \bigoplus \cdots \bigoplus \mathbb{C}W_{min(k_0,t_0)}^{t,k}$.*

2. *Using the notation of proposition 4.1.38, if $t_0 \leq k_0$, then the S_v-submodule*

$S_{t,k} = N_{t_0+1,k} \bigoplus \cdots \bigoplus N_{t_0,k} \subset C_k(X)$ *is in the* $ker(W)$ *for any* $W \in J(v,k,t)$.

3. *Using the notation of proposition 4.1.38, if* $k_0 \leq t_0$, *then the* S_v*-submodule* $S'_{t,k} = N_{k_0+1,t} \bigoplus \cdots \bigoplus N_{k_0,t} \subset C_t(X)$ *is in the* $coker(W)$ *for any* $W \in J(v,k,t)$.

4. *The dimension of* $J(v,k,t)$ *is* $dim_{\mathbb{C}}(J(v,k,t)) = min(t_0,k_0)$.

5. *If* $W \in J(v,k,t)$ *has full rank, then the* $ker(W) = \overline{S_{t,k}}$ *and the* $coker(W) = \overline{S_{t,k}}'$, *where:*

$$\overline{S_{t,k}} = \begin{cases} 0 & \text{If } k_0 < t_0, \\ S_{t,k} & \text{else,} \end{cases}$$

$$\overline{S_{t,k}}' = \begin{cases} 0 & \text{If } t_0 < k_0, \\ S'_{t,k} & \text{else.} \end{cases}$$

Proof. We show part 1. We will proceed as in the proof of proposition 4.1.37. It suffices to calculate the orbits of S_v on $C_t(X) \times C_k(X)$. That is, the orbits Ω of S_v on the set of pairs (T,K), where T is a t-subset and K is a k-subset.

We proceed to show that for a fixed orbit Ω and arbitrary (T,K) the quantity $|T \cap K|$ is constant. Let $(T,K),(T',K') \in \Omega$. Consider the following partions of $X = \{1,\ldots,v\}$ that are induced by (T,K) and by (T',K'):

$$T \cap K, \quad T \cap \sim K, \quad \sim T \cap K, \quad \sim T \cap \sim K,$$
$$T' \cap K', \quad T' \cap \sim K', \quad \sim T' \cap K', \quad \sim T' \cap \sim K'.$$

Clearly, one can find at least one permutation $\sigma \in S_v$ that takes the subset $T \cap K$ into $T' \cap K'$, the subset $T \cap \sim K$ into $T' \cap \sim K'$, the subset $\sim T \cap K$ into $\sim T' \cap K'$, and the subset $\sim T \cap \sim K$ into $\sim T' \cap \sim K'$. This permutation will map the pair (T,K) into (T',K') under the action of S_v. Clearly, this permutation will show $|T \cap K| = |T' \cap K'|$.

It remains to calculate the possible values of $|T \cap K|$. Clearly, $|T \cap K| \leq \min(t,k)$. We will leave as an exercise to show that $|T \cap K| \geq \min(t,k) - \min(t_0,k_0)$, and that $|T \cap K|$ takes on the values between $\min(t,k)$ and $\min(t,k) - \min(t_0,k_0)$.

Clearly, parts 2 and 3 follow from part 1 and propositions 4.1.38 and 4.1.11.

Part 4 is a consequence of part 1.

Part 5 is a consequence of parts 2 and 3. □

4.1.3.1 The Matrices $\mathbf{W_0^{t,k}}, \mathbf{W_{\min(t_0,k_0)}^{t,k}}$

We will study the matrices $W_0^{t,k}$ and $W_{\min(t_0,k_0)}^{t,k}$ where $t \leq k$, $t_0 = \min(t, v-t)$ and $k_0 = \min(k, v-k)$. These matrices are already known to us, since a direct calculation shows for $t < k \leq v - k$,

$$\begin{aligned} W_0^{t,k} &= \overline{W_{t,k}}, \\ W_{\min(t_0,k_0)}^{t,k} &= W_{t,k}. \end{aligned}$$

We will determine when the matrices $W_0^{t,k}, W_{\min(t_0,k_0)}^{t,k}$ are injective, surjective, or both. We will answer these questions by showing them directly, and by providing for a left inverse or a right inverse.

We will use the following lemma to reduce a surjectivity question to an injectivity question, and an injectivity question to a surjectivity question.

Lemma 4.1.48. *Let $T \in J(v,k,t)$. Then,*

1. *T is injective if and only if $\overline{T}^T$ is surjective.*

2. *T is surjective if and only if $\overline{T}^T$ is injective.*

Proof. We apply proposition 4.1.4, and proposition 4.1.4 parts 2a, 2b; where we use $G = S_v$, $V = C_k(X)$, and $W = C_t(X)$. It suffices to show that $\overline{T}^T = T^*$.

Clearly, because S_v is a permutation action, the inner product matrices $A_{S_v,C_k(X)} = I_{C_k(X)}$ and $A_{S_v,C_t(X)} = I_{C_t(X)}$. Hence, by proposition 4.1.4 part 1, $T^* = \overline{T}^T$. Therefore, the result follows. □

Proposition 4.1.49. *If $t \leq k$ and $\binom{v}{t} \leq \binom{v}{k}$, then $W_{t,k}^T$ is injective.*

Proof. Our assumptions are equivalent to $t \leq k \leq v - t$ and $t \leq v - k \leq v - t$. We

invoke an identity that can be found in [8] in chapter 15, section 8, lemma 8.4.

$$W_{t,k}W_{t,k}^T = \sum_{i=0}^{t} \binom{v-2t}{v-k-i} W_{i,t}^T W_{i,t}.$$

Let $G_{t,k} = W_{t,k}W_{t,k}^T$. By the previous equation, $G_{t,k}$ is a sum of positive semidefinite matrices where one of the summands is positive definite, namely $W_{t,t}^T W_{t,t} = I$. Thus, $G_{t,k}$ is positive definite and hence invertible.

The injectivity of $W_{t,k}^T$ is an easy deduction from the nonsingularity of $G_{t,k}$. □

By applying lemma 4.1.48 to the previous proposition, we deduce the following.

Corollary 4.1.50. *If* $\binom{v}{t} \leq \binom{v}{k}$, *then* $W_{t,k}$ *is surjective.*

Also,

Corollary 4.1.51. *Let* $k_0 = \min(k, v-k), k_1 = \max(k, v-k)$, *where* $0 \leq k \leq v$. *Then,* W_{k_0,k_1} *is an isomorphism.*

Proof. By letting $k = k_1$, $t = k_0$ in proposition 4.1.49, we conclude that W_{k_0,k_1}^T is injective. Since $C_{k_0}(X)$ and $C_{k_1}(X)$ have the same dimension, it follows that W_{k_0,k_1}^T is an isomorphism. Hence, W_{k_0,k_1} is an isomorphism. □

Proposition 4.1.52. *If* $t \leq k$ *and* $\binom{v}{k} \leq \binom{v}{t}$, *then* $W_{t,k}$ *is injective.*

Proof. Note that our assumptions are equivalent to $t \geq \min(k, v-k)$. Hence, $v-k \leq t \leq k$, $2k > v$, and $k+t \geq v$.

Suppose $x \in C_k(X)$ such that $W_{t,k}x = 0$. Consider

$$\begin{aligned} 0 &= W_{v-k,t}W_{t,k}x \\ &= \tbinom{k-(v-k)}{t-(v-k)} W_{v-k,k}x \\ &= \tbinom{2k-v}{k+t-v} W_{v-k,k}x, \end{aligned}$$

hence, $x \in Ker(W_{v-k,k})$. By corollary 4.1.51, $W_{v-k,k}$ is an isomorphism. Hence, we must have $x = 0$. Thus, $W_{t,k}$ is injective. □

We proceed to showing the matrices $W_0^{t,k}, W_{\min(t_0,k_0)}^{t,k}$ have full rank. The following result is due to my advisor through a private comunication.

Proposition 4.1.53. *Let $\binom{v}{t} \leq \binom{v}{k}$, then $W_{t,k}$ has a right inverse $U_{k,t}$ given by:*

$$U_{k,t} = \sum_{i=0}^{t} \frac{(-1)^i}{\binom{v-t-i}{k-t}} \overline{W_{k,i}} W_{i,t}. \tag{4.7}$$

Proof. Our assumption gives $t \leq k \leq v-t$. Thus, $k-t \leq v-t-t \leq v-t-(t-1) \leq \cdots \leq v-t$. Therefore, $k-t \leq v-t-i$ for $i = 0, \ldots, t$. Thus, the binomial coefficients of Equation (4.7) are nonzero. Therefore, $U_{k,t}$ is well defined.

Consider,

$$\begin{aligned} W_{t,k}\overline{W_{k,i}} &= \binom{v-t-i}{k-t} \overline{W_{t,i}}, \\ \sum_{i=0}^{t} (-1)^i \overline{W_{t,i}} W_{i,t} &= I. \end{aligned}$$

Using the previous equations, we can show $W_{t,k}U_{k,t} = I_t$ by direct calculation. □

In the following, we will need the following identities:

$$\begin{aligned} P_{v-k} W_{v-k,t} &= \overline{W_{k,t}} \text{ if } v-k \leq t, \\ W_{i,v-k} P_k &= \overline{W_{i,k}} \text{ if } i \leq v-k. \end{aligned}$$

We proceed to calculate the left inverse for $W_{\min(t_0,k_0)}^{t,k} = W_{v-k}^{t,k}$ when $t \leq k$ and $\binom{v}{k} \leq \binom{v}{t}$.

Proposition 4.1.54. *Let $\binom{v}{k} \leq \binom{v}{t}$ and $t \leq k$. Then, $W_{v-k}^{t,k}$ has a left inverse and is given by:*

$$V_{k,t} = \sum_{i=0}^{v-k} \frac{(-1)^i}{\binom{k-i}{t+k-v}} \overline{W_{k,i} W_{i,t}}.$$

Proof. Our assumptions give $v-k \leq t \leq k$ and $v-k \leq v-t \leq k$. Therefore, $v-k \leq t$ and $\binom{v}{v-k} = \binom{v}{k} \leq \binom{v}{t}$. Hence, by proposition 4.1.53, $W_{v-k,t}$ has a right inverse given

by:

$$U_{t,v-k} = \sum_{i=0}^{v-k} \frac{(-1)^i}{\binom{k-i}{t+k-v}} \overline{W_{t,i}} W_{i,v-k}. \tag{4.8}$$

Since $W_{v-k,t}U_{t,v-k} = I_{v-k}$, we have,

$$\begin{aligned} P_{v-k}W_{v-k,t}U_{t,v-k}P_k &= P_{v-k}I_{v-k}P_k \\ &= I_k, \end{aligned}$$

also, since $P_{v-k}W_{v-k,t} = W_{v-k}^{k,t}$, we have,

$$W_{v-k}^{k,t}(U_{t,v-k}P_k) = I_k.$$

By taking the transpose of the previous equation, we have,

$$(U_{t,v-k}P_k)^T W_{v-k}^{t,k} = I_k.$$

Thus, $V_{k,t} = (U_{t,v-k}P_k)^T$ is a left inverse for $W_{v-k}^{t,k}$. By using the identity $W_{i,v-k}P_k = \overline{W_{i,k}}$, the formula for $V_{k,t}$ follows readily from Equation (4.8). □

We proceed to calculating a right inverse of $W_{\min(t_0,k_0)}^{t,k} = \overline{W_{t,k}}$ whenever $\binom{v}{t} \leq \binom{v}{k}$.

Proposition 4.1.55. *Let $t \leq k$ and $\binom{v}{t} \leq \binom{v}{k}$. Then, $\overline{W_{t,k}}$ has a right inverse and is given by:*

$$T_{k,t} = \sum_{i=0}^{t} \frac{(-1)^i}{\binom{v-t-i}{k-i}} W_{i,k}^T W_{i,t}.$$

Proof. Our assumptions give $t \leq k \leq v-t$ and $t \leq v-k \leq v-t$. By proposition 4.1.53, $W_{t,v-k}$ has a right inverse given by:

$$U_{v-k,t} = \sum_{i=0}^{t} \frac{(-1)^i}{\binom{v-t-i}{v-t-k}} \overline{W_{v-k,i}} W_{i,t}.$$

Consider,

$$\begin{aligned} I_t &= W_{t,v-k}U_{v-k,t} \\ &= (W_{t,v-k}P_k)(P_{v-k}U_{v-k,t}). \end{aligned}$$

Using the identities: $W_{t,v-k}P_k = \overline{W_{t,k}}$, $P_{v-k}\overline{W_{v-k,i}} = W^T_{i,v-k}$, and $\binom{v-t-i}{v-k-t} = \binom{v-t-i}{k-i}$; we get the formula for the right inverse of $\overline{W_{t,k}}$. □

We calculate a left inverse of $W_{t,k}$ when $\binom{v}{k} \leq \binom{v}{t}$.

Proposition 4.1.56. *Let $t \leq k$ and $\binom{v}{k} \leq \binom{v}{t}$. Then, $W_{t,k}$ has a left inverse given by:*

$$S_{k,t} = \sum_{i=0}^{v-k} \frac{(-1)^i}{\binom{k-i}{t-i}} \overline{W_{k,i}} W_{i,t}.$$

Proof. Our assumptions give $v-k \leq t \leq k$ and $v-k \leq v-t \leq k$. By proposition 4.1.55, $\overline{W_{v-k,t}}$ has a right inverse given by:

$$T_{t,v-k} = \sum_{i=0}^{v-k} \frac{(-1)^i}{\binom{k-i}{t-i}} W^T_{i,t} W_{i,v-k}.$$

Consider,

$$\begin{aligned} (P_{v-k}\overline{W_{v-k,t}})(T_{t,v-k}P_k) &= P_{v-k}I_{v-k}P_k \\ &= I_k. \end{aligned}$$

Using the identity $P_{v-k}\overline{W_{v-k,t}} = W^T_{t,k}$, we get,

$$W^T_{t,k}(T_{t,v-k}P_k) = I_k.$$

Thus, by taking the transpose of the previous equation, we deduce a formula for a left inverse of $W_{t,k}$ given by $S_{k,t} = (T_{t,v-k}P_k)^T$. Using the identity $W_{i,v-k}P_k = \overline{W_{i,k}}$, the formula for $S_{k,t}$ follows. □

Corollary 4.1.57. *Let $t \leq k$. The matrices $W_0^{t,k}$ and $W_{\min(t_0,k_0)}^{t,k}$ have full rank.*

Proof. The previous propositions show that: if $\binom{v}{t} \leq \binom{v}{k}$, then $W_0^{t,k} = W_{t,k}$ and $W_{\min(t_0,k_0)}^{t,k} = W_{v-k}^{t,k}$ are surjective. That is, their rank is $\binom{v}{t} = \min(\binom{v}{t}, \binom{v}{k})$. Hence, these matrices have full rank.

The previous propositions also show that: if $\binom{v}{k} \leq \binom{v}{t}$, then $W_0^{t,k} = W_{t,k}$ and $W_{\min(t_0,k_0)}^{t,k} = \overline{W_{t,k}}$ are injective. That is, their rank is $\binom{v}{k} = \min(\binom{v}{t}, \binom{v}{k})$. Hence, these matrices have full rank. □

We close the subsection with some results about $W_{t,k}$. The following result can be found in [26]. It gives a diagonal form for the matrices $W_{t,k}$.

Proposition 4.1.58. *Let $t \leq \min(k, v-k)$, the matrix $W_{t,k}$ has as a diagonal form the $\binom{v}{t} \times \binom{v}{k}$ diagonal matrix D with diagonal entries*

$$\binom{k-i}{t-i} \text{ with multiplicity } \binom{v}{i} - \binom{v}{i-1}, \text{ where } i = 0, \ldots, t.$$

As a corrollary, we deduce a formula for the determinant of $W_{t,k}$ whenever $k+t = v$.

Corollary 4.1.59. *Let $v - k \leq k$, then*

$$\det(W_{v-k,k}) = \Pi_{i=0}^{v-k} \binom{k-i}{(v-k)-i}^{\binom{v}{i}-\binom{v}{i-1}}.$$

Alternatively, via a change of notation we deduce the following.

Corollary 4.1.60. *Let $k \leq v - k$, then*

$$\det(W_{k,v-k}) = \Pi_{i=0}^{k} \binom{v-k-i}{k-i}^{\binom{v}{i}-\binom{v}{i-1}}.$$

4.2 General Equivariant Results

In this section, we will consider a group $G \subset S_v$ to act on $X = \{1, \ldots, v\}$ as a permutation action. We will provide results analogous to the ones in section 4.1.3.1.

Clearly, as it was shown in the section of preliminaries, $C_k(X)$ decomposes into $k_0 = \min(k, v-k)$ S_v-irreducibles. We will denote the S_v-projections $P_{s,N_{s,k}}$ by $E_{s,k}$.

We will assume that $\phi_0, \phi_1, \ldots, \phi_l$ are the irreducible characters of G, where ϕ_0 is the trivial character. Since $G \subset S_v$, $C_k(X)$ is a G-module by restriction. Hence, $C_k(X)$ decomposes into G-irreducibles. We will denote the G-projections $P_{i,C_k(X),G}$ of proposition 4.1.2 that correspond to the irreducible character ϕ_i by $P_{i,k}$.

For $W \in Hom_G(C_k(X), C_t(X))$, we will use the notation $(W)_i$ for the map:

$$\begin{aligned} WP_{i,k} &= P_{i,t}W \\ &= P_{i,t}WP_{i,k}. \end{aligned}$$

The map $(W)_i$ will be called the ith projection of W onto the ith isotype of G in $C_k(X)$. We will denote $Im(P_{i,k})$ by $(C_k(X))_i$, and we will make no distinction between $(W)_i$ as a map from $C_k(X)$ to $C_t(X)$, and $(W)_i$ as a map from $(C_k(X))_i$ to $(C_t(X))_i$ — unless ambiguity leads to conflict. Also, we will denote $P_{s,k}(N_{i,k})$ by $(N_{i,k})_s$.

We start our study of the spaces $(C_k(X))_0$ and the maps $(T)_{0,0}$ where $T \in Hom_G(C_k(X), C_t(X))$. The sections that will follow will make use the results that we present here.

Proposition 4.2.1. *Let $\Omega_{K_1}, \ldots, \Omega_{K_{r_k(G)}}$ be the distinct orbits of the action of G on the k-subsets, where $r_k(G)$ is the number of orbits under the action of G on the k-subsets. Then,*

$$Im(P_{0,C_k(X)}) = \mathbb{C}\Omega_{K_1} \bigoplus \cdots \bigoplus \mathbb{C}\Omega_{K_{r_k(G)}}.$$

We will denote $\{\Omega_{K_1}, \ldots, \Omega_{K_{r_k(G)}}\}$ as the Canonical basis of $(C_k(X))_0$.

Proof. Clearly,

$$P_{0,C_k(X)} = \frac{1}{|G|} \sum_{g \in G} \rho_{C_k(X)}(g).$$

Consider the image of basis element $e_K \in C_k(X)$,

$$\begin{aligned} P_{0,C_k(X)}e_K &= \frac{1}{|G|}\sum_{g\in G}\rho_{C_k(X)}(g)e_K \\ &= \frac{1}{|G|}\sum_{g\in G}e_{g\cdot K} \\ &= \frac{|G_K|}{|G|}\Omega_K \\ &= \frac{1}{|\Omega_K|}\Omega_K, \end{aligned}$$

where G_K is the stabilizer of K under the action of G, and Ω_K is the orbit of K under the action of G. We note that we are using the symbol Ω_K to represent the collection of k-subsets that belong to the orbit of K and also to represent $\sum_{K'\in\Omega_K} e_{K'}$. Hence, we have that $P_{0,C_k(X)}\Omega_K = \Omega_K$. Therefore, $\Omega_K \in Im(P_{0,C_k(X)})$.

Since the e_Ks span $C_k(X)$, we must have the Ω_Ks span the $Im(P_{0,C_k(X)})$. Clearly, the Ω_Ks are linearly independent since they are disjoint sums of linearly independent vectors. Thus, $\{\Omega_K\}$ form a basis of $(C_k(X))_0 = Im(P_{0,C_k(X)})$. □

Using the canonical basis of $(C_k(X))_0$ and $(C_t(X))_0$, we introduce the matrices $(W)_0, (W)_0'$ defined using an arbitrary map $W \in Hom_G(C_k(X), C_t(X))$. We will study in great detail the matrices $(W)_0, (W)_0'$ that arise when $W = W_{t,k}$.

Definition 4.2.2. *Let W be G-map $W : C_k(X) \to C_t(X)$. By $(W)_0$, we will denote the matrix of W calculated using the canonical basis of $(C_k(X))_0$ and of $(C_t(X))_0$. That is, a matrix whose entries are given by:*

$$(W)_0(\Omega_{T_i}, \Omega_{K_j}) = \sum_{K\in\Omega_{K_j}} W(e_{T_i}, e_K).$$

We will refer to $(W)_0$ as the "row sum equivariant projection of W."

Also, we will denote the matrix $((W^*)_0)^T = ((\overline{W}^T)_0)^T$ by $(W)_0'$. That is, a matrix

whose entries are given by:

$$(W)_0'(\Omega_{T_i}, \Omega_{K_j}) \;=\; \sum_{T \in \Omega_{T_i}} \overline{W}(e_T, e_{K_j}).$$

where $(\bar{\cdot})$ *denotes complex conjugation. We will refer to* $(W)_0'$ *as the* "column sum equivariant projection of W."

We establish a relationhip between $(W)_0$ and $(W)_0'$ by using special inner products on $(C_k(X))_0$ and $(C_t(X))_0$.

Proposition 4.2.3. *Let* $W : C_k(X) \to C_t(X)$ *be an* S_v*-map. Let* $\langle , \rangle_t$ *be the standard Hermitian inner product on* $C_t(X)$ *and* $\langle , \rangle_k$ *be the standard Hermitian inner product on* $C_k(X)$*. Let* D_k *be the diagonal map on* $(C_k(X))_0$ *defined as:*

$$D_k(\Omega_K, \Omega_{K'}) \;=\; \begin{cases} |\Omega_K| & \text{if } \Omega_K = \Omega_{K'}, \\ 0 & \text{else.} \end{cases}$$

Let $\widehat{D_k}$ *be the diagonal map on* $C_k(X)$ *defined as:*

$$\widehat{D_k}(e_K, e_{K'}) \;=\; \begin{cases} |\Omega_K| & \text{if } K = K', \\ 0 & \text{else.} \end{cases}$$

Then,

1. *Using the standard basis of* $(C_k(X))_0$, $\langle x, y \rangle_k = x^T D_k y$ *whenever* $x, y \in (C_k(X))_0$.
2. *Using the standard basis of* $(C_t(X))_0$, $\langle x, y \rangle_t = x^T D_t y$ *whenever* $x, y \in (C_t(X))_0$.
3. *Let* $\langle , \rangle_k$ *and* $\langle , \rangle_t$ *be the inner products of parts 1 and 2. Using the standard basis of* $(C_t(X))_0$ *and* $(C_k(X))_0$,

$$\begin{aligned} \langle x, (W)_0 y \rangle_t &= \langle ((W)_0')^T x, y \rangle_k, \\ D_t (W)_0 D_k^{-1} &= (W)_0', \end{aligned}$$

whenever $x \in (C_t(X))_0$ *and* $y \in (C_k(X))_0$.

4. The following holds, $(M)'_0 = (\widehat{D_t} M \widehat{D_k}^{-1})_0$.

Proof. Parts 1 and 2 are clear since $\langle \Omega_K, \Omega_{K'} \rangle_k = \delta_{\Omega_K, \Omega_{K'}} |\Omega_K|$.

We show part 3. Consider, $\langle W^* x, y \rangle_k = \langle x, W y \rangle_t$ where $x \in C_t(X)$ and $y \in C_k(X)$. When we restrict this identity to the standard basis of $(C_t(X))_0$ and $(C_k(X))_0$ we deduce,

$$\begin{aligned} (W)'_0(\Omega_T, \Omega_K)|\Omega_K| &= \langle W^* \Omega_T, \Omega_K \rangle_k \\ &= \langle \Omega_T, W \Omega_K \rangle_t \\ &= |\Omega_T| (W)_0(\Omega_T, \Omega_K). \end{aligned} \tag{4.6}$$

Hence, we deduce $(W)'_0 D_k = D_t (W)_0$. Therefore, $(W)'_0 = D_t (W)_0 D_k^{-1}$.

We proceed to show $\langle x, (W)_0 y \rangle_t = \langle ((W)'_0)^T x, y \rangle_k$. Consider,

$$\begin{aligned} \langle x, (W)_0 y \rangle_t &= x^T D_t (W)_0 y \\ &= x^T D_t (W)_0 D_k^{-1} D_k y \\ &= x^T (W)'_0 D_k y \\ &= (((W)'_0)^T x)^T y \\ &= \langle ((W)'_0)^T x, y \rangle_k. \end{aligned}$$

Hence, part 2 follows.

Part 4 follows by direct calculation using Equation (4.6). □

Definition 4.2.4. *The inner products given by D_k and D_t will be called the* G-induced standard Hermitian inner products on $(C_t(X))_0$ and $(C_k(X))_0$.

We proceed to show the operators $(\cdot)_0, (\cdot)'_0$ preserve algebraic operations.

Proposition 4.2.5. *1. Let $f(x_1, x_2, \ldots, x_n)$ be a multivariable complex polynomial of n variables.*

2. Let $T_1, \ldots, T_n$ be G-maps from $C_k(X)$ to $C_t(X)$. For example, they could be S_v-maps.

3. *Let* $f(T_1, \ldots, T_n) = 0$.

4. *Let* $S_i = (T_i)_{0,0}$ *be maps from* $(C_k(X))_0$ *to* $(C_t(X))_0$ *having matrix representation with respect to the Canonical Basis of* $(C_k(X))_0$ *and* $(C_t(X))_0$.

Then, $f(S_1, \ldots, S_n) = 0$.

Proof. By proposition 4.1.15, $f(S_1, \ldots, S_n) = 0$ as maps. By using the Canonical Basis, we deduce the result. □

Proposition 4.2.6. *Let* $V \in Hom_G(C_k(X), C_t(X))$, $W \in Hom_G(C_r(X), C_k(X))$, $X \in Hom_G(C_r(X), C_t(X))$, *and* $\alpha \in \mathbb{C}$. *Then,*

$$\begin{aligned}(VW + \alpha X)_0 &= (V)_0(W)_0 + \alpha(X)_0,\\ (VW + \alpha X)'_0 &= (V)'_0(W)'_0 + \alpha(X)'_0.\end{aligned}$$

Proof. The first equation follows from proposition 4.2.5 by restricting the $()_{0,0}$ maps to the Canonical Basis of $(C_*(X))_0$.

To show the second equation, consider the map:

$$\widehat{D_t} V \widehat{D_k}^{-1} \widehat{D_k} W \widehat{D_r}^{-1} + \alpha \widehat{D_t} X \widehat{D_r}^{-1} = \widehat{D_t}(VW + \alpha X)\widehat{D_r}^{-1},$$

by taking the row sum equivariant projection operator of both sides, and using proposition 4.2.3 part 4, we can deduce,

$$(V)'_0(W)'_0 + \alpha(X)'_0 = (VW + \alpha X)'_0.$$

Hence, the result follows. □

The following result shows that $(T)_0, (T)'_0$ have full rank whenever T has full rank.

Proposition 4.2.7. *Let* $T \in Hom_G(C_k(X), C_t(X))$ *have full rank. Then,*

1. *The map* $(T)_0$ *has full rank.*

2. *The map* $(T)'_0$ *has full rank.*

Proof. Part 1 is a consequence of proposition 4.1.12.

We show part 2. Consider $S = T^T$, clearly S has full rank as T has full rank. Hence, $(S)_0$ has full rank by part 1. Therefore, $(T)'_0 = (S)_0^T$ also has full rank. □

We proceed to study the analogous version of $E_{s,k}$ in the equivariant case.

Definition 4.2.8. *Let $G \subset S_v$ be a permutation action. We will denote by,*

1. *The map $\mathrm{G_{s,k}} = (\mathrm{E_{s,k}})_0$ as the row sum equivariant projection of the sth S_v-irreducible projection of $C_k(X)$.*

2. *The map $\mathrm{G'_{s,k}} = (\mathrm{E_{s,k}})'_0$ as the column sum equivariant projection of the sth S_v-irreducible projection of $C_k(X)$.*

We note that the subscript s indexes the S_v-irreducibles of $C_k(X)$.

Using the operators $(\cdot)_0, (\cdot)'_0$, we deduce a few properties of $G_{s,k}, G'_{s,k}$.

Corollary 4.2.9. *The Row Sum and column sum equivariant projections of the family of maps $E_{s,k}$ form an orthogonal family of idempotents maps on $(C_k(X))_0$. That is,*

1. $G_{0,k} + \cdots + G_{k,k} = I$.

2. $G'_{0,k} + \cdots + G'_{k,k} = I$.

3. $G_{i,k}G_{j,k} = \delta_{i,j}G_{j,k}$.

4. $G'_{i,k}G'_{j,k} = \delta_{i,j}G'_{j,k}$.

5. $G'_{i,k} = G^T_{i,k}$.

6. $G_{i,k}$ *is a projection operator to the space* $(N_{i,k})_0$.

7. $G'_{i,k}$ *is a projection operator to the space* $D_k(N_{i,k})_0$.

Proof. By the results of the preliminary section on the Johnson Scheme, we have,

$$\begin{aligned} E_{0,k} + \cdots + E_{k,k} &= I, \\ E_{i,k}E_{j,k} &= \delta_{i,j}E_{i,k}. \end{aligned}$$

Using proposition 4.2.6, we can deduce the same for the Row Sum Equivariant projections. Hence, parts 1, 2, 3, and 4 follow.

We show part 5. Consider,

$$\begin{aligned} G'_{i,k} &= ((E^T_{i,k})_0)^T \\ &= ((E_{i,k})_0)^T \\ &= G^T_{i,k}, \end{aligned}$$

hence, part 5 follows.

Part 6 is obvious.

We show part 7. Since $G'_{i,k} = G^T_{i,k}$, $G'_{i,k}$ must be a projection operator. By proposition 4.2.3, $G'_{i,k}D_k = D_kG_{i,k}$. Choose $x \in (C_k(X))_0$, and let $x_i = G_{i,k}x$. We can deduce that $G'_{i,k}D_kx = D_kx_i$. Hence, $G'_{i,k}$ acts as a projection operator on the space $D_k(N_{i,k})_0$.

□

Corollary 4.2.10. *Assume $k = k_0 = \min(v-k, k)$. Let $A : C_k(X) \to C_k(X)$ be an S_v-map that decomposes into eigenspaces as $A = \sum_{s=0}^{k} a_kE_{s,k}$ where a_ks are the corresponding eigenvalues. Then,*

1. *The map $(A)_0$ decomposes into eigenspaces using the the row sum equivariant projections as:*

$$(A)_0 = \sum_{s=0}^{k} a_kG_{s,k}.$$

2. *The map $(A)'_0$ decomposes into eigenspaces using the column sum equivariant projections as:*

$$(A)'_0 = \sum_{s=0}^{k} a_kG'_{s,k}.$$

Proof. This is an obvious consequence of corollary 4.2.9. Alternatively, we can apply

the $(\cdot)_0$ operator to the equation $A = \sum_{s=0}^{k} a_k E_{s,k}$ to deduce the first part. Similarly, we can apply the $(\cdot)'_0$ operator to the equation $A = \sum_{s=0}^{k} a_k E_{s,k}$ to deduce the second part. □

Proposition 4.2.11. *Let $T = VW$ where $W \in J(v,k,t)$ and $V \in J(v,t,k)$. If T is nonsingular, then,*

$$\begin{aligned} ker(V) \cap Im(W) &= \{0\}, \\ ker((V)_0) \cap Im((W)_0) &= \{0\}, \\ ker((V)'_0) \cap Im((W)'_0) &= \{0\}. \end{aligned}$$

Proof. Let $x \in Ker(V) \cap Im(W)$. Clearly, there is z such that $x = Wz$ and $Vx = 0$. Thus, $VWz = Vx = 0$. Since T is nonsingular, we must have $x = 0$. Therefore, $Ker(V) \cap Im(W) = \{0\}$. Thus, part 1 follows.

To show the remainder parts, it suffices to show that $(VW)_0$ and $(VW)'_0$ are nonsingular. Note that $T = \sum_{s=0}^{t} a_s E_{s,t}$, where $a_s \neq 0$ are the eigenvalues. By corollary 4.2.10, $(T)_0$ and $(T)'_0$ are both nonsingular. □

The following result will prove useful in later sections.

Proposition 4.2.12. *Let $W \in J(v,k)$ have eigenspace decomposition $\sum_{s=0}^{k_0} \lambda_s E_{s,k}$. Using the notation of definition 4.1.14, we have,*

a. The map $(W)_i$ has eigenvalue λ_s with eigenspace $(N_{s,k})_i$.

b. The dimension of the space $(N_{s,k})_i$ is given by

$$dim_{\mathbb{C}}((N_{s,k})_i) = \langle \chi_s, \phi_i \rangle_G s_i,$$

where s_i is the dimension of the irreducible representation corresponding to ϕ_i, $\langle , \rangle_G$ is the "class function" inner product of character theory, and the character χ_s is defined in proposition 4.1.38.

c. The map $(W)_i$ decomposes as $(W)_i = \sum_{s=0}^{k_0} \lambda_s (E_{s,k})_i$.

d. The determinant of $(W)_i$ *is given by,*

$$det((W)_i) \quad = \quad \Pi_{s=0}^{k_0} \lambda_s^{\langle \chi_s, \phi_i \rangle_G s_i},$$

where $(W)_i$ *is viewed as a map from* $(C_k(X))_i$ *to* $(C_k(X))_i$.

Proof. Clearly, the spaces $N_{s,k}$ are S_v-spaces, hence they are G-spaces. Also, by assumption, $N_{s,k}$ is an eigenspace of W with eigenvalue λ_s. Consider the application of the $(\cdot)_{i,i} = (\cdot)_i$ operator using using proposition 4.1.15 to the equation:

$$W \quad = \quad \sum_{s=0}^{k_0} \lambda_s E_{s,k}.$$

we deduce,

$$(W)_i \quad = \quad \sum_{s=0}^{k_0} \lambda_s (E_{s,k})_i.$$

This establishes part c.

By proposition 4.1.15, we deduce that the operators $(E_{s,k})_i$ are a complete orthogonal set of maps from $(C_k(X))_i$ to the space $(C_k(X))_i$. Hence, $(N_{s,k})_i = Im((E_{s,k})_i)$ are eigenspaces of $(W)_i$ with eigenvalue λ_s. Hence, part a follows.

We proceed to show part b. Clearly, $N_{s,k}$ is an S_v-irreducible with character χ_s. By restriction, we can view χ_s as a character of G, not necessarily G-irreducible. Also, by a standard result in character theory, $N_{s,k}$ decomposes into G-irreducibles as,

$$N_{s,k} \simeq \bigoplus \langle \chi_s, \phi_i \rangle_G M_i,$$

where, ϕ_is are the G-irreducible characters of the G-irreducible spaces M_i, and $\langle \chi_s, \phi_i \rangle_G$ is the multiplicity of M_i in $N_{s,k}$. Clearly, $(N_{s,k})_i \simeq \langle \chi_s, \phi_i \rangle_G M_i$. Hence, part b follows.

Part d is a trivial application of the formula of the determinant of a linear map T in terms of its eigenvalues. □

In general a projection to $N_{s,t}$ that is a G-map is not necessarily integral. However, the projections $E_{s,t}$ can be shown to be rational. This is because the irreducible characters that arise from the action of S_v on the t-subsets are integer valued, a consequence that every irreducible character of S_v is integer valued. Hence,

$$E_{s,t} = \frac{1}{|S_v|} \sum_{\sigma \in S_v} \overline{\chi_s}(\sigma)\rho_t(\sigma),$$

has rational entries.

We will show that we can choose projections to $N_{s,t}$ that are G-maps and are almost integral up to a factor of $v_1 = |G|$. We will do this with the aid of a right inverse of $W_{t,k}$ found by Wilson in [26],

Proposition 4.2.13. (Wilson) *Let $t \leq k \leq v - t$. There exist $\binom{v}{k}$ by $\binom{v}{i}$ matrices A_i , where $i = 0, \ldots, t$, such that:*

$$U_{k,t} = \sum_{i=0}^{t} \frac{1}{\binom{k-i}{t-i}} A_i W_{i,t}.$$

Is a right inverse for $W_{t,k}$.

Corollary 4.2.14. *Let $G \subset S_v$, where $v_1 = |G|$. There are projections $Q_{s,k} : C_k(X) \to N_{s,k}$, such that:*

1. *The matrix $Q_{s,k}$ has rational entries.*
2. *The matrix $v_1 Q_{s,k}$ is integral.*
3. *The matrix $Q_{s,k}$ is a G-map.*

Proof. By using the right inverse provided by proposition 4.2.13, one can show that:

$$W_{t,k} U^G_{k,t} = v_1 I,$$

where

$$U^G_{k,t} = \sum_{g \in G} \pi_k(g) U_{k,t} \pi_t(g^{-1}).$$

Clearly, $\frac{1}{v_1}U^G_{k,t}$ is a right inverse of $W_{t,k}$, and in particular $rk(U^G_{k,t}) = \binom{v}{t}$. Define

$$D_{t,k} \;=\; W^T_{t,k}(\frac{1}{v_1}U_{k,t})^T.$$

A direct calculation shows that $D^2_{t,k} = D_{t,k}$ and $D_{t,k}W^T_{t,k} = W^T_{t,k}$. Hence, $D_{t,k}$ is a projection operator that is a G-map, has rational entries, $v_1 D_{t,k}$ is integral, and leaves the rows of $W_{t,k}$ invariant. Also, $rk(D_{t,k}) = rk((U^G_{k,t})^T) = rk(U^G_{k,t}) = \binom{v}{t}$ as $W^T_{t,k}$ and $U^G_{k,t}$ are injective.

Clearly, $rk(W^T_{t,k}) = \binom{v}{t}$ as $W^T_{t,k}$ is injective. Hence, it follows that $D_{t,k}$ is a projection onto the column space of $W^T_{t,k}$.

Note that the column space of $Col_{\mathbb{Q}}(W^T_{t,k}) = N_{0,k} \oplus N_{1,k} \oplus \cdots \oplus N_{t,k}$.

Define $Q_{s,k} = D_{s,k} - D_{s-1,k}$ where $D_{-1,k} = 0$. Clearly, $Q_{s,k}$ satisfies the conditions of the conclusion. □

Corollary 4.2.15. *Let $G \subset S_v$, where $|G| = v_1$. Define $K_{s,k} = (N_{s,k})_0 \cap \mathbb{Z}^{r_k(G)}$ where $r_k(G)$ is the dimension of $(C_k(X))_0$. Then,*

1. *The space $K_{s,k}$ is a finitely generated free abelian group of abelian rank $r_{s,k} = dim_{\mathbb{Q}}((N_{s,k})_0) = \langle \chi_s, \chi_0 \rangle_G = r_s(G) - r_{s-1}(G)$, where we make the convention $r_{-1}(G) = 0$ and χ_0 is the trivial character.*

2. *Let $\{\beta^j_s\}^{r_{s,k}}_{j=1}$ a $\mathbb{Z}$-basis of $K_{s,k}$. Set $\beta = \cup^k_{s=0}\{\beta^j_s\}^{r_{s,k}}_{j=1}$. Let $M \in J(v,k)$ with eigenspace decomposition $M = \sum^k_{s=0} \lambda_s E_{s,k}$. Using the basis β, $(M)_0$ diagonalizes to $(M)_0 B = BD_\lambda$, where,*

   (a) *The matrix $B = [[\beta]]$ is the matrix having β as its columns.*

   (b) *The matrix D_λ is the diagonal matrix of eigenvalues of $(M)_0$.*

Proof. By corollary 4.2.14, there is a projection $Q_{s,k}$ to $N_{s,k}$ such that: it is a G-map, and $v_1 Q_{s,k}$ is integral. Clearly, $(Q_{s,k})_0$ is a projection to $(N_{s,k})_0$ such that $(v_1 Q_{s,k})_0$ is integral. Let L be any subset of columns of $(Q_{s,k})_0$ that is linearly independent over $\mathbb{Q}$. Consider the $\mathbb{Z}$-module L' generated by the columns of L. Clearly, $v_1 L'$ is a submodule of integral vectors, and $v_1 L' \subset (N_{s,k})_0$ by construction. Hence, $v_1 L' \subset$

$(N_{s,k})_0 \cap \mathbb{Z}^{r_k(G)} = K_{s,k}$. Thus, $K_{s,k}$ has a finitely generated free abelian subgroup of maximal possible rank, i.e., $dim_{\mathbb{C}}((N_{s,k})_0)$. It suffices to show,

$$\begin{aligned} dim_{\mathbb{C}}((N_{s,k})_0) &= \langle \chi_s, \chi_0 \rangle_G \\ &= r_s(G) - r_s(G). \end{aligned}$$

By proposition 4.2.12 part b, the first equation follows. We proceed to show the second equation. Consider,

$$\begin{aligned} \langle \chi_s, \chi_0 \rangle_G &= \langle \pi_s - \pi_{s-1}, \chi_0 \rangle_G \\ &= \langle \pi_s, \chi_0 \rangle - \langle \pi_{s-1}, \chi_0 \rangle_G, \end{aligned}$$

where π_s is the character of the permutation action induced by G on the s-subsets. We note that by Burnside's theorem for group actions, $\langle \pi_s, \chi_0 \rangle = r_s(G)$. Hence, the second equation follows.

Part 2 is obvious. □

We remark that the projections of corollary 4.2.14 are not the same projections that arise from the representation of S_v. That is, $Q_{s,k}$ may not equal $E_{s,k}$. However, it is true that,

$$Q_{s,k}E_{s,k} = E_{s,k},\ E_{s,k}Q_{s,k} = Q_{s,k}.$$

But, $Q_{s,k}E_{i,k}$ may not equal 0 since $Q_{s,k}$ is not necessarily an S_v-map.

4.3 The $\mathbf{M_{t,k}}$ and $\mathbf{M'_{t,k}}$ Incidence Structures

In the following, we will study the matrices $M_{t,k}$ and $M'_{t,k}$ defined in the introduction. We will look at their Smith Groups; we will consider the integral preimage problem; we will provide consequence of the existence of (t,k)-basis; and we will close the subsection with a brief study of the kernel of $M_{t,k}$ and $M'_{t,k}$.

Clearly, by definition, $M_{t,k} = (W_{t,k})_0$ and $M'_{t,k} = (W_{t,k})'_0$. Consider the equation,

$$W_{t,k}W_{k,r} \quad = \quad \binom{r-t}{k-t} W_{t,r}, \tag{4.7}$$

which we call the "cocycle conditions."

By applying the $(\cdot)_0, (\cdot)'_0$, we can deduce the same for $M_{t,k}$ and $M_{t,k}$'.

Corollary 4.3.1. *Let $t \leq k \leq r$. Then,*

1. $M_{t,k}M_{k,r} = \binom{r-t}{k-t} M_{t,r}$.
2. $M'_{t,k}M'_{k,r} = \binom{r-t}{k-t} M'_{t,r}$.

Proof. We prove part 1 by applying the $(\cdot)_0$ operatory to Equation (4.7) via the use of proposition 4.2.5. Part 2 follows simililarly but instead we apply the $(\cdot)'_0$ operator. □

As short-hand notation, we will denote $M_{t,k}(\Omega_T, \Omega_K)$ by $m_{T,K}$, and $M'_{t,k}(\Omega_T, \Omega_K)$ by $m'_{T,K}$. The following proposition lists some properties for $m_{T,K}, m'_{T,K}$.

Proposition 4.3.2. *The following are true:*

1. *If $G_T \triangleright G$ or $G_K \triangleright G$, then $m_{T,K} = \beta_{T,K} \frac{|G_T|}{|G_T \cap G_K|}$, where $\beta_{T,K} \in \{0, \ldots, \frac{|G|}{|\langle G_T, G_K \rangle|}\}$.*
2. *If $G_K \triangleright G$ or $G_T \triangleright G$, then $m'_{T,K} = \alpha_{T,K} \frac{|G_K|}{|G_T \cap G_K|}$, where $\alpha_{T,K} \in \{0, \ldots, \frac{|G|}{|\langle G_T, G_K \rangle|}\}$.*
3. *If $G_K \triangleright G$ or $G_T \triangleright G$, then $m'_{T,K} = \beta_{T,K} \frac{|G_K|}{|G_T \cap G_K|}$ and $m_{T,K} = \beta_{T,K} \frac{|G_T|}{|G_T \cap G_K|}$, where $\beta_{T,K} \in \{0, \ldots, \frac{|G|}{|\langle G_T, G_K \rangle|}\}$.*
4. *If $G_T \triangleright G$ or $G_K \triangleright G$, and $\langle G_T, G_K \rangle = G$. Then,*
   (a) *The constant $m_{T,K} = |\Omega_K|$ whenever $T \subset K$.*
   (b) *The constant $m_{T,K} = 0$ whenever $T \backslash K \neq \phi$.*
   (c) *The constant $m'_{T,K} = |\Omega_T|$ whenever $T \subset K$.*
   (d) *The constant $m'_{T,K} = 0$ whenever $T \backslash K \neq \phi$.*
5. *The following holds, $|\Omega_T| m_{T,K} = m'_{T,K} |\Omega_K|$.*

Proof. Clearly, part 5 follows by proposition 4.2.3 part 4.

We show part 1. Let Ω_T and Ω_K be orbits of T and K under the action of G. Consider $f : \Omega_T \times \Omega_K \to \{0, 1\}$ defined by,

$$f(T', K') = \begin{cases} 1 & \text{if } T' \subset K', \\ 0 & \text{else.} \end{cases}$$

Clearly, f is a G-invariant function. Since f is either 0 or 1, f is the characteristic function of some of the orbits of G on $\Omega_T \times \Omega_K$.

Consider the quantity $g(T) = \sum_{K' \in \Omega_K} f(T, K')$. Clearly, $m_{T,K} = g(T)$. Let G_T be the stabilizer of T. Clearly, if $g \cdot (T, K') = (T, K'')$, then $g \in G_T$. Hence, $g(T)$ is the sum of the sizes of some of the orbits of G_T on Ω_K.

Consider the action of G_T on Ω_K. Clearly, if $K' \in \Omega_K$, then $(G_T)_{K'} = G_T \cap G_{K'}$, where $(G_T)_{K'}$ is the stabilizer of K' in the group G_T. Hence, the size of the orbit $\Theta_{K'}$ of K' under the action of G_T on Ω_K is,

$$|\Theta_{K'}| = \frac{|G_T|}{|G_T \cap G_{K'}|}.$$

Since $K' = g \cdot K$ for some $g \in G$, and $G^g_{g \cdot K} = G_K$; we must have $G_{K'} = (G_K)^{g^{-1}}$, where the operator $(\cdot)^g$ is taken as conjugation by g. Hence, if $G_T \triangleright G$ or $G_K \triangleright G$, then

$$\begin{aligned} |G_T \cap G_{K'}| &= |G_T \cap (G_K)^{g^{-1}}| \\ &= |(G_T)^g \cap G_K| \\ &= |G_T \cap G_K|. \end{aligned}$$

Therefore, all orbits of G_T on the k-sets of Ω_K have the same size given by $\frac{|G_T|}{|G_T \cap G_K|}$.

Hence,

$$\begin{aligned} m_{T,K} &= g(T) \\ &= \beta_{T,K} \frac{|G_T|}{|G_K \cap G_T|}, \end{aligned}$$

where $\beta_{T,K} \in \{0, \ldots, x(T,K)\}$. It suffices to calculate $x(T,K)$.

Clearly,

$$\begin{aligned} \frac{|G|}{|G_K|} &= |\Omega_K| \\ &= x(T,K)\frac{|G_T|}{|G_T \cap G_K|}, \end{aligned}$$

where $x(T,K)$ is the number of orbits of G_T on Ω_K. The previous equations give a formula for $x(T,K)$ as

$$\begin{aligned} x(T,K) &= \frac{|G||G_T \cap G_K|}{|G_T||G_K|} \\ &= \frac{|G|}{|\langle G_T, G_K \rangle|}, \end{aligned}$$

where $\langle G_T, G_K \rangle$ is the group generated by G_T and G_K in G. Hence, part 1 follows.

We proceed to prove part 2. The proof is similar to part 1. However, we consider the following function instead:

$$h(K) = \sum_{T' \in \Omega_T} f(T', K).$$

Clearly, h is the sum of the sizes of some of the orbits of G_K on Ω_T, and $m'_{T,K} = h(K)$. Using a similar analysis as part 1, we can show that all orbits of G_K on Ω_T have the size equal to $\frac{|G_K|}{|G_T \cap G_K|}$. Also, we can show there are exactly $\frac{|G|}{|\langle G_T, G_K \rangle|}$ orbits of G_K on Ω_T. Hence,

$$\begin{aligned} m'_{T,K} &= h(K) \\ &= \alpha_{T,K}\frac{|G_K|}{|G_T \cap G_K|}, \end{aligned}$$

where $\alpha_{T,K} \in \{0, \ldots, \frac{|G|}{|\langle G_T, G_K \rangle|}$. Hence, part 2 follows.

We proceed to prove part 3. From the analysis of parts 1 and 2, we have that

$$\begin{aligned} |\Omega_T| m_{T,K} &= \beta_{T,K} |\Omega_T| \frac{|G_T|}{|G_T \cap G_K|} \\ &= \beta_{T,K} \frac{|\Omega_T||G_T|}{|G_T \cap G_K|} \\ &= \beta_{T,K} \frac{|G|}{|G_T \cap G_K|}. \end{aligned}$$

Similarly,

$$\begin{aligned} |\Omega_K| m'_{T,K} &= \alpha_{T,K} |\Omega_K| \frac{|G_K|}{|G_T \cap G_K|} \\ &= \alpha_{T,K} \frac{|\Omega_K||G_K|}{|G_T \cap G_K|} \\ &= \alpha_{T,K} \frac{|G|}{|G_T \cap G_K|}. \end{aligned}$$

Hence, by using part 5, we have,

$$\begin{aligned} \alpha_{T,K} \frac{|G|}{|G_T \cap G_K|} &= m'_{T,K} |\Omega_K| \\ &= m_{T,K} |\Omega_T| \\ &= \beta_{T,K} \frac{|G|}{|G_T \cap G_K|}. \end{aligned}$$

Thus, $\alpha_{T,K} = \beta_{T,K}$ and part 3 follows.

Part 4 is a consequence of part 3. □

Corollary 4.3.3. $D_t M_{t,k} = M'_{t,k} D_k$.

Proof. This can be viewed as consequence of proposition 4.3.2 part 3; or it can be viewed as a deduction from proposition 4.2.3 part 4. □

Using proposition 4.2.12, we deduce the eigenspace decomposition of the matrices $M'^T_{t,k} M_{t,k}$.

Corollary 4.3.4. *Let* $\binom{v}{t} \leq \binom{v}{k}$. *The following hold:*

1. *The matrix* $M_{t,k}(M'_{t,k})^T$ *has eigenvalue* $\lambda_s = \binom{k-s}{t-s}\binom{v-t-s}{k-t}$ *with eigenspace* $(N_{s,t})_0$.

2. *The dimension of* $(N_{s,t})_0$ *is given by,*

$$dim_{\mathbb{C}}((N_{s,t})_0) \;=\; \langle \chi_s, \chi_0 \rangle_G,$$

where χ_s *is the irreducible* S_v*-character that corresponds to* $N_{s,t}$*, and* χ_0 *is the trivial character.*

3. *The quantity* $\langle \chi_s, \chi_0 \rangle_G$ *of the previous part is given by,*

$$\langle \chi_s, \chi_0 \rangle_G \;=\; r_s(G) - r_{s-1}(G),$$

where $r_s(G)$ *is the number of orbits of* G *on the* s*-subsets, and* $r_{-1}(G) = 0$*.*

4. *The map* $M_{t,k}(M'_{t,k})^T$ *decomposes into eigenspaces as,*

$$M_{t,k}(M'_{t,k})^T \;=\; \sum_{s=0}^{t_0} \lambda_s (E_{s,t})_0.$$

5. *The map* $M_{t,k}(M'_{t,k})^T$ *has determinant given by,*

$$det(M_{t,k}(M'_{t,k})^T) \;=\; \Pi_{s=0}^{t_0} \left(\binom{k-s}{t-s} \binom{v-t-s}{k-t} \right)^{\langle \chi_s, \chi_0 \rangle_G}.$$

Proof. By proposition 4.1.42, we have,

$$W_{t,k} W_{t,k}^T \;=\; \sum_{s=0}^{t} \binom{k-s}{t-s} \binom{v-t-s}{k-t} E_{s,t}. \tag{4.8}$$

By corollaries 4.2.10 and 4.2.9, $M_{t,k}(M'_{t,k})^T = (W_{t,k}W_{t,k}^T)_0$ has $(N_{s,k})_0$ as eigenspaces with eigenvalue $\binom{k-s}{t-s}\binom{v-t-s}{k-t}$. Hence, part 1 follows.

We proceed to show part 3. Consider,

$$\langle \chi_s, \chi_0 \rangle_G \;=\; \langle \pi_s, \chi_0 \rangle_G - \langle \pi_{s-1}, \chi_0 \rangle_G.$$

Note that by Burnside's theorem for group actions, $\langle \pi_s, \chi_0 \rangle_G = r_s(G)$. Hence, the

result follows.

The rest of the conclusions follow from applying proposition 4.2.12 to Equation (4.8) with $i = 0$. □

Corollary 4.3.5. *Let $t \leq v - t$. Then,*

$$\begin{aligned} det(M_{t,v-t}) &= \Pi_{s=0}^{t} \binom{v-t-s}{t-s}^{\langle \chi_s, \chi_0 \rangle_G}, \\ det(M'_{t,v-t}) &= \Pi_{s=0}^{t} \binom{v-t-s}{t-s}^{\langle \chi_s, \chi_0 \rangle_G}, \end{aligned}$$

where χ_0 is the trivial character.

Proof. By Corrollary(4.3.4), we have,

$$det(M_{t,v-t}(M'_{t,v-t})^T) = \Pi_{s=0}^{t} \binom{v-t-s}{t-s}^{2\langle \chi_s, 1 \rangle_G}.$$

It suffices to show $det(M_{t,v-t}) = det(M'_{t,v-t})$. By corollary 4.3.3, $D_t M_{t,v-t} = M'_{t,v-t} D_{v-t}$. Also note that $|\Omega_T| = |\Omega_{\sim T}|$ since $G_T = G_{\sim T}$. Hence, $det(D_t) = det(D_{v-t})$. Thus, $det(M_{t,v-t}) = det(M'_{t,v-t})$ and the result follows. □

We remark that the above equation comes from the eigenspace decomposition of $W_{t,k} W_{t,k}^T$, and in no way gives a diagonal form for $M_{t,v-t}$. However, computer computations with several nontrivial groups seem to verify the following conjecture.

Conjecture 4.3.6. *Let $t \leq v - t$. Then, the matrix $M_{t,v-t}$ has diagonal form D with diagonal entries $\lambda_s = \binom{v-t-s}{t-s}$ with multiplicity $\langle \chi_s, \chi_0 \rangle_G$, where $s = 0, \ldots, t$ and χ_0 is the trivial character.*

Also, direct calculations verify that the diagonal form conjectured above does not generalize to the nonsquared case, i.e., when $k + t < v$.

4.3.1 Full Rank Results

We start with consequences of $W_{t,k}$ having full rank.

Proposition 4.3.7. *Let π_t be the character of the induced action of G the t-subsets. Let ϕ_i be an irreducible complex character of G. The following are true:*

1. *If $\binom{v}{t} \leq \binom{v}{k}$, then $\langle \pi_t, \phi_i \rangle_G \leq \langle \pi_k, \phi_i \rangle_G$.*
2. *If $\binom{v}{k} \leq \binom{v}{t}$, then $\langle \pi_k, \phi_i \rangle_G \leq \langle \pi_t, \phi_i \rangle_G$.*

Where $\langle , \rangle_G$ is the class function inner product of character theory.

Proof. We show part 1. By proposition 4.1.53, $W_{t,k}$ is surjective whenever $\binom{v}{t} \leq \binom{v}{k}$. Thus, $(W_{t,k})_i$ is surjective by proposition 4.1.12. Hence,

$$dim_{\mathbb{C}}((C_t(X))_i) \leq dim_{\mathbb{C}}((C_k(X))_i).$$

Clearly, $(C_k(X))_i = (N_{0,k})_i \oplus (N_{1,k})_i \oplus \cdots \oplus (N_{k,k})_i$. Also, by proposition 4.2.12,

$$dim_{\mathbb{C}}((N_{s,k})_i) = \langle \chi_s, \phi_i \rangle_G s_i.$$

Hence,

$$\begin{aligned} dim_{\mathbb{C}}((C_k(X))_i) &= \sum_{s=0}^{k} dim_{\mathbb{C}}((N_{s,k})_i) \\ &= \sum_{s=0}^{k} \langle \chi_s, \phi_i \rangle_G s_i \\ &= \langle \pi_k, \phi_i \rangle_G s_i. \end{aligned}$$

where s_i is the dimension of the irreducible G-space corresponding to ϕ_i. Similarly, we can show $dim_{\mathbb{C}}((C_t(X))_i) = \langle \pi_t, \phi_i \rangle_G s_i$. Thus, we deduce,

$$\begin{aligned} \langle \pi_t, \phi_i \rangle_G s_i &= dim_{\mathbb{C}}((C_t(X))_i) \\ &\leq dim_{\mathbb{C}}((C_k(X))_i) \\ &= \langle \pi_t, \phi_i \rangle_G s_i. \end{aligned}$$

Hence, the conclusion follows.

Part 2 is a similar argument. □

Corollary 4.3.8. *Let $r_t(G)$ be the number of orbits of G on the t-subsets. Let $r_k(G)$ be the number of orbits of G on the k-subsets. Then,*

1. *If $\binom{v}{t} \leq \binom{v}{k}$, then $r_t(G) \leq r_k(G)$.*

2. *If $\binom{v}{k} \leq \binom{v}{t}$, then $r_k(G) \leq r_t(G)$.*

Proof. Apply proposition 4.3.7 to the trivial character χ_0 of G and use the fact that $\langle \pi_t, \chi_0 \rangle = r_t(G)$. □

Corollary 4.3.9. *The following hold.*

1. *If $r_t(G) < r_k(G)$, then $\binom{v}{t} < \binom{v}{k}$.*

2. *If $r_k(G) < r_t(G)$, then $\binom{v}{k} < \binom{v}{t}$.*

Proof. We show part 1. Suppose otherwise, that is, $r_t(G) < r_k(G)$ and $\binom{v}{t} \geq \binom{v}{k}$. By corollary 4.3.8 part 2, we must have $r_k(G) \leq r_t(G)$. Thus, $r_t(G) < r_k(G) \leq r_t(G)$. Clearly, this is a contradiction.

Part 2 follows similarly. □

Clearly, by proposition 4.2.7, it follows that the matrices $M_{t,k}$ and $M'_{t,k}$ have full rank.

Definition 4.3.10. *We define $\overline{\mathrm{M_{t,k}}}$ as $(\overline{W_{t,k}})_0$.*[2] *Hence, the entries of $\overline{M_{t,k}}$ are given by,*

$$\begin{aligned} \overline{M_{t,k}}(\Omega_T, \Omega_K) &= \overline{m_{T,K}} \\ &= |\{K' \in \Omega_K | T \cap K' = \phi\}|. \end{aligned}$$

Similary, we define $\overline{\mathrm{M_{t,k}}}'$ as $(\overline{W_{t,k}})'_0$.

We proceed to show the full rank results.

Proposition 4.3.11. *Let $\binom{v}{t} \leq \binom{v}{k}$. The following hold,*

[2] We warn the reader that the $\overline{(\cdot)}$ notation in $\overline{M_{t,k}}$ does not mean complex conjugation.

1. *The matrices $M_{t,k}$ have full rank.*

2. *The matrices $M'_{t,k}$ have full rank.*

3. *The matrices $\overline{M_{t,k}}$ have full rank.*

4. *The matrices $\overline{M_{t,k}}'$ have full rank.*

Proof. By corollary 4.1.57, the matrices $W_{t,k}$ and $\overline{W_{t,k}}$ have full rank. The result follows by applying proposition 4.2.7. □

We note that part 1 of proposition 4.3.11 has been shown by Kreher in theorem 11 of [16], but by using a different method.

We close this subsection by providing left and right inverses for $M_{t,k}$ and $\overline{M_{t,k}}'$ whenever possible. We note that the same technique can be used to show similar results for $\overline{M_{t,k}}$ and $\overline{M_{t,k}}'$.

Proposition 4.3.12. *Let $t \leq k$. Then,*

1. *If $\binom{v}{t} \leq \binom{v}{k}$, then $M_{t,k}$ is surjective and has a right inverse given by,*

$$(U_{k,t})_0 = \sum_{i=0}^{t} \frac{(-1)^i}{\binom{v-t-i}{k-t}} \overline{M_{k,i}} M_{i,t}.$$

2. *If $\binom{v}{k} \leq \binom{v}{t}$, then $M_{t,k}$ is injective and has a left inverse given by,*

$$(S_{k,t})_0 = \sum_{i=0}^{v-k} \frac{(-1)^i}{\binom{k-i}{t-i}} \overline{M_{k,i}} M_{i,t}.$$

3. *If $r_k(G) = r_t(G)$, then $M_{t,k}$ is invertible.*

Proof. We will show the details for part 1, a similar argument will follow for part 2. By proposition 4.1.53, there is a right inverse $U_{k,t}$ of $W_{t,k}$ given by,

$$U_{k,t} = \sum_{i=0}^{t} \frac{(-1)^i}{\binom{v-t-i}{k-t}} \overline{W_{k,i}} W_{i,t}.$$

We can deduce that $U_{k,t}$ is an S_v-map since $\overline{W_{k,i}}$ and $W_{i,t}$ are S_v-maps. By applying the $(\cdot)_0$ operator to the derived equation,

$$W_{t,k}U_{k,t} - I \;=\; 0,$$

we deduce,

$$M_{t,k}(U_{k,t})_0 - I \;=\; 0.$$

Hence, $(U_{k,t})_0$ is a right inverse. Clearly, part 1 follows by using the substitutions $(\overline{W_{k,i}})_0 = \overline{M_{k,i}}$, $(W_{i,t})_0 = M_{i,t}$.

We show part 2. We use the left inverse provided by proposition 4.1.56 and follow a similar argument as part 1.

We show part 3 by splitting it into two cases.

Case $\binom{\mathbf{v}}{\mathbf{t}} \leq \binom{\mathbf{v}}{\mathbf{k}}$. By part 1, $M_{t,k}$ is surjective. Since the range and the domain of $M_{t,k}$ have the same dimension, it follows that $M_{t,k}$ is an isomorphism.

Case $\binom{\mathbf{v}}{\mathbf{k}} \leq \binom{\mathbf{v}}{\mathbf{t}}$. By part 2, $M_{t,k}$ is injective. Since the range and the domain of $M_{t,k}$ have the same dimension, it follows that $M_{t,k}$ is an isomorphism. □

The following is the analogous result for $M'_{t,k}$.

Proposition 4.3.13. *Let $t \leq k$. Then,*

1. *If $\binom{v}{t} \leq \binom{v}{k}$, then $M'_{t,k}$ is surjective and has a right inverse given by,*

$$(V_{k,t})_0 \;=\; \sum_{i=0}^{t} \frac{(-1)^i}{\binom{v-t-i}{k-t}} \overline{M_{i,k}}^T M'_{i,t}.$$

2. *If $\binom{v}{k} \leq \binom{v}{t}$, then $M'_{t,k}$ is injective and has a left inverse given by,*

$$(X_{k,t})_0 \;=\; \sum_{i=0}^{v-k} \frac{(-1)^i}{\binom{k-i}{t-i}} \overline{M_{i,k}}^T M'_{i,t}.$$

3. *If $r_k(G) = r_t(G)$, then $M'_{t,k}$ is invertible.*

Proof. We will show the details for part 1, a similar argument will follow for part 2. By proposition 4.1.53, there is a right inverse $U_{k,t}$ of $W_{t,k}$ given by,

$$U_{k,t} \quad = \quad \sum_{i=0}^{t} \frac{(-1)^i}{\binom{v-t-i}{k-t}} \overline{W_{k,i}} W_{i,t}.$$

We can deduce that $U_{k,t}$ is an S_v-map since $\overline{W_{k,i}}$ and $W_{i,t}$ are S_v-maps. By applying the $(\cdot)'_0$ operator to the derived equation,

$$W_{t,k}U_{k,t} - I \quad = \quad 0,$$

we deduce,

$$M'_{t,k}(U_{k,t})'_0 - I \quad = \quad 0.$$

Hence, $(U_{k,t})'_0$ is a right inverse. Clearly, part 1 follows by using the substitutions $(\overline{W_{k,i}})'_0 = \overline{M_{k,i}}'$, $(W_{i,t})'_0 = M'_{i,t}$.

We show part 2. We use the left inverse provided by proposition 4.1.56 and follow a similar argument as part 1.

We show part 3 by splitting it into two cases.

Case $\binom{\mathbf{v}}{\mathbf{t}} \leq \binom{\mathbf{v}}{\mathbf{k}}$. By part 1, $M'_{t,k}$ is surjective. Since the range and the domain of $M'_{t,k}$ have the same dimension, it follows that $M'_{t,k}$ is an isomorphism.

Case $\binom{\mathbf{v}}{\mathbf{k}} \leq \binom{\mathbf{v}}{\mathbf{t}}$. By part 2, $M'_{t,k}$ is injective. Since the range and the domain of $M'_{t,k}$ have the same dimension, it follows that $M'_{t,k}$ is an isomorphism. □

4.3.2 The Smith Group of $\mathbf{M_{t,k}}$ and $\mathbf{M'_{t,k}}$

In this section, we will prove results that will bound the order of Smith Group of $M_{t,k}$ and $M'_{t,k}$.

4.3.2.1 Bounds on $|\mathbf{M_{t,k}}||\mathbf{M'_{t,k}}|$

We will begin by showing an identity involving $|M_{t,k}|$ and $|M'_{t,k}|$ by exploiting the equation $M'_{t,k}D_k = D_t M_{t,k}$.

Proposition 4.3.14. *The following are true:*

1. *There is an exact sequence such that,*

$$0 \to \overline{S}(M_{t,k}) \to \overline{S}(D_t M_{t,k}) \to \overline{S}(D_t) \to 0.$$

2. *The following holds,* $|D_t M_{t,k}| = |D_t||M_{t,k}|$.

Proof. By considering $D_t M_{t,k}$, we note that D_t is injective. Hence, proposition 4.1.32 applies, and we deduce the exact sequence:

$$0 \to S(M_{t,k}) \to S(D_t M_{t,k}) \to S(D_t) \to 0.$$

Since the matrices $M_{t,k}$, D_t, and $D_t M_{t,k}$ have full rank and $r_t(G) \leq r_k(G)$, these matrices must have zero abelian rank. Thus, $S(M_{t,k}) = \overline{S}(M_{t,k})$, $S(D_t) = \overline{S}(D_t)$, and $S(D_t M_{t,k}) = \overline{S}(D_t M_{t,k})$. Therefore, the first part follows.

The second part is a corollary to part 1. □

Proposition 4.3.15. *The following are true:*

1. *There is an exact sequence such that,*

$$0 \to \overline{S}(M'_{t,k}) \oplus (\mathbb{Z})^{r_k(G)-r_t(G)} \to \overline{S}(M'_{t,k}D_k) \oplus (\mathbb{Z})^{r_k(G)-r_t(G)} \to \overline{S}(D_t) \to 0.$$

2. *There is a finite abelian group* $\overline{H_3}$ *such that,*

$$\frac{\overline{S}(M'_{t,k}D_k)}{\overline{S}(M'_{t,k})} \oplus \overline{H_3} \simeq \overline{S}(D_k).$$

3. There is an integer h_3 dividing $|D_k|$ such that,

$$h_3|M'_{t,k}D_k| \;=\; |M'_{t,k}||D_k|.$$

Proof. Consider the product $M'_{t,k}D_k$. Clearly, D_k is onto. Hence, proposition 4.1.32 applies, and we can deduce,

$$0 \to S((M'_{t,k})^T) \to S((M'_{t,k}D_k)^T) \to S(D_k^T) \to 0.$$

Because $M'_{t,k}$ and D_k have full rank and $r_t(G) \leq r_k(G)$, we have,

$$\begin{aligned} S((M'_{t,k})^T) &= \overline{S}(M'_{t,k}) \oplus \mathbb{F}((M'_{t,k})^T), \\ S((M'_{t,k}D_k)^T) &= \overline{S}(M'_{t,k}D_k) \oplus \mathbb{F}((M'_{t,k}D_k)^T), \\ S(D_k^T) &= \overline{S}(D_k), \end{aligned}$$

where $r((M'_{t,k})^T) = r_k(G) - r_t(G)$ and $r((M'_{t,k}D_k)^T) = r_k(G) - r_t(G)$. Hence, part 1 follows.

Part 2 is an application of proposition 4.1.26. Part 3 follows from part 2. □

Corollary 4.3.16. *Let $t < k \leq v - k$. There is an integer h_3 dividing $|D_k|$ such that,*

$$\begin{aligned} h_3|D_t||M_{t,k}| &= h_3|D_tM_{t,k}| \\ &= h_3|M'_{t,k}D_k| \\ &= |M'_{t,k}||D_k|. \end{aligned}$$

Proof. This is a consequence of the previous propositions and the identity $M'_{t,k}D_k = D_tM_{t,k}$. □

By recalling a few identities involving $W_{t,k}$ and $W_{t,k}^T$ we will show some conditions on the product $|M_{t,k}||M'_{t,k}|$.

Proposition 4.3.17. (First Bound) *Let $t < k \leq v - k$.*

1. *Let* $J_{t,k} = M_{t,k}(M'_{t,k})^T$. *There are exact sequences and finite abelian groups* $\overline{H_1}$, $\overline{H'_1}$ *such that,*

$$0 \to \overline{S}(M'_{t,k}) \oplus \overline{H_1} \to \overline{S}(J_{t,k}) \to \overline{S}(M_{t,k}) \to 0,$$
$$0 \to \overline{S}(M_{t,k}) \oplus \overline{H'_1} \to \overline{S}(J_{t,k}) \to \overline{S}(M'_{t,k}) \to 0,$$

where $|\overline{H_1}| = |\overline{H'_1}|$.

2. *There is an integer* h_1 *such that,*

$$|J_{t,k}| \;=\; h_1|M_{t,k}||M'_{t,k}|.$$

3. *Let* $r_i(G) = \langle \pi_i, \chi_0 \rangle_G$ *be the number of orbits of* G *on the* i*-subsets, and define* $r_{-1}(G) = 0$. *Then,*

$$\begin{aligned} |J_{t,k}| &= |J^T_{t,k}| \\ &= \Pi^t_{s=0}(\binom{k-s}{t-s}\binom{v-t-s}{k-t})^{r_s(G)-r_{s-1}(G)}. \end{aligned}$$

4. *The* $exp(J_{t,k})$ *divides* $\Pi^t_{s=0}(\binom{k-s}{t-s}\binom{v-t-s}{k-t})^{\epsilon_s(G)}$, *where,*

$$\epsilon_s(G) \;=\; \begin{cases} 1 & \text{if } r_s(G) - r_{s-1}(G) \neq 0, \\ 0 & \text{else.} \end{cases}$$

5. *The* $exp(M_{t,k})$ *divides* $\Pi^t_{s=0}(\binom{k-s}{t-s}\binom{v-t-s}{k-t})^{\epsilon_s(G)}$.

6. *The* $exp(M'_{t,k})$ *divides* $\Pi^t_{s=0}(\binom{k-s}{t-s}\binom{v-t-s}{k-t})^{\epsilon_s(G)}$.

Proof. Consider the map $I_{t,k} = W_{t,k}W^T_{t,k}$. Clearly, $(I_{t,k})_0 = (W_{t,k}W^T_{t,k})_0 = (W_{t,k})_0(W^T_{t,k})_0 = M_{t,k}M'^T_{t,k} = J_{t,k}$. By proposition 4.2.11, $Ker(M_{t,k}) \cap M'^T_{t,k} = \{0\}$.

We deduce the first exact sequence by applying proposition 4.1.31 to the product $M_{t,k}(M'_{t,k})^T$. Hence, we have the exact sequence:

$$0 \to H \to S(M_{t,k}(M'_{t,k})^T) \to S(M_{t,k}) \to 0,$$

where $r(H) = rk(M_{t,k}) - rk(M_{t,k}M_{t,k}'^T) = r_k(G) - r_k(G) = 0$. By proposition 4.1.31 again, we can deduce that $H \simeq \overline{S}(M_{t,k}') \oplus \overline{H_1}$ for some finite abelian group $\overline{H_1}$.

Since $J_{t,k}$ and $M_{t,k}$ have full rank, it follows that $S(J_{t,k}) = \overline{S}(J_{t,k})$ and $S(M_{t,k}) = \overline{S}(M_{t,k})$. Thus the exact sequence of proposition 4.1.31 becomes:

$$0 \to \overline{S}(M_{t,k}') \oplus \overline{H_1} \to \overline{S}(J_{t,k}) \to \overline{S}(M_{t,k}) \to 0.$$

Hence, the first exact sequence follows.

We show the second exact sequence. Consider, $(I_{t,k})_0' = (W_{t,k}W_{t,k}^T)_0' = (W_{t,k})_0'(W_{t,k}^T)_0' = M_{t,k}'M_{t,k}^T = J_{t,k}^T$. By proposition 4.2.11, $Ker(M_{t,k}') \cap Im(M_{t,k}^T) = \{0\}$. By using a similar analysis that was used to deduce the first exact sequence, we can deduce the second. Hence, part 1 follows.

Part 2 is clear consequence of the exact sequences found in part 1.

By corollary 4.3.4 or by corollary 4.2.10, we can deduce that $(I_{t,k})_0$ is nonsingular with eigenvalues $\binom{k-s}{t-s}\binom{v-t-s}{v-k-s}$ of multiplicity $\langle \chi_s, 1 \rangle_G = r_s(G) - r_{s-1}(G)$. Thus, part 3 follows.

Part 4 is an application of proposition 4.1.34 (Rushanan's result).

Since $\overline{S}(M_{t,k})$ and $\overline{S}(M_{t,k}')$ are homeomorphic images of $\overline{S}(J_{t,k})$, it must be the case that $exp(J_{t,k})$ divides $exp(M_{t,k})$ and $exp(J_{t,k})$ divides $exp(M_{t,k}')$. Hence, parts 5 and 6 follow from part 4. □

Proposition 4.3.18. (Second Bound) *Let $t < k \leq v - k$. Define $\lambda_{t,k} = \binom{v-2t}{k-t}$. Then,*

1. *There are abelian groups $\overline{H_2}$ and $\overline{H_2'}$ such that*

$$0 \to \overline{H_2} \oplus \overline{S}(\overline{M_{k,t}}) \to \overline{S}(\lambda_{t,k}\overline{M_{t,t}}) \to \overline{S}(M_{t,k}) \to 0,$$
$$0 \to \overline{H_2'} \oplus \overline{S}(\overline{M_{k,t}}') \to \overline{S}(\lambda_{t,k}\overline{M_{t,t}}) \to \overline{S}(M_{t,k}') \to 0.$$

2. *The $exp(\overline{M_{t,t}})$ divides $\Pi_{s=0}^{t}\binom{v-t-s}{t-s}^{\epsilon_s(G)}$.*

3. *The $exp(\overline{M_{t,t}}')$ divides $\Pi_{s=0}^{t}\binom{v-t-s}{t-s}^{\epsilon_s(G)}$.*

4. *The* $exp(M_{t,k})$ *divides* $\lambda_{t,k}\Pi_{s=0}^{t}\binom{v-t-s}{t-s}^{\epsilon_s(G)}$.

5. *The* $exp(M'_{t,k})$ *divides* $\lambda_{t,k}\Pi_{s=0}^{t}\binom{v-t-s}{t-s}^{\epsilon_s(G)}$.

Proof. We show part 1. Consider the product from proposition 4.1.46,

$$W_{t,k}\overline{W_{k,t}} \;=\; \lambda_{t,k}\overline{W_{t,t}},$$

where $\lambda_{t,k} = \binom{v-t-k}{k-t}$. By applying $(\cdot)_0$ operator, we have

$$\begin{aligned}
\lambda_{t,k}\overline{M_{t,t}} &= (\lambda_{t,k}\overline{W_{t,t}})_0 \\
&= (W_{t,k}\overline{W_{k,t}})_0 \\
&= (W_{t,k})_0(\overline{W_{k,t}})_0 \\
&= M_{t,k}\overline{M_{k,t}}.
\end{aligned}$$

By proposition 4.3.11, $\overline{M_{t,t}}$, $\overline{M_{t,t}}'$ have full rank. Hence, $\overline{M_{t,t}}$, $\overline{M_{t,t}}'$ are nonsingular. By proposition 4.2.11, $Ker(M_{t,k}) \cap Im(\overline{M_{k,t}}) = \{0\}$ since $M_{t,k}\overline{M_{k,t}} = \lambda_{t,k}\overline{M_{t,t}}$ is nonsingular. We apply proposition 4.1.31 to the product $M_{t,k}\overline{M_{k,t}}$. Thus, we get the exact sequences:

$$\begin{array}{ccccccccc}
0 & \to & H & \to & S(M_{t,k}\overline{M_{k,t}}) & \to & S(M_{t,k}) & \to & 0, \\
0 & \to & K & \to & S(\overline{M_{k,t}}) & \to & H & \to & 0,
\end{array}$$

where $r(H) = rk(M_{t,k}) - rk(M_{t,k}\overline{M_{k,t}}) = n_t(G) - n_t(G) = 0$, and $\overline{S}(\overline{M_{k,t}})$ is injected into H in the second exact sequence. By proposition 4.1.31 again, we deduce that $H \simeq \overline{H_2} \oplus \overline{S}(M_{k,t})$ for some finite abelian group $\overline{H_2}$. Thus, the first exact sequence follows.

We show the second exact sequence of part 1. Consider the product $W_{t,k}\overline{W_{k,t}} =$

$\lambda_{t,k}\overline{W_{t,t}}$ again. By taking the $(\cdot)'_0$, we have

$$\begin{aligned}
\lambda_{t,k}\overline{M_{t,t}}' &= (\lambda_{t,k}\overline{W_{t,t}})'_0 \\
&= (W_{t,k}\overline{W_{k,t}})'_0 \\
&= (W_{t,k})'_0(\overline{W_{k,t}})'_0 \\
&= M'_{t,k}\overline{M_{k,t}}'.
\end{aligned}$$

By proposition 4.2.11, $Ker(M'_{t,k}) \cap Im(\overline{M_{k,t}}') = \{0\}$ since $M'_{t,k}\overline{M_{k,t}}' = \lambda_{t,k}\overline{M_{t,t}}'$ is nonsingular. We apply proposition 4.1.31 to the product $M'_{t,k}\overline{M_{k,t}}'$. Thus, we get the exact sequences:

$$\begin{array}{ccccccccc}
0 & \rightarrow & H & \rightarrow & S(M'_{t,k}\overline{M_{k,t}}') & \rightarrow & S(M'_{t,k}) & \rightarrow & 0, \\
0 & \rightarrow & K & \rightarrow & S(\overline{M_{k,t}}') & \rightarrow & H & \rightarrow & 0,
\end{array}$$

where $r(H) = rk(M'_{t,k}) - rk(M'_{t,k}\overline{M_{k,t}}') = n_t(G) - n_t(G) = 0$, and $\overline{S}(\overline{M_{k,t}}')$ is injected into H in the second exact sequence. By proposition 4.1.26, there is a finite abelian group $\overline{H'_2}$ such that,

$$H \simeq \overline{H'_2} \oplus \overline{S}(\overline{M_{k,t}}').$$

It suffices to show that $\overline{S}(\lambda_{t,k}\overline{M_{t,t}}) \simeq \overline{S}(\lambda_{t,k}\overline{M_{t,t}}')$.

Note that $\overline{M_{t,t}}' = ((\overline{W_{t,t}}^T)_0)^T = ((\overline{W_{t,t}})_0)^T = \overline{M_{t,t}}^T$. Also, for any matrix A, $\overline{S}(A) \simeq \overline{S}(A^T)$. Hence, the second exact sequence of part 1 follows and therefore part 1 follows.

We show part 2. We recall that the matrix A_t of proposition 4.1.44 is the matrix $\overline{W_{t,t}}$ as it is shown in proposition 4.1.46. By applying corollary 4.2.10 to proposition 4.1.44, we deduce that $\overline{M_{t,t}} = (\overline{W_{t,t}})_0$ is nonsingular with eigenspace decomposition:

$$\overline{M_{t,t}} = \sum_{s=0}^{t} \gamma_s \binom{v-t-s}{t-s} G_{s,k},$$

where $\gamma_s \in \{\pm 1\}$. By Rushanan's results, i.e., proposition 4.1.34, it follows that

$exp(\overline{M_{t,t}})$ divides $\Pi_{s=0}^{t}\binom{v-t-s}{t-s}^{\epsilon_s(G)}$. Hence, part 2 follows.

Part 3 follows from part 2 since $\overline{M_{t,t}}' = \overline{M_{t,t}}^T$, hence they have the same exponent.

We show parts 4 and 5. Clearly, by part 1, $\overline{S}(M_{t,k})$ and $\overline{S}(M'_{t,k})$ are homeomorphic images of $\overline{S}(\lambda_{t,k}\overline{M_{t,t}})$. Thus, $exp(M_{t,k})$ and $exp(M'_{t,k})$ each divide the $exp(\lambda_{t,k}\overline{M_{t,t}}) = \lambda_{t,k}exp(\overline{M_{t,t}})$. Therefore, they each divide the bounds given by parts 2 and 3. □

Corollary 4.3.19. *Let $v_1 = |G|$, and suppose that every prime that divides v_1 also divides v. Let $\gcd(v,t) = \gcd(v,t+1) = \cdots = \gcd(v,k+t-1) = 1$. That is,*

$$\gcd(v, \frac{(k+t-1)!}{(t-1)!}) \quad = \quad 1.$$

Let $t < k \leq v-k$. Then, v_1 is relatively prime to $|M_{t,k}|$ and $|M'_{t,k}|$.

Proof. It suffices to show that v_1 is relatively prime to $exp(M_{t,k})$ and to $exp(M'_{t,k})$.

By proposition 4.3.18, it suffices to show that v_1 is relatively prime to

$$\binom{v-2t}{k-t}\Pi_{s=0}^{t}\binom{v-t-s}{t-s}^{\epsilon_s(G)}.$$

Consider,

$$\binom{v-2t}{k-t} \quad = \quad \frac{(v-2t)(v-2t-1)\cdots(v-(k+t-1))}{(k-t)!}.$$

Since $\gcd(v-a,v) = \gcd(a,v)$ and

$$\gcd(v,t) = \cdots = \gcd(v,2t) = \cdots = \gcd(v,k+t-1) = 1,$$

it follows that v is relatively prime to $\binom{v-2t}{k-t}$.

Also, consider,

$$\binom{v-t-s}{t-s} \quad = \quad \frac{(v-t-s)(v-t-s-1)\cdots(v-2t+1)}{(t-s)!}.$$

Because,

$$\gcd(v,t) = \cdots = \gcd(v,t+s) = \gcd(v,t+s+1) = \cdots = \gcd(v,2t-1) = 1,$$

it follows that v is relatively prime to $\binom{v-t-s}{t-s}$.

Because v_1 and v have the same prime factors, it follows that v_1 is relatively prime to $\binom{v-2t}{k-t}\Pi_{s=0}^{t}\binom{v-t-s}{t-s}^{\epsilon_s(G)}$ and the result follows. □

4.3.3 The Integral Preimage Problem

The integral preimage problem for an integral matrix $M : V \to W$ involves determining when an integral $z \in W$ has an integral preimage in V. For the matrices $W_{t,k}$, the integral preimage problem is solved in [26] and is summarized by the next proposition.

Proposition 4.3.20. *Let $z \in C_t(X)$ be integral. Then,*

1. *If there is an integral $w \in C_k(X)$ such that $W_{t,k}w = z$, then $\binom{k-i}{t-i}$ divides $W_{i,t}z$ for $i = 0, \ldots, t$.*

2. *If $\binom{k-i}{t-i}$ divides $W_{i,t}z$ for $i = 0, \ldots, t$, then there is an integral $w \in C_k(X)$ such that $W_{t,k}w = z$.*

We note that the above proposition makes use the suitable right inverse of $W_{t,k}$ given in proposition 4.2.13.

Definition 4.3.21. *When the matrix $L_{t,k} = M_{t,k}$ or $M'_{t,k}$ has the same solution for its integral preimage problem as $W_{t,k}$, i.e.,*

1. *If there is an integral $w \in (C_k(X))_0$ and $z \in (C_t(X))_0$ such that $L_{t,k}w = z$, then $\binom{k-i}{t-i}$ divides $L_{i,t}z$ for $i = 0, \ldots, t$.*

2. *If for given $z \in (C_t(X))_0$, $\binom{k-i}{t-i}$ divides $L_{i,t}z$ for $i = 0, \ldots, t$, then there in an integral $w \in (C_k(X))_0$ such that $L_{t,k}w = z$.*

We will say that $L_{t,k}$ has a "trivial" solution for its integral preimage problem.

A trivial solution to the integral preimage problems has some implications on the exponent of the smith group. The next propositions shows this result.

Proposition 4.3.22. *Let $t < k \leq v - k$ and $L_{t,k} = M_{t,k}$ or $M'_{t,k}$ have a "trivial" solution for its integral preimage problem, then $exp(L_{t,k})$ divides $\Pi_{s=0}^{t}\binom{k-s}{t-s}$.*

Proof. Since $L_{t,k}$ is a surjective map, the Smith Group of $L_{t,k}$ is torsion. Thus, consider $z \in \overline{S}(L_{t,k}) = \frac{Col_{\mathbb{Q}}(L_{t,k})\cap\mathbb{Z}}{Col_{\mathbb{Z}}(L_{t,k})}$ such that for some $w \in \mathbb{Q}$, $L_{t,k}w = z$. Let $z' = \Pi_{s=0}^{t}\binom{k-s}{t-s}z$. Clearly, $\binom{k-i}{t-i}$ divides $L_{i,t}z'$ for $i = 0, \ldots, t$. Hence, z' has an integral preimage. Thus, $\Pi_{s=0}^{t}\binom{k-s}{t-s}z = z' = L_{t,k}w'$ where $w' \in \mathbb{Z}$. Therefore, $(\Pi_{s=0}^{t}\binom{k-s}{t-s})z = 0 \in \overline{S}(L_{t,k})$. Hence, the result follows. □

We will see that under certain conditions on the order of the group G, the matrices $M'_{t,k}$ and $M_{t,k}$ will have a trivial solution to their integral preimage problem; but, before that we introduce a major reduction for a general G.

Proposition 4.3.23. *Let $G \subset S_v$, $t+k \leq v$ and $L_{t,k} = M_{t,k}$ or $M'_{t,k}$. If $\binom{k-i}{t-i}$ divides $L_{i,t}c$ for $i = 0, \ldots, t$, then there is integral x such that $L_{t,k}x = v_1 c$, where $v_1 = |G|$.*

Proof. Will show the result for $M_{t,k}$ first. By proposition 4.2.13, it is shown that $W_{t,k}$ has a right inverse given by

$$U_{k,t} \quad = \quad \sum_{i=0}^{t} \frac{(-1)^i}{\binom{k-i}{t-i}} A_i W_{i,t}.$$

where the A_is are integral matrices from the $C_i(X)$ to $C_k(X)$. We note that $U_{k,t}$ may not be an S_v-map, but $W_{i,t}$ and $W_{t,k}$ are. Hence,

$$W_{t,k}\rho(g)U_{k,t}\rho(g^{-1}) \quad = \quad I,$$

for all $g \in G$. Therefore,

$$W_{t,k}U_{k,t}^{G} \quad = \quad v_1 I, \tag{4.9}$$

where,

$$\begin{aligned} U_{k,t}^G &= \sum_{i=0}^{t} \frac{(-1)^i}{\binom{k-i}{t-i}} A_i^G W_{i,t}, \\ A_i^G &= \sum_{g \in G} \rho(g) A_i \rho(g^{-1}). \end{aligned}$$

Clearly, $\rho(g)A_i^G x = A_i^G \rho(g)x$ for all $g \in G$. Hence, A_i^G is a G-map. Thus, $U_{k,t}^G$ is a integral G-map. Also, an application of the $(\cdot)_0$ operator gives

$$M_{t,k}(U_{k,t}^G)_0 = v_1 I.$$

We show that $v_1 c$ has an integral preimage under $M_{t,k}$. It suffices to show that: if y is a rational vector such that $y^T M_{t,k}$ is integral, then $y^T(v_1 c)$ is also integral.

Suppose y is rational, such that $y^T M_{t,k}$ is integral, then

$$\begin{aligned} y^T(v_1 c) &= y^T(v_1 I)c \\ &= y^T M_{t,k}(U_{k,t})_0 c \\ &= \sum_{i=0}^{t} (-1)^i (y^T M_{t,k})(A_i^G)_0 (\frac{M_{i,t} c}{\binom{k-i}{t-i}}). \end{aligned}$$

Hence, $y^T(v_1 c)$ is integral as: $\binom{k-i}{t-i}$ divides $M_{i,t}c$ for $i = 0, \ldots, t$, and $(A_i^G)_0$ is integral by construction.

We show the result for $M'_{t,k}$. We apply the $(\cdot)'_0$ operateor to Equation (4.9) instead, and we use an argument similar to the previous case. □

As a corollary, we deduce the integral preimage problem has trivial solution whenever the Smith Group is relatively prime to $|G|$.

Corollary 4.3.24. *Assume,*

1. *Let G be a permutation group in S_v, where $v_1 = |G|$.*
2. *Let $\gcd(|L_{t,k}|, v_1) = 1$, where $L_{t,k} = M_{t,k}$ or $M'_{t,k}$.*

Then,

1. *If* $\binom{k-i}{t-i}$ *divides* $L_{i,t}z$ *for an integral* $z \in (C_t(X))_0$*, then there is integral* $w \in (C_k(X))_0$ *such that* $L_{t,k}w = z$*.*

2. *The map* $L_{t,k}$ *has a trivial solution to the integral preimage problem.*

Proof. By proposition 4.3.23, we find a w' such that $M_{t,k}w' = v_1 z$, where $v_1 = |G|$. Let $e_1, \ldots, e_{r_k(G)}$ be an integral modular basis of $(C_k(X))_0$, and let $f_1, \ldots, f_{r_t(G)}$ be an integral modular basis of $(C_t(X))_0$. Let the bases $\{e_i\}$, $\{f_j\}$ give the Smith Normal Form of $L_{t,k}$. That is, $L_{t,k}e_i = d_i f_i$ for $i = 1, \ldots, r_t(G)$, and $L_{t,k}e_j = 0$ for $i = r_t(G)+1, \ldots, r_k(G)$. Where d_i are the invariant factors of $L_{t,k}$.

Clearly, since w' is integral, $w' = (\sum_{i=1}^{r_t(G)} c_i e_i) + (\sum_{i=r_t(G)+1}^{r_k(G)} c_i' e_i)$, where all c_is and c_i's are integral. Consider $w = w' - (\sum_{i=r_t(G)+1}^{r_k(G)} c_i' e_i)$, clearly w is integral and $L_{t,k}w = L_{t,k}w' = v_1 z$.

Let $z = \sum_{i=1}^{r_t(G)} g_i f_i$, where g_is are integral as z is integral. Because $L_{t,k}w = z$, we must have:

$$\begin{aligned}
\sum_{i=1}^{r_t(G)} (v_1 g_i) f_i &= v_1 z \\
&= L_{t,k} w \\
&= \sum_{i=1}^{r_t(G)} c_i L_{t,k} e_i \\
&= \sum_{i=1}^{r_t(G)} (d_i c_i) f_i.
\end{aligned}$$

By the $\mathbb{Z}$-linearly independence of the f_is, we must have $d_i c_i = v_1 g_i$ for all $i = 1, \ldots, r_t(G)$. By assumption, each d_i is relatively prime to v_1; hence, v_1 divides each c_i. Thus, $w_0 = \frac{w}{v_1} = \sum_{i=1}^{n_t} \frac{c_i}{v_1} e_i$ is an integral vector, and $L_{t,k}w_0 = z$. Hence, the result follows. □

Proposition 4.3.25. *Let,*

1. *The group* $G \subset S_v$*.*

2. *If* p *divides* $v_1 = |G|$*, then* p *divides* v*.*

3. *Let* $t < k \leq v - k$.

4. *Let* $\gcd(v, \frac{(k+t-1)!}{(t-1)!}) = 1$.

Then,

1. *The* $|G| = v_1$ *is relatively prime to* $|M_{t,k}|$ *and* $|M'_{t,k}|$.

2. *The maps* $M_{t,k}$ *and* $M'_{t,k}$ *have trivial solution for the integral preimage problem.*

3. *The* $exp(M_{t,k})$ *divides* $\Pi_{s=0}^{t}\binom{k-s}{t-s}$.

4. *The* $exp(M'_{t,k})$ *divides* $\Pi_{s=0}^{t}\binom{k-s}{t-s}$.

Proof. Part 1 follows by corollary 4.3.19. Part 2 follows by corollary 4.3.24. Parts 3 and 4 follow by proposition 4.3.22. □

We close this subsection with results about the Smith Group of $M'_{t,k}$ whenever the integral preimage problem of $M'_{t,k}$ has trivial solution.

Proposition 4.3.26. *Let* $M'_{2,3}$ *have a trivial solution to the integral preimage problem. Then,*

1. *If* G *is not* 1*-transitive then,*

$$2 \cdot \overline{S}(M'_{2,3}) \;=\; (\mathbb{Z}/3\mathbb{Z}) \text{ or } 0.$$

2. *If* G *is* 1*-transitive then,*

$$\overline{S}(M'_{2,3}) \;=\; (\mathbb{Z}/3\mathbb{Z}) \text{ or } 0.$$

Proof. Suppose G is not 1-transitive. Then, $z \in \mathbb{Z}^{r_2(G)}$ has an integral preimage under $M'_{2,3}$, i.e., $z = 0$ in $S(M_{2,3})$ if and only if:

1. 3 divides $M'_{0,2}z = j^T z$.

2. 2 divides $M'_{1,2}z$.

Clearly, the standard basis of $\mathbb{Z}^{r_2(G)}$, $\{e_1, \ldots, e_{r_2(G)}\}$, forms a set of not necessarily $\mathbb{Z}$-independent generators for $S(M'_{2,3})$ because $M'_{2,3}$ is onto.

Clearly, $2(e_i - e_j)$ satisfies the conditions of the solution of the integral preimage problem. Hence, $2(e_i - e_j)$ has in integral preimage and $2(e_i - e_j) = 0$ in $S(M'_{2,3})$. Therefore $2 \cdot S(M'_{2,3}) = \langle 2e_1, \ldots, 2e_{r_2(G)} \rangle = \langle 2e_1 \rangle$.

Clearly, $6e_1$ satisfies the conditions of the solution of the integral preimage problem. Hence, $6e_1 = 0$ in $S(M'_{2,3})$. Therefore, $2e_1$ has order 3 or 1 in $S(M'_{2,3})$. Part 1 follows.

Now, suppose that G is 1-transitive. Then, z has an integral preimage if and only if:

1. 3 divides $M'_{0,2}z = j^T z$.
2. 2 divides $M'_{1,2}z = 2j^T z$.

Thus, it is only necessary to check that 3 divides $j^T z$ because the second condition is checked trivially.

By using the standard basis $e_1, \ldots, e_{r_2(G)}$ as a set of not necessarily $\mathbb{Z}$-independent generators of $S(M'_{2,3})$, we can show that $(e_i - e_j)$ has an integral preimage by checking the above conditions. Thus, $(e_i - e_j) = 0$ in $S(M'_{2,3})$. Hence,

$$\begin{aligned} S(M'_{2,3}) &= \langle e_1, \ldots, e_{r_2(G)} \rangle \\ &= \langle e_1 \rangle. \end{aligned}$$

Consider, $3e_1$. It has an integral preimage by checking the above conditions. Thus, e_1 has order 3 or 1 in $S(M'_{2,3})$. Hence, part 2 follows. □

The next two results follow similar proofs that we exclude.

Proposition 4.3.27. *Let $M'_{2,4}$ have a trivial solution to the integral preimage problem. Then,*

1. *If G is not 1-transitive then,*

$$3 \cdot \overline{S}(M'_{2,4}) = (\mathbb{Z}/2\mathbb{Z}) \text{ or } 0.$$

2. If G is 1*-transitive then,*

$$\overline{S}(M'_{2,4}) \;=\; (\mathbb{Z}/6\mathbb{Z}) \text{ or } 0.$$

Proposition 4.3.28. *Let $M'_{3,4}$ have a trivial solution to the integral preimage problem. Then,*

1. If G is not 1*-transitive then,*

$$6 \cdot \overline{S}(M'_{3,4}) \;=\; (\mathbb{Z}/2\mathbb{Z}) \text{ or } 0.$$

2. If G is 1*-transitive then,*

$$2 \cdot \overline{S}(M'_{3,4}) \;=\; (\mathbb{Z}/2\mathbb{Z}) \text{ or } 0.$$

4.3.4 Integral $(\mathbf{t}, \mathbf{k})$-Bases

Given an matrix $M : (C_k(X))_0 \to (C_t(X))_0$. In general, the free $\mathbb{Z}$-module $Col_{\mathbb{Z}}(M)$ may not be generated by a $\mathbb{Z}$-basis consisting of a subset of the columns of M. However, when it is possible to find a $\mathbb{Z}$-basis for $Col_{\mathbb{Z}}(M)$ consisting columns of M, we call the $\mathbb{Z}$-basis a "column basis."

Definition 4.3.29. *A* (t,k)-basis *is a column basis for the matrix $M_{t,k}$ or the matrix $M'_{t,k}$.*

The notion of a (t,k)-basis can prove useful when calculating Smith Groups. This has been shown by Wilson in [26], where he used the existence of a (t,k)-basis to device an recursive algorithm to calculate the Smith Groups of the matrices $W_{t,k}$. In this section we will show a similar algorithm to calculate the Smith Groups of the matrices $M'_{t,k}$ whenever an $(i, i+1)$-basis exists and the matrices $M'_{i,i+1}$ have a trivial solution to the integral preimage problem for $i = 0, \ldots, t$.

We start with a general result about (t,k)-basis.

Proposition 4.3.30. *Let $\beta_{t,k}$ be a (t,k)-basis for $W_{t,k}$ that is invariant under the action of $G \subset S_v$. Define $\beta_{t,k}^G$ to be the orbits of G in β. Then,*

1. *The columns given by $\beta_{t,k}^G$ is a (t,k)-basis for the matrix $M'_{t,k}$.*
2. *The columns given by $\beta_{t,k}^G$ forms a column basis for the matrix $M_{t,k}D_k^{-1}$.*

Proof. Let $e_{\Omega_{K_0}}$ be an orbit in $\sim \beta_{t,k}^G$. By assumption, there is a c such that $W_{t,k}e_{K_0} = W_{t,k}c$, where $c = \sum_{K\in\beta_{t,k}} c_K e_K$ has support $\beta_{t,k}$. By applying the $P_{0,k} = P_{0,C_k(X),G}$ projection operator to the equation $W_{t,k}e_{K_0} = W_{t,k}c$, we deduce

$$W_{t,k}P_{0,k}e_K \;=\; W_{t,k}P_{0,k}c.$$

By direct calculation,

$$\begin{aligned} P_{0,k}e_{K_0} &= \frac{1}{|G|}\sum_{g\in G}\rho_k(g)e_{K_0} \\ &= \frac{|G_{K_0}|}{|G|}e_{\Omega_{K_0}} \\ &= \frac{e_{\Omega_{K_0}}}{|\Omega_{K_0}|}. \end{aligned}$$

Also,

$$\begin{aligned} P_{0,k}c &= \sum_{K\in\beta_{t,k}} c_K P_{0,k}e_K \\ &= \sum_{K\in\beta_{t,k}} c_K \frac{e_{\Omega_K}}{|\Omega_K|} \\ &= \sum_{\Omega_K\in\beta_{t,k}^G} \frac{(\sum_{K'\in\Omega_K} c_{K'})}{|\Omega_K|}e_{\Omega_K}. \end{aligned}$$

Thus, we can deduce that there is a $\underline{c} \in (C_k(X))_0$ given by

$$\underline{c} \;=\; \sum_{\Omega_K\in\beta_{t,k}^G} (\sum_{K'\in\Omega_K} c_{K'})e_{\Omega_K},$$

where,

$$M_{t,k}\frac{e_{\Omega_{K_0}}}{|\Omega_{K_0}|} \;=\; M_{t,k}\sum_{\Omega_K\in\beta_{t,k}}\frac{\underline{c}_{\Omega_K}}{|\Omega_K|}e_{\Omega_K}.$$

Thus,

$$M_{t,k}D_k^{-1}e_{\Omega_{K_0}} \;=\; M_{t,k}D_k^{-1}\underline{c}.$$

Hence, we deduce that $\beta^G_{t,k}$ forms a Column basis for $M_{t,k}D_k^{-1}$. By multiplying the previous equation by D_t on the left, we deduce,

$$\begin{aligned} M'_{t,k}e_{\Omega_{K_0}} &= D_tM_{t,k}D_k^{-1}e_{\Omega_{K_0}} \\ &= D_tM_{t,k}D_k^{-1}\underline{c} \\ &= M'_{t,k}\underline{c}. \end{aligned}$$

Hence, $\beta^G_{t,k}$ forms a column basis for $M'_{t,k}$. □

We proceed with a calculation of the Smith Normal form of $M'_{t,k}$ that depends on on the existence of an $(i, i+1)$-basis. Before we start, we state a few results that will be useful in our proof.

The following proposition can be found in Wilson's paper in [27].

Proposition 4.3.31. *Let A be an integral matrix and E an unimodular matrix such that $Ax = b$ has integral solution if and only if $Eb = Dy$ for a fixed diagonal matrix D and some integral y. Then, A has diagonal form given by D.*

The next proposition, which will use the concept of indexes of $\mathbb{Z}$-modules, can be found in an earlier work of Wilson in [26].

Definition 4.3.32. *Let $M \subset \mathbb{Z}^n$ be a $\mathbb{Z}$-module. Define,*

$$\overline{\mathrm{M}} \;=\; \{x \in \mathbb{Z}^n \mid cx \in M,\ \textit{for some } c \in \mathbb{Z}, c \neq 0\}.$$

Clearly, $\overline{M}$ has the same abelian rank as M. Hence, $\frac{\overline{M}}{M}$ is a torsion group. The index *of M is given by $[\overline{M} : M]$. That is, the order of $\frac{\overline{M}}{M}$.*

Proposition 4.3.33. *Let $e_1, \ldots, e_r$ be the $\mathbb{Z}$-basis for a module $M \subset \mathbb{Z}^n$ of index 1, then the matrix with rows $d_1e_1, \ldots, d_re_r$ has diagonal form:*

$$\begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & d_r & 0 & \cdots & 0 \end{bmatrix}.$$

Lemma 4.3.34. *Let,*

1. *The matrix U be unimodular.*
2. *The matrix F be surjective.*
3. *The matrix D be injective.*
4. *The following holds, $UM = DF$.*

Then,

1. *There is an exact sequence:*

$$0 \to \overline{S}(D) \to \overline{S}(M) \to \overline{S}(F) \to 0.$$

2. *The following holds, $|\overline{S}(M)| = |\overline{S}(D)||\overline{S}(F)|$.*

Proof. It suffices to show the exact sequence of part 1. Consider the product $M^TU^T = (UM)^T = (DF)^T = F^TD^T$. Clearly, U^T is unimodular. Also, because F is surjective, F^T must be injective. Similarly, because D is injective, D^T must be surjective. By proposition 4.1.32, we have the exact sequence,

$$0 \to S(D^T) \to S(F^TD^T) \to S(F^T) \to 0.$$

Clearly, $S(F^T D^T) = S(M^T U^T) = S(M^T)$ since U is unimodular. Also, $S(D^T) = \overline{S}(D^T)$ because D^T is surjective. Hence, $S(D^T)$ has abelian rank 0. By corollary 4.1.27, there is an exact sequence:

$$0 \to \overline{S}(D^T) \to \overline{S}(M^T) \to \overline{S}(F^T) \to 0.$$

Since $\overline{S}(A) \simeq \overline{S}(A^T)$ for any integral matrix A, it follows that

$$0 \to \overline{S}(D) \to \overline{S}(M) \to \overline{S}(F) \to 0.$$

The result follows. □

The next result reduces the calculation of the Smith Group of $M'_{t,k}$ to the existence of an $(i, i+1)$-basis.

Proposition 4.3.35. *Let $t \leq k \leq v - k$. We will assume that:*

1. *The matrices $M'_{i-1,i}$ afford an $(i-1, i)$-basis for $i = 1, \ldots, k$.*
2. *The matrices $M'_{i-1,i}$ have a trivial solution to the integral preimage problem, for $i = 1, \ldots, k$.*

Let $E_{t,k}$ be the rows of $M'_{t,k}$ after deleting the rows that correspond to an $(t-1, t)$-basis, where we allow $E_{t,k}$ to be the empty matrix. That is,

$$M'_{t,k} = \begin{bmatrix} C_{t,k} \\ E_{t,k} \end{bmatrix},$$

where $C_{t,k}$ are the rows that correspond to a $(t-1,t)$-basis. Let $F_{t,k}$ be defined as,

$$\begin{aligned} F_{t,k} &= \begin{bmatrix} \binom{k}{t} j^T \\ \binom{k-1}{t-1} E_{1,k} \\ \binom{k-2}{t-2} E_{2,k} \\ \vdots \\ \binom{k-t}{t-t} E_{t,k} \end{bmatrix} \\ &= D_{t,k} \begin{bmatrix} j^T \\ E_{1,k} \\ E_{2,k} \\ \vdots \\ E_{t,k} \end{bmatrix} \\ &= D_{t,k} \overline{F_{t,k}}, \end{aligned}$$

where $D_{t,k}$ is the appropriate diagonal matrix. The following must be the case,

1. *The matrices $\overline{F_{t,k}}$ are primitive of full rank. That is, they have trivial Smith group.*
2. *The matrices $\overline{F_{t,t}} = F_{t,t}$ are unimodular.*
3. *The $Row_{\mathbb{Z}}(M'_{t,k}) = Row_{\mathbb{Z}}(F_{t,k})$.*
4. *The matrix $M'_{t,k}$ admits a diagonal form given by $\binom{k-i}{t-i}$ with multiplicity $r_i(G) - r_{i-1}(G)$, where $i = 0, \ldots, t$ and $r_{-1}(G) = 0$.*
5. *The $S(M'_{t,k})$ is given by,*

$$(\mathbb{Z}/\binom{k}{t}\mathbb{Z})^{r_0(G)} \times (\mathbb{Z}/\binom{k-1}{t-1}\mathbb{Z})^{r_1(G)-r_0(G)} \times \cdots (\mathbb{Z}/\binom{k-t}{t-t}\mathbb{Z})^{r_t(G)-r_{t-1}(G)}.$$

Proof. A similar proof to that of lemma 2 of [27] will be given. The proof is by induction on k.

Note that for $k = 0$, the result is clearly true since $M'_{0,0} = 1$. Suppose G is t_0-transitive. That is, G acts transitivily on the 1-sets, 2-sets, $\cdots$, t_0-sets. Then, for $t \leq k \leq t_0$, $M'_{t,k} = \binom{k}{t}1$. Since $\overline{F_{t,t}} = 1$ and $F_{t,k} = \binom{k}{t}1$, the result follows trivially.

Let $k = t_0$ be the base case of our inductive proof. Assume the claim is true for $t_0 \leq k' \leq k$, we will show the claim for $k' = k + 1$. We will start by showing that the $S(M'_{k,k+1})$ is given as it is in part 5 by using proposition 4.3.31. The candidate matrix that we will use for E in proposition 4.3.31 is $\overline{F_{k,k}}$. Hence, proposition 4.3.31 will apply, if we show:

Lemma 4.3.36.

$$M'_{k,k+1}z = b \text{ for some integral } z \iff \overline{F_{k,k}}b = D_{k,k+1}y \text{ for some integral } y.$$

Proof. The $\Longrightarrow$ part is clear. Suppose that for a given integral b, there is an integral y such that $\overline{F_{k,k}}b = D_{k,k+1}y$. Since $M_{k,k+1}$ has trivial solution to the integral preimage problem, it suffices to show that $\binom{k+1-i}{k-i} = k + 1 - i$ divides $M'_{i,k}b$ for $i = 0, \ldots, k$.

Clearly, $k + 1$ divides $j^T b$ since this is the first row of $\overline{F_{k,k}}b = D_{k,k+1}y$. Also, note that for $i \leq t_0$,

$$\begin{aligned} M'_{i,k}b &= \binom{k}{i} j^T b \\ &= \binom{k}{i}(k+1)\frac{j^T b}{k+1} \\ &= (k-i+1)\binom{k+1}{i}\frac{j^T b}{k+1}. \end{aligned}$$

Hence, $(k + 1 - i)$ divides $M'_{i,k}b$. Therefore, assume $t_0 < i$.

Consider, $M'_{i,k} = \begin{bmatrix} C_{i,k} \\ E_{i,k} \end{bmatrix}$, where $C_{i,k}$ are the rows that correspond to an $(i-1, i)$-basis, and $E_{i,k}$ corresponds to the remaining rows. It suffices to show that $C_{i,k}b$ is divisible by $k + 1 - i$ for $i = 2, \ldots, k$. We will show this by induction on i.

Let $\overline{F_{i-1,i}} = \begin{bmatrix} \overline{F^*_{i-1,i}} & \overline{F^{**}_{i-1,i}} \end{bmatrix}$, where $\overline{F_{i-1,i}}^*$ are the columns of $\overline{F_{i-1,i}}$ that correspond to the $(i - 1, i)$-basis.

Claim 4.3.37. *We have:* $Col_{\mathbb{Z}}(\overline{F^*_{i-1,i}}) = Col_{\mathbb{Z}}(\overline{F_{i-1,i}})$. *In particular, as* $\overline{F_{i-1,i}}$ *has trivial Smith group and full rank,* $\overline{F^*_{i-1,i}}$ *is unimodular.*

Proof. Let $M'_{i-1,i} = \begin{bmatrix} A & B \end{bmatrix}$, where A consists of the columns that correspond to an $(i-1,i)$-basis. Clearly, $D_{i-1,i}\overline{F_{i-1,i}} = \overline{F_{i-1,i-1}}M'_{i-1,i}$. Thus, $\overline{F_{i-1,i}} = D^{-1}_{i-1,i}\overline{F_{i-1,i-1}}M'_{i-1,i}$. In particular, we have $\overline{F^*_{i-1,i}} = D^{-1}_{i-1,i}\overline{F_{i-1,i-1}}A$. Since A consists of the columns that correspond to an $(i-1,i)$-basis, we have that for every integral z, there is integral y such that $M'_{i-1,i}z = Ay$.

Let $x = \overline{F_{i-1,i}}z$ for some integral z. Then,

$$\begin{aligned} x &= \overline{F_{i-1,i}}z \\ &= D^{-1}_{i-1,i}\overline{F_{i-1,i-1}}M'_{i-1,i}z \\ &= D^{-1}_{i-1,i}\overline{F_{i-1,i-1}}Ay \\ &= \overline{F^*_{i-1,i}}y, \end{aligned}$$

hence, $Col_{\mathbb{Z}}(\overline{F_{i-1,i}}) \subset Col_{\mathbb{Z}}(\overline{F^*_{i-1,i}})$ and the claim follows. □

Resuming the proof of lemma 4.3.36. Clearly,

$$\begin{aligned} \overline{F_{i-1,i}}M'_{i,k} &= \begin{bmatrix} \binom{k}{i}j^T \\ \binom{k-1}{i-1}E_{1,k} \\ \vdots \\ \binom{k-(i-1)}{i-(i-1)}E_{i-1,k} \end{bmatrix} \\ &= D'_{i,k}\overline{F_{i-1,k}}, \end{aligned} \tag{4.10}$$

where $D'_{i,k}$ is the matrix $D_{i,k}$ after erasing the rows that have diagonal entry equal to 1. By Equation (4.10), we have,

$$\overline{F^*_{i-1,i}}C_{i,t} + \overline{F^{**}_{i-1,i}}E_{i,t} = D'_{i,k}\overline{F_{i-1,k}},$$

hence,

$$\frac{1}{k+1-i}\overline{F^{*}_{i-1,i}}C_{i,t} + \overline{F^{**}_{i-1,i}}(\frac{1}{k+1-i}E_{i,t}) \;=\; \frac{1}{k+1-i}D'_{i,k}\overline{F_{i-1,k}}.$$

Note that $\frac{1}{k+1-i}D'_{i,k}$ equals:

$$\begin{bmatrix} \binom{(k-0)+1}{(k-i)+1} & 0 & \cdots & 0 \\ 0 & \binom{(k-1)+1}{(k-i)+1} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \binom{(k-(i-1))+1}{(k-i)+1} \end{bmatrix} \begin{bmatrix} \frac{1}{k+1} & 0 & 0 & \cdots & 0 \\ 0 & \frac{1}{k-1} & 0 & \cdots & 0 \\ 0 & 0 & \frac{1}{k-2} & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \frac{1}{k-(i-1)+1} \end{bmatrix},$$

thus, $\frac{1}{k+1-i}D'_{i,k}\overline{F_{i-1,k}}b$ equals:

$$\begin{bmatrix} \binom{(k-0)+1}{(k-i)+1} & 0 & \cdots & 0 \\ 0 & \binom{(k-1)+1}{(k-i)+1} & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \binom{(k-(i-1))+1}{(k-i)+1} \end{bmatrix} \begin{bmatrix} \frac{1}{k+1}j^{T}b \\ \frac{1}{k-1}E_{2,k}b \\ \frac{1}{k-2}E_{3,k}b \\ \vdots \\ \frac{1}{k-(i-1)+1}E_{i-1,k}b \end{bmatrix},$$

where, the right-hand side is integral by assumption. Thus, $\frac{1}{k+1-i}D'_{i,k}\overline{F_{i-1,k}}b$ is integral.

Consider,

$$\frac{1}{k+1-i}\overline{F^{*}_{i-1,i}}C_{i,t}b + \overline{F^{**}_{i-1,i}}(\frac{1}{k+1-i}E_{i,t}b) \;=\; \frac{1}{k+1-i}D'_{i,k}\overline{F_{i-1,k}}b.$$

Since $\frac{1}{k+1-i}E_{i,t}b$ is integral and the right-hand side is integral, we must have,

$$\frac{1}{k+1-i}\overline{F^{*}_{i-1,i}}C_{i,t}b,$$

be integral. As $\overline{F^{*}_{i-1,i}}$ is unimodular, we have that $\frac{1}{k+1-i}C_{i,t}b$ is integral. The result follows. □

Resuming to the proof of the proposition 4.3.35, lemma 4.3.36 shows that the $S(M'_{k,k+1})$ is given by part 5. That is, $S(M'_{k,k+1}) = S(D_{k,k+1})$. Hence,

$$|Smith(M'_{k,k+1})| \;=\; |Smith(D_{k,k+1})|,$$

and by lemma 4.3.34 applied to the following equation:

$$D_{k,k+1}\overline{F_{k,k+1}} \;=\; \overline{F_{k,k}}M'_{k,k+1},$$

we deduce that $|Smith(M'_{k,k+1})| = |Smith(D_{k,k+1})||Smith(\overline{F_{k,k+1}})|$. Hence, $\overline{F_{k,k+1}}$ has trivial Smith group.

Let $\overline{F_{k,k+1}} = [UV]$, where U are the rows that correspond to a $(k, k+1)$-basis. By a similar argument as the one given in claim 4.3.37, we can show that,

$$Col_{\mathbb{Z}}(\overline{F_{k,k+1}}) \;=\; Col_{\mathbb{Z}}(U).$$

Thus, U is unimodular.

Consider,

$$\begin{aligned}\overline{F_{k+1,k+1}} &= \begin{bmatrix} \overline{F_{k,k+1}} \\ E_{k+1,k+1} \end{bmatrix} \\ &= \begin{bmatrix} U & V \\ 0 & I \end{bmatrix},\end{aligned}$$

where, we used for $E_{k+1,k+1}$ the resulting rows of $M'_{k+1,k+1} = I$, the identity matrix, after deleting those rows that correspond to the chosen $(k, k+1)$-basis. Clearly, $det(\overline{F_{k+1,k+1}}) = det(U) = \pm 1$. Hence, $\overline{F_{k+1,k+1}}$ is unimodular. Hence, part 2 follows.

Part 1 follows from the unimodularity of $\overline{F_{k+1,k+1}}$.

We show part 3. Clearly, $\overline{F_{t,t}}M'_{t,k+1} = F_{t,k+1}$. Also, $\overline{F_{t,t}}$ is unimodular for $t \leq k$ by the Inductive Hypothesis, and is is unidmodular for $t = k+1$ by part 2. Hence, $Row_{\mathbb{Z}}(M'_{t,k+1}) = Row_{\mathbb{Z}}(F_{t,k+1})$ and part 3 follows.

To show the remaining parts, let $t \leq k+1$. Consider the equation,

$$\begin{aligned} F_{t,k+1} &= D_{t,k+1}\overline{F_{t,k+1}} \\ &= \overline{F_{t,t}}M'_{t,k+1}. \end{aligned}$$

Since $\overline{F_{k+1,k+1}}$ is unimodular, it follows that $\overline{F_{t,k+1}}$ is primitive, i.e., it has trivial Smith Group. By lemma 4.3.34, $S(D_{t,k+1}) \simeq S(\overline{F_{t,t}}M'_{t,k+1}) \simeq S(M'_{t,k+1})$. Thus parts 4 and 5 follow. □

The following proposition shows a criterion for finding a (t,k)-basis.

Proposition 4.3.38. *Suppose that $t \leq k \leq v-k$, and the following,*

1. *The matrix $M'_{i-1,i}$ admits an $(i-1,i)$-basis for $i = 1,\ldots,t$.*
2. *The matrix $M'_{i-1,i}$ has trivial solution to the integral preimage problem for $i = 1,\ldots,t$.*
3. *The set β be a set of $\mathbb{Q}$-linearly independent columns of $M'_{t,k}$.*

Then,

1. *The matrix $\overline{F_{i,i}}$ is unimodular for $i = 0,\ldots,t$.*
2. *There is an exact sequence,*

$$0 \to \overline{S}(D_{t,k}) \to \overline{S}(M'_{t,k}) \to \overline{S}(\overline{F_{t,k}}) \to 0.$$

3. *There is a finite abelian group H_β such that:*

$$0 \to H_\beta \to \overline{S}(M'_\beta) \to \overline{S}(M'_{t,k}) \to 0.$$

4. *The following divisibility conditions holds, $|D_{t,k}|$ divides $|M'_{t,k}|$ divides $|M'_\beta|$.*
5. *If $|M'_\beta| = \pm|D_{t,k}|$, then β is a (t,k)-basis.*

Proof. The same proof of proposition 4.3.35 can be used to show that $\overline{F_{i,i}}$ is unimodular for $i = 0, \ldots, t$.

Part 2 is an application of lemma 4.3.34 to the equation $\overline{F_{t,t}}M'_{t,k} = D_{t,k}\overline{F_{t,k}}$.

We show part 3. Consider the following inclusion of free $\mathbb{Z}$-modules,

$$Col_{\mathbb{Z}}(M'_{\beta}) \subset Col_{\mathbb{Z}}(M'_{t,k}) \subset \mathbb{Z}^{r_t(G)}.$$

Thus, there is an exact sequence,

$$0 \to H_{\beta} \to S(M'_{\beta}) \to S(M'_{t,k}) \to 0,$$

where $H_{\beta} = \frac{Col_{\mathbb{Z}}(M'_{t,k})}{Col_{\mathbb{Z}}(M'_{\beta})}$. Clearly, $r(H_{\beta}) = r(M'_{\beta}) - r(M'_{t,k}) = 0 - 0$ since the matrices M'_{β} and $M'_{t,k}$ are onto. Thus, H_{β} is a torsion group and by corollary 4.1.27 there is an exact sequence:

$$0 \to H_{\beta} \to \overline{S}(M'_{\beta}) \to \overline{S}(M'_{t,k}) \to 0.$$

Hence, part 3 follows.

Parts 4 and 5 are obvious consequences of parts 2 and 3. □

We close this subsection with a proposition that shows how one can use a $(t-1, t)$-basis in the calculation of the Smith Group of $M_{t,k}$ or $M'_{t,k}$.

Proposition 4.3.39. *Let $L_{t,k} = M_{t,k}$ or $M'_{t,k}$. Assume,*

1. *The $\mathbb{Z}$-module $\mathbb{Z}^{r_t(G)} \cap Ker(L_{t-1,t})$ is contained in the $\mathbb{Z}$-module $Im_{\mathbb{Z}}(L_{t,k})$.*
2. *The set $\beta_{t-1,t}$ is a $(t-1, t)$-basis for $L_{t-1,t}$.*

Then,

1. *The set $\beta_{t-1,t}$ is a generating set for $\overline{S}(L_{t,k})$ but not necessarily $\mathbb{Z}$-independent. That is, $\langle \beta_{t-1,t} \rangle = \overline{S}(L_{t,k})$.*

2. If $\gcd(|L_{t-1,t}|, k-t+1) = 1$*, then* $\beta_{t-1,t}$ *is* $\mathbb{Z}$*-independent. That is,*

$$\overline{S}(L_{t,k}) \;=\; (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_{r_{t-1}(G)}\mathbb{Z}),$$

where $\beta_{t-1,t} = \{\Omega_{T_1}, \ldots, \Omega_{T_{r_{t-1}(G)}}\}$*, and* $\langle \Omega_{T_i} \rangle = (\mathbb{Z}/a_i\mathbb{Z})$ *is a nontrivial subgroup of* $\overline{S}(L_{t,k})$*.*

Proof. Let $\Omega_T \in (C_t(X))_0$. Since, $\beta_{t-1,t}$ is a $(t-1,t)$-basis for $L_{t-1,t}$, there are integral $c_{\Omega_{T'}}$ with support in $\beta_{t-1,t}$ such that:

$$0 \;=\; L_{t-1,t}(\Omega_T - \sum_{\Omega_{T'} \in \beta_{t-1,t}} c_{\Omega_{T'}} \Omega_{T'}).$$

By assumption, there is a $z \in \mathbb{Z}^{r_k(G)}$ such that:

$$L_{t,k} z \;=\; \Omega_T - \sum_{\Omega_{T'} \in \beta_{t-1,t}} c_{\Omega_{T'}} \Omega_{T'}.$$

Since $\overline{S}(L_{t,k}) = \frac{\mathbb{Z}^{r_t(G)}}{Im_{\mathbb{Z}}(L_{t,k})}$, it follows that $\Omega_T \in \langle \beta_{t-1,t} \rangle$ in $\overline{S}(L_{t,k})$. Since,

$$\langle \Omega_T \mid \Omega_T \in (C_k(X))_0 \rangle \;=\; \overline{S}(L_{t,k}),$$

part 1 follows.

We show part 2. Suppose otherwise. That is, there is some $\Omega_{T_0} \in \beta_{t-1,t}$ can be expressed as an integral linear combination of the other elements of $\beta_{t-1,t}$ in $\overline{S}(L_{t,k})$. Paraphrasing this condition, there is an integral vector c with at least one entry equal to 1, i.e., the entry corresponding to Ω_{T_0}, and with support $\beta_{t-1,t}$ such that:

$$c \;=\; L_{t,k} z,$$

where z is also integral. If we multiply the above equation by $L_{t-1,t}$ on the left, we deduce,

$$L_\beta c \;=\; (k-t+1) L_{t-1,k} z,$$

where L_β are the columns of $L_{t-1,t}$ that correspond to $\beta_{t-1,t}$. Clearly, $|L_{t-1,t}| = |L_\beta|$ since $\beta_{t-1,t}$ is a $(t-1,t)$-basis. Because $\gcd(|L_\beta|, k-t+1) = \gcd(|L_{t-1,t}|, k-t+1) = 1$, we can deduce that $k-t+1$ divides c. In particular, this means that the coefficient that corresponds to Ω_{T_0} in c is divisible by $k-t+1$. That is, $k-t+1$ divides 1. This is a contradiction. □

We give the remark that the first condition of proposition 4.3.39 is satisfied whenever $L_{t-1,t}$ has a trivial solution to the integral preimage problem.

4.3.5 The Kernel of $\mathbf{M'_{t,k}}$ and $\mathbf{M_{t,k}}$

The kernel of the matrix $W_{t,k}$ has been shown by Graver and Jurkat in [9] to be generated by elements of the form:

$$\Pi(A,B) \;=\; (x_{a_1} - x_{b_1})(x_{a_2} - x_{b_2}) \cdots (x_{a_{t+1}} - x_{b_{t+1}}) x_{a_{t+2}} \cdots x_{a_k},$$

where $A = \{a_1, \ldots, a_{t+1}, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_{t+1}\}$ are disjoint sets of $\{1, \ldots, v\}$, and $\Pi(A,B)$ is understood to be a formal sum of k-subsets of $\{1, \ldots, v\}$ where the monomial terms $x_{c_1} \cdots x_{c_k}$ are identified with their corresponding k-subsets $\{c_1, \ldots, c_k\}$. The elements $\Pi(A,B)$ are known as (t,k)-pods in the literature.

An effective way to calculate the (t,k)-pods, when the sets A and B are specified, is to think of every monomial $\pm x_{c_1} \cdots x_{c_k} \rightarrow \pm\{c_1, \ldots, c_k\} = C$ in the summation expansion of $\Pi(A,B)$ as a set C, with corresponding term $(-1)^{|C_2|} e_C$, where $C_1 = C \cap A$ and $C_2 = C \cap B$ have the properties:

$$\begin{aligned} 0 \leq \;& |C_2| \;\leq t+1, \\ \{a_{t+2}, \ldots, a_k\} \;& \subset \; C_1, \\ C_1 \cap C_2 \;& = \; \phi. \end{aligned}$$

Hence, one could think of every term in the summation expansion of $\Pi(A,B)$ as corresponding to a set $C_2 \subset \{1, \ldots, t+1\}$. Thus, one can formulate an equivalent definition as it is given by the following proposition.

Proposition 4.3.40. *Let* $A = \{a_1, \ldots, a_k\}$ *and* $B = \{b_1, \ldots, b_{t+1}\}$ *be such that* $A \cap B = \phi$. *For every* $T \subset \{1, \ldots, t+1\}$ *define* $f_T : \{1, \ldots, t+1\} \to \{1, \ldots, v\}$ *as:*

$$f_T(i) \quad = \quad \begin{cases} b_i & \text{if } i \in T, \\ a_i & \text{else.} \end{cases}$$

Then,

$$\Pi(A, B) \quad = \quad \sum_{T \subset \{1,\ldots,t+1\}} (-1)^{|T|} e_{\{f_T(1),\ldots,f_T(t+1),a_{t+2},\ldots,a_k\}}.$$

As a remark, we note that $\Pi(A, B)$ depends not only on A and B but also on the indexing of the elements of A and B. That is, if we consider a $(2, 3)$-pod where $A = \{a_1, a_2, a_3\} = \{a'_1, a'_2, a'_3\}$ and $a'_1 = a_2$, $a'_2 = a_3$, $a'_3 = a_1$, then in general each indexing will provide distinct $\Pi(A, B)$s.

We proceed to find corresponding generators of the $Ker(M'_{t,k})$ and $Ker(M_{t,k})$ by projecting $\Pi(A, B)$ to the equivariant case. The following proposition summarizes this result.

Proposition 4.3.41. *Let* A *be a* $(t+1)$*-subset and* B *a* k*-subset such that* $A \cap B = \phi$. *Let,*

$$\Pi(A, B) \quad = \quad e_{K_1} + \cdots + e_{K_r},$$

where summation allows for repetition. Let $\Pi(A, B)^G$ *be the equivariant projection given by:*

$$\Pi(A, B)^G \quad = \quad e_{\Omega_{K_1}} + \cdots + e_{\Omega_{K_r}}.$$

Then,

1. *The element* $D_k^{-1}\Pi(A, B)^G \in Ker(M_{t,k})$, *and the set of all* $D_k^{-1}\Pi(A, B)^G$ *generate* $Ker(M_{t,k})$.

2. *The element* $\Pi(A, B)^G \in Ker(M'_{t,k})$, *and the set of all* $\Pi(A, B)^G$ *generate*

$Ker(M'_{t,k})$.

Proof. We show part 1. Let A and B be given. Clearly, $W_{t,k}\Pi(A,B) = 0$. By use of the operator $P_{0,t,G} = \frac{1}{|G|}\sum_{g\in G}\rho_t(g)$, we deduce,

$$W_{t,k}P_{0,k,G}\Pi(A,B) \;=\; 0.$$

It is a quick exercise to show,

$$P_{0,t,G}\Pi(A,B) \;=\; \widehat{D_k}^{-1}\widetilde{\Pi(A,B)}^{G},$$

where,

$$\begin{aligned}\widetilde{\Pi(A,B)}^{G} &= \sum_{i=1}^{r}\widetilde{e_{\Omega_{K_i}}},\\ \widetilde{e_{\Omega_{K_i}}} &= \sum_{K'_i\in\Omega_{K_i}} e_{K'_i}.\end{aligned}$$

Hence, $W_{t,k}\widehat{D_k}^{-1}\widetilde{\Pi(A,B)}^{G} = 0$. By using the canonical basis of $(C_k(X))_0$ and $(C_t(X))_0$, we deduce

$$M_{t,k}D_k^{-1}\Pi(A,B)^G \;=\; 0,$$

where, we have identified $\widetilde{\Pi(A,B)}^{G} = \widetilde{e_{\Omega_{K_1}}}+\cdots+\widetilde{e_{\Omega_{K_r}}}$ in $C_k(X)$ with its counterpart $\Pi(A,B)^G = e_{\Omega_{K_1}}+\cdots+e_{\Omega_{K_r}}$ in $(C_k(X))_0$. Hence, $D_k^{-1}\Pi(A,B)^G \in Ker(M_{t,k})$.

We show that the elements of the form $D_k^{-1}\Pi(A,B)^G$ generate the kernel. Consider $x^G \in (C_k(X))_0$ such that $M_{t,k}x^G = 0$. Let $x^G = \sum c_{\Omega_K}e_{\Omega_K}$ and x its lift to $C_k(X)$ given by $x = \sum c_{\Omega_K}e_K$. Clearly, $W_{t,k}x = 0$ and $P_{0,k,G}x = x$. Hence, $x = \sum c_i\Pi(A_i,B_i)$, for constants c_i and sets A_i and B_i. Consider,

$$\begin{aligned}x &= P_{0,k,G}x\\ &= P_{0,k,G}(\sum c_i\Pi(A_i,B_i))\\ &= \sum c_i\widehat{D_k}^{-1}\widetilde{\Pi(A_i,B_i)}^{G}.\end{aligned}$$

Using the canonical basis of $(C_k(X))_0$ and $(C_t(X))_0$, we deduce,

$$x^G = \sum c_i D_k^{-1} \Pi(A_i, B_i)^G.$$

Thus, part 1 follows.

We show part 2. Because $M_{t,k} D_k^{-1} \Pi(A, B)^G = 0$, we have that $M'_{t,k} \Pi(A, B)^G = D_t M_{t,k} D_k^{-1} \Pi(A, B)^G = 0$. Hence, $\Pi(A, B)^G \in Ker(M'_{t,k})$.

We show that $\Pi(A, B)^G$ generate the $Ker(M'_{t,k})$. Let x^G be such that $M'_{t,k} x^G = 0$. Clearly, $D_t M_{t,k} D_k^{-1} x^G = 0$. Thus, $M_{t,k} D_k^{-1} x^G = 0$. By part 1, $D_k^{-1} x^G = \sum c_i D_k^{-1} \Pi(A_i, B_i)^G$. Hence, by multiplying by D_k, we deduce $x^G = \sum c_i \Pi(A_i, B_i)^G$. The conclusion follows. □

We close this subsection with a summary of a property of G-projections among images of $W_{t,k}$ that was used in proposition 4.3.41.

Proposition 4.3.42. *Let,*

$$W_{t,k} e_K = \sum_{T \subset K} e_T.$$

Assume that $G \subset S_v$ is a permutation action. Then,

1. *The following holds, $M_{t,k} D_k^{-1} \Omega_K = \sum_{T \subset K} D_t^{-1} \Omega_T$.*
2. *The following holds, $M'_{t,k} \Omega_K = \sum_{T \subset K} \Omega_T$.*

Proof. The proof uses the same procedure as proposition 4.3.41. Simply apply $P_{0,t,G}$ to both sides of the equation $W_{t,k} e_K = \sum_{T \subset K} e_T$ and proceed to simplify by using:

$$\begin{aligned} P_{0,t,G} e_T &= \widehat{D_t}^{-1} \Big(\sum_{T' \in \Omega_T} e_{T'} \Big), \\ P_{0,k,G} e_K &= \widehat{D_k}^{-1} \Big(\sum_{K' \in \Omega_K} e_{K'} \Big). \end{aligned}$$

Using the canonical basis of $(C_t(X))_0$ and $(C_k(X))_0$, we can deduce the first part.

Part 2 follows by multiplying both sides of part 1 by D_t. □

4.4 Positive Equivariant G-Signings

We will formalize a signing property about special (t,k)-basis of $W_{t,k}$ that has been observed by researchers through heuristics. We will do this by introducing the concept of a positive equivariant G-signing.

Definition 4.4.1. *Assume,*

1. *Let β be a set of $\mathbb{Q}$-linearly independent colums of $W : C_k(X) \to C_t(X)$.*
2. *Let W be a G-map and not necessarily an S_v-map.*
3. *Assume that β is G-invariant, i.e., $g \cdot K \in \beta$ for all $g \in G$ and $K \in \beta$.*
4. *Let $\epsilon : \beta \to \{\pm 1\}$ be a signing of the elements of β that is G-invariant. That is, $\epsilon(g \cdot K) = \epsilon(K)$ for all $g \in G$ and $K \in \beta$.*
5. *Define $\mathrm{W}_\beta = [\mathrm{We}_{\mathrm{K}_1}, \ldots, \mathrm{We}_{\mathrm{K}_\mathrm{r}}]$ and $\mathrm{W}^*_\beta = [\epsilon(\mathrm{K}_1)\mathrm{We}_{\mathrm{K}_1}, \ldots, \epsilon(\mathrm{K}_\mathrm{r})\mathrm{We}_{\mathrm{K}_\mathrm{r}}]$, where $\beta = \{e_{K_1}, \ldots, e_{K_r}\}$.*

Then,

1. *The map ϵ is a* "positive equivariant G-signing" *for (W, β) if and only if for all $e_K \in \sim \beta$:*

$$WP_{0,k,G}e_K = W\frac{\widetilde{e_{\Omega_K}}}{|\Omega_K|} \in C_+(W^*_\beta),$$

where $C_+(W^*_\beta) = \{W^*_\beta c \mid c \geq 0\}$ is the positive cone spanned by W^*_β, and,

$$\widetilde{e_{\Omega_K}} \;=\; \sum_{K' \in \Omega_K} e_{K'}.$$

2. *If the pair (W, β) admits a "positive equivariant G-signing" when $G = \{1\}$, then we say that (W, β) admits a* "trivial positive equivariant signing."

A well-known result about positive cones of matrices, which we will use shortly, is the Minkowski-Farkas Lemma.

Lemma 4.4.2. *(***Minkowski-Farkas)** *Let W be a real matrix, and $z \in \mathbb{R}$ a vector of real numbers. The following are equivalent,*

1. *The element $z \in C_+(W)$.*
2. *If $y \in \mathbb{R}$ is a vector of real numbers such that $y^T W \geq 0$, then $y^T z \geq 0$.*

The following proposition reduces the concept of positive equivariant G-signings to the concept of trivial positive equivariant signings.

Proposition 4.4.3. *Let $W : C_k(X) \to C_t(X)$ be matrix of rational entries that is a G-map but not necessarily an S_v map. Let β be a set of columns that is $\mathbb{Q}$-linearly independent, and let β be G-invariant. Then, the following are equivalent,*

1. *The pair (W, β) affords a positive equivariant G-signing.*
2. *The pair (M', β^G) affords a trivial positive equivariant signing, where $M' = (W)'_0$ and β^G is the set of G orbits in β.*

Proof. We proceed to show the equivalence in two separate cases.

Part 1 $\implies$ part 2. Let ϵ be a positive equivariant G-signing of (W, β). Note that,

1. The map W^*_β is a G-map.
2. Given $K \in \sim \beta$, there is $c \geq 0$ such that $W\frac{e_{\Omega_K}}{|\Omega_K|} = W^*_\beta c$.

Consider,

$$\begin{aligned} W\frac{e_{\Omega_K}}{|\Omega_K|} &= WP_{0,t,G}e_K \\ &= P_{0,k,G}WP_{0,t,G}e_K \\ &= P_{0,t,G}W\widetilde{\frac{e_{\Omega_K}}{|\Omega_K|}} \\ &= P_{0,k,G}W^*_\beta c \\ &= W^*_\beta P_{0,t,G}c \\ &= W^*_\beta \underline{c}, \end{aligned}$$

where $\underline{c} = \sum_{\Omega_K \in (C_k(X))_0} (\sum_{K' \in \Omega_K} c_{K'})(\widetilde{e_{\Omega_K}})$. Thus, $W \frac{\widetilde{e_{\Omega_K}}}{|\Omega_K|} = W^*_\beta \underline{c}$, where $P_{0,G}\underline{c} = \underline{c}$. Clearly, this implies that $M_{t,k} D_k^{-1} e_{\Omega_K} = M^*_{\beta^G} D_k^{-1} \underline{c}$. By multiplying both sides by D_t, we deduce that $M'_{t,k} e_{\Omega_K} = (M')^*_{\beta^G} \underline{c}$. Hence, (M', β^G) affords a trivial positive equivariant signing, where the signing is given by $\epsilon^G(\Omega_K) = \epsilon(K)$.

Part 2 $\Longrightarrow$ part 1. Let ϵ^G be the trivial signing for (M', β^G). Lift this signing to a of (W, β) by $\epsilon(K) = \epsilon^G(\Omega_K)$.

Let $K \in \sim \beta$. By the Minkowski-Farkas Lemma, it suffices to show that for every $y \in \mathbb{R}$, a vector of real numbers, such that $y^T W^*_\beta \geq 0$, then $y^T W \frac{\widetilde{e_{\Omega_K}}}{|\Omega_K|} \geq 0$.

So, assume that $y^T W^*_\beta \geq 0$. Consider,

$$\begin{aligned} 0 &\leq y^T W^*_\beta \\ &= y^T \rho_t(g)^T \rho_t(g) W^*_\beta \\ &= (\rho_t(g)y)^T W^*_\beta \rho_k(g) \\ &= ((\rho_t(g)y)^T W^*_\beta)\rho_k(g), \end{aligned}$$

hence, $0 \leq (\rho_t(g)y)^T W^*_\beta$ since $\rho_k(g)$ is a permutation action. Therefore, it follows that $\underline{y}^T W^*_\beta \geq 0$ where:

$$\begin{aligned} \underline{y} &= P_{0,G} y \\ &= \sum_{\Omega_T \in (C_t(X))_0} \frac{(\sum_{T' \in \Omega_T} y_{T'})}{|\Omega_T|} \widetilde{e_{\Omega_T}}. \end{aligned}$$

Clearly, $P_{0,t,G}\underline{y} = \underline{y}$. Hence, $0 \leq \underline{y}^T W^*_\beta = \underline{y}^T P_{0,t,G} W^*_\beta$. Thus, we can conclude $0 \leq (y')^T (M')^*_\beta$, where $y'_{\Omega_T} = \underline{y}_T$.

By assumption, $M' e_{\Omega_K} \in C_+((M')^*_\beta)$. Hence, it follows by the Minkowski-Farkas Lemma that $(y')^T (M'_{t,k} e_{\Omega_K}) \geq 0$. We can lift this equation to $C_k(X)$ as $\underline{y}^T W \frac{e_{\widetilde{\Omega_K}}}{|\Omega_K|} \geq 0$.

Consider,

$$\begin{aligned} 0 &\leq \underline{y}^T W \frac{\widehat{e_{\Omega_K}}}{|\Omega_K|} \\ &= (P_{0,t,G} y)^T W \frac{\widehat{e_{\Omega_K}}}{|\Omega_K|} \\ &= y^T P_{0,t,G} W \frac{\widehat{e_{\Omega_K}}}{|\Omega_K|} \\ &= y^T W (P_{0,k,G} \frac{\widehat{e_{\Omega_K}}}{|\Omega_K|}) \\ &= y^T W \frac{\widehat{e_{\Omega_K}}}{|\Omega_K|}, \end{aligned}$$

hence, by the Minkowski-Farkas Lemma, it follows that $W\frac{\widehat{e_{\Omega_K}}}{|\Omega_K|} \in C_+(W_\beta^*)$. The conclusion follows. □

Definition 4.4.4. *Sometimes a positive equivariant G-signing for (M, β) is also a trivial positive equivariant signing for (M, β). When this happens, we will call the signing a* "trivial positive equivariant G-signing" *for (M, β).*

In the next section, we will show examples of G-trivially positive equivariant signings where G is nontrivial.

We close this section with an algorithmic criterion that helps determine when a pair (M, β) affords a trivial positive equivariant signing.

Proposition 4.4.5. (Reduced Row Echelon Property). *Let M be an $n \times m$ matrix and β a subset of columns that is linearly independent and generate the column space of M. Let $N = [M_\beta, M_{\sim\beta}]$ be a reordering of the columns of M such that the columns in β are listed first. Assume that N has Reduced Row Echelon Form given by:*

$$\begin{bmatrix} & r_1 \\ & r_2 \\ I & \vdots \\ & r_n \end{bmatrix}.$$

The following are equivalent,

1. *The pair (M, β) affords a trivial positive equivariant signing.*

2. **(Reduced Row Echelon Property)**. *The r_is in the row reduced echelon form of N are either nonpositive or nonnegative.*

Proof. We proceed to show the equivalence in two separate cases.

Part 1 $\Longrightarrow$ part 2. Let (M, β) afford a trivial positive equivariant signing ϵ. Let $M_\beta = [M_1, \ldots, M_n]$. Let $M_s \in \sim \beta$ correspond to the sth column in N. Then,

$$M_s \;=\; \sum_{i=1}^{n} \epsilon(M_i) c_{i,s} M_i,$$

where $c_{i,s} \geq 0$.

Note that $\epsilon(M_i)c_{i,s}$ is the (i, s) entry in the Row Reduced Echelon Form of N. Thus, the signing of (i, s) in the Row Reduced Echelon Form of N only depends on i. Hence, r_i is either nonnegative or nonpositive.

Part 2 $\Longrightarrow$ part 1. Assume that N has the Reduced Row Echelon Property. By reversing the argument above, we can conclude that for,

$$M_s \;=\; \sum_{i=1}^{n} c_{i,s} M_i,$$

the signing of $c_{i,s}$ only depends on i not s. From this, we can construct the desired signing ϵ. □

4.5 The Case G = Stab(Ω)

In this section, we consider actions given by permutation groups G that are stabilizer groups of partitions of $\{1, \ldots, v\}$.

Definition 4.5.1. *Let Ω be partition of $\{1, \ldots, v\}$ given by:*

$$\Omega \;=\; \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_d,$$

where $|\Omega_i| = v_i$ *and* $v_1 + \cdots + v_d = v$. *The* stabilizer group $Stab(\Omega) \subset S_v$ of Ω *is the set of all permutations that leave* Ω *invariant. That is,* $\sigma \in Stab(\Omega)$ *if and only if as sets we have* $\sigma \cdot \Omega_i = \Omega_i$ *for* $i = 1, \ldots, d$.

We consider a family of partitions $\{\Omega(v)\}_{v=1}^{\infty}$. For each member of the family, we consider the action of the group $G_v = Stab(\Omega(v))$ on the k-subsets and t-subsets of $\{1, \ldots, v\}$. We also consider a family of sets of k-subsets $\{\beta_{t,k}(v)\}_{v=1}^{\infty}$, and we study the following questions:

1. How can we show $\beta_{t,k}(v)$ is a (t,k)-basis for $W_{t,k}(v)$?
2. How can we show $\beta_{t,k}(v)^{G_v}$ is a (t,k)-basis for $M'_{t,k}(v)$? Where $\beta_{t,k}^{G_v}$ are the k-subsets' orbits in $\beta_{t,k}$ under the action of G_v.
3. How can we find a trivial positive equivariant signing for $(\beta_{t,k}(v), W_{t,k}(v))$?
4. How can we find a trivial positive equivariant signing for $(\beta_{t,k}(v)^{G_v}, M'_{t,k}(v))$?

We provide a partial answer to these questions.

We give examples of families $\{\Omega(v)\}_{v=1}^{\infty}$ for which there exist $\{\beta_{t,k}(v)\}_{v=0}^{\infty}$ that are (t,k)-basis of $W_{t,k}(v)$, and admit a trivial positive equivariant signing when $(t,k) = (1,2), (2,3), (3,4), (4,5)$. We conjecture the existence of trivial positive equivariant signings for these examples.

We start with a study of the spaces $(C_k(X))_0$ when $G = Stab(\Omega(v))$. We assume for now that v is fixed.

Proposition 4.5.2. *The orbits under the action of* $G = Stab(\Omega)$ *on the* k*-subsets are in one to one correspondence with the set* $\mathbb{H}^{\Omega}(k)$ *defined as:*

$$\mathbb{H}^{\Omega}(k) \;=\; \{[x_1, \ldots, x_d] \mid x_1 + \cdots x_d = k \text{ and } 0 \leq x_i \leq v_i\}.$$

Proof. Clearly, for every $\Omega_K \in (C_k(X))_0$, one can construct a partition $[x_1, \ldots, x_d] \in \mathbb{H}^{\Omega}(k)$. Namely, the parition where $x_i = |K \cap \Omega_i|$.

It suffices to show,

1. If $K' \in \Omega_K$, then K' induces the same partition in $\mathbb{H}^{\Omega}(k)$ as K.

2. If Ω_K and $\Omega_{K'}$ induce the same partition in $\mathbb{H}^{\Omega}(k)$, then $\Omega_K = \Omega_{K'}$.

Clealry, $G \simeq S_{v_1} \times \cdots \times S_{v_d}$ where S_{v_i} acts on Ω_i as the Symmetric Group. Note that S_{v_i} acts transitively on $\binom{\Omega_i}{x_i}$. Hence, if $|K \cap \Omega_i| = |K' \cap \Omega_i|$, then one can find a $\sigma_i \in S_{v_i}$ such that $\sigma_i(K \cap \Omega_i) = K' \cap \Omega_i$.

Let $K' \in \Omega_K$. Clearly, there is $\sigma = (\sigma_1, \ldots, \sigma_d) \in Stab(\Omega)$ such that $\sigma(K) = K'$. Thus, $|K' \cap \Omega_i| = |\sigma_i(K \cap \Omega_i)| = |K \cap \Omega_i|$. Therefore, K' induces the same partition as K.

If K and K' induce the same partition then $|K \cap \Omega_i| = |K' \cap \Omega_i|$. Thus, one can construct a $\sigma = (\sigma_1, \ldots, \sigma_d)$ where $\sigma_i(K \cap \Omega_i) = K' \cap \Omega_i$. Clearly, $\sigma(K) = K'$. Hence, $\sigma \in Stab(\Omega)$. Therefore, $\Omega_K = \Omega'_K$. □

Definition 4.5.3. *Let K be k-subset, and $\Omega = \Omega_1 \cup \cdots \cup \Omega_d$ a partition of $\{1, \ldots, v\}$. We will denote the vector $[|K \cap \Omega_1|, \ldots, |K \cap \Omega_d|]$ by $[|\mathrm{K} \cap \Omega|]$. We will define $\omega = [|\Omega \cap \Omega|]$ as the vector $[v_1, \ldots, v_d]$ where $v_i = |\Omega_i|$.*

Proposition 4.5.4. *Let $t < k \leq v - k$ and $G = Stab(\Omega)$. Let $\omega = [|\Omega|]$. Choose a k-subset K, and a t-subset T. Define $\phi = [|K \cap \Omega|]$ and $\psi = [|T \cap \Omega|]$. Then,*

1. *The sizes of the orbits Ω_K, Ω_T are given by:*

$$\begin{aligned} |\Omega_K| &= \binom{\omega}{\phi}, \\ |\Omega_T| &= \binom{\omega}{\psi}. \end{aligned}$$

2. *The (Ω_T, Ω_K) entry of $M'_{t,k}$ is given by:*

$$M'_{t,k}(\Omega_T, \Omega_K) = \binom{\phi}{\psi},$$

where,

$$\binom{\phi}{\psi} = \Pi_{i=1}^{d} \binom{\phi_i}{\psi_i}.$$

3. The (Ω_T, Ω_K) entry of $M_{t,k}$ is given by:

$$M_{t,k}(\Omega_T, \Omega_K) \;=\; \binom{\omega - \psi}{\phi - \psi},$$

where,

$$\binom{\omega - \psi}{\phi - \psi} \;=\; \Pi_{i=1}^{d} \binom{\omega_i - \psi_i}{\phi_i - \psi_i}.$$

Proof. Part 1 follows from the decomposition of $G \simeq S_{v_1} \times \cdots \times S_{v_d}$.

We show part 2. Let $\phi = [\phi_1, \ldots, \phi_d] = [|K \cap \Omega|]$ and $\psi = [\psi_1, \ldots, \psi_d] = [|T \cap \Omega|]$. Define $K_i = K \cap \Omega_i$ and $T_i = T \cap \Omega_i$. We wish to find all t-subsets $T' \in \Omega_T$ for which $T' \subset K$. Clearly, any $T' \in \Omega_T$ has decomposition $T' = T'_1 \cup \cdots \cup T'_d$ where $T'_i = T' \cap \Omega_i$. The condition that $T' \subset K$ is warranted exactly when $T'_i \subset K_i$ for $i = 1, \ldots, d$. Thus, we wish to find all subsets T'_i of K_i that have size ψ_i. Clearly, there are $\binom{\phi_i}{\psi_i}$ choices for T'_i. Hence, there are $\Pi_{s=0}\binom{\phi_s}{\psi_s} = \binom{\phi}{\psi}$ choices for $T' \in \Omega_T$ that satisfy $T' \subset K$. Therefore, $M'_{t,k}(\psi, \phi) = \binom{\phi}{\psi}$.

Part 3 uses a similar argument. □

Now, we consider a family of partitions $\{\Omega(v)\}_{v=1}^{\infty}$, where each $\Omega(v)$ is a partition of $\{1, \ldots, v\}$.

Definition 4.5.5. *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be a family of partitions where $f_i(v) = |\Omega_i(v)|$ is monotonically increasing with respect to v. That is, if $v \leq v'$, then $f_i(v) \leq f_i(v')$. We will call $\{\Omega(v)\}_{v=1}^{\infty}$ a* "monotone family." *We will denote $[f_1(v), \ldots, f_d(v)]$ by $\omega(\mathrm{v})$, the* numeric partition of v generated by $\Omega(v)$.

Proposition 4.5.6. *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be monotone family. Then,*

1. *If $v \leq v'$, then $\omega(v) \leq \omega(v')$.*

2. *If $\omega(v) \leq \omega(v')$, then $v \leq v'$.*

Proof. Part 1 follows by the definition of a monotone family.

We show part 2. Suppose $\omega(v) \leq \omega(v')$. If $v' < v$, then by part 1 $\omega(v') \leq \omega(v)$. Hence, $\omega(v) = \omega(v')$ and this forces $v = v'$. This is a contradiction. □

Definition 4.5.7. *Given a monotone family* $\{\Omega(v)\}_{v=1}^{\infty}$*, an* "inclusion map" ι *is defined as a family of inclusion maps* $\iota_{v,v'} : \Omega(v) \hookrightarrow \Omega(v')$*, where* $v \leq v'$*, with the property that for all* $i = 1, \ldots, d$*:*

$$\iota_{v,v'} : \Omega_i(v) \hookrightarrow \Omega_i(v'),$$

that is, $i_{v,v'}$ *injects* $\Omega_i(v)$ *into* $\Omega_i(v')$*. We will drop the subscripts* v, v' *in the notation of* $\iota_{v,v'}$ *unless it brings ambiguity.*

In principle, for fixed $v \leq v'$, there are $\binom{\omega(v')}{\omega(v)}$ possible inclusion maps. Since $\Omega(v)$ is a Monotone Family, $\omega(v) \leq \omega(v')$. Hence, there is at least $1 \leq \binom{\omega(v')}{\omega(v)}$ possible inclusion map from $\Omega(v)$ into $\Omega(v')$. However, depending on the structure of Ω, this inclusion map may not be unique.

Proposition 4.5.8. *Let* $\{\Omega(v)\}_{v=1}^{\infty}$ *be a monotone family, and* ι *an inclusion map for* $\{\Omega(v)\}_{v=1}^{\infty}$*. Denote by* $\binom{v}{s}$ *the set of all* s*-subsets of* $\{1, \ldots, v\}$*. Then,*

1. *Let* $s \leq v - s \leq v' - s$ *and* $v \leq v'$*, then* ι *induces an injection from the* s*-subsets of* $\{1, \ldots, v\}$ *to the* s*-subsets of* $\{1, \ldots, v'\}$*. That is,* $\iota : \binom{v}{s} \hookrightarrow \binom{v'}{s}$*.*

2. *Let* $s \leq v - s \leq v' - s$ *and* $v \leq v'$*, then* ι *induces an injection* $\iota : \mathbb{H}^{\Omega(v)}(s) \hookrightarrow \mathbb{H}^{\Omega(v')}(s)$*. More precisely, given* $\phi = [\phi_1, \ldots, \phi_d] \in \mathbb{H}^{\Omega(v)}(s)$*,* $\iota([\phi_1, \ldots, \phi_d]) = [\phi_1, \ldots, \phi_d]$ *is the desired injection.*

3. *Let* $v \leq v'$*, then* ι *induces an injection* $\iota : Stab(\Omega(v)) \hookrightarrow Stab(\Omega(v'))$ *given by* $\sigma \to \iota(\sigma)$*, where* $\iota(\sigma)$ *is defined as:*

$$\iota(\sigma)(x) \quad = \quad \begin{cases} \iota_{v,v'} \circ \sigma \circ \iota_{v,v'}^{-1}(x) & \text{if } x \in \iota(\Omega(v)), \\ x & \text{otherwise.} \end{cases}$$

4. *Let* $v \leq v'$ *and* $S \in \binom{v'}{s}$*. If* $[|S \cap \Omega(v')|] \leq \omega(v)$*, then there is a* $\sigma \in Stab(\Omega(v'))$ *such that* $\sigma(S) \in \iota(\binom{v}{s})$*.*

5. *Let* $v \leq v'$*,* $r \leq s \leq v - s \leq v' - s$*,* $\sigma \in Stab(\Omega(v))$ *and* $S \in \binom{v}{s}$*. Then,*

(a) The map $\iota_{v,v'}$ satisfies $\iota_{v,v'}(\sigma \cdot S) = \iota_{v,v'}(\sigma) \cdot \iota_{v,v'}(S)$.

(b) The map $\iota_{v,v'}$ satisfies $\iota_{v,v'}(W_{r,s}(v)e_S) = W_{r,s}(v')e_{\iota_{v,v'}(S)}$.

(c) Let $\phi = [|S \cap \Omega(v)|] \in \mathbb{H}^{\Omega(v)}(s)$. Then,

$$\iota_{v,v'}(M'_{r,s}(v)e_\phi) = M'_{r,s}(v')e_{\iota_{v,v'}(\phi)}.$$

Proof. Since ι is indeed an injection, part 1 is clear.

We show part 2. Consider $\phi \in \mathbb{H}^{\Omega(v)}(s)$. Choose $S \in \phi$. Clearly, $[|S \cap \Omega(v)|] = \phi$. Note that $|S \cap \Omega_i(v)| = |\iota_{v,v'}(S) \cap \Omega_i(v')|$, since $\iota_{v,v'}$ is an injection. Define $\iota_{v,v'} : \mathbb{H}^{\Omega(v)}(s) \hookrightarrow \mathbb{H}^{\Omega(v')}(s)$ by $\iota_{v,v'}(\phi) = [|\iota_{v,v'}(S) \cap \Omega(v')|]$. Clearly, $\iota_{v,v'}$ is well defined, and $\iota_{v,v'}(\phi) = \phi$ as numeric partitions of s. It suffices to show that $\iota_{v,v'}$ is injective. Suppose that,

$$\begin{aligned} [|\iota_{v,v'}(S) \cap \Omega(v')|] &= \iota_{v,v'}(\phi) \\ &= \iota_{v,v'}(\phi') \\ &= [|\iota_{v,v'}(S') \cap \Omega(v')|], \end{aligned}$$

where $S \in \phi$ and $S' \in \phi'$. Note that,

$$\begin{aligned} |S \cap \Omega_i(v)| &= |\iota_{v,v'}(S) \cap \Omega_i(v')| \\ &= |\iota_{v,v'}(S') \cap \Omega_i(v')| \\ &= |S' \cap \Omega_i(v)|. \end{aligned}$$

Hence, S and S' belong to the same orbit in $\mathbb{H}^{\Omega(v)}(s)$. That is, $\phi = \phi'$. The result follows.

We show part 3. Note that, we can partition $\Omega_i(v')$ into $\iota(\Omega_i(v)) \cup \Omega_i(v')'$. The injection that $\iota : Stab(\Omega(v)) \hookrightarrow Stab(\Omega(v'))$ induces essentially maps $\sigma = (\sigma_1, \ldots, \sigma_d) \in Stab(\omega(v)) = S_{\Omega_1(v)} \times \cdots \times S_{\Omega_d(v)}$ to a $\iota(\sigma) = (\iota(\sigma_1), \ldots, \iota(\sigma_d))$, where $\iota(\sigma_i)$ acts op $\Omega_i(v')$ via pullback on the image $\iota(\Omega_i(v))$, and as identity on the remaing part $\Omega_i(v')'$. Clearly, this is an injection of groups. Hence, part 3 follows.

We show part 4. By assumption, $S_i = S \cap \Omega_i(v')$ has size $\leq |\Omega_i(v)|$. Let $s_i = |S_i|$. Since $S_{\Omega_i(v')}$ acts transitively on the s_i-subsets of $\Omega_i(v')$, we can find a $\sigma_i \in S_{\Omega_i(v')}$ that maps S_i to a subset of $\iota(\Omega_i(v))$. This is possible since $s_i \leq |\Omega_i(v)|$. Hence, for each $i = 1, \ldots, d$, we can find $\sigma_i \in S_{\Omega_i(v')}$ such that $\sigma_i(S_i) \subset \iota(\Omega_i(v))$. Clearly, $\sigma = (\sigma_1, \ldots, \sigma_d) \in Stab(\Omega(v'))$ is a map such that $\sigma(S) \in \iota(\binom{v}{s})$.

We show part 5. To show part a, note that $\iota_{v,v'}(S) \subset \iota_{v,v'}(\Omega(v))$. Hence, by definition of $\iota_{v,v'}(\sigma)$,

$$\begin{aligned} \iota_{v,v'}(\sigma) \cdot \iota_{v,v'}(S) &= \iota_{v,v} \circ \sigma \circ \iota_{v,v'}^{-1}(\iota_{v,v'}(S)) \\ &= \iota_{v,v'}(\sigma(S)) \\ &= \iota_{v,v'}(\sigma \cdot S). \end{aligned}$$

Hence, part a follows.

Part b follows because $\iota_{v,v'}$ preserves inclusions since it is an injection. That is, if $R \subset S$, then $\iota_{v,v'}(R) \subset \iota_{v,v'}(S)$.

For part c, it suffices to show:

$$\iota_{v,v'}(W_{r,s}(v)\widetilde{e_{\Omega_S}}) = W_{r,s}(v')\widetilde{e_{\iota_{v,v'}(S)}},$$

where $\widetilde{e_{\Omega_S}} = \sum_{S' \in \Omega_S} e_{S'}$. Clearly, this follows by part b. □

Proposition 4.5.8 shows that we can think of the spaces $\mathbb{H}^{\Omega(v)}(s)$ as an ascending chain of vector spaces or $\mathbb{Z}$-modules. The next proposition shows that this chain stabilizes.

Proposition 4.5.9. *Let $v_i(\infty) = \max_v f_i(v)$, where we allow $v_i(\infty) = \infty$. Define $\gamma_i(s) = \min(v_i(\infty), s)$, where we assume $\infty \geq s$ for all s. Let $v_i^\infty(s)$ be defined as the first value of v for which $f_i(v) = \gamma_i(s)$. Define:*

$$v_0(s) = \max_{i=1}^{d} v_i^\infty(s).$$

Then,

1. *If* $v_0(s) \leq v$, *then* $\iota : \mathbb{H}^{\Omega(v_0(s))}(s) \hookrightarrow \mathbb{H}^{\Omega(v)}(s)$ *is onto.*

2. *If* $v < v_0(s)$, *then* $\iota : \mathbb{H}^{\Omega(v)}(s) \hookrightarrow \mathbb{H}^{\Omega(v_0(s))}(s)$ *is not onto.*

Proof. We show part 1, Let $S \in \binom{v}{s}$ be an s-subset, and $\phi = [|S \cap \Omega(v)|]$. Note that $\phi_i = |S \cap \Omega_i(v)| \leq f_i(v)$ and $\phi_i = |S \cap \Omega_i(v)| \leq s$. Consider,

$$\begin{aligned} \phi_i &\leq \min(f_i(v), s) \\ &\leq \min(f_i(v_i(\infty)), s) \\ &= f_i(v_i^{\infty}(s)) \\ &\leq f_i(v_0(s)), \end{aligned}$$

hence, $\phi \leq \omega(v_0(s))$. By proposition 4.5.8 part 4, it follows that there is $\sigma \in Stab(\Omega(v))$ such that $\sigma(S) \in \iota(\binom{v_0(s)}{s})$. Thus, ϕ has a preimage under ι. Because ϕ was arbitrary, it follows that ι is onto.

We show part 2. It suffices to construct a $\phi \in \mathbb{H}^{\Omega(v_0(s))}(s)$ that does not have a preimage under ι. Since $v < v_0(s)$, it must be the case that for some i_0, $\min(f_{i_0}(v), s) < \gamma_{i_0}(s)$. If this is not possible, then $v_i^{\infty}(s) \leq v$ for all i and this forces $v_0(s) \leq v$. Hence, we assume that there is an i_0 is such that $\min(f_{i_0}(v), s) < \gamma_{i_0}(s)$. Consider,

$$\begin{aligned} \min(f_{i_0}(v), s) &< \gamma_{i_0}(s) \\ &= \min(f_{i_0}(v_{i_0}^{\infty}(s)), s) \\ &= \min(f_{i_0}(v_0(s)), s), \end{aligned}$$

hence, there is an i_0 such that $\min(f_{i_0}(v), s) < \min(f_{i_0}(v_0(s)), s)$.

Consider any partition $\phi \in \mathbb{H}^{\Omega(v_0(s))}(s)$ for which $\phi_{i_0} = \min(f_{i_0}(v_0(s)), s)$. Clearly, this ϕ will not have a preimage under ι. □

The quantities $v_0(s)$ will be important later. The next proposition shows that $v_0(s)$ is a strictly monotonic function of s.

Proposition 4.5.10. *If* $s < s'$, *then* $v_0(s) < v_0(s')$.

Proof. Let $s < s'$. Using the monotonicity of $\{\Omega(v)\}_{v=1}^{\infty}$, we can show that there is an i for which $\gamma_i(s) = \min(v_i(\infty), s) < \min(v_i(\infty), s') = \gamma_i(s')$. Since the $f_i(v)$s are monotonically increasing, it follows that $v_i^{\infty}(s) < v_i^{\infty}(s')$ for some i. Thus, we conclude $v_0(s) < v_0(s')$. □

We introduce a few definitions that will be used in the reduction results of the next subsection.

Definition 4.5.11. *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be a monotone family, and ι an inclusion map for $\{\Omega(v)\}_{v=1}^{\infty}$. A* "compatible set for $\{\Omega\}_{v=1}^{\infty}$" *is a family of sets of k-subsets $\{\beta_{t,k}(v)\}_{v=1}^{\infty}$ such that,*

1. *The set $\beta_{t,k}(v) \subset \binom{v}{k}$, where we use $\binom{v}{k}$ to denote the set of all k-subsets.*
2. *The size of $\beta_{t,k}(v)$ is $\binom{v}{t}$.*
3. *The set $\beta_{t,k}(v)$ is invariant under the action of $Stab(\Omega(v))$.*
4. *If $v \leq v'$, then,*

$$\iota(\beta_{t,k}(v)) \quad \subset \quad \beta_{t,k}(v').$$

Similarly, we can introduce the notion of equivariant compatible sets.

Definition 4.5.12. *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be a monotone family, and ι an inclusion map for $\Omega(v)$. An* "equivariant compatible set for $\{\Omega(v)\}_{v=1}^{\infty}$" *is a family of sets of k-subsets' orbits $\{\beta_{t,k}^{G}(v)\}_{v=1}^{\infty}$ under the action of $G = Stab(\Omega(v))$ such that:*

1. *The set $\beta_{t,k}^{G}(v) \subset \mathbb{H}^{\Omega(v)}(k)$.*
2. *The size of $\beta_{t,k}^{G}(v)$ is $r_G(t)$.*
3. *If $v \leq v'$, then,*

$$\iota(\beta_{t,k}^{G}(v)) \quad \subset \quad \beta_{t,k}^{G}(v').$$

Definition 4.5.13. *Let ϵ be a trivial positive equivariant signing for (M, β), where $M : \binom{v}{k} \to \binom{v}{t}$ is a G-map. We say that ϵ is* G-invariant *if and only if $\epsilon(\sigma \cdot K) = \epsilon(K)$ for all $\sigma \in G$ and all $K \in \beta$.*

4.5.1 Reduction Results

In this subsection, we consider a monotone family $\{\Omega(v)\}_{v=1}^{\infty}$ with inclusion map ι, a compatible set $\{\beta_{t,k}(v)\}_{v=1}^{\infty}$, and an equivariant compatible set $\{\beta_{t,k}^{G}(v)\}_{v=1}^{\infty}$ for $\{\Omega(v)\}_{v=1}^{\infty}$ such that the columns of $\beta_{t,k}(v)$ in $W_{t,k}(v)$ are $\mathbb{Q}$-linearly independent and the columns of $\beta_{t,k}^{G}(v)$ in $M'_{t,k}(v)$ are $\mathbb{Q}$-linearly independent. We show,

1. The set $\beta_{t,k}(v)$ is a (t,k)-basis of $W_{t,k}(v)$ for $v \geq k+t+1$ if and only if the set $\beta_{t,k}(v)$ is a (t,k)-basis of $W_{t,k}(v)$ for $v = v_0(k)$.

2. The pair $(\beta_{t,k}(v), W_{t,k}(v))$ admits a trivial positive equivariant signing that is $G_v = Stab(\Omega(v))$-invariant for $v \geq k+t+1$ if and only if the pair $(\beta_{t,k}(v), W_{t,k}(v))$ admits a trivial positive equivariant signing that is $G_v = Stab(\Omega(v))$-invariant for $v = v_0(k)$.

3. The set $\beta_{t,k}^{G}(v)$ is a (t,k)-basis of $M'_{t,k}(v)$ for $v \geq k+t+1$ if and only if the set $\beta_{t,k}^{G}(v)$ is a (t,k)-basis of $M'_{t,k}(v)$ for $v = v_0(k)$.

4. The pair $(\beta_{t,k}^{G}(v), M'_{t,k}(v))$ admits a trivial positive equivariant signing for $v \geq k+t+1$ if and only if the pair $(\beta_{t,k}^{G}(v), M'_{t,k}(v))$ admits a trivial positive equivariant signing for $v = v_0(k)$.

Proposition 4.5.14. (First Reduction). *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be a Monotone Family, and ι an inclusion map for $\{\Omega(v)\}_{v=1}^{\infty}$. Assume that $\{\beta_{t,k}(v)\}_{v=1}^{\infty}$ is Compatible Set for $\{\Omega(v)\}_{v=1}^{\infty}$ such that the corresponding columns of $\beta_{t,k}(v)$ in $W_{t,k}(v)$ are $\mathbb{Q}$-linearly independent. The following are equivalent,*

1. *The set $\beta_{t,k}(v)$ is a (t,k)-basis of $W_{t,k}(v)$ for $v \geq k+t+1$.*

2. *The set $\beta_{t,k}(v_0)$ is a (t,k)-basis of $W_{t,k}(v)$ for $v = v_0(k)$.*

Proof. It suffices to show part 2 implies part 1. We proceed to show this by considering two separate cases.

Case $\mathbf{v_0 \leq v}$. Let $K \in \binom{v}{k}$ be a k-subset. By using the same argument of proposition 4.5.9, we can show that there is $\sigma \in Stab(\Omega(v))$ such that $\sigma(K) \in \iota(\Omega(v_0))$. Hence, $\sigma(K) = \iota(K')$ for some $K' \in \binom{v_0}{k}$. Therefore, $K = \sigma^{-1} \circ \iota(K')$ for some $K' \in \binom{v_0}{k}$.

Since $\beta_{t,k}(v_0)$ is a (t,k)-basis for $W_{t,k}(v_0)$, there is an integral vector c with support in $\beta_{t,k}(v_0)$ such that $W_{t,k}(v_0)e_{K'} = W_{t,k}(v_0)c$. By applying $\iota_{v_0,v}$ to this equation, we deduce,

$$\begin{aligned} W_{t,k}(v)e_{\iota(K')} &= \iota(W_{t,k}(v_0)e_{K'}) \\ &= \iota(W_{t,k}(v_0)c) \\ &= W_{t,k}(v)c', \end{aligned}$$

where c' is an integral vector with support in $\iota(\beta_{t,k}(v_0)) \subset \beta_{t,k}(v)$. By applying σ^{-1} to both sides of the above equation, we can deduce,

$$\begin{aligned} W_{t,k}(v)e_K &= W_{t,k}(v)e_{\sigma^{-1}(\iota(K'))} \\ &= \sigma^{-1}(W_{t,k}(v)e_{\iota(K')}) \\ &= \sigma^{-1}(W_{t,k}(v)c') \\ &= W_{t,k}(v)c'', \end{aligned}$$

where c'' is an integral vector with support in $\sigma^{-1}(\iota(\beta_{t,k}(v_0))) \subset \beta_{t,k}(v)$. Hence, the result follows.

Case $\mathbf{v < v_0}$. Let $K \in \binom{v}{k}$ be a k-subset. Clearly, because the corresponding columns of $\beta_{t,k}(v)$ in $W_{t,k}(v)$ are $\mathbb{Q}$-linearly independent, there is a rational vector c with support in $\beta_{t,k}(v)$ such that $W_{t,k}(v)e_K = W_{t,k}(v)c$. Hence, by applying ι_{v,v_0} we get that $W_{t,k}(v_0)e_{\iota(K)} = W_{t,k}(v_0)c'$ where c' is a rational vector with support $\iota(\beta_{v,k}(v)) \subset \beta_{t,k}(v_0)$. Since $\beta_{t,k}(v_0)$ is a (t,k)-basis, it follows that c' is integral and this forces c to be integral as well. $\square$

Proposition 4.5.15. (Second Reduction). *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be a Monotone Family and ι an inclusion map for $\{\Omega(v)\}_{v=1}^{\infty}$. Assume that $\beta_{t,k}(v)$ is Compatible Set for $\{\Omega(v)\}_{v=1}^{\infty}$ such that the corresponding columns of $\beta_{t,k}(v)$ in $W_{t,k}(v)$ are $\mathbb{Q}$-linearly independent. The following are equivalent,*

1. *The pair $(W_{t,k}(v), \beta_{t,k}(v))$ affords a trivial positive equivariant signing that is $G = Stab(\Omega(v))$-invariant for $v \geq k + t + 1$.*

2. *The pair $(W_{t,k}(v_0), \beta_{t,k}(v))$ affords a trivial positive equivariant signing that is $G = Stab(\Omega(v))$-invariant. for $v = v_0(k)$.*

Proof. It suffices to show part 2 implies part 1. Let $v_0 = v_0(k)$. Let ϵ_{v_0} be a trivial positive equivariant signing for $(W_{t,k}(v_0), \beta_{t,k}(v_0))$ that is $G_{v_0} = Stab(\Omega(v_0))$-invariant. We will extend this signing to a signing ϵ_v for $(W_{t,k}(v), \beta_{t,k}(v))$ that is $G_v = Stab(\Omega(v))$-invariant by considering two separate cases.

Case $\mathbf{v_0 \leq v}$. Let $K \in \binom{v}{k}$ be a k-subset. By using a similar argument as in proposition 4.5.9, we can show that there is $\sigma \in Stab(\Omega(v))$ such that $\sigma(K) \in \iota(\Omega(v_0))$. Hence, $\sigma(K) = \iota(K')$ for some $K' \in \binom{v_0}{k}$. Define $\epsilon_v(K) = \epsilon_{v_0}(K')$. Clearly, ϵ_v is well defined since ϵ_{v_0} is G_{v_0}-invariant. Also, by construction, ϵ_v is G_v-invariant, and $\epsilon_v(\iota(K')) = \epsilon_{v_0}(K')$.

We show that ϵ_v is a trivial positive equivariant signing. Consider $K \in\sim \beta_{t,k}(v)$. Choose $\sigma \in Stab(\Omega(v))$ such that $\sigma(K) = \iota(K')$ where $K' \in \binom{v_0}{k}$. By assumption, there is a rational c with support $\beta_{t,k}(v_0)$ and signing given by ϵ_{v_0} such that $W_{t,k}(v_0)e_{K'} = W_{t,k}(v_0)c$. By applying ι to both sides of this equation, we deduce,

$$\begin{aligned} W_{t,k}(v)e_{\sigma(K)} &= W_{t,k}(v)e_{\iota(K')} \\ &= W_{t,k}(v)c', \end{aligned}$$

where c' is a rational vector with support $\iota(\beta_{t,k}(v_0)) \subset \beta_{t,k}(v)$. Note that the signing of c' is given by ϵ_v since: if K' has sign given by $\epsilon_{v_0}(K')$ in the summation expansion of c, then $\iota(K')$ has sign given by $\epsilon_{v_0}(K') = \epsilon_v(\iota(K'))$ in the summation expansion of c'.

Because ϵ_v is G_v-invariant, by applying σ^{-1} to both sides of the above equation, we deduce $W_{t,k}(v)e_K = W_{t,k}c''$ where c'' has support $\beta_{t,k}(v)$ and signing given by ϵ_v. Hence, ϵ_v is indeed a trivial positive equivariant signing.

Case $\mathbf{v < v_0}$. It suffices to construct a signing for $(W_{t,k}(v), \beta_{t,k}(v))$. Let $K \in \binom{v}{k}$, consider the signing given by $\epsilon_v(K) = \epsilon_{v_0}(\iota(K))$. Clearly, this signing is well defined. We show that ϵ_v is G_v-invariant. Consider,

$$\begin{aligned}
\epsilon_v(\sigma \cdot K) &= \epsilon_{v_0}(\iota(\sigma \cdot K)) \\
&= \epsilon_{v_0}(\iota(\sigma) \cdot \iota(K)) \\
&= \epsilon_{v_0}(\iota(K)) \\
&= \epsilon_v(K).
\end{aligned}$$

where, we have used the fact that $\iota(Stab(\Omega(v))) \subset Stab(\Omega(v_0))$.

We show that ϵ_v is a trivial positive equivariant signing. Consider $K \in\sim \beta_{t,k}(v)$. Clearly, there is a rational c with support in $\beta_{t,k}(v)$ such that $W_{t,k}(v)e_K = W_{t,k}(v)c$. After applying ι to both sides of this equation, we deduce $W_{t,k}(v_0)e_{\iota(K)} = W_{t,k}(v_0)c'$ where c' has support in $\iota(\beta_{t,k}(v)) \subset \beta_{t,k}(v_0)$. Since ϵ_{v_0} is a trivial positive equivariant signing, it follows that c' has signing given by ϵ_{v_0}. Hence, c has signing given by $\epsilon_{v_0} \circ \iota = \epsilon_v$. □

Proposition 4.5.16. (Third Reduction). *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be a Monotone Family, and ι an inclusion map for $\{\Omega(v)\}_{v=1}^{\infty}$. Assume that $\beta_{t,k}^G(v)$ is an equivariant compatible set for $\{\Omega(v)\}_{v=1}^{\infty}$ such that the corresponding columns of $\beta_{t,k}^G(v)$ in $M'_{t,k}(v)$ are $\mathbb{Q}$-linearly independent. The following are equivalent,*

1. *The set $\beta_{t,k}^G(v)$ is a (t,k)-basis for $v \geq k+t+1$.*
2. *The set $\beta_{t,k}^G(v)$ is a (t,k)-basis for $v = v_0(k)$.*

Proof. It suffices to show part 2 implies part 1. We show this by considering two separate cases.

Case $\mathbf{v_0 \leq v}$. Note that $v_0(t) \leq v_0(k)$. Hence, by proposition 4.5.9, the spaces

$\mathbb{H}^{\Omega(v)}(k) = \mathbb{H}^{\Omega(v_0)}(k)$ and $\mathbb{H}^{\Omega(v)}(t) = \mathbb{H}^{\Omega(v_0)}(t)$. Thus, by proposition 4.5.4, $M'_{t,k}(v) = M'_{t,k}(v_0)$. Hence, the result follows.

Case $\mathbf{v} < \mathbf{v_0}$. Let $\phi \in \mathbb{H}^{\Omega(v)}(k)$. Clearly, since the corresponding columns of $\beta^G_{t,k}(v)$ in $M'_{t,k}(v)$ are $\mathbb{Q}$-linearly independent, there is a rational vector c with support in $\beta^G_{t,k}(v)$ such that $M_{t,k}(v)'\phi = M_{t,k}(v)'c$. Hence, by applying ι_{v,v_0}, we deduce that $M'_{t,k}(v_0)\iota(\phi) = M'_{t,k}(v_0)'c'$ where c' is a rational vector with support $\iota(\beta_{v,k}(v)^G) \subset \beta^G_{t,k}(v_0)$. Since $\beta_{t,k}(v_0)$ is a (t,k)-basis, it follows that c' is integral. Hence, c is integral as well. □

Proposition 4.5.17. (Fourth Reduction). *Let $\{\Omega(v)\}_{v=1}^{\infty}$ be a Monotone Family and ι an inclusion map for $\{\Omega(v)\}_{v=1}^{\infty}$. Assume that $\{\beta^G_{t,k}(v)\}_{v=1}^{\infty}$ is an equivariant compatible set for $\{\Omega(v)\}_{v=1}^{\infty}$ such that the corresponding columns of $\beta^G_{t,k}(v)$ in $M'_{t,k}(v)$ are $\mathbb{Q}$-linearly independent. The following are equivalent,*

1. *The pair $(M'_{t,k}(v), \beta^G_{t,k}(v))$ affords a trivial positive equivariant signing for $v \geq k+t+1$.*

2. *The pair $(M'_{t,k}(v), \beta^G_{t,k}(v))$ affords a trivial positive equivariant signing for $v = v_0(k)$.*

Proof. It suffices to show part 2 implies part 1. Let $v_0 = v_0(k)$, and let ϵ_{v_0} be a trivial positive equivariant signing for $(M'_{t,k}(v_0), \beta^G_{t,k}(v_0))$. Consider the following two cases.

Case $\mathbf{v_0} \leq \mathbf{v}$. Note that $v_0(t) \leq v_0(k)$. Hence, by proposition 4.5.9, the spaces $\mathbb{H}^{\Omega(v)}(k) = \mathbb{H}^{\Omega(v_0)}(k)$ and $\mathbb{H}^{\Omega(v)}(t) = \mathbb{H}^{\Omega(v_0)}(t)$. Thus, by proposition 4.5.4, $M'_{t,k}(v) = M'_{t,k}(v_0)$. Hence, the result follows.

Case $\mathbf{v} < \mathbf{v_0}$. It suffices to construct a signing ϵ_v for $(M'_{t,k}, \beta^G_{t,k}(v))$. Let $\phi \in \mathbb{H}^{\Omega(v)}(k)$. Consider the signing ϵ_v given by $\epsilon_v(\phi) = \epsilon_{v_0}(\iota(\phi))$. Clearly, this signing is well defined since it is just the restriction of ϵ_{v_0} to $\mathbb{H}^{\Omega(v)}(k)$.

We show that ϵ_v is a trivial positive equivariant signing. Consider $\phi \in\sim \beta^G_{t,k}(v)$. Clearly there is a rational c with support in $\beta^G_{t,k}(v)$ such that $M'_{t,k}(v)\phi = M'_{t,k}(v)c$. After applying ι to both sides, we deduce $M'_{t,k}(v_0)\iota(\phi) = M'_{t,k}(v_0)c'$ where c' has support in $\iota(\beta^G_{t,k}(v)) \subset \beta^G_{t,k}(v_0)$. Since ϵ_{v_0} is a trivial positive equivariant signing, it follows that c' has signing given by ϵ_{v_0}. Hence, c has signing given by $\epsilon_{v_0} \circ \iota = \epsilon_v$. □

4.5.2 Monotone Families $\{\Omega\}_{v=1}^{\infty}$ Induced by (t,k)-Bases

We provide examples of (t,k)-bases $\{\beta_{t,k}(v)\}_{v=1}^{\infty}$ which admit stabilizer groups of the form $Stab(\Omega(v))$.

Our first example is the Khosrovshahi-Ajoodani basis, which was introduced Ajoodani-Namini and Khosrovshahi in [1]. One defines this basis by introducing the concept of a "starting block."

Definition 4.5.18. *Let $K = \{b_1 < \cdots < b_k\}$ be a k-subset of $\{1,\ldots,v\}$. Let $t < k \leq v-k$. K is a "*starting (t,k)-block*" if and only if all the following inequalities hold,*

$$\begin{cases} b_l \leq v-k-t+2l-2 & 1 \leq l \leq t+1, \\ b_l \leq v-k+l & t+2 \leq l \leq k. \end{cases}$$

*We call K a "*nonstarting (t,k)-block*," if it is not a (t,k)-starting block.*

Definition 4.5.19. *The* Khosrovshahi-Ajoodani (K-Aj) (t,k)-basis *is defined to be the set of all nonstarting (t,k)-blocks.*

Proposition 4.5.20. *The Khosrovshahi-Ajoodani (t,k)-basis is indeed a (t,k)-basis for $W_{t,k}$.*

Our second example is the Bier-Frankl basis, which can be deduced indirectly to be a (t,k)-basis from the work of Bier in [3]. However, because this basis has not been shown to be a (t,k)-basis in the literature, we will provide a proof showing that it is a (t,k)-basis by using the K-Aj basis. For now, we will call the Bier-Frankl basis, the Bier-Frankl set.

One needs to introduce the concept of the Frankl rank to define the Bier-Frankl set.

Definition 4.5.21. *Let K be a k-subset in $\{1,\ldots,v\}$. The* Frankl-Graham density *of K is defined as:*

$$fgd(K) \;=\; \max_{s=1,\ldots,v}\{|[1,\ldots,s]\cap K| - |[1,\ldots,s]\cap([1,\ldots,k]\backslash K)|\}.$$

The Frankl rank of K *is given by* $r(K) = k - fgd(K)$.

A geometrical interpretation of the Frankl rank uses the mapping of a k-subset K to a walk $w(K)$ on the lattice $\mathbb{Z} \times \mathbb{Z}$. Given K, define the walk induced by K on $\mathbb{Z} \times \mathbb{Z}$, by starting from the origin $(0, 0)$ and ending in $(v - k, k)$ by steps of length 1 where: the ith step is to the right, if $i \notin K$; or, up, if $i \in K$. The Frankl rank can now be defined as $k - f$ where f is the y-intercept of the unique line with slope 1 that touches $w(K)$ from above.

Let us consider the following example. Let $K = \{1, 3, 4\} \subset \{1, \ldots, 7\}$. Figure 4.4 shows the graphical representation of the walk induced by K and the y-intercept of the unique line with slope 1 that touches $w(K)$ from above. For this example, the y-intercept is 2. Hence, $r(K) = 3 - 2 = 1$.

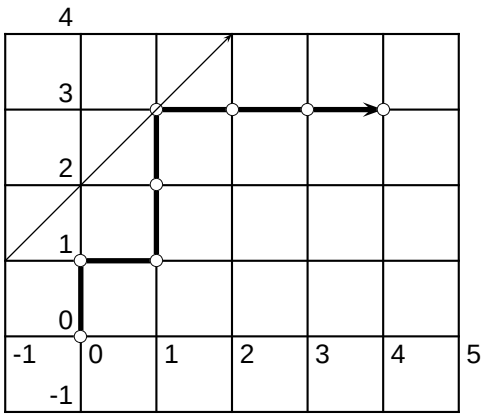

Figure 4.4. Calculating the Frankl rank for the 3-subset $\{1, 3, 4\} \subset \{1, \ldots, 7\}$.

One can also give an inequality definition of the Frankl rank.

Proposition 4.5.22. *Let* $K = \{a_1 < \cdots < a_k\}$ *be a* k*-subset in* $\{1, \ldots, v\}$. K *has Frankl rank* r *if and only if the following hold,*

1. *The following inequality holds,* $a_i + (k - r) \geq 2i$ *for* $i = 1, \ldots, k$.
2. *There is an* i_0 *such that* $a_{i_0} + (k - r) = 2i_0$.

Proof. Let $K = \{a_1 < \cdots < a_k\}$ be a k-subset. Let $f = fgd(K)$. Then, $y = x + f$ bounds $w(K)$ tightly from above. That is, $y(i) \geq w_i$, where (i, w_i) is a lattice point

on $w(K)$. Clearly, if $(i, w_i) \in w(K)$, then (i, w_i) is the end of the $i + w_i = s$th edge of $w(K)$ where the 1st edge starts at the origin. Also, if $i + w_i = s \in K$, then $s = a_{s_0}$ for some s_0. By construction, it is clear that s_0 must equal w_i. Hence, $i + w_i = a_{w_i} \in K$.

By choice of f,

1. The following inequality holds, $y(i) = i + f \geq w_i$. Thus, $a_{w_i} + f = w_i + i + f \geq 2w_i$. Hence, $a_s + f \geq 2s$.

2. There is an i_0 such that $y(i_0) = i_0 + f = w_{i_0}$. Thus, $a_{w_{i_0}} + f = w_{i_0} + i_0 + f = w_{i_0} + w_{i_0} = 2w_{i_0}$. Hence, there is an $s_0 = w_{i_0}$ such that $a_{s_0} + f = 2s_0$.

Since $f + r = k$, the result follows. □

Definition 4.5.23. *The* Bier-Frankl (B-F) (t, k)-set *is defined to be the set of all K-subsets with $0 \leq r(K) \leq t$.*

The next result shows that the K-Aj basis is equivalent to the B-F set.

Proposition 4.5.24. *Let $\beta_{t,k}$ be the K-Aj basis, and $\beta'_{t,k}$ the B-F set. Let $\theta : \{1, \ldots, v\} \to \{1, \ldots, v\}$ be defined as $\theta(s) = v - s + 1$. Then, $\theta(\beta_{t,k}) = \beta'_{t,k}$.*

Proof. It suffices to show that $\theta(\sim \beta_{t,k}) = \sim \beta'_{t,k}$. Clearly,

$$K \quad = \quad \{b_1 < \cdots < b_k\} \in \sim \beta_{t,k},$$

if and only if the following hold:

$$\begin{cases} b_l \leq v - k - t + 2l - 2 = \theta(k + t + 1 - 2(l-1)) & 1 \leq l \leq t+1, \\ b_l \leq v - k + l = \theta(k - l + 1) & t+2 \leq l \leq k. \end{cases}$$

Since, $\theta(a) \leq \theta(b)$ if and only if $a \geq b$, and $\theta(\theta(a)) = a$; it follows that:

$$\begin{cases} \theta(b_l) \geq k + t + 1 - 2(l-1) & 1 \leq l \leq t+1, \\ \theta(b_l) \geq k - l + 1 & t+2 \leq l \leq k. \end{cases}$$

Note that, $\theta(b_1) > \cdots > \theta(b_1)$. Let $a_s = \theta(b_{k-s+1})$. Clearly $\theta(K) = \{a_1 < \cdots < a_k\}$.

It suffices to show that,

$$a_i + (k - t - 1) \geq 2i, \text{ for } i = 1, \ldots, k.$$

Because, this will imply that $r(\theta(K)) \geq t + 1$ by proposition 4.5.22. Let us consider the first $(t + 1)$ inequalities:

$$\begin{aligned} a_k &\geq k + t + 1, \\ a_{k-1} &\geq k + t - 1, \\ a_{k-2} &\geq k + t - 3, \\ &\vdots \\ a_{k-t} &\geq k - t + 1. \end{aligned}$$

By adding $k - t - 1$ to all the inequalities, we deduce:

$$\begin{aligned} a_k + k - t - 1 &\geq 2k, \\ a_{k-1} + k - t - 1 &\geq 2(k - 1), \\ a_{k-2} + k - t - 1 &\geq 2(k - 2), \\ &\vdots \\ a_{k-t} + k - t - 1 &\geq 2(k - t). \end{aligned}$$

Now, let us consider the last $(k - t - 1)$ inequalities:

$$a_s \geq s \text{ where } 1 \leq s \leq k - t - 1.$$

Note that, $a_s + k - t - 1 \geq s + k - t - 1 \geq s + s = 2s$. Thus, $a_s + k - t - 1 \geq 2s$ for $s = 1, \ldots, k$. The result follows. □

Corollary 4.5.25. *The B-F (t, k)-set is indeed a (t, k)-basis. We will refer to the B-F (t, k)-set as the B-F (t, k)-basis.*

Proof. This is a clear consequence of $\theta(\beta_{t,k}) = \beta'_{t,k}$ and the fact that $W_{t,k}$ is an S_v-map

hence commuting with θ. □

Using the definition of the K-Aj basis, one can deduce a stabilizer group.

Proposition 4.5.26. *Let $\beta_{t,k}$ be the K-Aj basis. Let,*

$$\begin{aligned}\Omega_{t,k} &= \Omega_1 \cup \cdots \cup \Omega_{t+2} \\ &= \{1, \ldots, v-k-t\} \cup \{v-k-t+1, v-k-t+2\} \cup \\ &\quad \cup \cdots \cup \{v-k+t-1, v-k+t\} \cup \{v-k+t+1, \ldots, v\}.\end{aligned}$$

Then, $G = Stab(\Omega_{t,k})$ is a stabilizer group of $\beta_{t,k}$.

Proof. It suffices to show that G stabilizes $\sim \beta_{t,k}$. Let $K = \{b_1 < \cdots < b_k\} \in \sim \beta_{t,k}$, then the following must hold:

$$\begin{cases} b_l \leq v-k-t+2l-2 & 1 \leq l \leq t+1, \\ b_l \leq v-k+l & t+2 \leq l \leq k. \end{cases}$$

Clearly, if we show the first $(t+1)$ inequalities, then the remaining follow by the monotonicity of the b_is.

It is a clear exercise that the G preserves the first $(t+1)$ inequalites. □

Corollary 4.5.27. *Let $\beta'_{t,k}$ be the B-F basis. Let,*

$$\begin{aligned}\Omega'_{t,k} &= \Omega'_{t+2} \cup \cdots \cup \Omega'_1 \\ &= \{v, \ldots, k+t+1\} \cup \{k+t, k+t-1\} \cup \\ &\quad \cup \cdots \cup \{k-t+2, k-t+1\} \cup \{k-t, \ldots, 1\}.\end{aligned}$$

Then, $G = Stab(\Omega'_{t,k})$ is a stabilizer group of $\beta'_{t,k}$.

Proof. Because $\beta'_{t,k} = \theta(\beta_{t,k})$, it must be necessary that $\theta Stab(\Omega_{t,k})\theta^{-1} = Stab(\theta(\Omega_{t,k}))$ is a stabilizer group of $\theta(\beta_{t,k}) = \beta'_{t,k}$. Since $\Omega'_{t,k} = \theta(\Omega_{t,k})$ the result follows. □

For the K-Aj basis $\beta_{t,k}$, one can characterize the orbits in $(C_k(X))_0$ that belong to $\beta_{t,k}$. We summarize this in the next proposition.

Proposition 4.5.28. *Let $\beta_{t,k}$ be the K-Aj basis, and $G = Stab(\Omega_{t,k})$. Then,*

$$\mathbb{H}^{\Omega_{t,k}}(k)\cap \sim \beta_{t,k}^{G} \quad = \quad \{[\phi_1, \ldots, \phi_{t+1}, \phi_{t+2}] \mid r \leq \sum_{s=1}^{r} \phi_s, r = 1, \ldots, t+1\}.$$

Proof. Let $K = \{b_1 < \cdots < b_k\} \in \sim \beta_{t,k}$. The following must hold:

$$\begin{cases} b_l \leq v - k - t + 2l - 2 & 1 \leq l \leq t+1, \\ b_l \leq v - k + l & t+2 \leq l \leq k. \end{cases}$$

Consider $[\phi_1, \ldots, \phi_{t+1}, \phi_{t+2}] = [|K \cap \Omega_{t,k}|]$. Clearly, the first $(t+1)$ inequalities translate to:

$$r \leq \sum_{s=1}^{r} \phi_s \text{ where } r = 1, \ldots, t+1. \tag{4.11}$$

Because the remaining inequalites follow from the first $(t+1)$ inequalites by using the assumption that the b_is are monotonic, it must follow that Equation (4.11) is necessary and sufficient. □

4.5.3 The Equivariant Sign Conjecture

Let $\beta_{t,k}$ be the K-Aj basis or the B-F basis. Given the triple $(W_{t,k}, \beta_{t,k}, G)$, where $Stab(\Omega_{t,k})$); one can ask whether $(M'_{t,k}, \beta_{t,k}^{G})$ affords a trivial positive equivariant signing that is G-invariant. We will conjecture that these signing exist.

Conjecture 4.5.29. The Equivariant Sign Conjecture for the K-Aj basis. *Let $t \leq k \leq v - k$, $\beta_{t,k}$ be the K-Aj basis, and $G = Stab(\Omega_{t,k})$. Then, the pair $(W_{t,k}, \beta_{t,k})$ affords a trivial positive equivariant signing that is G-invariant.*

Because the K-Aj basis is equivalent to the B-F basis, one can formulate an analogous conjecture for the B-F basis.

Conjecture 4.5.30. The Equivariant Sign Conjecture for the B-F basis. *Let $t \leq k \leq v - k$, $\beta'_{t,k}$ be the B-F basis, and $G' = Stab(\Omega'_{t,k})$. Then, the pair $(W_{t,k}, \beta'_{t,k})$ affords a trivial positive equivariant signing that is G-invariant.*

Using the results of the previous subsection, one can reduce the Equivariant Sign Conjecture for the B-F basis.

Proposition 4.5.31. *Let $t \leq k \leq v-k$, $\beta'_{t,k}(v)$ be the B-F basis, and $G' = Stab(\Omega'_{t,k}(v))$ its Stabilizer group. Then, the following are equivalent,*

1. *The pair $(W_{t,k}(v), \beta'_{t,k}(v))$ affords a trivial positive equivariant signing that is G-invariant where $v \geq k+t+1$.*

2. *The pair $(W_{t,k}(v_0), \beta'_{t,k}(v_0))$ affords a trivial positive equivariant signing that is G-invariant where $v_0 = 2k+t$.*

Proof. We will use the Second Reduction of the last subsection. Clearly, $\{\Omega'_{t,k}(v)\}_{v=1}^{\infty}$ is a Monotone Family. Also, we can use the natural inclusion $\iota : \{1,\ldots,v\} \hookrightarrow \{1,\ldots,v'\}$ to extend to an inclusion map for $\{\Omega'_{t,k}(v)\}_{v=1}^{\infty}$. By construction, the B-F basis is a Compatible Set for $\{\Omega'_{t,k}(v)\}_{v=1}^{\infty}$. This is because $\beta_{t,k}(v)' \subset \beta_{t,k}(v')'$ naturally. Clearly, the columns that corresponds to $\beta_{t,k}(v)'$ in $W_{t,k}(v)$ are $\mathbb{Q}$-linearly independent since $\beta_{t,k}(v)'$ is a (t,k)-basis. Thus, the Second Reduction applies, and it suffices to calculate $v_0(k)$.

Clearly, $f_1(v) = k-t$, $f_2(v) = 2, \ldots, f_{t+1}(v) = 2$, and $f_{t+1} = f$ where $v = k+t+f$. Hence, $\gamma_1(k) = k-t$, $\gamma_2(k) = 2, \ldots, \gamma_{t+1}(k) = 2$, and $\gamma_{t+2}(k) = k$. Thus, $v_1^{\infty} = v_2^{\infty} = \cdots = v_{t+1}^{\infty} = k+t+1$, and $v_{t+1}^{\infty} = k+t+k = 2k+t$. Therefore, $v_0(k) = 2k+t$. □

As a corollary, we formulate a similar reduction for the K-Aj basis.

Corollary 4.5.32. *Let $t \leq k \leq v-k$, $\beta_{t,k}(v)$ be the K-Aj basis, and $G = Stab(\Omega_{t,k}(v))$. Then, the following are equivalent,*

1. *The pair $(W_{t,k}(v), \beta_{t,k}(v))$ affords a trivial positive equivariant signing that is G-invariant where $v \geq k+t+1$.*

2. *The pair $(W_{t,k}(v_0), \beta_{t,k}(v_0))$ affords a trivial positive equivariant signing that is G-invariant where $v_0 = 2k+t$.*

Proof. It suffices to show part 2 implies part 1. Let ϵ_{v_0} be a trivial positive equivariant signing for $(W_{t,k}(v_0), \beta_{t,k}(v_0))$ that is G-invariant. Since $\beta'_{t,k}(v_0) = \theta(\beta_{t,k}(v_0))$, $\epsilon'_{v_0} = \theta \circ \epsilon_{v_0} \circ \theta^{-1}$ is a trivial positive equivariant signing for $(W_{t,k}(v_0), \beta'_{t,k}(v_0))$ that is $Stab(\Omega_{t,k}(v_0)')$-invariant. Hence, by proposition 4.5.31, there is a trivial positive equivariant signing ϵ'_v of $\beta_{t,k}(v)'$ that is $Stab(\Omega_{t,k}(v)')$-invariant. By defining, $\epsilon_v = \theta^{-1} \circ \epsilon'_v \circ \theta$, one can check that ϵ_v is a trivial positive equivariant signing for $(\beta_{t,k}(v), W_{t,k}(v))$ that is $Stab(\Omega_{t,k}(v))$-invariant. □

We proceed to check the conjectures for the cases $(t,k) = (1,2)$ and $(2,3)$. By using the Second Reduction, it suffices to check the conjecture for the case $v = 2k+t$. In the following proposition we will show a much stronger result than the Equivariant Sign Conjecture. We will show the existence of trivial positive equivariant G-signing for $v = 2k+1$.

Proposition 4.5.33. *Let $\beta_{1,2}$ be the K-Aj basis, and $G = Stab(\Omega_{1,2})$. Let $v = v_0(2) = 1 + 2 * 2 = 5$. Then,*

1. *A basis for $\mathbb{H}^{\Omega_{1,2}}(1)$ is given by:*

$$\{[0,0,1],[0,1,0],[1,0,0]\}.$$

2. *A basis for $\mathbb{H}^{\Omega_{1,2}}(2)$ is given by:*

$$\beta_{1,2} \cup (\sim \beta_{1,2}) \quad = \quad \{[1,0,1],[0,1,1],[0,2,0]\} \cup \{[2,0,0],[1,1,0]\}.$$

3. *The pair $(M'_{1,2}, \beta^G_{1,2})$ affords a trivial positive equivariant signing.*

4. *The pair $(W_{1,2}, \beta_{1,2})$ affords a trivial positive equivariant G-signing.*

Proof. Parts 1 and 2 follow by direct computation, and by proposition 4.5.28.

We show part 3. Using the basis of parts 1 and 2, $M'_{1,2}$ has matrix representation:

$$\begin{pmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 2 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Note that $M'_{1,2}$ has Reduced Row Echelon Form:

$$\begin{pmatrix} 1 & 0 & 0 & 2 & 1 \\ 0 & 1 & 0 & -2 & -1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Hence, we deduce that $(M'_{1,2}, \beta^G_{1,2})$ has a trivial positive equivariant signing by proposition 4.4.5. This signing is given by,

$$\epsilon^G([1,0,1]) = 1, \quad \epsilon^G([0,1,1]) = -1, \quad \epsilon^G([0,2,0]) = 1.$$

We show that $(W_{1,2}, \beta_{1,2})$ affords a trivial positive equivariant G-signing, We will use the signing inhereted from $(M'_{1,2}, \beta^G_{1,2})$. That is, $\epsilon(K) = \epsilon^G([|K \cap \Omega_{1,2}|])$.

Define $\bar{e} = v - e$, and $\bar{1}^* = \bar{2}$, $\bar{2}^* = \bar{1}$. Let $a, b \in \{1, \ldots, v-3\}$. We will consider each orbit of $\sim \beta_{1,2}$ as a case. Hence, giving a total of two cases. We proceed to show these cases.

Case $[\mathbf{2}, \mathbf{0}, \mathbf{0}]$. Let $\{a, b\} \in [2, 0, 0]$. Let:

$$v_{[2,0,0]} \quad = \quad \{a, \bar{0}\} + \{b, \bar{0}\} + \{\bar{1}, \bar{1}^*\} - \{\bar{1}, \bar{0}\} - \{\bar{1}^*, \bar{0}\}.$$

Clearly, $v_{[2,0,0]} \in Col_{\mathbb{Z}}(W_{\beta_{1,2}})$, and affords the same signing as ϵ^G. Also, a direct calculation shows that $W_{1,2}\{a, b\} = W_{1,2}v_{[2,0,0]}$.

Case $[\mathbf{1}, \mathbf{1}, \mathbf{0}]$. Let $\{a, \bar{e}\} \in [1, 1, 0]$, where $e = 1$ or 2. Let:

$$v_{[1,1,0]} \quad = \quad \{a, \bar{0}\} + \{\bar{e}, \bar{e}^*\} - \{\bar{e}^*, \bar{0}\}.$$

Clearly, $v_{[1,1,0]} \in Col_{\mathbb{Z}}(W_{\beta_{1,2}})$, and affords the same signing as ϵ^G. Also, a direct calculation shows that $W_{1,2}\{a, \bar{e}\} = W_{1,2}v_{[1,1,0]}$. □

Proposition 4.5.34. *Let $\beta_{2,3}$ be the K-Aj basis, and $G = Stab(\Omega_{2,3})$. Let $v = v_0(d) = 2 + 3 * 2 = 8$. Then,*

1. *A basis for $\mathbb{H}^{\Omega_{2,3}}(2)$ is given by:*

$$\{[0,1,1,0],[1,0,1,0],[1,1,0,0],[0,1,0,1],[1,0,0,1],[0,0,1,1],$$
$$[0,2,0,0],[0,0,2,0],[2,0,0,0]\}.$$

2. *A basis for $\mathbb{H}^{\Omega_{2,3}}(3)$ is given by $\beta_{2,3}\cup \sim \beta_{2,3}$ where:*

$$\begin{aligned}\beta_{2,3} &= \{[0,2,1,0],[1,1,0,1],[1,0,1,1],[0,1,2,0],[1,0,2,0],\\ &\quad [2,0,0,1],[0,1,1,1],[0,0,2,1],[0,2,0,1]\},\\ \sim \beta_{2,3} &= \{[3,0,0,0],[1,2,0,0],[1,1,,1,0],[2,1,0,0],[2,0,1,0]\}.\end{aligned}$$

3. *The pair $(M'_{2,3}, \beta^G_{2,3})$ affords a trivial positive equivariant signing.*

4. *The pair $(W_{2,3}, \beta_{2,3})$ affords a trivial positive equivariant G-signing.*

Proof. Parts 1 and 2 follow by direct computation, and by proposition 4.5.28.

We show part 3. Using the basis of parts 1 and 2, $M'_{2,3}$ has matrix representation:

$$\begin{pmatrix}
2 & 0 & 0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2\\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 0\\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0\\
0 & 1 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 1 & 1
\end{pmatrix}.$$

A calculation of the Reduced Row Echelon Form gives:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -6 & -2 & -1 & -4 & -2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -4 & -2 & -1 & -3 & -2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 3 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 3 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 4 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -2 & -1 & -1 & -2 & -1 \end{pmatrix}.$$

Hence, we can deduce that $(M'_{2,3}, \beta^G_{2,3})$ affords a trivial positive equivariant signing by proposition 4.4.5. This signing is given by:

$$\begin{aligned} \epsilon^G([0,2,1,0]) = 1, \quad \epsilon^G([1,1,0,1]) = 1, \quad \epsilon^G([1,0,1,1]) = -1, \\ \epsilon^G([0,1,2,0]) = -1, \quad \epsilon^G([1,0,2,0]) = 1, \quad \epsilon^G([2,0,0,1]) = 1, \\ \epsilon^G([0,1,1,1]) = 1, \quad \epsilon^G([0,0,2,1]) = 1, \quad \epsilon^G([0,2,0,1]) = -1. \end{aligned}$$

We show part 4. We will use the signing inhereted from $(M'_{2,3}, \beta^G_{2,3})$. Define $\epsilon(K)$, for $K \in \beta_{2,3}$, by lettting $\epsilon(K) = \epsilon^G([|K \cap \Omega_{2,3}|])$.

Define $\bar{e} = v - e$. Define $\bar{1}^* = \bar{2}$, $\bar{2}^* = \bar{1}$, $\bar{3}^* = \bar{4}$, and $\bar{4}^* = \bar{3}$. Let $a, b, c \in \{1, \ldots, v-5\}$. Consider the following parametrization for the orbits of $\sim \beta_{2,3}$.

- $\{a, \bar{3}, \bar{3}^*\}$ be a representative of the orbit $[1,2,0,0]$.
- $\{a, \bar{e}, \bar{f}\}$ (where $e = 3, 4$ and $f = 1, 2$) be a representative of the orbit $[1,1,1,0]$.
- $\{a, b, \bar{e}\}$ (where $e = 3, 4$) be a representative of the orbit $[2,1,0,0]$.
- $\{a, b, \bar{f}\}$ (where $f = 1, 2$) be a representative of the orbit $[2,0,1,0]$.
- $\{a, b, c\}$ be a representative of the orbit $[3,0,0,0]$.

We will consider each orbit of $\sim \beta_{2,3}$ as a case. Thus, giving a total of five cases.

Case $[\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0}]$. This case can be solved by considering the following calculation. Let,

$$\begin{aligned} v_{[3,0,0,0]} &= \{\bar{1},\bar{1}^*,\bar{0}\}+\{\bar{3},\bar{1},\bar{0}\}+\{\bar{3},\bar{1}^*,\bar{0}\}+\{\bar{3}^*,\bar{1},\bar{0}\}+\{\bar{3}^*,\bar{1}^*,\bar{0}\} \\ &\quad -2\{\bar{3},\bar{1},\bar{1}^*\}-2\{\bar{3}^*,\bar{1},\bar{1}^*\}-2\{\bar{3},\bar{3}^*,\bar{0}\}+\{\bar{3},\bar{3}^*,\bar{1}\}+\{\bar{3},\bar{3}^*,\bar{1}^*\} \\ &\quad -\{a,\bar{1},\bar{0}\}-\{a,\bar{1}^*,\bar{0}\}-\{b,\bar{1},\bar{0}\}-\{b,\bar{1}^*,\bar{0}\} \\ &\quad -\{c,\bar{1},\bar{0}\}-\{c,\bar{1}^*,\bar{0}\}+\{a,\bar{1},\bar{1}^*\}+\{b,\bar{1},\bar{1}^*\} \\ &\quad +\{c,\bar{1},\bar{1}^*\}+\{a,b,\bar{0}\}+\{b,c,\bar{0}\}+\{a,c,\bar{0}\}. \end{aligned}$$

It can be shown by direct calculation that $W_{2,3}\{a,b,c\} = W_{2,3}v_{[3,0,0,0]}$. Clearly, $v_{[3,0,0,0]}$ has the signing given by ϵ.

Case $[\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{0}]$. This case can be solved by considering,

$$\begin{aligned} v_{[2,0,1,0]} &= \{\bar{3},\bar{f}^*,\bar{0}\}+\{\bar{3}^*,\bar{f}^*,\bar{0}\}-\{\bar{3},\bar{1},\bar{1}^*\}-\{\bar{3}^*,\bar{1},\bar{1}^*\} \\ &\quad -\{\bar{3},\bar{3}^*,\bar{0}\}+\{\bar{3},\bar{3}^*,\bar{f}\}-\{a,\bar{f}^*,\bar{0}\}-\{b,\bar{f}^*,\bar{0}\} \\ &\quad +\{a,\bar{1},\bar{1}^*\}+\{b,\bar{1},\bar{1}^*\}+\{a,b,\bar{0}\}. \end{aligned}$$

It can be shown by direct calculation that $W_{2,3}\{a,b,\bar{f}\} = W_{2,3}v_{[2,0,1,0]}$ where $f = 1,2$. Clearly, $v_{[2,0,1,0]}$ has the signing given by ϵ.

Case $[\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0}]$. Let,

$$\begin{aligned} v_{[2,1,0,0]} &= \{\bar{1},\bar{1}^*,\bar{0}\}+\{\bar{e}^*,\bar{1},\bar{0}\}+\{\bar{e}^*,\bar{1}^*,\bar{0}\}-2\{\bar{e}^*,\bar{1},\bar{1}^*\} \\ &\quad -\{\bar{e},\bar{1},\bar{1}^*\}-2\{\bar{3},\bar{3}^*,\bar{0}\}+\{\bar{3},\bar{3}^*,\bar{1}\}+\{\bar{3},\bar{3}^*,\bar{1}^*\} \\ &\quad -\{a,\bar{1},\bar{0}\}-\{a,\bar{1}^*,\bar{0}\}-\{b,\bar{1},\bar{0}\}-\{b,\bar{1}^*,\bar{0}\} \\ &\quad +\{a,\bar{1},\bar{1}^*\}+\{b,\bar{1},\bar{1}^*\}+\{a,\bar{e},\bar{0}\}+\{b,\bar{e},\bar{0}\} \\ &\quad +\{a,b,\bar{0}\}. \end{aligned}$$

As the previous cases, it can be shown by direct calculation that: $W_{2,3}\{a,b,\bar{e}\} = W_{2,3}v_{[2,1,0,0]}$ where $e = 3,4$. Clearly, $v_{[2,1,0,0]}$ has the signing given by ϵ.

Case $[\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0}]$. Let,

$$\begin{aligned} v_{[1,2,0,0]} &= \{\bar{1},\bar{1}^*,\bar{0}\} - \{\bar{3},\bar{1},\bar{1}^*\} - \{\bar{3}^*,\bar{1},\bar{1}^*\} - \{\bar{3},\bar{3}^*,\bar{0}\} \\ &\quad +\{\bar{3},\bar{3}^*,\bar{1}\} + \{\bar{3},\bar{3}^*,\bar{1}^*\} - \{a,\bar{1},\bar{0}\} - \{a,\bar{1}^*,\bar{0}\} \\ &\quad +\{a,\bar{1},\bar{1}^*\} + \{a,\bar{3},\bar{0}\} + \{a,\bar{3}^*,\bar{0}\}. \end{aligned}$$

As the previous cases, it can be shown by direct calculation that: $W_{2,3}\{a,\bar{3},\bar{3}^*\} = W_{2,3}v_{[1,2,0,0]}$. Clearly, $v_{[1,2,0,0]}$ has the signing given by ϵ.

Case $[\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0}]$. Let,

$$\begin{aligned} v_{[1,1,1,0]} &= \{\bar{e}^*,\bar{f}^*,\bar{0}\} - \{\bar{e}^*,\bar{1},\bar{1}^*\} - \{\bar{3},\bar{3}^*,\bar{0}\} + \{\bar{3},\bar{3}^*,\bar{f}\} \\ &\quad -\{a,\bar{f}^*,\bar{0}\} + \{a,\bar{1},\bar{1}^*\} + \{a,\bar{e},\bar{0}\}. \end{aligned}$$

As the previous cases, it can be shown that: $W_{2,3}\{a,\bar{e},\bar{f}\} = W_{2,3}v_{[1,1,1,0]}$ where $e = 3,4$ and $f = 1,2$. Clearly, $v_{[1,1,1,0]}$ has the signing given by ϵ.

□

We note that we have checked the Equivariant Sign Conjecture for the cases $(t,k) = (3,4),(4,5)$ and $(5,6)$ by using a computer program. We do not include the proofs of these cases since they involve a large number of cases.

4.6 The Case G = (Z/nZ)

In what follows, we will define s^* as $n-s$. We consider the matrices $M_{t,k}$ and $M'_{t,k}$ when the action is given by $G = (\mathbb{Z}/n\mathbb{Z})$, the cyclic group of order n, and $v = n$.

We propose the following conjectures:

Conjecture 4.6.1. The $(\mathbf{t},\mathbf{k})$**-basis conjecture. Weak version**. *Let* $t < k \leq n-k \leq n-t$. *If* $\gcd(tk,n) = 1$, *then,*

1. *The matrix* $M'_{t,k}(n)$ *affords a* (t,k)*-basis.*

2. *The matrix* $M_{t,k}(n)$ *affords a* (t,k)*-basis.*

Conjecture 4.6.2. The (t, k)-basis conjecture. Strong version. *Let* $t < k \leq n - k \leq n - t$ *then* $M'_{t,k}(n)$ *affords a* (t, k)*-basis.*

We will show under the assumption $\gcd(tk, n) = 1$ that $M_{t,k}(n) = M'_{t,k}(n)$. Thus, the weak (t, k)-basis conjecture is really a conjecture about the matrices $M'_{t,k}(n)$. We will check the these conjectures by finding a (t, k)-basis for the cases $(t, k) = (2, 3), (2, 4)$, and show some progress for the case $(3, 4)$. Using the found (t, k)-basis, we will calculate the Smith Group of $M_{2,3}, M'_{2,3}, M_{2,4}, M'_{2,4}$. Also, we will show the following consequence of the (t, k)-basis conjecture:

Proposition 4.6.3. *Let* $\gcd(n, (2(k-1))!) = 1$*, and* $t < k \leq n - k \leq n - t$*. Assume the* (t, k)*-basis conjecture holds for* n *and all* t, k *where* $t < k \leq n - k$*. Then,* $M'_{t,k}(n)$ *has Smith Group given by:*

$$(\mathbb{Z}/\binom{k}{t}\mathbb{Z}) \times (\mathbb{Z}/\binom{k-2}{t-2}\mathbb{Z})^{r_2(n)-1} \times (\mathbb{Z}/\binom{k-3}{t-3}\mathbb{Z})^{r_3(n)-r_2(n)} \times \cdots \times (\mathbb{Z}/\binom{k-(t-1)}{t-(t-1)}\mathbb{Z})^{r_{t-1}(n)-r_{t-2}(n)},$$

where $r_i(n) = \frac{\binom{n}{i}}{n}$ *is the number of orbits of* $(\mathbb{Z}/n\mathbb{Z})$ *on the* i*-subsets for* $i = 2, \ldots, t$*.*

We close the section with some ideas on how to find a (t, k)-basis for $M_{t,k}(n)'$.

4.6.1 The Orbits of (Z/nZ) On the k-subsets

We will propose a method for counting the orbits of k-subsets under the action of $(\mathbb{Z}/n\mathbb{Z})$ by partitioning the k-subsets' orbits into classes corresponding to partitions of k. We will use the results of this subsection in the (t, k)-basis results.

Let us introduce the notion of a "cyclic ordered partition" to algebraically manipulate the orbits of $(\mathbb{Z}/n\mathbb{Z})$.

Definition 4.6.4. *Let* $n = a_1 + \cdots + a_k$ *be a partition of* n *with exactly* k *parts where the order of the* a_i*s matter. Denote this partition by* $[a_1, \ldots, a_k]$*. We will call* $[a_1, \ldots, a_k]$ *an* ordered partition of n with k parts.

Let $G = \mathbb{Z}/k\mathbb{Z}$ act on the ordered partitions by $t \cdot [a_1, \ldots, a_k] = [a_{1+t}, \ldots, a_{k+t}]$, where the subscripts are taken modulo k.

An orbit of the action of $\mathbb{Z}/k\mathbb{Z}$ on the ordered partitions of n with exactly k parts will be called a "cyclic ordered partition" *of n with k parts.*

The following proposition motivates our defintion.

Proposition 4.6.5. *There is a one to one correspondence between the orbits of G on the k-subsets and the set of cyclic ordered partitions of n with k parts.*

Proof. We will show the proposition by example. Take for instance $n = 7$ and consider the 3-subset $K = \{1, 3, 7\}$. Let us think of the set $\{1, \ldots, 7\}$ as 7 points evenly spaced on the unit circle, where we number the points in increasing order using the clockwise direction. Label the points of K with a circle. figure 4.5 shows the set K, and all the other sets $K + i$ that are in the orbit of K under the action of $(\mathbb{Z}/7\mathbb{Z})$. As

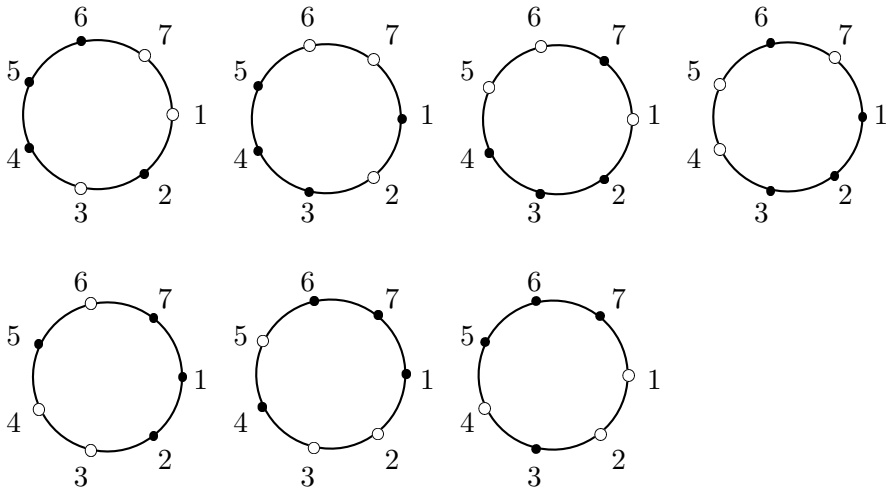

Figure 4.5. The orbits of $\{1, 3, 7\}$ under the action of $(\mathbb{Z}/7\mathbb{Z})$.

it is shown by the pictures of figure 4.5, the circular distances between consecutive points of K are the same to the circular distances between consecutive points of $K' \in \Omega_K$. Hence, the circular distances and their order in the clockwise direction are an invariant of the action of $(\mathbb{Z}/7\mathbb{Z})$ on the orbit $\Omega_{\{1,2,6\}}$. Clearly, this invariant information is represented by the cyclic ordered partition $[1, 2, 4]$ using the clockwise

direction. Similary, we can generate a cyclic ordered partition of n of size 3 for every 3-subsets' orbit Ω_K. It is a clear exercise to show that if two orbits generate the same cyclic ordered partition of n of size three then they must be the same.

One can define the following map,

$$\psi(\Omega_{\{x_1<x_2<x_3\}}) \quad = \quad [x_2 - x_1, x_3 - x_2, 7 - x_3 + x_1],$$

clearly an injection between the orbits of $(\mathbb{Z}/7\mathbb{Z})$ on the 3-subsets and the cyclic ordered partitions of 7 of size 3. Conversely, one can define an inverse of ψ given by ϕ as:

$$\phi([a_1, a_2, a_3]) \quad = \quad \Omega_{\{0,a_1,a_1+a_2\}},$$

It is an easy exercise to show that ϕ and ψ are inverses of one another. Hence, the result follows for $(\mathbb{Z}/7\mathbb{Z})$ and the 3-subsets.

For the general case, ϕ and ψ are given by:

$$\begin{aligned}
\psi(\Omega_{\{x_1<\cdots<x_k\}}) &= [x_2 - x_1, x_3 - x_2, \ldots, x_k - x_{k-1}, n - x_k + x_1], \\
\phi([a_1, \ldots, a_k]) &= \Omega_{\{0,a_1,a_1+a_2,\ldots,a_1+\cdots+a_{k-1}\}}.
\end{aligned}$$

□

For the rest of the section, we will use the language of cyclic ordered partitions of n of size k to refer to the orbits of $(\mathbb{Z}/n\mathbb{Z})$ on the k-subsets. We will also use the functions ψ,ϕ of proposition 4.6.5 whenever needed. The following Propsition characterizes the k-subsets' orbits.

Proposition 4.6.6. *Let $K \subset \{0, \ldots, n-1\}$ be a k-subset, and $G = (\mathbb{Z}/n\mathbb{Z})$. Then,*

1. *If $0 \in K$, and $g + K = K$, then $g \in K$.*

2. *Let G_K be the stabilizer of K in G, then there are $g_1, \ldots, g_r$ with $0 \leq r \leq [G :$*

$G_K]$ *such that:*

$$K \quad = \quad (G_K + g_1) \cup (G_K + g_2) \cup \cdots \cup (G_K + g_r),$$

where the above equation is viewed as an equation of sets.

3. *For some integer* r, $k = |G_K|r$.

4. *The* $\gcd(k, n)$ *divides* $|G_K|$.

5. *Let* $a = [G : G_K]$, *and* $r = \frac{|G_K|}{k}$. *Let* ψ *be the function defined in the proof of proposition 4.6.5. The cyclic ordered partition of* Ω_K *is given by:*

$$\psi(\Omega_K) \quad = \quad [b_1, \ldots, b_r, b_1, \ldots, b_r, \ldots, b_1, \ldots, b_r],$$

where the expansion $b_1, \ldots, b_r$ *is a partition of* a, *i.e.,* $b_1 + \cdots + b_r = a$ *where the order of the* b_i*s is not important, and repeats itself* $|G_K|$ *times.*

6. *The following holds,* $|\Omega_K| = \frac{n}{|G_K|} = a$.

Proof. Part 1 is clear.

We show part 2. It suffices to show the claim when $0 \in K$. Hence, we can assume that $G_K \subset K$. By considering the set $\frac{K}{G_K}$, we will be able to deduce the claim as long as we show that: if $(G_K + g) \cap K \neq \phi$, then $(G_K + g) \subset K$. Thus, let $g + g' \in K$, where $g' \in G_K$. Let $g'' \in G_K$, then $g + g' + g$" $\in (K + g'') = K$. Hence, the claim follows since $g'' \in G_K$ is arbitrary.

Part 3 is a clear consequence of part 2. Part 4 is a clear consequence of part 3.

We show part 5. Assume that $K \in \Omega_K$, where $0 \in K$. Let $s = |G_K|$, $r = \frac{|G_K|}{k}$, and $a = [G : G_K]$. By part 2, there are $g_2, \ldots, g_r$ such that:

$$K \quad = \quad G_K \cup (G_K + g_2) \cup \cdots \cup (G_K + g_r),$$

In particular, $G_K \subset K$. Since G is cyclic, G_K is also cyclic. Thus, $G_K = \langle \frac{n}{s} \rangle = \langle a \rangle$. As K is a the union of cosets of G_K, we can choose the g_is in the decomposition of

part 2 to be such that $0 \leq g_i < a$. Let $K_0 = \{0, g_2, \ldots, g_r\} \subset \{0, \ldots, a\}$. Define, $b_1 = g_2, b_2 = g_3 - g_2, \cdots b_{r-1} = g_r - g_{r-1}, b_r = a - g_r$. Clearly, the b_is denote the consecutive circular distances of the points of K in $\{0, \ldots, a\}$. Because G_K translates these circular distances to the set $\{a, \ldots, 2a\}$, and then to $\{2a, \ldots, 3a\}$, and so on; it follows that the cyclic ordered partition for K has form:

$$\psi(\Omega_K) \quad = \quad [b_1, \ldots, b_r, b_1, \ldots, b_r, \ldots, b_1, \ldots, b_r].$$

Hence, the result follows.

Part 6 is clear. □

As Corollaries, we calculate the sizes of orbits for small cases.

Corollary 4.6.7. (2-subsets). *Let $(\mathbb{Z}/n\mathbb{Z})$ act on the 2-subsets, and let K be a 2-subset. Then,*

1. *If* $\gcd(n, 2) = 1$, *then* $|\Omega_K| = n$ *for all* K.
2. *Assume* $\gcd(n, 2) = 2$. *Then,*

$$|\Omega_K| \quad = \quad \begin{cases} \frac{n}{2} & \text{if } \psi(\Omega_K) = [\frac{n}{2}, \frac{n}{2}], \\ n & \text{else.} \end{cases}$$

Corollary 4.6.8. (3-subsets). *Let $(\mathbb{Z}/n\mathbb{Z})$ act on the 3-subsets, and let K be a 3-subset. Then,*

1. *If* $\gcd(n, 3) = 1$, *then* $|\Omega_K| = n$ *for all* K.
2. *Assume* $\gcd(n, 3) = 3$. *Then,*

$$|\Omega_K| \quad = \quad \begin{cases} \frac{n}{3} & \text{if } \psi(\Omega_K) = [\frac{n}{3}, \frac{n}{3}, \frac{n}{3}], \\ n & \text{else.} \end{cases}$$

Corollary 4.6.9. (4-subsets). *Let $(\mathbb{Z}/n\mathbb{Z})$ act on the 4-subsets, and let K be a 4-subset. Then,*

1. *If* $\gcd(n,4)=1$, *then* $|\Omega_K|=n$ *for all* K.

2. *Assume* $\gcd(n,4)=2$. *Then,*

$$|\Omega_K| \;=\; \begin{cases} \frac{n}{2} & \text{if } \psi(\Omega_K)=[a,b,a,b] \text{ where } a+b=\frac{n}{2}, \\ n & \text{else.} \end{cases}$$

3. *Assume* $\gcd(n,4)=4$. *Then,*

$$|\Omega_K| \;=\; \begin{cases} \frac{n}{4} & \text{if } \psi(\Omega_K)=[\frac{n}{4},\frac{n}{4},\frac{n}{4},\frac{n}{4}], \\ \frac{n}{2} & \text{if } \psi(\Omega_K)=[a,b,a,b] \text{ where } a+b=\frac{n}{2}, a\neq b, \\ n & \text{else.} \end{cases}$$

Definition 4.6.10. *Let* $\{\mathrm{x}\}$ *be a partition of* n *given by* $f_1a_1+\cdots+f_ra_r$ *where part* a_1 *repeats* f_1 *times, part* a_2 *repeats* f_2 *times, ... , and part* a_r *repeats* f_r *times. We will denote* $\{x\}$ *by* $\mathrm{a_1^{f_1}\cdots a_r^{f_r}}$.

Given a partition $\{x\}=a_1^{f_1}\cdots a_r^{f_r}$, one can ask how many cyclic ordered partitions with $k=f_1+\cdots+f_r$ parts of n afford the partition $\{x\}$. An effective answer to this question will help us find $(2,3)$-bases and $(2,4)$-bases. One can find the number of such cyclic ordered partitions by using Burnside's Formula for Group Actions applied to the group $(\mathbb{Z}/k\mathbb{Z})$ acting on the set of Ordered Partitions $X=\{[a_0,\ldots,a_{k-1}] \mid [a_0,\ldots,a_{k-1}] \text{ affords } \{x\}\}$ where the action is defined by $r\cdot[a_0,\ldots,a_{k-1}]=[a_{0+r},\cdots.a_{k-1+r}]$ with the subscripts taken modulo k. The following proposition summarizes the calculation.

Proposition 4.6.11. *Let* $\{x\}=a_1^{f_1}\cdots a_r^{f_r}$ *be a partition of* n *with* k *parts. The number of cyclic ordered partitions affording* $\{x\}$ *is given by the sum:*

$$\frac{1}{k}\sum_{t\in\mathbb{Z}/k\mathbb{Z}}\chi(t),$$

where,

$$\chi(t) \;=\; \begin{cases} \frac{(\frac{k}{o(t)})!}{(\frac{f_1}{o(t)})!(\frac{f_2}{o(t)})!\cdots(\frac{f_r}{o(t)})!} & \text{if } o(t) \text{ divides } f_i \text{ for all } i, \\ 0 & \text{else,} \end{cases}$$

and $o(t) = \frac{k}{\gcd(k,t)}$.

As a corrollary, when $\gcd(n,k) = 1$, we can tell how many cyclic ordered partitions are afforded by a fixed partition of n with exactly k parts.

Corollary 4.6.12. *Let* $\{x\} = a_1^{f_1} \cdots a_r^{f_r}$ *be a partition of* n *with* k *parts, and let* $\gcd(n,k) = 1$. *The number of cyclic ordered partitions affording* $\{x\}$ *is:*

$$\frac{(k-1)!}{(f_1)!\cdots(f_r)!}.$$

Proof. It suffices to show in the formula of proposition 4.6.11 that $\chi(t) = 0$ whenever $t \neq 0$.

If $o(t)$ divides all f_i, then $o(t)$ divides $f_1 + \cdots + f_r = k$, and $o(t)$ divides $f_1 a_1 + \cdots + f_r a_r = n$. Hence, $o(t)$ divides $\gcd(n,k) = 1$. Thus, $o(t) = 1$. That is, $t = 0$. We have shown: if $\chi(t) \neq 0$ then $t = 0$. The result follows. □

We close this subsection with a calculation of the number of k-subsets' orbits when $\gcd(n,k) = 1$.

Proposition 4.6.13. *Let* $\gcd(n,k) = 1$, *then number of orbits of* $\mathbb{Z}/n\mathbb{Z}$ *on the* k*-subsets is* $\frac{\binom{n}{k}}{n}$.

Proof. By using Burnside's formula, it suffices to calculate the number $r_k(n)$ given by:

$$r_k(n) \;=\; \frac{1}{n}\sum_{i=0}^{n-1} \pi_k(i),$$

where $\pi_k(i) = |\{K \in \binom{n}{k} \mid i + K = K\}|$. By assumption and proposition 4.6.6, it

follows that:

$$\pi_k(i) = \begin{cases} \binom{n}{k} & \text{if } i = 0, \\ 0 & \text{else.} \end{cases}$$

Hence, the result follows. □

4.6.2 A Partition of the k-subsets' Orbits of $(\mathbf{Z}/\mathbf{nZ})$

We will propose a partition of the orbits of $(\mathbb{Z}/n\mathbb{Z})$ on the k-subsets by using the partitions of k. This partition will prove instrumental when showing the existence of a $(2,3)$-basis and $(2,4)$-basis.

We will denote the number of partitions of n with r parts by $p_r(n)$. The partition of the k-orbits is motivated by the following result.

Proposition 4.6.14. *If $n \geq 2k$, then $p_{n-k}(n) = p(k)$. That is, the number of partitions of n with exactly $n-k$ parts is equal to the number of partitions of k.*

Proof. Define,

$$\begin{aligned} T_k &= \{\{x\} \mid \{x\} \text{ is a partition of } n \text{ with } n-k \text{ parts}\}, \\ S_k &= \{\{p\} \mid \{p\} \text{ is a partition of } k\}. \end{aligned}$$

It suffices to show a bijection $\eta : T_k \to S_k$.

Consider a partition $\{x\} = a_1^{f_1} a_2^{f_2} \cdots a_r^{f_r}$ of n with $n-k$ parts, i.e., $f_1 + \cdots + f_r = n-k$ and $1 = a_1 < a_2 < \cdots < a_r$. Clearly,

$$\begin{aligned} n &= f_1 + a_2 f_2 + \cdots + a_r a_r \\ &\geq f_1 + 2f_2 + \cdots + 2f_r \\ &= 2(n-k) - f_1, \end{aligned}$$

hence, $f_1 \geq n - 2k \geq 0$. Consider,

$$\begin{aligned}(f_1 - (n-2k)) + f_2 a_2 + \cdots + f_r a_r &= n - (n-2k) \\ &= 2k,\end{aligned}$$

hence, we get a partition of $2k$ with $(f_1 - (n-2k)) + f_2 + \cdots + f_r = k$ parts. By substracting 1 from each of the parts, we get a partition of $k = f_2(a_2 - 1) + \cdots + f_r(a_r - 1)$. Thus, $\{p\} = (a_2 - 1)^{f_2} \cdots (a_r - 1)^{f_r}$ is a partition of k. We use this construction to define η.

Define $\eta : T_k \to S_k$ as:

$$\eta(a_1^{f_1} \cdots a_r^{f_r}) = (a_2 - 1)^{f_2} \cdots (a_r - 1)^{f_r}.$$

Clearly, η is well-defined. We show that η has an inverse.

Consider a partition $\{p\} = (a_2')^{f_2'} \cdots (a_r')^{f_r'}$ of k, where $s = f_2' + \cdots + f_r'$ is the number of parts. Let $f_1' = k - s$. Clearly, $f_1' + \cdots + f_r' = k$. Note that, $2k = f_1' + f_2'(a_2' + 1) + \cdots + f_r'(a_r' + 1)$. Clearly, this is a partition of $2k$ having k parts where f_1' may equal 0. Let $f_1'' = n - 2k + f_1'$. Note that $f_1'' \geq 0$ since $n - 2k \geq 0$. Clearly, $n = f_1'' + f_2'(a_2' + 1) + \cdots + f_r'(a_r' + 1)$ is a partition of n having $f_1'' + f_2' + \cdots + f_r' = n - 2k + f_1' + \cdots + f_r' = n - k$ parts. Define $\gamma : S_k \to T_k$ by,

$$\gamma((a_2')^{f_2'} \cdots (a_r')^{f_r'}) = 1^{f_1''}(a_2' + 1)^{f_2'} \cdots (a_r' + 1)^{f_r'},$$

where $f_1'' = n - k - (f_2' + \cdots + f_r')$. Clearly, γ is a well defined map.

It is an easy exercise to show that $\gamma = \eta^{-1}$. □

We proceed to describe the partition of the k-subsets' orbits of $(\mathbb{Z}/n\mathbb{Z})$.

Definition 4.6.15. *Let $2k \leq n$, and let K a k-subset of $\{0, \ldots, n-1\}$. Let,*

$$[a_1, \ldots, a_{n-k}] = \psi(\Omega_{\sim K}).$$

Let $\{x\} = 1^{f_1} b_2^{f_2} \cdots b_r^{f_r}$ be the partition of n with $(n-k)$ parts afforded by $[a_1, \ldots, a_{n-k}]$.

Using the map of proposition 4.6.14, define the partition of k corresponding to the orbit Ω_K *by:*

$$\{p\} \quad = \quad (b_2 - 1)^{f_2} \cdots (b_r - 1)^{f_r}.$$

Alternatively, the partition of k corresponding to the orbit Ω_K is $\eta(\psi(\Omega_{\sim \mathrm{K}}))$, where η is defined in the proof of proposition 4.6.14.

Let us illustrate map given by definition 4.6.15. Let $n = 7$ and $k = 3$. Figure 4.6 shows the correspondence between the partitions of 3 and the orbits of $(\mathbb{Z}/7\mathbb{Z})$ on the 3-subsets.

K	$\psi(K)$	$\sim K$	$\psi(\sim K)$	$p(k)$
$\{0,1,2\}$	$[1,1,5]$	$\{3,4,5,6\}$	$[1,1,1,4]$	3^1
$\{0,1,3\}$	$[1,2,4]$	$\{2,4,5,6\}$	$[2,1,1,3]$	$1^1 2^1$
$\{0,1,5\}$	$[1,4,2]$	$\{2,3,4,6\}$	$[1,1,2,3]$	$1^1 2^1$
$\{0,2,5\}$	$[2,3,2]$	$\{1,3,4,6\}$	$[2,1,2,2]$	1^3
$\{0,1,4\}$	$[1,3,3]$	$\{2,3,5,6\}$	$[1,2,2,2]$	1^3

Figure 4.6. Correspondence between the 3-subsets' orbits of $(\mathbb{Z}/7\mathbb{Z})$ and the partitions of 3.

From the table of figure 4.6, we deduce that the number of 3-subsets' orbits that correspond to the partition 3^1 is 1, to the partition $1^1 2^1$ is 2, and to the partition 1^3 is 2.

In general, we can calculate the exact number $f(\{p\})$ of k-subsets' orbits that correspond to a fixed partition $\{p\} = b_1^{f_1} \cdots b_r^{f_r}$ of k with $s = f_1 + \cdots + f_r$ parts by using proposition 4.6.11. That is, we calculate the number of cyclic ordered partitions of n with $(n-k)$-parts that afford the partition $\{g(p)\} = \gamma(\{p\}) = 1^{n-k-s}(b_1 + 1)^{f_1} \cdots (b_r + 1)^{f_r}$.

The tables in figures 4.9, 4.10, 4.7, and 4.8 summarize the values of $f(\{p\})$ for the cases $k = 2, 3, 4, 5$.

$\{p\}$	$\{g(p)\}$	$f(\{p\})$	$\gcd(n,4)$
1^4	$1^{n-8}2^4$	$\frac{(n-5)(n-6)(n-7)}{4!}$	1
$1^2 2^1$	$1^{n-7}2^2 3^1$	$\frac{(n-5)(n-6)}{2!}$	1
$1^1 3^1$	$1^{n-6}2^1 4^1$	$(n-5)$	1
2^2	$1^{n-6}3^2$	$\frac{(n-5)}{2!}$	1
4^1	$1^{n-5}5^1$	1	1
1^4	$1^{n-8}2^4$	$\frac{(n-6)((n-5)(n-7)+3)}{4!}$	2
$1^2 2^1$	$1^{n-7}2^2 3^1$	$\frac{(n-5)(n-6)}{2!}$	2
$1^1 3^1$	$1^{n-6}2^1 4^1$	$(n-5)$	2
2^2	$1^{n-6}3^2$	$\frac{(n-4)}{2!}$	2
4^1	$1^{n-5}5^1$	1	2
1^4	$1^{n-8}2^4$	$\frac{(n-5)(n-6)(n-7)+3(n-2)}{4!}$	4
$1^2 2^1$	$1^{n-7}2^2 3^1$	$\frac{(n-5)(n-6)}{2!}$	4
$1^1 3^1$	$1^{n-6}2^1 4^1$	$(n-5)$	4
2^2	$1^{n-6}3^2$	$\frac{(n-4)}{2!}$	4
4^1	$1^{n-5}5^1$	1	4

Figure 4.7. $f(\{p\})$ for $k = 4$.

$\{p\}$	$\{g(p)\}$	$f(\{p\})$	$\gcd(n,5)$
1^5	$1^{n-10}2^5$	$\frac{(n-6)(n-7)(n-8)(n-9)}{5!}$	1
$1^3 2^1$	$1^{n-9}2^3 3^1$	$\frac{(n-6)(n-7)(n-8)}{3!}$	1
$1^2 3^1$	$1^{n-8}2^2 4^1$	$\frac{(n-6)(n-7)}{2!}$	1
$1^1 4^1$	$1^{n-7}2^1 5^1$	$(n-6)$	1
$1^1 2^2$	$1^{n-8}2^1 3^2$	$\frac{(n-6)(n-7)}{2!}$	1
$2^1 3^1$	$1^{n-7}3^1 4^1$	$(n-6)$	1
5^1	$1^{n-6}6^1$	1	1
1^5	$1^{n-10}2^5$	$\frac{(n-6)(n-7)(n-8)(n-9)+4\cdot 4!}{5!}$	5
$1^3 2^1$	$1^{n-9}2^3 3^1$	$\frac{(n-6)(n-7)(n-8)}{3!}$	5
$1^2 3^1$	$1^{n-8}2^2 4^1$	$\frac{(n-6)(n-7)}{2!}$	5
$1^1 4^1$	$1^{n-7}2^1 5^1$	$(n-6)$	5
$1^1 2^2$	$1^{n-8}2^1 3^2$	$\frac{(n-6)(n-7)}{2!}$	5
$2^1 3^1$	$1^{n-7}3^1 4^1$	$(n-6)$	5
5^1	$1^{n-6}6^1$	1	5

Figure 4.8. $f(\{p\})$ for $k = 5$.

$\{p\}$	$\{g(p)\}$	$f(\{p\})$	$\gcd(n,2)$
1^2	$1^{n-4}2^2$	$\frac{n-3}{2}$	1
2^1	$1^{n-3}3^1$	1	1
1^2	$1^{n-4}2^2$	$\frac{n-2}{2}$	2
2^1	$1^{n-3}3^1$	1	2

Figure 4.9. $f(\{p\})$ for $k = 2$.

$\{p\}$	$\{g(p)\}$	$f(\{p\})$	$\gcd(n,3)$
1^3	$1^{n-6}2^3$	$\frac{(n-4)(n-5)}{3!}$	1
$1^1 2^1$	$1^{n-5}2^1 3^1$	$(n-4)$	1
3^1	$1^{n-4}4^1$	1	1
1^3	$1^{n-6}2^3$	$\frac{n(n-9)}{3!}+4$	3
$1^1 2^1$	$1^{n-5}2^1 3^1$	$(n-4)$	3
3^1	$1^{n-4}4^1$	1	3

Figure 4.10. $f(\{p\})$ for $k = 3$.

Using the partition of the k-subsets' orbits given by definition 4.6.15, we introduce some notation that will prove useful later.

Definition 4.6.16. *Let $t < k \leq n - k$. Let $\{p_1\}, \ldots, \{p_r\}$ be the distinct partitions of k. Let x and y, be linear combination of cyclic ordered partitions of n of size k. Then,*

1. *We say that* $\mathrm{x} = \mathrm{y} \bmod 0$ *using $M'_{t,k}$, whenever $x - y \in Ker(M'_{t,k})$.*
2. *We say that* $\mathrm{x} = \mathrm{y} \bmod \{\mathrm{p_{i_1}}\}, \ldots, \{\mathrm{p_{i_s}}\}$ *using $M'_{t,k}$, whenever $M'_{t,k}(x - y) = M'_{t,k}z$ where z has support on cyclic ordered partitions corresponding to classes $\{p_{i_1}\}, \ldots, \{p_{i_s}\}$.*

4.6.3 The $\mathbf{Ker}(\mathbf{M'_{t,k}})$

Proposition 4.3.41 shows a set the generators of $Ker(M'_{t,k})$ using the equivariant projections of the (t,k)-pods. In this section, we will illustrate a calculation of a

projected (t,k)-pod $\Pi(A,B)^G$ by defining B "relative" to A. We will do this to help the reader understand the details. In later subsections, we will skip these details.

Definition 4.6.17. (Relative $(\mathbf{t},\mathbf{k})$-pods). *A (t,k)-pod given by $\Pi(A,B)$ is called a* relative (t,k)-pod *whenever B is specified relative to A. That is, if*

$$A \;=\; \{a_1,\ldots,a_{t+1},\cdots a_k\},$$

then $B=\{b_1,\ldots,b_{t+1}\}$ where $b_i = f_i(a_1,\ldots,a_k)$ and f_i is the ratio of two multivariable polynomials mod n.

In the calculations that will follow, we will specify f_i as linear functions. The following proposition illustrates the calculation of a projected relative $(2,3)$-pod.

Proposition 4.6.18. *Let $[a_1,a_2,a_3]$ be a cyclic ordered partition of n with three parts where the $a_i \geq 2$. The following expresion is a projected relative $(2,3)$-pod, i.e., an element of the $Ker(M'_{2,3})$,*

$$\begin{aligned}&[a_1,a_2,a_3]-[1,a_2,a_2^*-1]-[1,a_3^*,a_3-1]-[a_1,1,a_1^*-1]\\ +&[a_1,a_2+1,a_3-1]+[1,1,2^*]+[1,a_1+1,a_1^*-2]-[a_1,2,a_1^*-2],\end{aligned}$$

where $a^*=n-a$.

Proof. Let $A=\{x_1<x_2<x_3\}\in\Omega_{[a_1,a_2,a_3]}$, where magnitudes are taken in the clockwise direction. For instance, $A=\{0,a_1,a_1+a_2\}$ is a possible choice. We will define B relative to A as $B=\{y_1,y_2,y_3\}$, where,

1. The element y_1 is one unit before x_2 in the counter clockwise direction. That is, $y_1 = x_2-1 \bmod n$.

2. The element y_2 is one unit before x_1 in the counter clockwise direction. That is, $y_2 = x_1-1 \bmod n$.

3. The element y_3 is one unit after x_2 in the clockwise direction. That is, $y_3 = x_2+1 \bmod n$.

We know that y_1, y_2, y_3 exist since each $a_i \geq 2$. Also, by construction $A \cap B = \phi$. Hence, we can construct a $(2,3)$-pod. Figure 4.11 shows a graphical representation of A and B using relative distances.

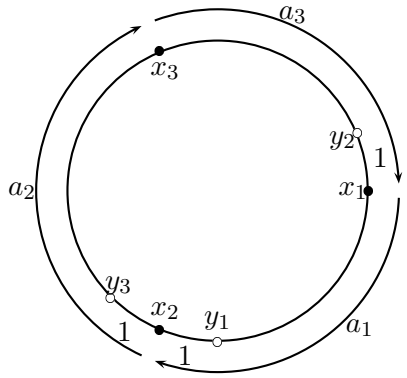

Figure 4.11. Relative $(2,3)$-pod.

Using the notation of proposition 4.3.40, we calculate $\Pi(A, B)$. Let us take for instance the set $T = \{\} \subset \{1, \ldots, 3\}$. This set corresponds to the term $\{x_1, x_2, x_3\} = A$ with sign $(-1)^0 = +1$. Also, $K = \{x_1, x_2, x_3\}$ has cyclic ordered partition $\psi(K) = [a_1, a_2, a_3]$, by assumption.

Let us consider the set $T = \{1\}$. This set corresponds to the term $K = \{y_1, x_2, x_3\}$ having sign $(-1)^1 = -1$. By using the assumption on the relative distances of y_1, y_2, y_3 with respect to x_1, x_2, x_3, we can calculate $\psi(K)$ as $[1, a_2, a_2^* - 1]$. Similarly, using the relative distance conditions one can calculate $\psi(K)$ for each term K in the expansion of $\Pi(A, B)$.

Figure 4.12 shows the calculations of $\psi(K)$ for each term K in the expansion of $\Pi(A, B)$ using the notation of proposition 4.3.40, and using the relative distances of $x_1, \ldots, x_3$ and $y_1, \ldots, y_3$.

We note that in figure 4.12, we have represented T using binary notation. For example, 101 corresponds to $T = \{1, 3\}$.

T	$(-1)^{\|T\|}$	K	$\psi(K)$
000	$+1$	$\{x_1, x_2, x_3\}$	$[a_1, a_2, a_3]$
100	-1	$\{y_1, x_2, x_3\}$	$[1, a_2, a_2^* - 1]$
010	-1	$\{x_1, y_2, x_3\}$	$[1, a_3^*, a_3 - 1]$
001	-1	$\{x_1, x_2, y_3\}$	$[a_1, 1, a_1^* - 1]$
110	$+1$	$\{y_1, y_2, x_3\}$	$[a_1, a_2 + 1, a_3 - 1]$
011	$+1$	$\{x_1, y_2, y_3\}$	$[1, a_1 + 1, a_1^* - 2]$
101	$+1$	$\{y_1, x_2, y_3\}$	$[1, 1, 2^*]$
111	-1	$\{y_1, y_2, y_3\}$	$[a_1, 2, a_1^* - 2]$

Figure 4.12. Projected relative $(2, 3)$-pod.

Clearly, it follows that,

$$\begin{aligned}\Pi(A, B)^G &= [a_1, a_2, a_3] - [1, a_2, a_2^* - 1] - [1, a_3^*, a_3 - 1] - [a_1, 1, a_1^* - 1] \\ &\quad + [a_1, a_2 + 1, a_3 - 1] + [1, 1, 2^*] + [1, a_1 + 1, a_1^* - 2] - [a_1, 2, a_1^* - 2].\end{aligned}$$

By proposition 4.3.41, it follows that $\Pi(A, B)^G \in Ker(M'_{2,3})$. □

In the next subsections, we will construct relative (t, k)-pods by specifying relative distances using diagrams similar to figure 4.11. From these relative (t, k)-pods, we will calculate their corresponding projections by showing explicit calculations similar to figure 4.12.

4.6.4 The $(2, 3)$ Case

In this subsection, we will calculate a $(2, 3)$-basis for $M'_{2,3}$, for general n, with the aid of special relative projected $(2, 3)$-pods. From the basis calculation, we will deduce the Smith Group of $M'_{2,3}$ and $M_{2,3}$.

4.6.4.1 The Space $(\mathbf{C_3(X)})_\mathbf{0}$

Using the classification of definition 4.6.15, we divide the cyclic ordered partitions of n of size 3 into classes, where each class corresponds to a partition of 3. Since there are 3 partitions of 3, the possible classes are:

$$\begin{aligned} \{p_1\} &= 3^1, \\ \{p_2\} &= 2^1 1^1, \\ \{p_3\} &= 1^3. \end{aligned}$$

Each class $\{p_i\}$ imposes conditions on the a_is of $[a_1, a_2, a_3]$ whenever $[a_1, a_2, a_3] \in \{p_i\}$. Figure 4.13 shows these conditions.

$\{p\}$	$\psi(K)$
1^3	$[a_1, a_2, a_3]$ where $a_i \geq 2$
$2^1 1^1$	$[1, a_2, a_3]$ where $a_i \geq 2$
3^1	$[1, 1, 2^*]$

Figure 4.13. Classes of 3-subsets' orbits.

The $(2,3)$-basis calculation, and similarly the $(2,4)$-basis calculation, will follow by steps. First, we start by showing that any cyclic ordered partition $[a_1, a_2, a_3]$ in the class corresponding to $\{p_3\}$ reduces to zero mod $\{p_1\}, \{p_2\}$ using $M'_{2,3}$. Second, we use properties of $M'_{2,3}$ to find a minimal possible generating set for the column space of $M'_{2,3}$ among the cyclic ordered partitions in the classes $\{p_1\}$ and $\{p_2\}$. We will be able to tell that we have a minimal generating set, hence a basis, with the aid of the calculations of $r_2(n)$ given in figure 4.9. This will show the existence of a $(2,3)$-basis.

4.6.4.2 Projected Relative $(\mathbf{2,3})$-Pods

The following projected relative $(2,3)$-pod will be used in later calculations.

Proposition 4.6.19. *Let $a_1 \leq 5^* = n-5$, i.e., $a_1^* - 2 \geq 3$. Then, the following expression is a projected relative $(2,3)$-pod.*

$$[2, a_1, a_1^* - 2] - [a_1, 1, a_1^* - 1] - [1, a_1 + 2, a_1^* - 3]$$
$$+[1, a_1^* - 4, a_1 + 3] + [1, a_1 + 1, a_1^* - 2] - [2, a_1 + 2, a_1^* - 4].$$

Proof. Let $A = \{x_1, x_2, x_3\} \in \Omega_{[2,a_1,a_1^*-2]}$. For instance, $A = \{0, 2, 2+a_2\}$ is a possible choice. Consider the following relative $(2,3)$-pod,

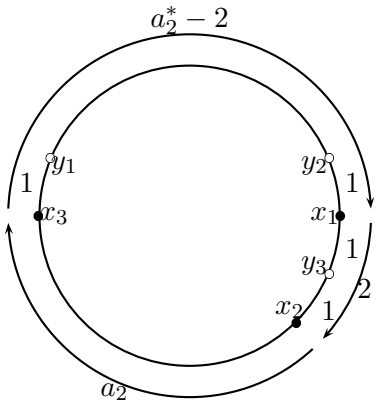

Figure 4.14. Relative $(2,3)$-pod.

We calculate the corresponding projected relative $(2,3)$-pod as it is show in figure 4.15.

Thus, the result follows. □

4.6.4.3 Finding a $(2,3)$-Basis

Using the relative projected $(2,3)$-pods of propositions 4.6.19 and 4.6.18, we proceed to find a generating set of the column space of $M'_{2,3}(n)$ over $\mathbb{Z}$.

Proposition 4.6.20. *The following are true:*

1. *If $[a_1, a_2, a_3]$ is such that $a_i \geq 2$. Then,*

$$[a_1, a_2, a_3] \;=\; [a_1, a_2 + 1, a_3 - 1] - [a_1, 2, a_1^* - 2] \; mod \; \{p_1\}, \{p_2\}.$$

T	$(-1)^{\lvert T\rvert}$	K	$\psi(K)$
000	$+1$	$\{x_1, x_2, x_3\}$	$[2, a_2, a_2^* - 2]$
100	-1	$\{y_1, x_2, x_3\}$	$[a_2, 1, a_2^* - 1]$
010	-1	$\{x_1, y_2, x_3\}$	$[1, a_2 + 2, a_2^* - 3]$
001	-1	$\{x_1, x_2, y_3\}$	$[1, 1, 2^*]$
110	$+1$	$\{y_1, y_2, x_3\}$	$[a_2 + 3, 1, a_2^* - 4]$
011	$+1$	$\{x_1, y_2, y_3\}$	$[1, 1, 2^*]$
101	$+1$	$\{y_1, x_2, y_3\}$	$[1, a_2 + 1, a_2^* - 2]$
111	-1	$\{y_1, y_2, y_3\}$	$[2, a_2 + 2, a_2^* - 4]$

Figure 4.15. Projected relative $(2, 3)$-pod.

2. If $a_2 \leq n - 5$. Then,

$$[2, a_2, a_2^* - 2] \;=\; [2, a_2 + 2, a_2^* - 4] \; mod \; \{p_1\}, \{p_2\}.$$

3. If $2 \leq a_2 \leq n - 4$. Then,

$$[2, a_2, a_2^* - 2] \;=\; [2, a_2 + 1, a_2^* - 3] + [2, 2, 4^*] \; mod \; \{p_1\}, \{p_2\}.$$

Proof. Parts 1 and 2 are clear applications of proposition 4.6.19 and proposition 4.6.18. It suffices to show part 3. Clearly, part 3 is an application of part 1. □

Our first objective will to show that: if $[a_1, a_2, a_3] \in \{p_3\}$, then $[a_1, a_2, a_3] = 0 \bmod \{p_1, p_2\}$. That is, for any cyclic order partition $[a_1, a_2, a_3]$ of size three in the class $\{p_3\}$, there is x with support in the classes $\{p_1\}, \{p_2\}$ such that $M'_{2,3}[a_1, a_2, a_3] = M'_{2,3}x$. Hence, reducing a possible generating set of the column space of $M'_{2,3}$ to the classes $\{p_1\}, \{p_2\}$.

We will start by reducing the cyclic ordered partitions of the form $[2, a_2, a_2^* - 2]$.

Proposition 4.6.21. *The following are true:*

1. *Let* $1 \leq a_2 \leq 3^*$. *Then,*

$$[2, a_2, a_2^* - 2] \;=\; \begin{cases} 0 \ mod\ \{p_1\}, \{p_2\} & \text{if } n \text{ is odd,} \\ 0 \ mod\ \{p_1\}, \{p_2\} & \text{if } 2|n \text{ and } a_2 \text{ is odd,} \\ -[2, 2, 4^*] \ mod\ \{p_1\}, \{p_2\} & \text{if } 2|n \text{ and } 2|a_2. \end{cases}$$

2. *If* n *is odd, then,*

$$[2, 2, 4^*] \;=\; 0 \ mod\ \{p_1\}, \{p_2\}.$$

3. *If* n *is even, then,*

$$2[2, 2, 4^*] \;=\; 0 \ mod\ \{p_1\}, \{p_2\}.$$

Proof. The proposition is clear whenever $a_2 = 1, 3^*$. If $a_2 = 4^*$, then $[2, a_2, a_2^* - 2] = [2, 4^*, 2] = [2, 2, 4^*]$. Hence, $a_2 = 4^*$ reduces to the case $a_2 = 2$. Thus, without loss of generality, assume $2 \leq a_2 \leq n - 5 = 5^*$. We will show part 1 by considering two cases; within each case, we will also show the remainder parts.

Case n is odd. Let a_2 be even, and let $n - a_2 = 2l + 1$. By proposition 4.6.20,

$$[2, a_2, a_2^* - 2] \;=\; [2, a_2 + 2, a_2^* - 4] \bmod \{p_1\}, \{p_2\}.$$

We apply the above congruence $(l-1)$ times to deduce,

$$\begin{aligned}
[2, a_2, a_2^* - 2] &= [2, a_2 + 2, a_2^* - 4] \bmod \{p_1\}, \{p_2\} \\
&= [2, a_2 + 2, a_2^* - 4] \bmod \{p_1\}, \{p_2\} \\
&\vdots \\
&= [2, a_2 + 2(l-1), a_2^* - 2l] \bmod \{p_1\}, \{p_2\} \\
&= [2, 3^*, 1] \bmod \{p_1\}, \{p_2\} \\
&= 0 \bmod \{p_1\}, \{p_2\}.
\end{aligned}$$

In particular, we have shown that $[2, 2, 4^*] = 0 \bmod \{p_1\}, \{p_2\}$. Hence, part 2 follows.

Let a_2 be odd. By proposition 4.6.20, we have

$$\begin{aligned}
[2, a_2, a_2^* - 2] &= [2, a_2 + 1, a_2^* - 3] - [2, 2, 4^*] \bmod \{p_1\}, \{p_2\} \\
&= [2, a_2 + 1, a_2^* - 3] \bmod \{p_1\}, \{p_2\}.
\end{aligned}$$

Hence, the above congruence reduces to the case $a_1' = a_1 + 1$, where a_1' is even.

In particular, we have shown that $[2, a_2, a_2^* - 4] = 0 \bmod \{p_1\}, \{p_2\}$ whenever n is odd.

Case n is even. Assume a_2 is odd. Clearly, a_2^* is odd since n is even. Let $a_1 = 2l + 1$ and $a_1^* = 2s + 1$. Clearly, $n = 2(l + s + 1)$. We apply proposition 4.6.20 to itself $2(s-1)$ times,

$$\begin{aligned}
[2, a_2, a_2^* - 2] &= [2, a_2 + 2, a_2^* - 4] \bmod \{p_1\}, \{p_2\} \\
&\vdots \\
&= [2, a_2 + 2(s-1), a_2^* - 2s] \bmod \{p_1\}, \{p_2\} \\
&= [2, 3^*, 1] \bmod \{p_1\}, \{p_2\} \\
&= 0 \bmod \{p_1\}, \{p_2\}.
\end{aligned}$$

Thus, we have shown that $[2, a_2, a_2^* - 2] = 0 \bmod \{p_1\}, \{p_2\}$ whenever n is even and a_2 is odd.

Assume a_2 is even. Clearly, $a_2 + 1$ is odd. By proposition 4.6.20,

$$\begin{aligned}[2, a_2, a_2^* - 4] &= [2, a_2 + 1, a_2^* - 3] - [2, 2, 4^*] \bmod \{p_1\}, \{p_2\} \\ &= -[2, 2, 4^*] \bmod \{p_1\}, \{p_2\},\end{aligned}$$

where we have used $[2, a_2 + 1, a_2^* - 3] = 0 \bmod \{p_1\}, \{p_2\}$ by the previous deductions.

In particular, we have shown that $[2, 2, 4^*] = -[2, 2, 4^*] \bmod \{p_1\}, \{p_2\}$. Hence, $2[2, 2, 4^*] = 0 \bmod \{p_1\}, \{p_2\}$ and part 3 follows. Also, we have shown that $[2, a_2, a_2^* - 2] = -[2, 2, 4^*] \bmod \{p_1\}, \{p_2\}$ whenever both n and a_2 are even.

Clearly, part 1 follows by the previous deductions. □

We reduce the remaining elements of the class $\{p_3\}$ by making use of the following lemma.

Lemma 4.6.22. *Let σ be any permutation of $\{1, 2, 3\}$. Then,*

1. *The following holds,*

$$M'_{2,3}[a_1, a_2, a_3] = [a_1, a_1^*] + [a_2, a_2^*] + [a_3, a_3^*].$$

2. *The following invariance holds,*

$$M'_{2,3}[a_1, a_2, a_3] = M'_{2,3}[a_{\sigma(1)}, a_{\sigma(2)}, a_{\sigma(3)}].$$

Proof. Let $A = \{x_1, x_2, x_3\} \in [a_1, a_2, a_3]$. For example, $A = \{0, a_1, a_1 + a_2\}$. By calculating the cicular distances in the clockwise direction, part 1 follows from proposition 4.3.40 applied to:

$$W_{2,3} e_{\{x_1, x_2, x_3\}} = e_{\{x_1, x_3\}} + e_{\{x_1, x_2\}} + e_{\{x_2, x_3\}}.$$

Part 2 is a clear consequence of part 1. □

We proceed to reduce the other elements of the class $\{p_3\}$.

Proposition 4.6.23. *Let $[a_1, a_2, a_3]$ be such that $a_i \geq 2$, i.e., $[a_1, a_2, a_3]$ is in the class of $\{p_3\}$. Then,*

1. *If n is odd, then $[a_1, a_2, a_3] = 0$ mod $\{p_1\}, \{p_2\}$.*

2. *If n is even, then $[a_1, a_2, a_3] = \alpha[2, 2, 4^*]$ mod $\{p_1\}, \{p_2\}$ for some integer α.*

Proof. We show part 1. Thus, assume n is odd. By proposition 4.6.19, we know that $[a_1, a_2, a_3] = [a_1, a_2 + 1, a_3 - 1] - [a_1, 2, a_1^* - 2] \bmod \{p_1\}, \{p_2\}$. By proposition 4.6.21, $[a_1, 2, a_1^* - 2] = [2, a_1^* - 2, a_1] = 0 \bmod \{p_1\}, \{p_2\}$. Hence,

$$[a_1, a_2, a_3] \;=\; [a_1, a_2 + 1, a_3 - 1] \bmod \{p_1\}, \{p_2\} \tag{4.12}$$

By lemma 4.6.22, we can always rearrange the a_is such that a_3 is the minimum of all the a_is in $[a_1, a_2, a_3]$. Thus, by repeated applications of Equation (4.12), we deduce,

$$\begin{aligned} [a_1, a_2, a_3] &= [*, *, 1] \bmod \{p_1\}, \{p_2\} \\ &= 0 \bmod \{p_1\}, \{p_2\}. \end{aligned}$$

We proceed to show part 2. Thus, assume n is even. By proposition 4.6.19, we know that $[a_1, a_2, a_3] = [a_1, a_2 + 1, a_3 - 1] - [a_1, 2, a_1^* - 2] \bmod \{p_1\}, \{p_2\}$. By proposition 4.6.21, $[a_1, 2, a_1^* - 2] = [2, a_1^* - 2, a_1] = \alpha'[2, 2, 4^*] \bmod \{p_1\}, \{p_2\}$ for some integral α'. Hence,

$$[a_1, a_2, a_3] \;=\; [a_1, a_2 + 1, a_3 - 1] + \alpha'[2, 2, 4^*] \bmod \{p_1\}, \{p_2\}. \tag{4.13}$$

By lemma 4.6.22, we can always re-arrange the a_is such that a_3 is the minimum of all the a_is in $[a_1, a_2, a_3]$. Thus, by repeated applications of Equation (4.13) we can find an integral α such that:

$$\begin{aligned} [a_1, a_2, a_3] &= [*, *, 1] + \alpha[2, 2, 4^*] \bmod \{p_1\}, \{p_2\} \\ &= \alpha[2, 2, 4^*] \bmod \{p_1\}, \{p_2\}. \end{aligned}$$

□

The previous results are sufficient to deduce a $(2,3)$-basis.

Proposition 4.6.24. *The following are true:*

1. *Let n be odd. Then, $\beta_{2,3} = \{[1, a, a^* - 1] | a = 1, \ldots, \frac{n-1}{2}\}$ is a $(2,3)$-basis for $M'_{2,3}$.*

2. *Let n be even. Then, $\beta_{2,3} = \{[1, a, a^* - 1] | a = 1, \ldots, \frac{n-2}{2}\} \cup \{[2, 2, 4^*]\}$ is a $(2,3)$-basis for $M'_{2,3}$.*

Proof. We show part 1. Assume n is odd. Clearly, $r_2(n) = \frac{n-1}{2}$. It suffices to find a set of columns of $M'_{2,3}$ that has size $\frac{n-1}{2}$ and generates the integral column space of $M'_{2,3}$.

By proposition 4.6.23, the column space of $M'_{2,3}$ is generated by cyclic ordered partitions of classes $\{p_1\}, \{p_2\}$. By using lemma 4.6.22, $[1, a_2, a_3] = [1, a_3, a_2] \bmod 0$. Hence, it suffices to pick $[1, a, b] \in \{p_2\}$ with $a < b$ to generate all the columns of class $\{p_2\}$. Thus, $\beta_{2,3} = \{[1, a, a^* - 1] | a = 1, \ldots, \frac{n-1}{2}\}$ generates all the columns of class $\{p_1\}$ and $\{p_2\}$. Since $\beta_{2,3}$ has size $\frac{n-1}{2}$, it must follow that it is a column basis.

Part 2 follows similarly. By using a similar argument as part 1, one can show that $\beta_{2,3}$ generates the column space of $M'_{2,3}$ and has size $\frac{n}{2}$. Since $r_2(n) = \frac{n}{2}$, it must follow that $\beta_{2,3}$ is a column basis. □

4.6.4.4 The Smith Group of $\mathbf{M'_{2,3}}$ and $\mathbf{M_{2,3}}$

By using the $(2,3)$-basis for $M'_{2,3}$ of proposition 4.6.24, we calculate the Smith Group of $M'_{2,3}$.

Proposition 4.6.25. *The following are true:*

1. *If $n \geq 7$ is odd, then $M'_{2,3}(n)$ has Smith Group $(\mathbb{Z}/3\mathbb{Z})$.*

2. *If $n \geq 8$ is even, then $M'_{2,3}(n)$ has Smith Group $(\mathbb{Z}/6\mathbb{Z})$.*

Proof. We will show that:

1. If $n \geq 7$ is odd, then M'_β has determinant 3.

2. If $n \geq 8$ is even, then M'_β has determinant 6.

where β is the $(2,3)$-basis of proposition 4.6.24, and M'_β is the matrix consisting columns of $M'_{2,3}$ that correspond to $\beta_{2,3}$. Because the abelian groups of order 3 and 6 are unique, the result will follow.

In the following calculations, we will use $\beta_2 = \{[1,1^*],\ldots,[n_0,n_0^*]\}$ as a basis of the 2-subsets' orbits, where,

$$n_0 \;=\; \begin{cases} \frac{n-1}{2} & \text{if } n \text{ is odd,} \\ \frac{n}{2} & \text{if } n \text{ is even.} \end{cases}$$

Also, we will use the following consequence of lemma 4.6.22.

$$M'_{2,3}[1,a,a^*-1] \;=\; [1,1^*]+[a,a^*]+[a+1,(a+1)^*].$$

Case n is odd. Using the basis β_2 and $\beta_{2,3}$, M'_β has matrix representation:

$$\begin{bmatrix} 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 2 \end{bmatrix},$$

where the above matrix is $m \times m$ with $m = \frac{n-1}{2}$. Define f_m as the determinant of the above matrix. By using the minor expansion along the last column, we calculate:

$$f_m \;=\; 2g_{m-1} + (-1)^{m+1},$$

where g_m is the determinant of the following $m \times m$ matrix:

$$\begin{bmatrix} 2 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 1 \end{bmatrix}.$$

Note that g_m can also be calculated recursively, by doing a determinant expansion along the last column. Hence, we deduce:

$$g_m = (-1)^{m+1} + g_{m-1}.$$

Therefore, for $m \geq 2$,

$$g_m = \begin{cases} 1 & \text{if } 2 \mid n, \\ 2 & \text{if } n \text{ is odd.} \end{cases}$$

From the value of g_m, we deduce that $f_m = 3$ for $m \geq 3$. Therefore, M'_β has determinant 3.

Case n is even. Using the basis β_2 and $\beta_{2,3}$, M'_β has matrix representation:

$$\begin{bmatrix} 2 & 1 & 1 & \cdots & 1 & 1 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 & 2 \\ 0 & 1 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 1 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix},$$

where the above matrix is $m \times m$ with $m = \frac{n}{2}$. Define f_m as the determinant of the above matrix. By using the minor expansion along the last row, we calculate:

$$f_m \;\; = \;\; -f_{m-1}.$$

Hence $f_m = \pm f_4$. Also, by direct calculation $f_4 = 6$. Hence, the result follows. □

We will calculate the Smith Group of the matrices $M_{2,3}(n)$. Figure 4.16 summarizes the results.

$\gcd(2,n)$	$\gcd(3,n)$	$\overline{S}(M_{2,3}(n))$
1	1	$(\mathbb{Z}/3\mathbb{Z})$
1	3	$\{1\}$ (primitive)
2	1	$(\mathbb{Z}/12\mathbb{Z})$ or $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$
2	3	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ or $(\mathbb{Z}/4\mathbb{Z})$

Figure 4.16. The Smith Group of $M_{2,3}(n)$.

Figure 4.17 shows the values calculated for the Smith Group of $M_{2,3}$ with the aid of a computer program.

We proceed with the Smith Group calculations.

Proposition 4.6.26. *Let* $\gcd(n,2) = 1 = \gcd(n,3)$*, then* $\overline{S}(M_{2,3}(n)) = (\mathbb{Z}/3\mathbb{Z})$.

Proof. Because $\gcd(n,2) = 1 = \gcd(n,3)$, we must have $D_2 = nI$ and $D_3 = nI$. Thus, $M'_{2,3}D_3 = D_2M_{2,3}$ implies $M'_{2,3} = M_{2,3}$. The result follows from proposition 4.6.25. □

Proposition 4.6.27. *Let* $\gcd(2,n) = 1$ *and* $\gcd(3,n) = 1$*. Then,* $M_{2,3}(n)$ *has trivial Smith Group. That is,* $M_{2,3}(n)$ *is primitive.*

n	$\overline{S}(M_{2,3}(n))$	n	$\overline{S}(M_{2,3}(n))$	n	$\overline{S}(M_{2,3}(n))$
7	$(\mathbb{Z}/3\mathbb{Z})$	8	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$	9	$\{1\}$
10	$(\mathbb{Z}/12\mathbb{Z})$	11	$(\mathbb{Z}/3\mathbb{Z})$	12	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
13	$(\mathbb{Z}/3\mathbb{Z})$	14	$(\mathbb{Z}/12\mathbb{Z})$	15	$(\mathbb{Z}/15\mathbb{Z})$
16	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$	17	$(\mathbb{Z}/3\mathbb{Z})$	18	$(\mathbb{Z}/4\mathbb{Z})$
19	$(\mathbb{Z}/3\mathbb{Z})$	20	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$	21	$\{1\}$
22	$(\mathbb{Z}/12\mathbb{Z})$	23	$(\mathbb{Z}/3\mathbb{Z})$	24	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
25	$(\mathbb{Z}/3\mathbb{Z})$	26	$(\mathbb{Z}/12\mathbb{Z})$	27	$\{1\}$
28	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$	29	$(\mathbb{Z}/3\mathbb{Z})$	30	$(\mathbb{Z}/4\mathbb{Z})$
31	$(\mathbb{Z}/3\mathbb{Z})$	32	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$	33	$\{1\}$
34	$(\mathbb{Z}/12\mathbb{Z})$	35	$(\mathbb{Z}/3\mathbb{Z})$		

Figure 4.17. The Smith Group of $M_{2,3}(n)$.

Proof. Under the assumptions for n, we have that $D_2 = nI$ and:

$$D_3 \;=\; \begin{bmatrix} nI & 0 \\ 0 & \frac{n}{3} \end{bmatrix},$$

where the last column of D_3 corresponds to the orbit $\alpha_0 = [\frac{n}{3}, \frac{n}{3}, \frac{n}{3}]$. Thus, we deduce from $M'_{2,3}D_3 = D_2M_{2,3}$ that:

$$M'_{2,3} \;=\; M_{2,3} \begin{bmatrix} I & 0 \\ 0 & 3 \end{bmatrix}.$$

Therefore,

$$Col_{\mathbb{Z}}(M'_{2,3}) \subset \;\; Col_{\mathbb{Z}}(M_{2,3}) \;\; \subset \mathbb{Z}^{r_2(n)}.$$

Clearly, $r(Col_{\mathbb{Z}}(M'_{2,3})) = r(Col_{\mathbb{Z}}(M_{2,3})) = 0$ since these matrices have full rank. Hence, $H = \frac{Col_{\mathbb{Z}}(M_{2,3})}{Col_{\mathbb{Z}}(M'_{2,3})}$ has abelian rank 0 by proposition 4.1.21. Thus, one can construct the following exact sequence of torsion groups:

$$0 \to H \to S(M'_{2,3}) = \frac{\mathbb{Z}^{r_2(n)}}{Col_{\mathbb{Z}}(M'_{2,3})} \to S(M_{2,3}) = \frac{\mathbb{Z}^{r_2(n)}}{Col_{\mathbb{Z}}(M_{2,3})} \to 0.$$

By proposition 4.6.25, $|M'_{2,3}| = 3$. Hence, it suffices to show that $|H| = 3$ to show that $|M_{2,3}|$ is trivial.

Note that $M_{2,3}$ and $M'_{2,3}$ differ at only one column, namely the column given by α_0. Let $\beta_{2,3}$ be the $(2,3)$-basis of proposition 4.6.24. Since α_0 does not belong to $\beta_{2,3}$, clearly:

$$\begin{aligned} M_\beta &= M'_\beta, \\ Col_{\mathbb{Z}}(M_{2,3}) &= Col_{\mathbb{Z}}([M_\beta, M_{2,3}\alpha_0]), \\ Col_{\mathbb{Z}}(M'_{2,3}) &= Col_{\mathbb{Z}}([M_\beta, 3M_{2,3}\alpha_0]). \end{aligned}$$

Hence, $H = \langle M_{2,3}\alpha_0 \rangle$ has order either 3 or 1. We will show that $M_{2,3}\alpha_0$ has order 3 in H.

Suppose that $\langle M_{2,3}\alpha_0 \rangle$ is the trivial group, then there is an integral vector c and an integer d such that:

$$M_{2,3}\alpha_0 = M_\beta c + 3dM_{2,3}\alpha_0.$$

Hence, $(1+3d)M_{2,3}\alpha_0 = M_\beta c$. Since $M_\beta = M'_\beta$, M'_β has Smith Group with order 3, and $(1+3d)$ is relatively prime to 3; we conclude that $(1+3d)$ divides c. Therefore, $M_{2,3}\alpha_0 = M_\beta c' = M'_\beta c'$, where $c' = \frac{c}{1+3d}$ is integral.

Note that $M'_{2,3}\alpha_0 = 3[\frac{n}{3}, \frac{n}{3}^*]$. Hence, $M_{2,3}\alpha_0 = [\frac{n}{3}, \frac{n}{3}]$ and $j^T M_{2,3}\alpha_0 = 1$. On the other hand, $j^T M'_\beta c' = 3j^T c'$. This is a contradiction.

Therefore, H has order 3 and the result follows. □

Proposition 4.6.28. *Let* $\gcd(2,n)=2$ *and* $\gcd(3,n)=1$. *Then,*

$$\overline{S}(M_{2,3}(n)) \;=\; (\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/6\mathbb{Z}) \text{ or } (\mathbb{Z}/12\mathbb{Z}).$$

Proof. Based on the assumptions for n, we can deduce that $D_3 = nI$ and,

$$D_2 \;=\; \begin{bmatrix} nI & 0 \\ 0 & \frac{n}{2} \end{bmatrix},$$

where the last column of D_2 corresponds to the orbit $\alpha_0 = [\frac{n}{2}, \frac{n}{2}]$. Therefore, by using $M'_{2,3}D_3 = D_2 M_{2,3}$, we deduce,

$$\begin{bmatrix} I & 0 \\ 0 & 2 \end{bmatrix} M'_{2,3} \;=\; M_{2,3}.$$

Hence, the following inclusion of free $\mathbb{Z}$-modules holds,

$$Row_{\mathbb{Z}}(M_{2,3}) \subset \;\; Row_{\mathbb{Z}}(M'_{2,3}) \;\; \subset \mathbb{Z}^{r_3(n)}.$$

Therefore, we deduce:

$$0 \to H = \frac{Row_{\mathbb{Z}}(M'_{2,3})}{Row_{\mathbb{Z}}(M_{2,3})} \to \frac{\mathbb{Z}^{r_3(n)}}{Row_{\mathbb{Z}}(M_{2,3})} \to \frac{\mathbb{Z}^{r_3(n)}}{Row_{\mathbb{Z}}(M'_{2,3})} \to 0.$$

Note that H is the factor of two free $\mathbb{Z}$-modules of the same abelian rank. Hence, H is torsion. Also, note that the torsion part of $\frac{\mathbb{Z}^{r_3(n)}}{Row_{\mathbb{Z}}(M_{2,3})}$ is $\overline{S}(M_{2,3})$, and the torsion part of $\frac{\mathbb{Z}^{r_3(n)}}{Row_{\mathbb{Z}}(M'_{2,3})}$ is $\overline{S}(M'_{2,3})$. Hence, we can deduce by proposition 4.1.26 that:

$$0 \to H \to \overline{S}(M_{2,3}) \to \overline{S}(M'_{2,3}) \to 0.$$

By proposition 4.6.25, $\overline{S}(M'_{2,3}) = (\mathbb{Z}/6\mathbb{Z})$. We will show that $H = (\mathbb{Z}/2\mathbb{Z})$. From these calculations, we will deduce:

$$0 \to (\mathbb{Z}/2\mathbb{Z}) \to \overline{S}(M_{2,3}) \to (\mathbb{Z}/6\mathbb{Z}) \to 0.$$

Which gives the possible solutions $\overline{S}(M_{2,3}) = (\mathbb{Z}/12\mathbb{Z})$ or $\overline{S}(M_{2,3}) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$.

Therefore, it suffices to show that $H = (\mathbb{Z}/2\mathbb{Z})$. Clearly, the rows of $M_{2,3}$ are linearly independent. Also, $M_{2,3}$ and $M'_{2,3}$ different at the row corresponding to α_0. Let M' be $M'_{2,3}$ without the row corresponding to α_0 and m' be the row of $M'_{2,3}$ corresponding to α_0. Clearly,

$$\begin{aligned} Row_{\mathbb{Z}}(M'_{2,3}) &= Row_{\mathbb{Z}}(\begin{bmatrix} M' \\ m' \end{bmatrix}), \\ Row_{\mathbb{Z}}(M_{2,3}) &= Row_{\mathbb{Z}}(\begin{bmatrix} M' \\ 2m' \end{bmatrix}). \end{aligned}$$

Hence, $H = \frac{Row_{\mathbb{Z}}(M'_{2,3})}{Row_{\mathbb{Z}}(M_{2,3})} = \langle m' \rangle$ has order 2 or 1. Suppose H has order 1. Then, there are integral c and d such that:

$$m' = c^T M' + 2dm'.$$

Hence $0 = c^T M' + (2d+1)m'$. Since the rows $M'_{2,3}$ are linearly independent, it must be the case that $c = 0$ and $(2d+1) = 0$. Therefore, $d = \frac{1}{2}$ giving a contradiction to the assumption that it was integral.

Hence, H has order 2 and the result follows. □

Proposition 4.6.29. *Let* $\gcd(2,n) = 2$ *and* $\gcd(3,n) = 3$. *Then,*

$$\overline{S}(M_{2,3}(n)) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \text{ or } (\mathbb{Z}/4\mathbb{Z}).$$

Proof. Based on the assumptions for n, we deduce that:

$$\begin{aligned} D_2 &= \begin{bmatrix} nI & 0 \\ 0 & \frac{n}{2} \end{bmatrix}, \\ D_3 &= \begin{bmatrix} nI & 0 \\ 0 & \frac{n}{3} \end{bmatrix}, \end{aligned}$$

where the last column of D_2 corresponds to the orbit $\alpha_0 = [\frac{n}{2}, \frac{n}{2}]$, and the last column of D_3 corresponds to the orbit $\beta_0 = [\frac{n}{3}, \frac{n}{3}, \frac{n}{3}]$.

Because $M'_{2,3}D_3 = D_2M_{2,3}$, we deduce that:

$$\begin{aligned} F &= \begin{bmatrix} I & 0 \\ 0 & 2 \end{bmatrix} M'_{2,3} \\ &= M_{2,3} \begin{bmatrix} I & 0 \\ 0 & 3 \end{bmatrix}. \end{aligned}$$

Therefore, we can consider,

$$Row_{\mathbb{Z}}(F) \subset Row_{\mathbb{Z}}(M'_{2,3}) \subset \mathbb{Z}^{r_3(n)}.$$

Using the same analysis in the proof of proposition 4.6.28, we deduce an exact sequence:

$$0 \to (\mathbb{Z}/2\mathbb{Z}) \to \overline{S}(F) \to (\mathbb{Z}/6\mathbb{Z}) \to 0.$$

Hence, $\overline{S}(F) = (\mathbb{Z}/12\mathbb{Z})$ or $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$. Consider,

$$Col_{\mathbb{Z}}(F) \subset Col_{\mathbb{Z}}(M_{2,3}) \subset \mathbb{Z}^{r_2(n)}.$$

Using the same analysis in the proof of proposition 4.6.27, we deduce an exact sequence:

$$0 \to (\mathbb{Z}/3\mathbb{Z}) \to \overline{S}(F) \to \overline{S}(M_{2,3}) \to 0.$$

If $\overline{S}(F) = (\mathbb{Z}/12\mathbb{Z})$, then $\overline{S}(M_{2,3}) = (\mathbb{Z}/4\mathbb{Z})$. Also, if $\overline{S}(F) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/6\mathbb{Z})$, then $\overline{S}(M_{2,3}) = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. Hence, the result follows. □

4.6.5 The $(2,4)$ Case

We will proceed in a similar fashion as the $(2,3)$ case. First, we will introduce contrived projected relative $(2,4)$-pods to help us find a $(2,4)$-basis. Then, we will proceed to calculate the Smith Groups of $M'_{2,4}$ and $M_{2,4}$.

4.6.5.1 The Space $(\mathbf{C_4(X)})_\mathbf{0}$

By using the map of definition 4.6.15, we can partition all the 4-subsets' orbits into classes corresponding to the partitions of 4. Figure 4.18 shows theses classes along with the the membership conditions on the cyclic ordered partitions $[a_1, a_2, a_3, a_4]$.

Id	$\{p\}$	$\psi(K)$ where $a_i \geq 2$
$\{p_5\}$	1^4	$[a_1, a_2, a_3, a_4]$
$\{p_4\}$	$2^1 1^2$	$[1, a_1, a_2, a_3]$
$\{p_3\}$	$3^1 1^1$	$[1, 1, a_1, a_2]$
$\{p_2\}$	2^2	$[1, a_1, 1, a_2]$
$\{p_1\}$	4^1	$[1, 1, 1, 3^*]$

Figure 4.18. Classes of 4-subsets' orbits.

4.6.5.2 Projected Relative $(2,4)$-Pods

The following projected relative $(2,4)$-pods will be used in the calculation of the $(2,4)$-basis.

Proposition 4.6.30. *Let $a_1, a_2, a_4 \geq 2$ and $a_3 \geq 1$. Then,*

$$\begin{aligned}[a_1, a_2, a_3, a_4] \;=\; & [1, a_2, a_3, a_4 + a_1 - 1] + [1, a_1 + a_2, a_3, a_4 - 1] + [1, a_2 + a_3 - 1, a_4, a_1] \\ & -[a_1, a_2 + 1, a_3, a_4 - 1] - [1, a_1 + 1, a_2 + a_3 - 1, a_4 - 1] \\ & -[1, 1, a_2 + a_3 - 1, (a_2 + a_3)^* - 1] + [a_1, 2, a_2 + a_3 - 1, a_4 - 1] \ \textit{mod}\ 0.\end{aligned}$$

Proof. Let $A = \{x_1, x_2, x_3, x_4\} \in [a_1, a_2, a_3, a_4]$, and choose $B = \{y_1, y_2, y_3\}$ as shown in figure 4.19.

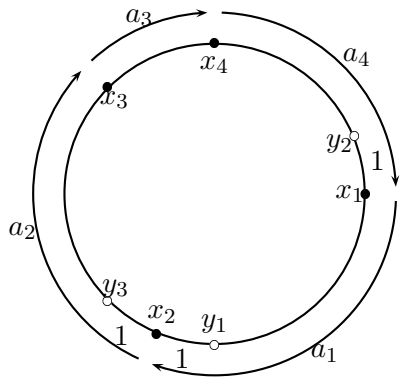

Figure 4.19. Relative $(2, 4)$-pod.

The result follows from the projected relative $(2, 4)$-pod that results from the relative $(2, 4)$-pod of figure 4.19. The calculation is shown in the table of figure 4.20.

T	$(-1)^{\lvert T\rvert}$	K	$\psi(K)$
000	$+1$	$\{x_1, x_2, x_3, x_4\}$	$[a_1, a_2, a_3, a_4]$
100	-1	$\{y_1, x_2, x_3, x_4\}$	$[1, a_2, a_3, a_4 + a_1 - 1]$
010	-1	$\{x_1, y_2, x_3, x_4\}$	$[1, a_1 + a_2, a_3, a_4 - 1]$
001	-1	$\{x_1, x_2, y_3, x_4\}$	$[1, a_2 + a_3 - 1, a_4, a_1]$
110	$+1$	$\{y_1, y_2, x_3, x_4\}$	$[a_1, a_2 + 1, a_3, a_4 - 1]$
011	$+1$	$\{x_1, y_2, y_3, x_4\}$	$[1, a_1 + 1, a_2 + a_3 - 1, a_4 - 1]$
101	$+1$	$\{y_1, x_2, y_3, x_4\}$	$[1, 1, a_2 + a_3 - 1, (a_2 + a_3)^* - 1]$
111	-1	$\{y_1, y_2, y_3, x_4\}$	$[a_1, 2, a_2 + a_3 - 1, a_4 - 1]$

Figure 4.20. Projected relative $(2, 4)$-pod.

□

Proposition 4.6.31. *Let* $2 \leq a \leq n-5$. *Then,*

$$\begin{aligned} 0 \;=\; & [1,1,a,a^*-2]-[1,a-1,1,a^*-1]-[1,1,1,3^*]-[1,a+1,1,a^*-3] \\ & +[2,1,a-1,a^*-2]+[1,1,a+2,a^*-4]+[a,1,1,a^*-2] \\ & -[2,a,2,a^*-4] \ \mathit{mod}\ 0. \end{aligned}$$

Proof. Let $A=\{x_1,x_2,x_3,x_4\}\in[1,1,a,a^*-2]$, and choose $B=\{y_1,y_2,y_3\}$ as shown in the relative $(2,4)$-pod of figure 4.21.

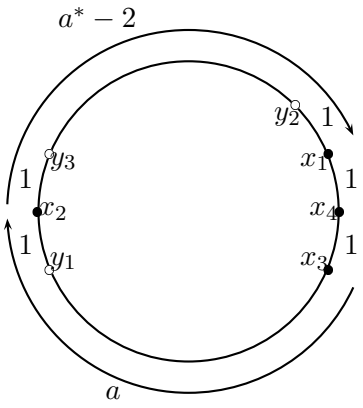

Figure 4.21. Relative $(2,4)$-pod.

The result follows from the projected relative $(2,4)$-pod that results from the relative $(2,4)$-pod of figure 4.21. The calculation is shown in the table of figure 4.22.

□

Proposition 4.6.32. *Let* $3 \leq a \leq n-4$. *Then,*

$$\begin{aligned} 0 \;=\; & [1,1,a,a^*-2]-[1,a,1,a^*-2]-[1,1,1,3^*]-[1,a,1,a^*-2] \\ & +[1,1,a,a^*-2]+[1,2,a-2,a^*-1]+[1,1,a^*-2,a] \\ & -[2,a-2,2,a^*-2] \ \mathit{mod}\ 0. \end{aligned}$$

Proof. Let $A=\{x_1,x_2,x_3,x_4\}\in[1,1,a,a^*-2]$, and choose $B=\{y_1,y_2,y_3\}$ as shown in the relative $(2,4)$-pod of figure 4.21.

T	$(-1)^{\lvert T\rvert}$	K	$\psi(K)$
000	$+1$	$\{x_1, x_2, x_3, x_4\}$	$[1, 1, a, a^* - 2]$
100	-1	$\{y_1, x_2, x_3, x_4\}$	$[1, a - 1, 1, a^* - 1]$
010	-1	$\{x_1, y_2, x_3, x_4\}$	$[1, 1, 1, 3^*]$
001	-1	$\{x_1, x_2, y_3, x_4\}$	$[1, a + 1, 1, a^* - 3]$
110	$+1$	$\{y_1, y_2, x_3, x_4\}$	$[2, 1, a - 1, a^* - 2]$
011	$+1$	$\{x_1, y_2, y_3, x_4\}$	$[1, 1, a + 2, a^* - 4]$
101	$+1$	$\{y_1, x_2, y_3, x_4\}$	$[a, 1, 1, a^* - 2]$
111	-1	$\{y_1, y_2, y_3, x_4\}$	$[2, a, 2, a^* - 4]$

Figure 4.22. Projected relative $(2, 4)$-pod.

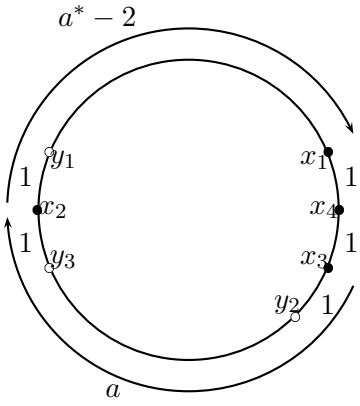

Figure 4.23. Relative $(2, 4)$-pod.

The result follows from the projected relative $(2,4)$-pod that results from the relative $(2,4)$-pod of figure 4.23. The calculation is shown in the table of figure 4.24.

T	$(-1)^{\lvert T\rvert}$	K	$\psi(K)$
000	$+1$	$\{x_1, x_2, x_3, x_4\}$	$[1, 1, a, a^* - 2]$
100	-1	$\{y_1, x_2, x_3, x_4\}$	$[1, a, 1, a^* - 2]$
010	-1	$\{x_1, y_2, x_3, x_4\}$	$[1, 1, 1, 3^*]$
001	-1	$\{x_1, x_2, y_3, x_4\}$	$[1, a, 1, a^* - 2]$
110	$+1$	$\{y_1, y_2, x_3, x_4\}$	$[1, 1, a, a^* - 2]$
011	$+1$	$\{x_1, y_2, y_3, x_4\}$	$[1, 2, a - 2, a^* - 1]$
101	$+1$	$\{y_1, x_2, y_3, x_4\}$	$[1, 1, a^* - 2, a]$
111	-1	$\{y_1, y_2, y_3, x_4\}$	$[2, a - 2, 2, a^* - 2]$

Figure 4.24. Projected relative $(2,4)$-pod.

□

4.6.5.3 Finding a $(2,4)$-Basis

The technique that we will use is the same as the one used for finding a $(2,3)$-basis. Using the classification of 4-subsets' orbits of figure 4.18, we will reduce any cyclic ordered partition of class $\{p_5\}$ to 0 mod $\{p_1\}, \ldots, \{p_4\}$. Then, we will proceed to reduce every cyclic ordered partition of class $\{p_4\}$ to 0 mod $\{p_1\}, \ldots, \{p_3\}$. From the classes $\{p_1\}, \ldots, \{p_3\}$, we will find a $(2,4)$-basis.

Before we start the reductions, we will state a lemma that will help us with our calculations.

Lemma 4.6.33. *Let $[a_1, a_2, a_3, a_4]$ be cyclic ordered partition. Then,*

1. The value of $M'_{2,4}$ is

$$\begin{aligned} M'_{2,4}[a_1, a_2, a_3, a_4] &= [a_1, a_1^*] + [a_2, a_2^*] + [a_3, a_3^*] + [a_4, a_4^*] \\ &\quad + [a_1 + a_2, (a_1 + a_2)^*] + [a_1 + a_4, (a_1 + a_4)^*]. \end{aligned}$$

2. The following symmetries hold:

$$\begin{aligned} M'_{2,4}[a_1, a_2, a_3, a_4] &= M'_{2,4}[a_1, a_4, a_3, a_2] \\ &= M'_{2,4}[a_3, a_2, a_1, a_4]. \end{aligned}$$

Proof. Clearly, part 2 is an application of part 1. Hence, it suffices to show part 1.

Let $\{x_1, x_2, x_3, x_4\} \in [a_1, a_2, a_3, a_4]$ be such that: $a_1 = x_2 - x_1, a_2 = x_3 - x_2, a_3 = x_4 - x_3, a_4 = n - x_4 + x_1$. Clearly,

$$\begin{aligned} W_{2,4}\{x_1, x_2, x_3, x_4\} &= \{x_1, x_2\} + \{x_2, x_3\} + \{x_3, x_4\} + \{x_4, x_1\} \\ &\quad + \{x_1, x_3\} + \{x_2, x_4\}. \end{aligned}$$

Part 1 follows by applying proposition 4.3.40 to the above equation. □

Our first goal is to reduce the elements of the class $\{p_5\}$. The next proposition shows the reduction.

Proposition 4.6.34. *Let $[a_1, a_2, a_3, a_4] \in \{p_5\}$, i.e., $a_i \geq 2$. Then,*

$$[a_1, a_2, a_3, a_4] = 0 \ mod \ \{p_1\}, \ldots, \{p_4\}.$$

Proof. By applying proposition 4.6.30 to $[a_1, a_2, a_3, a_4]$, we deduce:

$$\begin{aligned} [a_1, a_2, a_3, a_4] &= [a_1, 2, (a_2 + a_3) - 1, a_4 - 1] \\ &\quad - [a_1, a_2 + 1, a_3, a_4 - 1] \bmod \{p_1\}, \cdots \{p_4\}. \end{aligned} \tag{4.14}$$

If $a_4 - 1 = 1$, then were are done. Suppose that $a_4 - 1 \geq 2$. By applying Equation

(4.14) to $[a_1, 2, (a_2 + a_3) - 1, a_4 - 1] = [a_2 + a_3 - 1, a_4 - 1, a_1, 2]$, we deduce:

$$\begin{aligned}[a_2 + a_3 - 1, a_4 - 1, a_1, 2] &= [a_2 + a_3 - 1, 2, a_1 + a_4 - 2, 1] - [a_2 + a_3 - 1, a_4, a_1, 1] \\ &= 0 \bmod \{p_1\}, \ldots, \{p_4\}.\end{aligned}$$

Hence, Equation (4.14) reduces to:

$$[a_1, a_2, a_3, a_4] = -[a_1, a_2 + 1, a_3, a_4 - 1] \bmod \{p_1\}, \cdots \{p_4\}.$$

Clearly, one can apply the above equation to itself $(a_4 - 1)$ times to deduce:

$$\begin{aligned}[a_1, a_2, a_3, a_4] &= \pm[a_1, a_2 + a_4 - 1, a_3, 1] \\ &= 0 \bmod \{p_1\}, \cdots \{p_4\}.\end{aligned}$$

Hence, the result follows. □

We proceed to reduce cyclic ordered partitions in the class $\{p_4\}$.

Proposition 4.6.35. *Let $a_1, a_2, a_4 \geq 2$, and $[a_1, a_2, 1, a_4] \in \{p_4\}$. Then,*

$$[a_1, a_2, 1, a_4] = 0 \text{ mod } \{p_1\}, \ldots, \{p_3\}.$$

Proof. When we apply proposition 4.6.30 to $[a_1, a_2, 1, a_4]$, we deduce:

$$\begin{aligned}[a_1, a_2, 1, a_4] &= [1, a_2, a_4, a_1] \\ &\quad -[a_1, a_2 + 1, 1, a_4 - 1] - [1, a_1 + 1, a_2, a_4 - 1] \\ &\quad +[a_1, 2, a_2, a_4 - 1] \bmod \{p_1\}, \ldots, \{p_3\}.\end{aligned} \tag{4.15}$$

Without loss of generality, assume that $a_4 - 1 \geq 2$. By applying the above congruence

to $[a_2, a_4 - 1, a_1, 2] = [a_1, 2, a_2, a_4 - 1]$, we deduce:

$$\begin{aligned}[a_2, a_4 - 1, a_1, 2] &= [1, a_4 - 1, a_1, a_2 + 1] \\ &\quad + [1, a_4 + a_1 - 2, 2, a_2] - [a_2, a_4, a_1, 1] \\ &\quad + [a_2, 2, a_4 + a_1 - 2, 1] \bmod \{p_1\}, \ldots, \{p_3\}.\end{aligned} \tag{4.16}$$

By substituting congruence 4.16 into congruence 4.15, we deduce that if $a_4 \geq 3$, then:

$$\begin{aligned}[a_1, a_2, 1, a_4] &= 2[1, a_2, 2, a_4 + a_1 - 2] \\ &\quad - [1, a_1 + 1, a_2, a_4 - 1] \bmod \{p_1\}, \ldots, \{p_3\}.\end{aligned} \tag{4.17}$$

We proceed by cases that depend on the size of a_4.

Case $\mathbf{a_4 = 2}$. By use of lemma 4.6.33, we can assume that both $a_2 = 2$ and $a_4 = 2$. Otherwise, we can reduce to the case $a_3 \geq 3$. Hence, it suffices to reduce $[5^*, 2, 1, 2]$.

By applying congruence 4.15 to $[5^*, 2, 1, 2]$, we deduce that:

$$\begin{aligned}[5^*, 2, 1, 2] &= [1, 2, 2, 5^*] - [5^*, 3, 1, 1] - [1, 4^*, 2, 1] + [5^*, 2, 2, 1] \\ &= [1, 2, 2, 5^*] + [5^*, 2, 2, 1] \bmod \{p_1\}, \ldots, \{p_3\}.\end{aligned}$$

By application of lemma 4.6.33, $[1, 2, 2, 5^*] = [2, 2, 1, 5^*] = [5^*, 2, 2, 1] \bmod 0$. Hence, the above congruence yields $[5^*, 2, 1, 2] = 2[1, 2, 2, 5^*] \bmod \{p_1\}, \ldots, \{p_3\}$.

We proceed to reduce $[1, 2, 2, 5^*]$ by applying congruence 4.13 to $[2, 5^*, 1, 2]$.

$$\begin{aligned}[2, 5^*, 1, 2] &= [1, 5^*, 2, 2] - [2, 4^*, 1, 1] - [1, 3, 5^*, 1] + [2, 2, 5^*, 1] \\ &= [1, 5^*, 2, 2] + [1, 2, 2, 5^*] \bmod \{p_1\}, \ldots, \{p_3\}.\end{aligned}$$

Note that $[1, 5^*, 2, 2] = [1, 2, 2, 5^*] \bmod \{p_1\}, \ldots, \{p_3\}$ by lemma 4.6.33. Hence, it follows that $[2, 5^*, 1, 2] = 2[1, 2, 2, 5^*] \bmod \{p_1\}, \ldots, \{p_3\}$.

Note that $[1, 2, 2, 5^*] = [2, 5^*, 1, 2] \bmod 0$ by lemma 4.6.33. Thus, $[1, 2, 2, 5^*] = 2[1, 2, 2, 5^*] \bmod \{p_1\}, \ldots, \{p_3\}$ and therefore $[1, 2, 2, 5^*] = 0 \bmod \{p_1\}, \ldots, \{p_3\}$.

Hence, $[2, 5^*, 1, 2] = 0 \bmod \{p_1\}, \ldots, \{p_3\}$, and the result follows.

Case $\mathbf{a_4 \geq 3}$. Suppose that in congruence 4.17, we have shown that $[1, a_2, 2, a_4 + a_1 - 2] = 0 \bmod \{p_1\}, \ldots, \{p_3\}$. Then, it will follow that:

$$[a_1, a_2, 1, a_4] \;=\; -[1, a_1 + 1, a_2, a_4 - 1] \bmod \{p_1\}, \ldots, \{p_3\}.$$

By applying the above congruence $(a_4 - 1)$ times to itself, we deduce that:

$$\begin{aligned} [a_1, a_2, 1, a_4] &= \pm[1, a_1 + a_4 - 1, a_2, 1] \\ &= 0 \bmod \{p_1\}, \ldots, \{p_3\}. \end{aligned}$$

Therefore, it suffices to show that $[1, a_2, 2, a_4 + a_1 - 2] = 0 \bmod \{p_1\}, \ldots, \{p_3\}$. We will show this in lemma 4.6.36. □

Lemma 4.6.36. *Let $a, b \geq 2$. Then,*

$$[1, a, 2, b] \;=\; 0 \textit{ mod } \{p_1\}, \ldots, \{p_3\}.$$

Proof. Clearly, because $[1, a, 2, b]$ is a cyclic ordered partition, we have $[1, a, 2, b] = [2, b, 1, a]$. By applying congruence 4.15 to $[2, b, 1, a]$, we deduce:

$$[2, b, 1, a] \;=\; 2[1, b, 2, a] - [1, 3, b, a - 1] \bmod \{p_1\}, \ldots, \{p_3\}.$$

By lemma 4.6.33, $[1, b, 2, a] = [2, b, 1, a] \bmod 0$, and hence $\bmod \{p_1\}, \ldots, \{p_3\}$. Thus, the above congruence yields:

$$[2, b, 1, a] \;=\; [1, 3, b, a - 1] \bmod \{p_1\}, \ldots, \{p_3\}.$$

It suffices to reduce $[1, 3, b, a - 1]$ to $0 \bmod \{p_1\}, \ldots, \{p_3\}$.

Clearly, $[1, 3, b, a - 1] = [b, a - 1, 1, 3]$. Without loss of generality, we can assume

that $a-1 \geq 2$. Hence, we can apply congruence 4.15 to $[b, a-1, 1, 3]$ to deduce:

$$[b, a-1, 1, 3] \;=\; 2[1, a-1, 2, b+1] - [1, b+1, a-1, 2] \bmod \{p_1\}, \ldots, \{p_3\}.$$

We will show that $2[1, a-1, 2, b+1] = [1, b+1, a-1, 2] \bmod \{p_1\}, \ldots, \{p_3\}$. This will give the result.

By lemma 4.6.33, $[1, b+1, a-1, 2] = [a-1, b+1, 1, 2] \bmod \{p_1\}, \ldots, \{p_3\}$. By applying congruence 4.15 to $[a-1, b+1, 1, 2]$, we deduce that:

$$\begin{aligned} [a-1, b+1, 1, 2] &= 2[1, b+1, 2, a-1] + [1, a, b+1, 1] \\ &= 2[1, b+1, 2, a-1] \bmod \{p_1\}, \ldots, \{p_3\}. \end{aligned}$$

By lemma 4.6.33, $[1, b+1, 2, a-1] = [1, a-1, 2, b+1] \bmod \{p_1\}, \ldots, \{p_3\}$. Hence, $[1, b+1, a-1, 2] = [a-1, b+1, 1, 2] = 2[1, a-1, 2, b+1] \bmod \{p_1\}, \ldots, \{p_3\}$.

Thus, the result follows. □

Having shown that any cyclic ordered partition of class $\{p_4\}$ is reduced to 0 mod $\{p_1\}, \ldots, \{p_3\}$; we will proceed to find a $(2,4)$-basis.

We will first establish a congruence equation, given by lemma 4.6.37, among the cyclic ordered partitions of class $\{p_3\}$. By using lemma 4.6.37, we will be able to calculate a $(2,4)$-basis.

Lemma 4.6.37. *Let $5 \leq a \leq n-4$. Then, the following holds mod $\{p_1\}, \{p_2\}$,*

$$[1, 1, a, a^* - 2] \;=\; 2[1, 1, a-2, a^*] - [1, 1, a-4, a^* + 2].$$

Proof. This will be a long argument, so we will summarize the first step. By using the projected relative $(2,4)$-pods found in propositions 4.6.35 and 4.6.32), we will deduce the following congruence mod $\{p_1\}, \{p_2\}$ for $4 \leq a \leq n-4$:

$$2([1, 1, a, a^* - 2] - [1, 1, a-2, a^*]) = [2, 1, a-3, a^*] - [1, 2, a-2, a^* - 1]. \quad (4.18)$$

We will proceed to reduce the right-hand side of the above congruence.

By using the explicit definition of $M'_{2,4}$, or by applying lemma 4.6.33; we calculate,

$$\begin{aligned} M'_{2,4}([2,1,a-3,a^*]-[1,2,a-2,a^*-1]) &= [a-3,(a-3)^*] \\ &\quad -[a+1,(a+1)^*], \end{aligned} \tag{4.19}$$

$$M'_{2,4}([1,1,a,a^*-2]-[1,a,1,a^*-2]) = [2,2^*]-[a+1,(a+1)^*]. \tag{4.20}$$

Clearly, $a-4 \geq 1$, since $a \geq 5$. By substituting $a = a-4$ in Equation (4.20), we deduce:

$$M'_{2,4}([1,1,a-4,a^*+2]-[1,a-4,1,a^*+2]) = [2,2^*]-[a-3,(a-3)^*]. \tag{4.21}$$

Clearly, Equation (4.20) minus Equation (4.19) yields $[2,2^*]-[a-3,(a-3)^*]$ on the right-hand side. Hence, Equation (4.20) minus Equation (4.19) must equal the left-hand side of Equation (4.21). Summarizing, we have shown that,

$$M'_{2,4}([1,1,a-4,a^*+2]-[1,a-4,1,a^*+2]) = [2,2^*]-[a-3,(a-3)^*],$$

and, we have shown,

$$\begin{aligned} [2,2^*]-[a-3,(a-3)^*] = M'_{2,4}([1,1,a,a^*-2]-[1,a,1,a^*-2]) \\ - M'_{2,4}([2,1,a-3,a^*]-[1,2,a-2,a^*-1]). \end{aligned}$$

Hence, we can show mod 0,

$$\begin{aligned} [2,1,a-3,a^*]-[1,2,a-2,a^*-1] &= [1,1,a,a^*-2]-[1,a,1,a^*-2] \\ &\quad -([1,1,a-4,a^*+2]-[1,a-4,1,a^*+2]). \end{aligned}$$

Thus, we deduce mod $\{p_1\}, \{p_2\}$ that,

$$\begin{aligned} 2([1,1,a,a^*-2]-[1,1,a-2,a^*]) &= [2,1,a-3,a^*]-[1,2,a-2,a^*-1] \\ &= [1,1,a,a^*-2]-[1,1,a-4,a^*+2]. \end{aligned}$$

Clearly, the result follows by an algebraic manipulation of the above congruence.

Therefore, it suffices to show congruence 4.18. Clearly, by lemma 4.6.33, $[1,1,a,a^*-2] = [1,1,a^*-2,a]$. Hence, proposition 4.6.31 yields the following congruence mod 0 whenever $3 \leq a \leq n-4$:

$$\begin{aligned} 3[1,1,a,a^*-2]-2[1,a,1,a^*-2]-[1,1,1,3^*] \\ +[1,2,a-2,a^*-1]-[2,a-2,2,a^*-2] &= 0. \end{aligned} \tag{4.22}$$

Similarly, proposition 4.6.32 yields the following mod 0, whenever $2 \leq a \leq n-5$:

$$\begin{aligned} 2[1,1,a^*-2,a]-[1,a-1,1,a^*-1]-[1,1,1,3^*] \\ -[1,a+1,1,a^*-3]+[2,1,a-1,a^*-2]+[1,1,a+2,a^*-4] \\ -[2,a,2,a^*-4] &= 0. \end{aligned} \tag{4.23}$$

By letting $a = a-2$ in congruence 4.23, we deduce the following mod 0, whenever $4 \leq a \leq n-3$:

$$\begin{aligned} 2[1,1,a^*,a-2]-[1,a-3,1,a^*+1]-[1,1,1,3^*] \\ -[1,a-1,1,a^*-1]+[2,1,a-3,a^*]+[1,1,a,a^*-2] \\ -[2,a-2,2,a^*-2] &= 0. \end{aligned} \tag{4.24}$$

By setting the left-hand side of congruence 4.24 equal to the left-hand side of con-

gruence 4.22, we deduce the following mod 0, whenever $4 \leq a \leq n-4$:

$$\begin{aligned} 2[1,1,a,a^*-2]-2[1,a,1,a^*-2]+[1,2,a-2,a^*-1] \\ -2[1,1,a^*,a-2]+[1,a-3,1,a^*+1]+[1,a-1,1,a^*-1] \\ -[2,1,a-3,a^*] &= 0. \end{aligned}$$

Hence, we deduce the following mod $\{p_1\},\{p_2\}$, whenever $4 \leq a \leq n-4$:

$$\begin{aligned} 2[1,1,a,a^*-2]+[1,2,a-2,a^*-1]-2[1,1,a^*,a-2] \\ -[2,1,a-3,a^*] &= 0. \end{aligned}$$

The above congruence is clearly equivalent to congruence 4.18. □

Corollary 4.6.38. *Let $n \geq 7$. Define,*

$$\begin{aligned} \beta_0 &= \{[1,1,a,a^*-2]|a=1,\ldots,\frac{n-2}{2}\} \\ &\quad \cup\{[1,1,2,4^*],[1,1,3,5^*],[1,1,4,6^*]\}, \\ \beta_1 &= \{[1,1,a,a^*-2]|a=1,\ldots,\frac{n-3}{2}\} \\ &\quad \cup\{[1,1,2,4^*],[1,1,3,5^*],[1,1,4,6^*]\}. \end{aligned}$$

Then,

1. *If n is odd, then β_1 is a generating set for the column space of $M'_{2,4}$.*
2. *If n is even, then β_0 is a generating set for the column space of $M'_{2,4}$.*

Proof. It suffices to reduce the cyclic ordered partitions of class $\{p_3\}$.

Clearly, by repeated applications of lemma 4.6.37, we can deduce for a an odd integer, with $5 \leq a \leq n-4$, there is an integer m such that:

$$\begin{aligned} [1,1,a,a^*-2] &= m[1,1,5,7^*] \\ &= m(2[1,1,3,5^*]-[1,1,1,3^*]) \\ &= 2m[1,1,3,5^*] \bmod \{p_1\},\{p_2\}. \end{aligned}$$

Similarly, by repeated applications of lemma 4.6.37, we can deduce for a an even integer, with $5 \leq a \leq n-4$, there is an integer m' such that:

$$\begin{aligned}[1,1,a,a^*-2] &= m'[1,1,6,7^*] \\ &= m'(2[1,1,4,6^*]-[1,1,2,4^*]) \bmod \{p_1\},\{p_2\}.\end{aligned}$$

Hence, we have reduced all cyclic ordered partitions of the form $[1,1,a,a^*-2]$, with $5 \leq a \leq n-4$, to the generating set β_0 or β_1 – depending on the parity of n.

It suffices to reduce the cyclic ordered partition $[1,1,3^*,1]$. Clearly, this is 0 mod $\{p_1\},\{p_2\}$. □

We proceeed to calculate a $(2,4)$-basis.

Proposition 4.6.39. *Let $n \geq 7$. Then,*

1. *Let n be odd, and $\beta_{2,4}$ be defined as:*

$$\begin{aligned}\beta_{2,4} &= \{[1,a,1,a^*-2] | a = 1,\ldots,\frac{n-3}{2}\} \\ &\quad \cup \{[1,1,3,5^*]\}.\end{aligned}$$

   Then, $\beta_{2,4}$ is a $(2,4)$-basis for $M'_{2,4}$.

2. *Let n be even, and $\beta_{2,4}$ be defined as:*

$$\begin{aligned}\beta_{2,4} &= \{[1,a,1,a^*-2] | a = 1,\ldots,\frac{n-2}{2}\} \\ &\quad \cup \{[1,1,2,4^*]\}.\end{aligned}$$

   Then, $\beta_{2,4}$ is a $(2,4)$-basis for $M'_{2,4}$.

Proof. By using the generating sets provided by corollary 4.6.38, we will give a $(2,4)$-basis by reducing these sets to sets of minimal size, i.e., of size $r_2(n)$. This will force the reduced generating set to be a $(2,4)$-basis. We proceed by considering cases that depend on the parity of n.

Case n is odd. Clearly, by lemma 4.6.33, $[1,1,2,4^*] = [1,1,4^*,2]$ and $[1,1,4,6^*] = [1,1,6^*,4]$ mod 0. Because n is odd, $4^* = n-4$ and $6^* = n-6$ are also odd. Hence, using a similar reasoning as corollary 4.6.38, we can apply lemma 4.6.37 repeatedly to deduce the existence of integral m_1 and m_2 such that mod $\{p_1\}, \{p_2\}$:

$$\begin{aligned}
[1,1,2,4^*] &= [1,1,4^*,2] \\
&= 2m_1[1,1,3,5^*], \\
[1,1,4,6^*] &= [1,1,6^*,4] \\
&= 2m_2[1,1,3,5^*].
\end{aligned}$$

Thus, $\beta_{2,4}$ is indeed a generating set for the Column Space of $M'_{2,4}$. Since $\beta_{2,4}$ has minimal size, it must be a $(2,4)$-basis.

Case n is even. It suffices to reduce $[1,1,3,5^*]$ and $[1,1,4,6^*]$ to show that $\beta_{2,4}$ is a generating set for the column space of $M'_{2,4}$. Because $\beta_{2,4}$ has minimal size, i.e., has size $r_2(n)$; it will follow that $\beta_{2,4}$ is a $(2,4)$-basis.

Consider the following equations that will be proven in lemma 4.6.40.

$$\begin{aligned}
[1,1,3,5^*] &= [1,2,1,4^*] + 2\sum_{a=4}^{\frac{n}{2}-2}(-1)^a[1,a,1,(a+2)^*] \qquad (4.25) \\
&\quad -[1,3,1,5^*] + (-1)^{\frac{n}{2}-1}[1,\frac{n}{2}-1,1,\frac{n}{2}-1] \text{ mod } 0, \\
[1,1,4,6^*] &= [1,1,2,4^*] - [1,2,1,4^*] + [1,3,1,5^*] \qquad (4.26) \\
&\quad -[1,4,1,6^*] + 2\sum_{a=5}^{\frac{n}{2}-2}(-1)^a[1,a,1,(a+2)^*] \\
&\quad -(-1)^{\frac{n}{2}-1}[1,\frac{n}{2}-1,1,\frac{n}{2}-1] \text{ mod } 0.
\end{aligned}$$

where Equation (4.25) holds for $n \geq 16$, and Equation (4.26) holds for $n \geq 18$.

Equation (4.25) shows that $[1,1,3,5^*] = 0$ mod $\{p_1\}, \{p_2\}$ for $n \geq 16$. We leave it as an exercise to check this congruence for $8 \leq n \leq 14$.

Similary, Equation (4.26) shows that $[1,1,4,6^*] = [1,1,2,4^*]$ mod $\{p_1\}, \{p_2\}$ for $n \geq 18$. We leave it as an exercise to check this congruence for $8 \leq n \leq 16$.

Hence, it follows that $\beta_{2,4}$ is indeed a generating set. Therefore the conclusion follows. □

Lemma 4.6.40. *The following hold mod* 0 *using* $M'_{2,4}$.

1. *Let* $n \geq 16$. *Then,*

$$\begin{aligned}[1,1,3,5^*] &= [1,2,1,4^*] + 2\sum_{a=4}^{\frac{n}{2}-2}(-1)^a[1,a,1,(a+2)^*] \\ &\quad -[1,3,1,5^*] + (-1)^{\frac{n}{2}-1}[1,\frac{n}{2}-1,1,\frac{n}{2}-1] \ mod\ 0.\end{aligned} \tag{4.27}$$

2. *Let* $n \geq 8$. *Then,*

$$\begin{aligned}[1,1,4,6^*] &= [1,1,2,4^*] - [1,2,1,4^*] + [1,3,1,5^*] \\ &\quad -[1,4,1,6^*] + 2\sum_{a=5}^{\frac{n}{2}-2}(-1)^a[1,a,1,(a+2)^*] \\ &\quad -(-1)^{\frac{n}{2}-1}[1,\frac{n}{2}-1,1,\frac{n}{2}-1] \ mod\ 0.\end{aligned} \tag{4.28}$$

Proof. We show part 1. It suffices to show that both sides of Equation (4.27) are the same when we apply $M'_{2,4}$.

By direct application of lemma 4.6.33, we deduce for $\frac{n}{2}-2 \geq 4$ that:

$$\sum_{a=4}^{\frac{n}{2}-2}(-1)^a M'_{2,4}[1,a,1,(a+2)^*] =$$
$$2[1,1^*]f(n) + \sum_{a=4}^{\frac{n}{2}-2}(-1)^a([a,a^*] + 2[a+1,(a+1)^*] + [a+2,(a+2)^*]),$$

where,

$$f(n) = \begin{cases} 0 & \text{if } n = 2 \bmod 4, \\ 1 & \text{if } n = 0 \bmod 4. \end{cases}$$

Also, a direct calculation yields:

$$\sum_{a=4}^{\frac{n}{2}-2}(-1)^a([a,a^*]+2[a+1,(a+1)^*]+[a+2,(a+2)^*]) = \\ [4,4^*]+[5,5^*]+(-1)^{\frac{n}{2}-2}\{[\frac{n}{2}-1,(\frac{n}{2}-1)^*]+[\frac{n}{2},(\frac{n}{2})^*]\},$$

whenever $\frac{n}{2}-2 \geq 6$, i.e., $n \geq 16$. Thus,

$$\begin{aligned}(-1)^{\frac{n}{2}-1}M'_{2,4}[1,\frac{n}{2}-1,1,\frac{n}{2}-1] \;+\; & 2\sum_{a=4}^{\frac{n}{2}-2}(-1)^a M'_{2,4}[1,a,1,(a+2)^*] \\ = \;& \{4f(n)-2(-1)^{\frac{n}{2}-2}\}[1,1^*]+2[4,4^*]+2[5,5^*] \\ = \;& 2[1,1^*]+2[4,4^*]+2[5,5^*], \qquad (4.29)\end{aligned}$$

where, we have used $4f(n)-2(-1)^{\frac{n}{2}-2}=2$ whenever n is even.

Independently of the above, by using lemma 4.6.33, we can calculate:

$$M'_{2,4}([1,1,3,5^*]-[1,2,1,4^*]+[1,3,1,5^*]) = 2[1,1^*]+2[4,4^*]+2[5,5^*]. \qquad (4.30)$$

By setting Equation (4.30) equal to Equation (4.29), we deduce the conclusion.

We show part 2. We will show that both sides of Equation (4.28) are the same.

Clearly, for $\frac{n}{2}-2 \geq 7$, i.e., $n \geq 18$; we deduce by using lemma 4.6.33 that:

$$\sum_{a=5}^{\frac{n}{2}-2}(-1)^a M'_{2,4}[1,a,1,(a+2)^*] = \\ -[5,5^*]-[6,6^*]+(-1)^{\frac{n}{2}-2}\{[\frac{n}{2}-1,(\frac{n}{2}-1)^*]+[\frac{n}{2},(\frac{n}{2})^*]\}+g(n)[1,1^*],$$

where,

$$g(n) \;=\; \begin{cases} -1 & \text{if } n=2 \bmod 4, \\ 0 & \text{if } n=0 \bmod 4. \end{cases}$$

Consider,

$$\begin{aligned}(-1)^{\frac{n}{2}-1}M'_{2,4}[1,\frac{n}{2}-1,1,\frac{n}{2}-1] &+ 2(\sum_{a=5}^{\frac{n}{2}-2}(-1)^a M'_{2,4}[1,a,1,(a+2)^*]) \\ &= -2[5,5^*]-2[6,6^*]+\{2(-1)^{\frac{n}{2}-1}+4g(n)\}[1,1^*] \\ &= -2[5,5^*]-2[6,6^*]-2[1,1^*], \qquad (4.31)\end{aligned}$$

where, we have used $2(-1)^{\frac{n}{2}-1}+4g(n)=-2$ whenever n is even.

Independently of the above, by using lemma 4.6.33, we can calculate:

$$\begin{aligned}M'_{2,4}([1,1,4,6^*]-[1,2,1,4^*]+[1,3,1,5^*])+M'_{2,4}(-[1,4,1,6^*]+[1,1,2,4^*]) \\ = -2[5,5^*]-2[6,6^*]-2[1,1^*]. \quad (4.32)\end{aligned}$$

By setting Equation (4.31) equal to Equation (4.32), we deduce the conclusion. □

4.6.5.4 The Smith Group of $\mathbf{M'_{2,4}}$ and $\mathbf{M_{2,4}}$

The $(2,4)$-basis of proposition 4.6.39 can be used to calculate the Smith Group of $M'_{2,4}$. The following proposition shows this result.

Proposition 4.6.41. *Let $n \geq 7$. Then, $\overline{S}(M_{2,4}(n)') = (\mathbb{Z}/6\mathbb{Z})$.*

Proof. We will proceed by cases. In each case, we will calculate the determinant of M'_β, where M'_β is the matrix consisting columns of $M'_{2,4}$ that correspond to $\beta_{2,4}$. Because there is a unique abelian group of order 6, the result will follow.

Case n is odd. We will assume that $n \geq 11$, i.e., $\frac{n-1}{2} \geq 5$. The cases for $n = 7, 9$ will follow by direct calculation.

Order the members of $\beta_{2,4}$ in the following manner,

$$\{[1,1,3,5^*]\} \cup \{[1,a,1,(a+2)^*] \mid a = 1,\ldots,\frac{n-3}{2}\},$$

and order the 2-subsets' orbits canonical basis in the following manner,

$$\{[a, a^*] | a = 1, \ldots, \frac{n-1}{2}\}.$$

With respect to these orderings, M'_β has matrix representation:

$$A_m = \begin{bmatrix} 2 & 3 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 3 \end{bmatrix},$$

where $m = \frac{n-1}{2}$.

Because we are calculating the $det(A_m) = a_m$, we can perform elementary row and column operations without modifying the answer. Consider the following elementar column operation:

$$C_1 - C_2 + C_3 - C_4 \quad \rightarrow \quad C_1.$$

That is, Column 1 minus Column 2 plus Column 3 minus Column 4 store the result in Column 1. The resulting matrix A'_m, shown below, will have the same determinant

as A_m.

$$A'_m = \begin{bmatrix} 2 & 3 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 2 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 2 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 3 \end{bmatrix}.$$

Clearly, $a_m = det(A_m) = det(A'_m) = 2det(B'_m)$, where B'_m is given by:

$$B'_m = \begin{bmatrix} 1 & 3 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 3 \end{bmatrix}.$$

We apply the following Elementary Column operation to B'_m:

$$C_1 - C_2 \rightarrow C_1.$$

We get the following matrix B_m with the same determinant as B'_m.

$$B_m = \begin{bmatrix} 2 & 3 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 3 \end{bmatrix}.$$

Summarizing, $a_m = det(A_m) = 2det(B_m)$. Thus, it suffices to calculate $b_m = det(B_m)$.

Clearly, b_m can be calculated by performing a determinant minor expansion along the first row of B_m. Hence, we have:

$$\begin{aligned} b_m &= 2c_{m-1} - 3c_{m-2} + \cdots + 2(-1)^{(m-2)+1}c_2 \\ &\quad +2(-1)^{(m-1)+1}c_1 + 2(-1)^{m+1}, \end{aligned}$$

where $c_m = det(C_m)$, and C_m is given as the following $m \times m$ matrix:

$$C_m = \begin{bmatrix} 2 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 3 \end{bmatrix}.$$

By performing a determinant minor expansion along the first row of C_m, we deduce the following recursive formula:

$$c_m = 2c_{m-1} - c_{m-2},$$

where $c_1 = 3$ and $c_2 = 5$. It can be shown by induction that with these initial conditions, $c_m = 2m + 1$ for general m. By substituting this value of c_m into the previous formula for b_m, we deduce:

$$\begin{aligned} b_m &= 2(-1)^m\{c_1 - c_2 + \cdots + (-1)^m c_{m-1}\} + 2(-1)^{m+1} - c_{m-2} \\ &= 2(-1)^m\{\sum_{i=1}^{m-1}(-1)^{i+1}(2i+1)\} + 2(-1)^{m+1} - 2(m-2) - 1 \\ &= 2(-1)^m\{1 - (-1)^{m-1}m\} + 2(-1)^{m+1} - 2(m-2) - 1 \\ &= 2m - 2(m-2) - 1 \\ &= 3. \end{aligned}$$

Therefore, $a_m = 2b_m = 6$.

Case n is even. Order the members of $\beta_{2,4}$ in the following manner,

$$\{[1,1,2,4^*]\} \cup \{[1,a,1,(a+2)^*] | a = 1,\ldots,\frac{n-2}{2}\},$$

and order the canonical basis of the 2-subsets' orbits in the following manner,

$$\{[a,a^*] \mid a = 1,\ldots,\frac{n}{2}\}.$$

With respect to these orderings, M'_β has matrix representation:

$$A_m = \begin{bmatrix} 2 & 3 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 2 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 \end{bmatrix},$$

where $m = \frac{n}{2}$. Consider the following column operation:

$$C_1 + C_2 - C_3 \rightarrow C_1.$$

That is, Column 1 plus Column 2 minus Column 3 store the result in Column 1. The

resulting matrix A'_m, shown below, will have the same determinant as A_m.

$$A'_m = \begin{bmatrix} 3 & 3 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 3 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 \end{bmatrix}.$$

Clearly, $a_m = det(A_m) = det(A'_m) = 3det(B'_m)$, where B'_m is given by:

$$B'_m = \begin{bmatrix} 1 & 3 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 \end{bmatrix}.$$

Summarizing, $a_m = det(A_m) = 3det(B'_m)$. Thus, it suffices to calculate $b'_m = det(B'_m)$.

Clearly, b'_m can be calculated by performing a determinant minor expansion along

the first row of B'_m. Hence, we have:

$$\begin{aligned} b'_m &= d_{m-1} - 3d_{m-2} + \cdots + 2(-1)^{(m-2)+1}d_2 \\ &\quad +2(-1)^{(m-1)+1}d_1 + 2(-1)^{m+1}, \end{aligned}$$

where $d_m = det(D_m)$, and D_m is given as the following $m \times m$ matrix:

$$D_m = \begin{bmatrix} 2 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 \end{bmatrix}.$$

By performing a determinant minor expansion along the first row of D_m, we deduce the following recursive formula:

$$d_m = 2d_{m-1} - d_{m-2},$$

where $d_1 = 2$ and $d_2 = 2$. It can be shown by induction that with these initial conditions, $d_m = 2$ for general m. By substituting this value of d_m into the previous formula for b'_m, we deduce:

$$\begin{aligned} b'_m &= 2(-1)^m\{d_1 - d_2 + \cdots + (-1)^m d_{m-1}\} + 2(-1)^{m+1} - d_{m-2} - d_{m-1} \\ &= 4(-1)^m\{\sum_{i=1}^{m-1}(-1)^{i+1}\} + 2(-1)^{m+1} - 2 - 2 \\ &= 4(-1)^m f(m) + 2(-1)^{m+1} - 4, \end{aligned}$$

where,

$$f(m) \quad = \quad \begin{cases} 1 & \text{if } m \text{ is even,} \\ 0 & \text{else.} \end{cases}$$

Clearly, by using the value of $f(m)$, we can deduce that $b'_m = -2$ for all m. Hence, $a_m = 3b'_m = -6$ and the result follows. □

We proceed to calculate the Smith Group of $M_{2,4}$. The following table summarizes the result.

$\gcd(4,n)$	$\overline{S}(M_{2,4}(n))$
1	$(\mathbb{Z}/6\mathbb{Z})$
2	$(\mathbb{Z}/6\mathbb{Z})$
4	$(\mathbb{Z}/3\mathbb{Z})$

Figure 4.25. The Smith Group of $M_{2,4}(n)$.

Proposition 4.6.42. *Let* $\gcd(n,4) = 1$. *Then,* $\overline{S}(M_{2,4}(n)) = (\mathbb{Z}/6\mathbb{Z})$.

Proof. Because $\gcd(n,2) = 1 = \gcd(n,4)$, we must have $D_2 = nI$, and $D_4 = nI$. By considering $M'_{2,4}D_4 = D_2M_{2,4}$, and the previous equations for D_2 and D_4, we must have $M'_{2,4} = M_{2,4}$. The result follows from proposition 4.6.41. □

Proposition 4.6.43. *Let* $\gcd(n,4) = 2$. *Then,*

1. *The set* $\beta_{2,4}$ *is a* $(2,4)$*-basis for* $M_{2,4}$ *as well.*

2. *The following holds,* $\overline{S}(M_{2,4}) = (\mathbb{Z}/6\mathbb{Z})$.

Proof. Under the assumption for n, we can calculate:

$$\begin{aligned} D_2 &= \begin{bmatrix} nI & 0 \\ 0 & \frac{n}{2} \end{bmatrix}, \\ D_4 &= \begin{bmatrix} nI & 0 \\ 0 & \frac{n}{2}I \end{bmatrix}, \end{aligned}$$

where the last column of D_2 corresponds to $\alpha_0 = [\frac{n}{2}, \frac{n}{2}]$, and the last columns of D_4 corresponds to orbits of the form $\beta_0 = [a, b, a, b]$ with $a + b = \frac{n}{2}$. Define $X_n = \{[a, b, a, b] \mid a + b = \frac{n}{2}\}$. Because $M'_{2,4}D_4 = D_2M_{2,4}$, we can deduce:

$$\begin{bmatrix} I & 0 \\ 0 & 2 \end{bmatrix} M'_{2,4} = M_{2,4} \begin{bmatrix} I & 0 \\ 0 & 2I \end{bmatrix}.$$

Hence, we can partition the columns and rows of $M_{2,4}$ and $M'_{2,4}$ such that:

$$\begin{aligned} M'_{2,4} &= \begin{bmatrix} A & 2B \\ a & 2j^T \end{bmatrix}, \\ M_{2,4} &= \begin{bmatrix} A & B \\ 2a & 2j^T \end{bmatrix}, \end{aligned}$$

where the columns corresponding to $\begin{bmatrix} B \\ 2j^T \end{bmatrix}$ of $M_{2,4}$ are the columns corresponding to orbits in X_n, and the row corresponding to $\begin{bmatrix} a & 2j^T \end{bmatrix}$ of $M'_{2,4}$ is the row corresponding to the orbit $[\frac{n}{2}, \frac{n}{2}]$.

Clearly, $\beta_{2,4} \cap X_n = \{[1, \frac{n-2}{2}, 1, \frac{n-2}{2}]\}$. Let M_β be the columns of $M_{2,4}$ corresponding to $\beta_{2,4}$, and let M'_β be the columns of $M'_{2,4}$ corresponding to $\beta_{2,4}$. By the previous

decompositions of $M_{2,4}, M'_{2,4}$, we have the following decompositions of M'_β, M_β.

$$\begin{aligned} M_\beta &= \begin{bmatrix} A_1 & B_1 \\ 2a_1 & 2 \end{bmatrix}, \\ M'_\beta &= \begin{bmatrix} A_1 & 2B_1 \\ a_1 & 2 \end{bmatrix}. \end{aligned}$$

Claim 4.6.44. *$\beta_{2,4}$ is a $(2,4)$-basis for $M_{2,4}$.*

Proof. Let

$$M_{2,4}\Omega_K = \begin{bmatrix} B_2 \\ 2 \end{bmatrix},$$

be a column of $M_{2,4}$ corresponding to an element of $X_n \backslash \beta_{2,4}$.

Clearly, since $\beta_{2,4}$ is a $(2,4)$-basis for $M'_{2,4}$, there is an integral vector $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ such that:

$$\begin{bmatrix} A_1 & 2B_1 \\ a_1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 2B_2 \\ 2 \end{bmatrix}. \tag{4.33}$$

We can manipulate the previous equation algebraically to deduce:

$$\begin{bmatrix} A_1 & B_1 \\ 2a_1 & 2 \end{bmatrix} \begin{bmatrix} \frac{x_1}{2} \\ x_2 \end{bmatrix} = \begin{bmatrix} B_2 \\ 2 \end{bmatrix}.$$

It suffices to show that $\frac{x_1}{2}$ is integral to reduce Ω_K to the column space of $\beta_{2,4}$.

Let us consider Equation (4.33) mod 2:

$$\begin{aligned} M'_\beta \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} &= \begin{bmatrix} A_1 & 0 \\ a_1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \\ &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \end{aligned}$$

Hence, $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ is in the kernel of M'_β over $\mathbb{F}_2$. Because $\overline{S}(M'_\beta) = (\mathbb{Z}/6\mathbb{Z})$, it follows that $rk(M'_\beta) = r_2(n) - 1$ when M'_β is viewed as a map of $\mathbb{F}_2$-vector spaces. Therefore, the kernel of M'_β is one dimensional. Clearly, $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is also in the kernel of M'_β. Hence, mod 2, we must have:

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Therefore, 2 divides x_1.

It remains to show that for any $\Omega_K \in \sim X_n$, $M_{2,4}\Omega_K$ is in the column span of $\beta_{2,4}$. Consider $\Omega_K \in \sim X_n$. Clearly,

$$M_{2,4}\Omega_K = \begin{bmatrix} A_2 \\ 2a_2 \end{bmatrix},$$

Because $\beta_{2,4}$ is a $(2,4)$-basis for $M'_{2,4}$, there is an integral vector $\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ such that:

$$\begin{bmatrix} A_1 & 2B_1 \\ a_1 & 2 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} A_2 \\ a_2 \end{bmatrix}.$$

The previous equation is equivalent to:

$$\begin{bmatrix} A_1 & B_1 \\ a_1 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ 2y_2 \end{bmatrix} = \begin{bmatrix} A_2 \\ a_2 \end{bmatrix}.$$

By multiplying the previous equation by 2 on the last row, we deduce:

$$\begin{bmatrix} A_1 & B_1 \\ 2a_1 & 2 \end{bmatrix} \begin{bmatrix} y_1 \\ 2y_2 \end{bmatrix} = \begin{bmatrix} A_2 \\ 2a_2 \end{bmatrix}.$$

Hence, $M_{2,4}\Omega_K$ is in the column span of $\beta_{2,4}$. This proves claim 4.6.44. □

We resume to the proof of proposition 4.6.43. We show the second assertion. We will calculate the $det(M_\beta)$ as 6. The result will follow because there is only one abelian group of order 6.

Consider,

$$det(M_\beta) = 2det\left(\begin{bmatrix} A_1 & B_1 \\ a_1 & 1 \end{bmatrix}\right).$$

Similarly,

$$\begin{aligned} 6 &= det(M'_\beta) \\ &= 2det\left(\begin{bmatrix} A_1 & B_1 \\ a_1 & 1 \end{bmatrix}\right). \end{aligned}$$

Hence, $det(M_\beta) = 6$ and the result follows. □

Proposition 4.6.45. *Let* $\gcd(n, 4) = 4$. *Then,* $\overline{S}(M_{2,4}(n)) = (\mathbb{Z}/3\mathbb{Z})$.

Proof. Under the assumption for n, we can calculate:

$$\begin{aligned} D_2 &= \begin{bmatrix} nI & 0 \\ 0 & \frac{n}{2} \end{bmatrix}, \\ D_4 &= \begin{bmatrix} nI & 0 & 0 \\ 0 & \frac{n}{2}I & 0 \\ 0 & 0 & \frac{n}{4} \end{bmatrix}, \end{aligned}$$

where the last column of D_2 corresponds to $\alpha_0 = [\frac{n}{2}, \frac{n}{2}]$, the middle columns of D_4 corresponds to orbits of the form $\beta_0 = [a, b, a, b]$ with $a + b = \frac{n}{2}, a \neq b$, and the last column of D_4 corresponds to the orbit $\gamma_0 = [\frac{n}{4}, \frac{n}{4}, \frac{n}{4}, \frac{n}{4}]$. Define $X_n = \{[a, b, a, b] \mid a + b = \frac{n}{2}, a \neq b\}$.

Because $M'_{2,4}D_4 = D_2 M_{2,4}$, we can deduce:

$$\begin{bmatrix} I & 0 \\ 0 & 2 \end{bmatrix}, M'_{2,4} = M_{2,4} \begin{bmatrix} I & 0 & 0 \\ 0 & 2I & 0 \\ 0 & 0 & 4 \end{bmatrix}.$$

Using the equations above, we can partition the columns and rows of $M_{2,4}$ and $M'_{2,4}$ such that:

$$M'_{2,4} = \begin{bmatrix} A & 2B & 4C \\ a & 2j^T & 2 \end{bmatrix},$$
$$M_{2,4} = \begin{bmatrix} A & B & C \\ 2a & 2j^T & 1 \end{bmatrix},$$

where the columns corresponding to $\begin{bmatrix} B \\ 2j^T \end{bmatrix}$ of $M_{2,4}$ are the columns corresponding to orbits in X_n, the column corresponding to $\begin{bmatrix} C \\ 1 \end{bmatrix}$ of $M_{2,4}$ is the column corresponding to the orbit γ_0, and the row corresponding to $\begin{bmatrix} a & 2j^T & 2 \end{bmatrix}$ of $M'_{2,4}$ is the row corresponding to the orbit $[\frac{n}{2}, \frac{n}{2}]$.

Clearly, $\beta_{2,4} \cap X_n = \{[1, \frac{n-2}{2}, 1, \frac{n-2}{2}]\}$, and $\gamma_0 \notin \beta_{2,4}$. Let M_β be the columns of $M_{2,4}$ corresponding to $\beta_{2,4}$, and let M'_β be the columns of $M'_{2,4}$ corresponding to $\beta_{2,4}$. We have the decompositions:

$$M_\beta = \begin{bmatrix} A_1 & B_1 \\ 2a_1 & 2 \end{bmatrix},$$
$$M'_\beta = \begin{bmatrix} A_1 & 2B_1 \\ a_1 & 2 \end{bmatrix}.$$

Claim 4.6.46. *Let,*

$$F = \begin{bmatrix} A & B & 2C \\ 2a & 2j^T & 2 \end{bmatrix}.$$

Then, $Col_{\mathbb{Z}}(M_\beta) = Col_{\mathbb{Z}}(F)$.

Proof. The same proof of claim 4.6.44 can be used to show that for any $\Omega_K \in \sim \{\gamma_0\}$, $F\Omega_K = M_{2,4}\Omega_K$ is in the column space of M_β. Hence, it suffices to show that $F\gamma_0 = 2M_{2,4}\gamma_0$ is in the column span of M_β.

Because $\beta_{2,4}$ is a $(2,4)$-basis for $M'_{2,4}$, there is an integral vector $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ such that:

$$\begin{bmatrix} A_1 & 2B_1 \\ a_1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 4C_1 \\ 2 \end{bmatrix}.$$

Using the same argument that we used in claim 4.6.44, we can show that 2 divides x_1. Also, we can manipulate the above equation algebraically to deduce:

$$\begin{bmatrix} A_1 & B_1 \\ 2a_1 & 2 \end{bmatrix} \begin{bmatrix} \frac{x_1}{2} \\ x_2 \end{bmatrix} = \begin{bmatrix} 2C_1 \\ 2 \end{bmatrix} = 2M_{2,4}\gamma_0.$$

Thus, the result follows. This finishes the proof of claim 4.6.46. □

We resume to the proof of proposition 4.6.45. Consider the following inclusion of free $\mathbb{Z}$-modules.

$$Col_{\mathbb{Z}}(F) \subset Col_{\mathbb{Z}}(M_{2,4}) \subset \mathbb{Z}^{r_2(n)}$$

Hence, we deduce the following exact sequence:

$$0 \to H \to \overline{S}(F) \to \overline{S}(M_{2,4}) \to 0,$$

where $H = \frac{Col_{\mathbb{Z}}(M_{2,4})}{Col_{\mathbb{Z}}(F)}$.

Suppose that H has order 2. From claim 4.6.46, we know that $\overline{S}(F) = \overline{S}(M_\beta)$. Also, we know that $\overline{S}(M_\beta) = (\mathbb{Z}/6\mathbb{Z})$ by using a similar reasoning as in the proof of proposition 4.6.43. Therefore, from the above exact sequence, we can deduce that $\overline{S}(M_{2,4})$ has order 3, and therefore it must be $(\mathbb{Z}/3\mathbb{Z})$. Thus, it suffices to show that H has order 2.

Clearly,

$$\begin{aligned} H &= \frac{Col_{\mathbb{Z}}\left(\begin{bmatrix} A & B & C \\ 2a & 2j^T & 1 \end{bmatrix}\right)}{Col_{\mathbb{Z}}\left(\begin{bmatrix} A & B & 2C \\ 2a & 2j^T & 2 \end{bmatrix}\right)} \\ &= \langle \begin{bmatrix} C \\ 1 \end{bmatrix} \rangle. \end{aligned}$$

Hence, H has order 2 or 1. Suppose that H is trivial. Clearly,

$$\begin{aligned} H &= \frac{Col_{\mathbb{Z}}(M_{2,4})}{Col_{\mathbb{Z}}(F)} \\ &= \frac{Col_{\mathbb{Z}}(M_{2,4})}{Col_{\mathbb{Z}}(M_\beta)} \\ &= \frac{Col_{\mathbb{Z}}\left(\begin{bmatrix} A & B & C \\ 2a & 2j^T & 1 \end{bmatrix}\right)}{Col_{\mathbb{Z}}(M_\beta)}. \end{aligned}$$

Using a proof similar to the proof of claim 4.6.44, we can deduce:

$$Col_{\mathbb{Z}}\left(\begin{bmatrix} A & B \\ 2a & 2j^T \end{bmatrix}\right) = Col_{\mathbb{Z}}(M_\beta).$$

Hence, there is integral $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ such that:

$$\begin{bmatrix} A_1 & B_1 \\ 2a_1 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} C \\ 1 \end{bmatrix}.$$

Clearly, this implies:

$$2(\langle a_1, x_1 \rangle + x_2) = 1,$$

which is a contradiction. □

4.6.6 The $(3, 4)$ Case

We show partial results toward finding a $(3, 4)$-basis, and we show partial results toward calculating the Smith Group of $M'_{3,4}$.

4.6.6.1 Projected Relative $(3, 4)$-Pods

We will calculate 3 relative projected $(3, 4)$-pods to show a reduction result for the $(3, 4)$ case.

Using the classification given by figure 4.18, we can partition the cyclic ordered partitions of size 4 into 5 classes, where each class corresponds to a partition of 4. The following propositions will use the notation of figure 4.18. All congruences will use $M'_{3,4}$.

Proposition 4.6.47. *Let* $[a_1, a_2, a_3, a_4] \in \{p_5\}$*, i.e.,* $a_i \geq 2$*. Then,*

$$2[a_1, a_2, a_3, a_4] = 0 \ mod \ \{p_1\}, \ldots, \{p_4\}.$$

Proof. Let $A = \{x_1, x_2, x_3, x_4\} \in [a_1, a_2, a_3, a_4]$, and choose $B = \{y_1, y_2, y_3, y_4\}$ as shown in the relative $(3, 4)$-pod of figure 4.26.

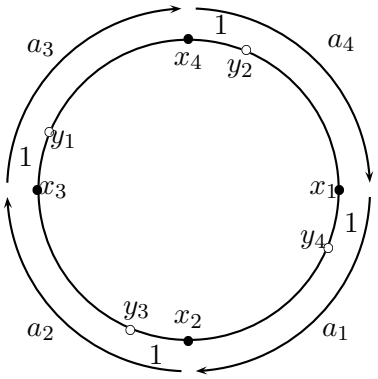

Figure 4.26. Relative $(3, 4)$-pod.

The result follows from the projected relative $(3, 4)$-pod, shown in figure 4.27, that results from the relative $(3, 4)$-pod of figure 4.26.

□

Proposition 4.6.48. *Let* $[a_1, a_2, a_3, a_4] \in \{p_5\}$*, i.e.,* $a_i \geq 2$*. Then,*

$$[a_1, a_2 + 1, a_3 - 1, a_4] \;=\; [a_1, a_2 - 1, a_3 + 1, a_4] \; mod \; \{p_1\}, \ldots, \{p_4\}.$$

Proof. Let $A = \{x_1, x_2, x_3, x_4\} \in [a_1, a_2, a_3, a_4]$, and choose $B = \{y_1, y_2, y_3, y_4\}$ as shown in the Relative $(3, 4)$-pod of figure 4.26.

The projected relative $(3, 4)$-pod that corresponds to the relative $(3, 4)$-pod of figure 4.28 is shown in figure 4.29.

From the projected relative $(3, 4)$-pod of figure 4.29, we deduce mod $\{p_1\}, \ldots, \{p_4\}$ that:

$$2[a_1, a_2, a_3, a_4] - [a_1, a_2 + 1, a_3 - 1, a_4] - [a_1, a_2 - 1, a_3 + 1, a_4] \;=\; 0.$$

By proposition 4.6.47, $2[a_1, a_2, a_3, a_4] = 0$ mod $\{p_1\}, \ldots, \{p_4\}$. Hence, we have:

$$[a_1, a_2 + 1, a_3 - 1, a_4] \;=\; -[a_1, a_2 - 1, a_3 + 1, a_4],$$

T	$(-1)^{\lvert T\rvert}$	K	$\psi(K)$
0000	$+1$	$\{x_1, x_2, x_3, x_4\}$	$[a_1, a_2, a_3, a_4]$
1000	-1	$\{y_1, x_2, x_3, x_4\}$	$[a_2, 1, a_3 - 1, a_1 + a_4]$
0100	-1	$\{x_1, y_2, x_3, x_4\}$	$[a_1 + a_2, a_3, 1, a_4 - 1]$
0010	-1	$\{x_1, x_2, y_3, x_4\}$	$[a_1, 1, a_2 + a_3 - 1, a_4]$
0001	-1	$\{x_1, x_2, x_3, y_4\}$	$[1, a_1 - 1, a_2, a_3 + a_4]$
1100	$+1$	$\{y_1, y_2, x_3, x_4\}$	$[1, a_3 - 1, 1, a_1 + a_2 + a_4 - 1]$
1010	$+1$	$\{y_1, x_2, y_3, x_4\}$	$[1, a_2, a_3 - 1, a_1 + a_4]$
1001	$+1$	$\{y_1, x_2, x_3, y_4\}$	$[a_1 - 1, a_2, 1, a_3 + a_4]$
0110	$+1$	$\{x_1, y_2, y_3, x_4\}$	$[a_1 + 1, a_2 + a_3 - 1, 1, a_4 - 1]$
0101	$+1$	$\{x_1, y_2, x_3, y_4\}$	$[1, a_1 + a_2 - 1, a_3 + 1, a_4 - 1]$
0011	$+1$	$\{x_1, x_2, y_3, y_4\}$	$[1, a_1 - 1, 1, a_2 + a_3 + a_4 - 1]$
1110	-1	$\{y_1, y_2, y_3, x_4\}$	$[a_2, a_3 - 1, 1, a_1 + a_4]$
1101	-1	$\{y_1, y_2, x_3, y_4\}$	$[a_1 + a_2 - 1, 1, a_3, a_4]$
1011	-1	$\{y_1, x_2, y_3, y_4\}$	$[a_1 - 1, 1, a_2, a_3 + a_4]$
0111	-1	$\{x_1, y_2, y_3, y_4\}$	$[1, a_1, a_2 + a_3, a_4 - 1]$
1111	$+1$	$\{y_1, y_2, y_3, y_4\}$	$[a_1, a_2, a_3, a_4]$

Figure 4.27. Projected relative $(3, 4)$-pod.

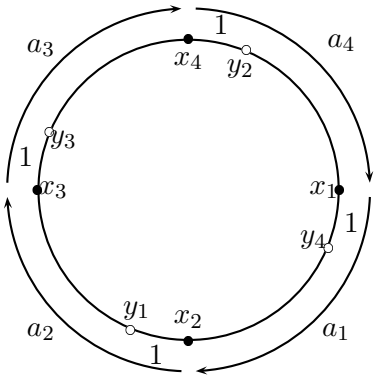

Figure 4.28. Relative $(3, 4)$-pod.

mod $\{p_1\}, \ldots, \{p_4\}$.

If $a_2 \geq 3$, then by proposition 4.6.47 we deduce $[a_1, a_2 - 1, a_3 + 1, a_4] = -[a_1, a_2 - 1, a_3 + 1, a_4]$ mod $\{p_1\}, \ldots, \{p_4\}$. Hence, the result follows for $a_2 \geq 3$.

For $a_2 = 2$, the result is trivial since

$$\begin{aligned}
[a_1, 2 + 1, a_3 - 1, a_4] &= [a_1, a_2 + 1, a_3 - 1, a_4] \\
&= -[a_1, a_2 - 1, a_3 + 1, a_4] \\
&= -[a_1, 2 - 1, a_3 + 1, a_4] \\
&= 0 \\
&= [a_1, 2 - 1, a_3 + 1, a_4],
\end{aligned}$$

mod $\{p_1\}, \ldots, \{p_4\}$. □

4.6.6.2 Partial Reduction for a $(3, 4)$-Basis

Our research efforts on projected relative $(3, 4)$-pods did not yield a $(3, 4)$-basis. However, the following result was the best concise reduction.

T	$(-1)^{\lvert T\rvert}$	K	$\psi(K)$
0000	$+1$	$\{x_1, x_2, x_3, x_4\}$	$[a_1, a_2, a_3, a_4]$
1000	-1	$\{y_1, x_2, x_3, x_4\}$	$[1, a_2 - 1, a_3, a_1 + a_4]$
0100	-1	$\{x_1, y_2, x_3, x_4\}$	$[a_1 + a_2, a_3, 1, a_4 - 1]$
0010	-1	$\{x_1, x_2, y_3, x_4\}$	$[a_1, a_2 + 1, a_3 - 1, a_4]$
0001	-1	$\{x_1, x_2, x_3, y_4\}$	$[1, a_1 - 1, a_2, a_3 + a_4]$
1100	$+1$	$\{y_1, y_2, x_3, x_4\}$	$[a_2 - 1, a_3, 1, a_1 + a_4]$
1010	$+1$	$\{y_1, x_2, y_3, x_4\}$	$[1, a_2, a_3 - 1, a_1 + a_4]$
1001	$+1$	$\{y_1, x_2, x_3, y_4\}$	$[a_1 - 1, 1, a_2 - 1, 1 + a_3 + a_4]$
0110	$+1$	$\{x_1, y_2, y_3, x_4\}$	$[a_1 + a_2 + 1, a_3 - 1, 1, a_4 - 1]$
0101	$+1$	$\{x_1, y_2, x_3, y_4\}$	$[1, a_1 + a_2 - 1, a_3 + 1, a_4 - 1]$
0011	$+1$	$\{x_1, x_2, y_3, y_4\}$	$[1, a_1 - 1, a_2 + 1, a_3 + a_4 - 1]$
1110	-1	$\{y_1, y_2, y_3, x_4\}$	$[a_2, a_3 - 1, 1, a_1 + a_4]$
1101	-1	$\{y_1, y_2, x_3, y_4\}$	$[a_1, a_2 - 1, a_3 + 1, a_4]$
1011	-1	$\{y_1, x_2, y_3, y_4\}$	$[a_1 - 1, 1, a_2, a_3 + a_4]$
0111	-1	$\{x_1, y_2, y_3, y_4\}$	$[1, a_1 + a_2, a_3, a_4 - 1]$
1111	$+1$	$\{y_1, y_2, y_3, y_4\}$	$[a_1, a_2, a_3, a_4]$

Figure 4.29. Projected relative $(3, 4)$-pod.

Proposition 4.6.49. *Let* $[a_1, a_2, a_3, a_4] \in \{p_5\}$*, i.e.,* $a_i \geq 2$*. Then, using* $M'_{3,4}$*:*

$$[a_1, a_2, a_3, a_4] \;=\; \begin{cases} [2, 2, 2, 6^*] \; mod \; \{p_1\}, \ldots, \{p_4\} & \text{if all } a_i s \text{ are even,} \\ 0 \; mod \; \{p_1\}, \ldots, \{p_4\} & \text{else.} \end{cases}$$

Proof. Suppose that some $a_i \geq 3$ is odd. Without loss of generality, asssume $a_3 \geq 3$. Clearly, proposition 4.6.48 applies and it implies that for $a_1 \geq 2, a_2 \geq 1, a_3 \geq 3, a_4 \geq 2$:

$$[a_1, a_2, a_3, a_4] \;=\; [a_1, a_2 + 2, a_3 - 2, a_4] \bmod \{p_1\}, \ldots, \{p_4\}. \tag{4.34}$$

Let $a_3 = 2s + 1$. We can apply the congruence 4.34 to itself s times to deduce:

$$\begin{aligned} [a_1, a_2, a_3, a_4] &= [a_1, a_2 + 2, a_3 - 2, a_4] \\ &= [a_1, a_2 + 4, a_3 - 4, a_4] \\ &\vdots \\ &= [a_1, a_2 + a_3 - 1, 1, a_4] \\ &= 0 \bmod \{p_1\}, \ldots, \{p_4\}. \end{aligned}$$

Hence, the result follows, and it suffices to show the proposition when all the a_is are even.

Let $a_3 = 2s$. After applying congruence 4.34 to itself $(s-1)$ times, we can deduce mod $\{p_1\}, \ldots, \{p_4\}$:

$$\begin{aligned} [a_1, a_2, a_3, a_4] &= [a_1, a_2 + 2, a_3 - 2, a_4] \\ &\vdots \\ &= [a_1, a_2 + a_3 - 2, 2, a_4]. \end{aligned}$$

Now, we apply the previous argument to $[a_4, a_1, a_2{+}a_3{-}2, 2]$ to deduce mod $\{p_1\}, \ldots, \{p_4\}$:

$$[a_4, a_1, a_2 + a_3 - 2, 2] \;=\; [a_4, a_1 + a_2 + a_3 - 4, 2, 2].$$

And, we proceed to do the same argument to $[2, a_4, a_1 + a_2 + a_3 - 4, 2]$ to deduce mod $\{p_1\}, \ldots, \{p_4\}$:

$$\begin{aligned} [2, a_4, a_1 + a_2 + a_3 - 4, 2] &= [2, a_4 + a_1 + a_2 + a_3 - 6, 2, 2] \\ &= [2, 6^*, 2, 2]. \end{aligned}$$

Hence, the result follows. □

As a corollary, we deduce the following.

Corollary 4.6.50. *Let $[a_1, a_2, a_3, a_4] \in \{p_5\}$, i .e . $a_i \geq 2$. Then, using $M'_{3,4}$:*

$$[a_1, a_2, a_3, a_4] = \begin{cases} [2, 2, 2, 6^*] \text{ mod } \{p_1\}, \ldots, \{p_4\} & \text{if } n \text{ is even and all } a_i s \text{ are even,} \\ 0 \text{ mod } \{p_1\}, \ldots, \{p_4\} & \text{if } n \text{ is even and at least one } a_i \text{ is odd,} \\ 0 \text{ mod } \{p_1\}, \ldots, \{p_4\} & \text{if } n \text{ is odd.} \end{cases}$$

4.6.6.3 Partial Results for $\overline{\mathbf{S}}(\mathbf{M'_{3,4}})$

We calculate the Smith Group of $M'_{3,4}$ whenever the integral preimage problem has trivial solution. The following proposition summarizes the result.

Proposition 4.6.51. *Let $M'_{i-1,i}$ have trivial solution to the integral preimage problem for $i = 1, 2, 3, 4$. Assume that n is odd, and $n \geq 9$. Then,*

$$\overline{S}(M'_{3,4}) = (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^{r_2(n)-1}.$$

Proof. By proposition 4.3.38, we deduce:

$$\begin{aligned} (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^{r_2(n)-1} &= \overline{S}(D_{3,4}) \\ &\subset \overline{S}(M'_{3,4}). \end{aligned} \tag{4.35}$$

By proposition 4.6.25, $|M'_{2,3}| = 3$. Hence, $\gcd(|M'_{2,3}|, 4-3+1) = \gcd(3,2) = 1$. Thus, by proposition 4.3.39, we deduce that:

$$\langle \beta_{2,3} \rangle \;=\; \overline{S}(M'_{3,4}),$$

where $\beta_{2,3}$ is $\mathbb{Z}$-linearly independent in $\overline{S}(M'_{3,4})$. Hence, $\overline{S}(M'_{3,4})$ decomposes into $r_2(n)$ nontrivial cyclic groups. By proposition 4.3.28 and Equation (4.35), $\overline{S}(M'_{3,4})$ has exponent dividing 4. Therefore, by Equation (4.35),

$$\overline{S}(M'_{3,4}) \;=\; (\mathbb{Z}/a_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/a_{r_2(n)}\mathbb{Z}),$$

where $a_i = 2$ or 4, and at least one a_i is 4. It suffices to show that $\overline{S}(M'_{3,4})$ has exactly one cyclic factor of size 4.

Suppose $\overline{S}(M'_{3,4})$ has two invariant factors of size 4. There are Ω_{T_1} and Ω_{T_2} be two orbits in $\beta_{2,3}$ such that there are integral z_1, z_2 satisfying:

$$\begin{aligned} 4\Omega_{T_1} &= M'_{3,4} z_1, \\ 4\Omega_{T_2} &= M'_{3,4} z_2. \end{aligned}$$

By multiplying the previous equations by $M'_{2,3}$ on the left, we deduce:

$$\begin{aligned} 4M'_{2,3}\Omega_{T_1} &= 2M'_{2,4} z_1, \\ 4M'_{2,3}\Omega_{T_2} &= 2M'_{2,4} z_2. \end{aligned}$$

Let $\beta_{2,4}$ be a $(2,4)$-basis of $M'_{2,4}$. The previous equations give,

$$\begin{aligned} 2M'_{2,3}\Omega_{T_1} &= M'_{2,4} z_1 \\ &= M'_{\beta_{2,4}} w_1, \\ 2M'_{2,3}\Omega_{T_2} &= M'_{2,4} z_2 \\ &= M'_{\beta_{2,4}} w_2, \end{aligned}$$

for some integral vectores w_1 and w_2. In particular, $M'_{2,3}\Omega_{T_1}$ and $M'_{2,3}\Omega_{T_2}$ have order 2 in $\overline{S}(M'_{\beta_{2,4}})$.

Clearly, $\overline{S}(M'_{2,4}) = (\mathbb{Z}/6\mathbb{Z})$ has a unique element of order 2. Thus, there is an integral w_3 such that:

$$M'_{2,3}\Omega_{T_1} = M'_{2,3}\Omega_{T_2} + M'_{\beta_{2,4}}w_3.$$

Therefore,

$$0 = M_{2,3}(2\Omega_{T_1} - 2\Omega_{T_2} - M'_{3,4}w_3),$$

where w_3 has support in $\beta_{2,4}$.

Since $M'_{3,4}$ has trivial solution to the integral preimage problem, it follows that $Ker(M'_{2,3}) \cap \mathbb{Z}^{r_3(n)} \subset Im_{\mathbb{Z}}(M'_{3,4})$. Hence,

$$2\Omega_{T_1} - 2\Omega_{T_2} - M'_{3,4}w_3 = M'_{3,4}w_4$$

for some integral w_4. Therefore, $2\Omega_{T_1} = 2\Omega_{T_2}$ in $\overline{S}(M'_{3,4})$. Thus, in $\overline{S}(M'_{3,4})$,

$$\Omega_{T_1} = \Omega_{T_2} + z_2 \tag{4.36}$$

where z_2 is some element of order 2 of $\overline{S}(M'_{3,4})$.

We show that Equation (4.36) gives a contradiction. We will contradict the $\mathbb{Z}$-linear independence of $\beta_{2,3}$. Clearly, since z_2 has order 2, $z_2 = \sum \Omega_{T_i}$. Where Ω_{T_i} are elements of order 2 when viewed as elements of $\overline{S}(M'_{3,4})$, and $\Omega_{T_i} \in \beta_{2,3} \backslash \{\Omega_{T_1}, \Omega_{T_2}\}$. Thus, in $\overline{S}(M'_{3,4})$:

$$\Omega_{T_1} = \Omega_{T_2} + \sum \Omega_{T_i}.$$

This contradicts the $\mathbb{Z}$-linear independence of $\beta_{2,3}$ in $\overline{S}(M'_{3,4})$. □

Corollary 4.6.52. *Let* $\gcd(n, 6!) = 1$. *Then,*

$$\overline{S}(M'_{3,4}) \;=\; (\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^{r_2(n)-1}.$$

Proof. By proposition 4.3.25, the matrices $M'_{i-1,i}$ have trivial solution to the integral preimage problem whenever $i = 1, 2, 3, 4$. Hence, the result follows by proposition 4.6.51. □

4.6.7 Conjectures, Consequences, and Observations

We close this chapter with a conjecture related to the (t, k)-basis conjectures, and a proposition that shows how to calculate the Smith Group of $M'_{t,k}(n)$ whenever the (t, k)-basis conjecture holds.

We start with an observation about the integral preimage problem.

Proposition 4.6.53. *Let* $t < k \leq n - k$, *and let* n *be a prime. Then,* $M'_{t,k}$ *and* $M_{t,k}$ *have trivial solution to the integral preimage problem.*

Proof. Note that the hypotheses of proposition 4.3.25 are satisfied whenever n is a prime. Hence, the result follows by applying proposition 4.3.25. □

We proceed to show a consequence of the weak (t, k)-basis conjecture.

Proposition 4.6.54. *Let* $\gcd(n, (2(k-1))!) = 1$, *and* $1 \leq t < k \leq n - k \leq n - t$. *Assume the* (t, k)*-basis conjecture holds for* n, *and for all* $(i-1, i)$ *where* $i = 1, \ldots, k$. *Then,* $M'_{t,k}(n)$ *has Smith Group given by:*

$$(\mathbb{Z}/\binom{k}{t}\mathbb{Z}) \times (\mathbb{Z}/\binom{k-2}{t-2}\mathbb{Z})^{r_2(n)-1} \times (\mathbb{Z}/\binom{k-3}{t-3}\mathbb{Z})^{r_3(n)-r_2(n)} \times \cdots \times (\mathbb{Z}/\binom{k-(t-1)}{t-(t-1)}\mathbb{Z})^{r_{t-1}(n)-r_{t-2}(n)},$$

where $r_i(n) = \frac{\binom{n}{i}}{n}$ *is the number of orbits on the* i*-subsets for* $i = 2, \ldots, t$.

Proof. Under the assumption of n, we can deduce that $M'_{i-1,i}$ has trivial solution to the integral preimage problem for $i = 1, \ldots, k$ by using proposition 4.3.25. Hence, proposition 4.3.35 applies and the result follows. □

Remark: The conclusion of proposition 4.6.54 has been verified for n a prime, and $n \leq 19$ with the aid of a computer program.

We close this chapter with another conjecture that has been verified by the work of the previous sections for the cases $(2,3), (2,4)$, and partly for the case $(3,4)$.

Conjecture 4.6.55. *Let* $\gcd(tk, n) = 1$, $t < k \leq n - k$, *and let* $\{p_1\}, \ldots, \{p_r\}$ *be the distinct partitions of* k. *Given* $\{p_i\} = a_1^{f_1} \cdots a_l^{f_l}$, *define* $s(\{p_i\}) = f_1 + \cdots + f_l$ *as the number of parts of* $\{p_i\}$. *Let,*

$$\begin{aligned} X_s &= \{\Omega_K \mid \Omega_K \text{ affords } \{p_i\} \text{ where } \{p_i\} \text{ satisfies } s(\{p_i\}) \leq s\}, \\ Y_s &= \{\{p_i\} \mid s(\{p_i\}) \leq s\}. \end{aligned}$$

Then,

1. *The set* X_t *contains a* (t,k)*-basis of* $M'_{t,k}$.
2. *If* $\Omega_K \in \sim X_t$, *then* $\Omega_K = 0 \bmod Y_s$ *using* $M'_{t,k}$.

Bibliography

[1] Shahin Ajoodani-Namini and Gholamreza Baradan Khosrovshahi. A new basis for trades. *SIAM Journal on Discrete Mathematics*, 3(3):364–372, 1990.

[2] Eiichi Bannai and Tatsuro Ito. *Algebraic Combinatorics I, Association Schemes*. Menlo Park, California : The Benjamin/Cummings Publishing Company, 1984.

[3] Thomas Bier. Remarks on recent formulas of Wilson and Frankl. *European Journal of Combinatorics*, 14(1):1–8, 1993.

[4] Richard Brualdi and Vera Pless. Polyadic codes. *Discrete Applied Mathematics*, 25:3–17, 1989.

[5] Paul Camion and Henry Berthold Mann. Antisymmetric difference sets. *Journal of Number Theory*, 4(3):266–268, 1972.

[6] Yu Qing Chen, Qing Xiang, and Surinder K. Sehgal. An exponent bound on skew-hadamard abelian difference sets. *Designs, Codes Cryptography*, 4(4):313–317, 1994.

[7] David Dummit and Richard Foote. *Abstract Algebra*. Upper Saddle, New Jersey : Prentice Hall, 1999.

[8] Chris D. Godsil. *Algebraic Combinatorics*. New York, New York : Chapman and Hall Mathematics, 1993.

[9] Jack Edward Graver and Wolfgang B. Jurkat. The module structure of integral designs. *Journal of Combinatoral Theory, Series A*, 15:75–90, 1973.

[10] Irving Martin Isaacs. *Character Theory of Finite Groups*. New York, New York : Dover Publications, 1994.

[11] Eugene Carlyle Johnsen. Skew-hadamard abelian group difference sets. *Journal of Algebra*, 4:388–402, 1966.

[12] Dieter Jungnickel. Difference sets. In J. Dinitz and D.R. Stinson, editors, *Contemporary Design Theory, A Collection of Surveys*, Wiley Interscience Series in Discrete Mathematics and Optimization, pages 241–324. New York, New York : Wiley Interscience, 1992.

[13] Helmut Kramer. Inversion of incidence mappings. *Séminaire Lotharingien de Combinatoire*, 39(B39f):20, 1997.

[14] Helmut Kramer. Eigenspace decompositions with respect to symmetrized incidence mappings. *Séminaire Lotharingien de Combinatoire*, 41(B41c):20, 1998.

[15] Helmut Kramer. Binary Moore-Penrose inverses of set inclusion incidence matrices. *Séminaire Lotharingien de Combinatoire*, 45(B45d):18, 2001.

[16] Donald L. Kreher. An incidence algebra for t-designs with automorphisms. *Journal of Combinatorial Theory, Series A*, 42:239–251, 1986.

[17] Eric S. Lander. *Symmetric Designs, An Algebraic Approach*. Oxford, England : Cambridge University Press, 1983.

[18] San Ling and Chaoping Xing. Polyadic codes revisited. *IEEE Transactions on Information Theory*, 50(1):200–207, 2004.

[19] James R. Munkres. *Elements of Algebraic Topology*. The Advanced Book Program. Reading Massachusetts: Perseus Books Publishing, 1984.

[20] Vera Pless. Binary cyclic codes. In *Computers in Algebra*, volume 111 of *Lecture Notes in Pure and Applied Mathematics*, pages 129–133. New York, New York : Dekker, 1988.

[21] Vera Pless and Joseph Rushanan. Triadic codes. *Linear Algebra and Its Applications*, 98:415–433, 1988.

[22] Joseph Rushanan. Topics in integral matrices and algebraic group codes. PhD thesis, California Institute of Technology, 1986.

[23] Joseph Rushanan. Duadic codes and difference sets. *Journal of Combinatorial Theory, Series A*, 57:254–261, 1991.

[24] Joseph Rushanan. Eigenvalues and the smith normal form. *Linear Algebra and its Applications*, 216:177–184, 1995.

[25] Michiel H. M. Smid. Duadic codes. *IEEE Transactions on Information Theory*, 33(3):432–433, 1987.

[26] Richard M. Wilson. A diagonal form for the incidence matrices of t-subsets vs. k-subsets. *European Journal of Combinatorics*, 11:609–615, 1990.

[27] Richard M. Wilson. Signed hypergraph designs and diagonal form for some incidence matrices. *Designs, Codes and Cryptography*, 17:289–297, 1999.