2014

A classification of class two and class three nilpotent table algebras

Caroline Kettlestrings

ABSTRACT

A CLASSIFICATION OF CLASS TWO AND CLASS THREE NILPOTENT TABLE ALGEBRAS

Caroline Kettlestrings, Ph.D.
Department of Mathematical Sciences
Northern Illinois University, 2014
Harvey Blau, Director

Table algebras are generalizations of adjacency algebras, and of the character ring of a finite group. Extensions of groups by groups have been well studied, and Hirasaka and Bang [5] have generalized this to the study of extensions of association schemes by association schemes. In this dissertation, we study central extensions of table algebras by table algebras, in the case where the extension is either class two nilpotent (which means it is an extension of a group algebra by a group algebra), or class three nilpotent (which means it is an extension of a class two nilpotent table algebra by a group algebra) with order p^3 for an arbitrary prime p. We classify these algebras up to exact isomorphism. In the class two case, we determine exactly when the algebra is the adjacency algebra of an association scheme, and in the class three case, we determine which sets of the parameters of our classification determine isomorphic algebras.

NORTHERN ILLINOIS UNIVERSITY
DE KALB, ILLINOIS

DECEMBER 2014

A CLASSIFICATION OF CLASS TWO AND CLASS THREE NILPOTENT TABLE ALGEBRAS

BY

CAROLINE KETTLESTRINGS

A DISSERTATION SUBMITTED TO THE GRADUATE SCHOOL
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICAL SCIENCES

Dissertation Director:
Harvey Blau

TABLE OF CONTENTS

Chapter		Page
1	INTRODUCTION	1
2	PRELIMINARIES	3
	2.1 Definitions and Examples	3
	2.2 Previous Results	8
3	EXTENSIONS OF GROUP ALGEBRAS BY GROUP ALGEBRAS	11
4	EXTENSIONS OF TABLE ALGEBRAS BY GROUP ALGEBRAS	30
	4.1 System of Equations	32
	4.2 Proof of Main Theorem	44
	4.3 Isomorphic Redundancy	63
REFERENCES		74

CHAPTER 1

INTRODUCTION

The purpose of this thesis will be to study extensions of a table algebra by a central group algebra. In certain cases, we will characterize such extensions up to isomorphism type, and investigate whether the algebras occur as adjacency algebras of association schemes. In particular, we will classify all class three nilpotent standard integral table algebras of order p^3, for any prime p. Table algebras are algebras over the complex numbers with a distinguished basis and non-negative real structure constants that satisfy certain other properties (Definition 2.1). Several important objects are examples of table algebras, such as the group algebra of a finite group. The set of class functions from a finite group to the complex numbers forms a table algebra with basis the irreducible characters of the group, and the center of the group algebra of a finite group with a basis of sums over the conjugacy classes of the group forms a table algebra that is dual (in some sense) to the class function algebra. The adjacency algebra of an association scheme (Definitions 2.3 and 2.4) also forms a table algebra. Table algebras were introduced by Blau and Arad in 1991 ([2]) to study the characters and conjugacy classes of a finite group. Because both the class function algebra and the center of a group algebra are obviously commutative, table algebras were initially defined to be commutative algebras. Shortly thereafter, however, it became clear that several other objects were examples of table algebras, such as hypergroups, fusion rule algebras, C-algebras, and, as mentioned, adjacency algebras of association schemes – with the exception that these are not necessarily commutative. The commutativity condition was dropped and the current definition

of a table algebra formulated by Arad, Fisman, and Muzychuk in [3]. See [6] for an overview of the relationships between table algebras and various other mathematical objects.

We can define a nilpotent table algebra in a way that arises naturally from the definition of a nilpotent group (Definition 2.12). The process of forming a group G by extending a group H by a group F has been well studied, and this process has been generalized by Hirasaka and Bang in [5] to form an association scheme as an extension of an association scheme by an association scheme in the case where the schemes are thin (Definition 2.7). Blau and Xu [9] have developed a classification of commutative table algebras formed by extending an abelian group algebra $\mathbb{C}H$ by an abelian group algebra $\mathbb{C}F$, and any table algebra formed in this way will be nilpotent of class 2. Blau and Xu's work includes necessary and sufficient conditions for such an algebra to arise as the adjacency algebra of an association scheme.

For this dissertation, we begin by extending Blau and Xu's work to cover the case where the group H is central in the algebra but the group F is not necessarily abelian, and hence the table algebra formed as the extension of $\mathbb{C}F$ by $\mathbb{C}H$ is not necessarily commutative (Theorem 3.1).

We then investigate table algebras formed as extensions of table algebras by central group algebras. Because classifying all such algebras seems intractable, we have narrowed the scope to a classification of table algebras of order p^3 that are formed as extensions of class 2 nilpotent standard table algebras by central group algebras (Theorem 4.1). Table algebras formed in this way (even if they are not of order p^3) are class 3 nilpotent table algebras. We then use this classification to characterize the isomorphism classes of such algebras (Proposition 4.2).

CHAPTER 2

PRELIMINARIES

2.1 Definitions and Examples

The information in this section regarding table algebras can be found in [6]; the information regarding association schemes can be found in [12]; and the information regarding wreath products can be found in [8].

Definition 2.1. A *table algebra* is a (not necessarily commutative) algebra A over $\mathbb{C}$ with a distinguished basis B for which the following properties hold:

i) For $b_i, b_j \in B, b_i b_j = \sum_{b_k \in B} \beta_{ijk} b_k$, where $\beta_{ijk} \in \mathbb{R}_{\geq 0}$ for all i, j, k.

ii) $b_0 = 1_A \in B$.

iii) There is an anti-automorphism of A denoted by $*$ which is of order at most 2 and permutes B. We define $b_{i^*} = b_i^*$.

iv) For any $b_i, b_j \in B, \beta_{ij0} = 0$ unless $j = i^*$, and $\beta_{ii^*0} = \beta_{i^*i0} > 0$.

Every table algebra has a unique algebra homomorphism from A to $\mathbb{C}$ with $\delta(B) \subseteq \mathbb{R}^+$ called the *degree map*; the values $\delta(b_i)$ for $b_i \in B$ are called the *degrees* of B. This map has the property that $\delta(b_i) = \delta(b_i^*)$. A table algebra whose structure constants and degrees lie in the integers is called *integral*, and if $\delta(b_i) = \beta_{ii^*0}$ for each i, the algebra is called *standard*. Note that any table algebra may be made standard by changing the distinguished basis from $\{b_i \in B\}$ to $\{(\delta(b_i)/\beta_{ii^*0})b_i : b_i \in B\}$. Such

a change of basis, where each basis element b_i is replaced by $\lambda_i b_i$ for $\lambda_i \in \mathbb{R}^+$ with $\lambda_i = \lambda_{i^*}$ and $\lambda_0 = 1$, is called a *rescaling* of (A, B). A rescaling of (A, B) is still a table algebra.

Definition 2.2. An *exact table algebra isomorphism* from (A, B) to (U, V) is an algebra isomorphism $\phi : A \to U$ with $\phi(B) = V$.

Throughout this paper, if A_1 and A_2 are table algebras, $A_1 \cong A_2$ will indicate that there is an exact table algebra isomorphism.

Lemma 2.1. *For any table algebra (A, B), there is a sesquilinear map $\langle \cdot, \cdot \rangle : A \times A \to \mathbb{C}$ defined by $\langle x, y \rangle = \sum \beta_{ii^*0} \gamma_i \overline{\lambda_i}$ where $x = \sum \gamma_i b_i, y = \sum \lambda_i b_i$, and the bar denotes complex conjugation. For $x \in A, b_i, b_j, b_k \in B$, this map has the following properties:*

i) $\langle b_i, b_j \rangle = \delta_{ij} \beta_{ii^*0}$ *where δ_{ij} is the Kronecker delta function.*

ii) $\langle b_i b_j, b_k \rangle = \langle b_j, b_i^* b_k \rangle , \langle b_i, b_j b_k \rangle = \langle b_i b_k^*, b_j \rangle$.

Example 2.1. Let G be a finite group. Then $(\mathbb{C}G, G)$ forms a standard, integral table algebra. Its structure constants are clearly non-negative integers (either one or zero, in fact). The anti-automorphism is the usual group inversion, and $\delta(g) = 1$ for all g in the group.

Example 2.2. $(Z(\mathbb{C}G), \{C_g^+\})$, the center of a group algebra with a basis of sums over the conjugacy classes of the group, also forms a standard, integral table algebra. The anti-automorphism sends the sum over the conjugacy class of g to the sum over the conjugacy class of g^{-1}. The degree map is given by $\delta(g) = |C_g|$.

Example 2.3. The class functions from a finite group G to $\mathbb{C}$ form an integral table algebra with basis $Irr(G)$. The anti-automorphism is defined by $\chi_{i^*}(g) = \overline{\chi_i(g)}$

where the bar denotes complex conjugation, and the degree map gives the usual degree of a character. We know that $\beta_{ii^*0} = 1$ for every i in this algebra, so it is not standard unless G is abelian.

Definition 2.3. An *association scheme* (S, R) is a set S together with a collection $R = \{R_i : 0 \leq i \leq d\}$ of subsets of $S \times S$ with the following properties:

i) $R_0 = \{(x, x) : x \in S\}$.

ii) $\cup_{i=0}^{d} R_i = S \times S$ and $R_i \cap R_j = \emptyset$ if $i \neq j$.

iii) For each i, $(R_i)^T = \{(x, y) : (y, x) \in R_i\} = R_{i^*}$ for some $0 \leq i^* \leq d$.

iv) For any $0 \leq i, j, k \leq d$ and any pair $(x, y) \in R_k$, the number of elements $z \in S$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is independent of the particular choice of x and y. This integer is denoted p_{ijk}.

The elements of R are called *relations*.

An association scheme gives rise to a standard, integral table algebra in the following way. Let A_i be the matrix indexed by the elements of S with entries defined by

$$(A_i)_{xy} = \begin{cases} 1 & \text{if } (x, y) \in R_i \\ 0 & \text{if not.} \end{cases}$$

Such a matrix is called the i^{th} *adjacency matrix* of the association scheme.

Definition 2.4. The *adjacency algebra* of an association scheme is the subalgebra of $M_n(\mathbb{C})$ spanned by the adjacency matrices of the association scheme, where $n = |S|$.

Definition 2.5. The *valency* k_i of an adjacency matrix is the sum across any row of the matrix. It is equal to the number of z with $(x, z) \in R_i$ for any $x \in S$; so $k_i = p_{ii^*0}$.

Using the properties in Definition 2.3, it can be shown that the adjacency algebra of an association scheme (S, R) with adjacency matrices A_i forms an integral table algebra with basis $B = \{A_i : R_i \in R\}$ and structure constants p_{ijk}. The anti-automorphism is matrix transpose. It is standard; $\delta(A_i) = k_i = p_{ii^*0}$.

Definition 2.6. Let (A, B) be a table algebra. We define the *linear elements* of B by $L(B) = \{b \in B : bb^* = \lambda 1, \lambda \in \mathbb{R}\}$.

If a table algebra is standard, then its linear elements are exactly the elements of degree one, and these form a group.

Definition 2.7. An association scheme (S, R) is called *thin* if its set of adjacency matrices forms a group. In this case, the adjacency matrices are permutation matrices.

We now discuss the quotient of a table algebra by a subset of its basis. For any two elements $b_i, b_j \in B$, we define $Supp(b_i b_j) = \{b_k : \beta_{ijk} \neq 0\}$. We then define a set multiplication on the subsets of B by $ST = \bigcup_{s \in S, t \in T} Supp(st)$. We will regularly use the notation st in place of $\{s\}\{t\}$, and the reader should be able to tell from context which multiplication is meant. We will also be using the notation $S^+ = \sum_{s \in S} s$.

Definition 2.8. Let (A, B) be a table algebra. A *closed subset* of B is a subset with the property that $CC^* \subseteq C$.

This is equivalent to $C = C^*$ and $CC \subseteq C$.

Definition 2.9. The *order* of a subset C of B is $o(C) = \sum_{b_i \in C} \frac{\delta(b_i)^2}{\beta_{ii^*0}}$.

Note that if the algebra is standard, the order of a subset is simply the sum of the degrees of its elements. In the case of the adjacency algebra of an association scheme, the order of the basis is the sum of the valencies of the matrices, and this sum is exactly the size of the underlying set S.

Definition 2.10. Let (A, B) be a standard table algebra and C a closed subset. For $b \in B$, let $b//C = \dfrac{(CbC)^+}{o(C)}$ and $B//C = \{b//C : b \in B\}$. The *quotient algebra of* (A, B) *by* C is the table algebra $(A//C, B//C)$, where $A//C$ is the span over $\mathbb{C}$ of $B//C$.

The quotient algebra $(A//C, B//C)$ is also standard. Its anti-automorphism and degree map are simply the anti-automorphism and degree map for (A, B), restricted to $A//C$. This algebra has the properties that $o(B//C) = o(B)/o(C)$ and $(B//C)//(D//C) \cong B//D$ for any closed subsets C and D of B with $C \subseteq D$.

We now discuss nilpotency of table algebras.

Definition 2.11. The *upper central series* of a commutative standard table algebra is a chain of closed subsets of the basis $L^{(0)} \subseteq L^{(1)} \subseteq L^{(2)} \subseteq \cdots$, where $L^{(0)} = \{1\}$ and for $i \geq 1, L^{(i)}$ is the preimage in B of $L(B//L^{(i-1)}(B))$.

This definition arises from the definition of the upper central series of a group in that if $(A, B) = (Z(\mathbb{C}G), \{C_g^+\})$, then the chain $L^{(0)} \subseteq L^{(1)} \subseteq L^{(2)} \subseteq \cdots$ corresponds to the chain $Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots$ via $L^{(i)} = \{C_g^+ : gZ_{i-1} \in Z(G/Z_{i-1})\} = \{C_g^+ : g \in Z_i\}$.

Definition 2.12. A commutative table algebra is said to be *nilpotent of class* n if its upper central series terminates in B after n steps, i.e. $L^{(n)} = L^{(n+1)} = B$.

Definition 2.13. Let H be a group and let $(\mathbb{C}F, F)$ be a standard table algebra. We say that a standard table algebra (A, B) is an *extension of* $(\mathbb{C}F, F)$ *by* $(\mathbb{C}H, H)$ if there is a subgroup H' of $L(B)$ with $H' \cong H$ and $B//H' \cong F$.

Definition 2.14. Let (A, B) and (C, D) be standard table algebras, with $B = \{b_0 = 1_B, b_1, \ldots, b_k\}$ and $D = \{d_0 = 1_C, d_1, \ldots, d_m\}$. Let

$$B \wr D = \{b_0 \otimes d_j : 0 \leq j \leq m\} \cup \{b_i \otimes D^+ : 1 \leq i \leq k\}.$$

Then $B \wr D$ is a linearly independent subset of $A \otimes_{\mathbb{C}} C$. Let $A \wr C$ be the $\mathbb{C}-$space spanned by $B \wr D$. Then $(A \wr C, B \wr D)$ is a standard table algebra, which we call the *wreath product of* (A, B) *and* (C, D).

Theorem 2.1. *Let* (A, B) *be a standard table algebra and let* N *be a closed subset of* B. *Then* $(A, B) \cong_x (A//N, B//N) \wr (\mathbb{C}N, N)$ *if and only if for any* $n \in N$ *and* $b \in B \setminus N, Supp(nb) = Supp(bn) = \{b\}$.

Definition 2.15. A matrix $Circ(c_0, c_1, \ldots, c_n)$ is said to be *circulant* if it has the form

$$\begin{bmatrix} c_0 & c_1 & \cdots & c_n \\ c_n & c_0 & \cdots & c_{n-1} \\ & & \vdots & \\ c_1 & c_2 & \cdots & c_0 \end{bmatrix}.$$

2.2 Previous Results

The following results provide a summary of previous work done on the problem of classifying extensions of table algebras. In [5], Hirasaka and Bang study an association scheme (X, G) that is an extension of an association scheme (Y, H) by an association scheme (Z, F). They cover the case where (Y, H) and (Z, F) are both thin, so that (X, G) is an extension of a group by a group. They develop the construction of such an extension, and give necessary and sufficient conditions for its existence. These conditions then produce a bound on the number of schemes of this type, up to isomorphism.

In [9], Blau and Xu investigate commutative, standard table algebras (A, B) formed as the extension of a group algebra $\mathbb{C}H$ by a group algebra $\mathbb{C}F$. These are

exactly the class 2 nilpotent standard table algebras. Given abelian groups F and H, and an analogue of a 2-cocycle $\alpha : F \times F \to H$, they develop the construction of such an extension, and show that any extension of this type must have exactly this construction. They also find necessary and sufficient conditions for an extension of this type to be the adjacency algebra of an association scheme. In this dissertation, we will generalize these results to noncommutative, standard table algebras within which the group H is central, but the proofs are similar to Blau and Xu's. The results by Blau and Xu are as follows.

Theorem 2.2 ([9])**.** *Let (A, B) be a standard, commutative table algebra with a group $H \hookrightarrow B$ and $B//H \cong F$, where F is a group. (A, B) is necessarily integral, and B can be written $B = \{t_\sigma h : \sigma \in F, h \in H\}$ where the t_σ comprise a set of coset representatives for H in B. For each $\sigma \in F$, let $S_\sigma = \{h \in H : t_\sigma h = t_\sigma\}$, a subgroup of H. For each $\sigma \in F, S_\sigma = S_{\sigma^{-1}}$ and $S_{\sigma\tau} \subseteq S_\sigma S_\tau$. There also exists a function $\alpha : F \times F \to H$, called a factor set, satisfying $\alpha(\sigma, \tau\rho)\alpha(\tau, \rho) \equiv \alpha(\sigma\tau, \rho)\alpha(\sigma, \tau)$ mod $S_\sigma S_\tau S_\rho$ for all $\sigma, \tau, \rho \in F$, such that*

$$(t_\sigma h_1)(t_\tau h_2) = |S_\sigma \cap S_\tau| \sum_{\substack{h \text{ coset} \\ \text{reps of } S_{\sigma\tau} \\ \text{in } S_\sigma S_\tau}} t_{\sigma\tau}\alpha(\sigma, \tau)hh_1h_2.$$

Conversely, given abelian groups H and F, a collection of subgroups $\{S_\sigma : \sigma \in F\}$ of H satisfying $S_\sigma = S_{\sigma^{-1}}$ and $S_{\sigma\tau} \subseteq S_\sigma S_\tau$, and a factor set α satisfying the above-mentioned congruence, these determine a unique standard, integral table algebra

(A, B) with $H \hookrightarrow B$ and $B//H \cong F$, such that $S_\sigma = \{h \in H : t_\sigma h = t_\sigma\}$ for a set $\{t_\sigma : \sigma \in F\}$ of coset representatives for H in B, and

$$(t_\sigma h_1)(t_\tau h_2) = |S_\sigma \cap S_\tau| \sum_{\substack{h \text{ coset} \\ \text{reps of } S_{\sigma\tau} \\ \text{in } S_\sigma S_\tau}} t_{\sigma\tau}\alpha(\sigma, \tau)hh_1h_2.$$

Theorem 2.3. *The algebra described in Theorem 2.2 arises as the adjacency algebra of an association scheme if and only if there is a choice of factor set α such that $\alpha(\sigma\tau, \rho)\alpha(\sigma, \tau) \equiv \alpha(\sigma, \tau\rho)\alpha(\tau, \rho)$ mod $S_\sigma S_\tau \cap S_\tau S_\rho$ for all $\sigma, \tau, \rho \in F$.*

CHAPTER 3

EXTENSIONS OF GROUP ALGEBRAS BY GROUP ALGEBRAS

In this section we prove the non-commutative generalizations of Theorems 2.2 and 2.3.

Theorem 3.1. *Let (A, B) be a standard table algebra with a central group $H \hookrightarrow B$ and $B//H \cong F$, where F is a group. (A, B) is necessarily integral, and B can be written $B = \{t_\sigma h : \sigma \in F, h \in H\}$ where the t_σ comprise a set of coset representatives for H in B. For each $\sigma \in F$, let $S_\sigma = \{h \in H : t_\sigma h = t_\sigma\}$, a subgroup of H. For $\sigma, \tau \in F$, these satisfy $S_\sigma = S_{\sigma^{-1}}$ and $S_{\sigma\tau} \subseteq S_\sigma S_\tau$. There also exists a function $\alpha : F \times F \to H$, called a factor set, satisfying $\alpha(\sigma, \tau\rho)\alpha(\tau, \rho) \equiv \alpha(\sigma\tau, \rho)\alpha(\sigma, \tau)$ mod $S_\sigma S_\tau S_\rho$ for all $\sigma, \tau, \rho \in F$, such that*

$$(t_\sigma h_1)(t_\tau h_2) = |S_\sigma \cap S_\tau| \sum_{\substack{h \text{ coset} \\ \text{reps of } S_{\sigma\tau} \\ \text{in } S_\sigma S_\tau}} t_{\sigma\tau}\alpha(\sigma, \tau)hh_1h_2.$$

Conversely, given an abelian group H, a group F, a collection of subgroups $\{S_\sigma : \sigma \in F\}$ of H satisfying $S_\sigma = S_{\sigma^{-1}}$ and $S_{\sigma\tau} \subseteq S_\sigma S_\tau$, and a factor set α satisfying the above-mentioned congruence, these determine a unique standard, integral table

algebra (A, B) *with* $H \hookrightarrow B$ *and* $B//H \cong F$*, such that if* $\{t_\sigma : \sigma \in F\}$ *is a set of coset representatives for* H *in* B*, then* $S_\sigma = \{h \in H : t_\sigma h = t_\sigma\}$ *and*

$$(t_\sigma h_1)(t_\tau h_2) = |S_\sigma \cap S_\tau| \sum_{\substack{h \text{ coset} \\ \text{reps of } S_{\sigma\tau} \\ \text{in } S_\sigma S_\tau}} t_{\sigma\tau}\alpha(\sigma,\tau)hh_1h_2.$$

Proof. For the first direction, suppose (A, B) is a standard table algebra satisfying the given conditions. Since $B//H \cong F$, $B = \{t_\sigma h : \sigma \in F, h \in H\}$ for a set of coset representatives t_σ. We choose $t_1 = 1$. It is easily shown that the sets S_σ for $\sigma \in F$ are in fact subgroups of $L(B)$.

Since F is a group, $(t_\sigma//H) \cdot (t_\sigma^*//H) = 1//H$, so $t_\sigma^* = t_{\sigma^{-1}}h_\sigma$ for some $h_\sigma \in H$. Hence $S_\sigma = S_{\sigma^{-1}}$ since $h \in S_\sigma \Rightarrow t_{\sigma^{-1}}h_\sigma = t_\sigma^* = (t_\sigma h)^* = t_\sigma^* h^{-1} = t_{\sigma^{-1}}h_\sigma h^{-1} \Rightarrow t_{\sigma^{-1}} = t_{\sigma^{-1}}h^{-1} \Rightarrow h^{-1} \in S_{\sigma^{-1}} \Rightarrow h \in S_{\sigma^{-1}}$. Similarly, $S_{\sigma^{-1}} \subseteq S_\sigma$.

To show that $S_{\sigma\tau} \subseteq S_\sigma S_\tau$, note that $(t_\sigma//H) \cdot (t_\sigma^*//H) = 1//H \Rightarrow Supp(t_\sigma t_\sigma^*) \subseteq H$, and $\langle t_\sigma t_\sigma^*, h\rangle = \langle t_\sigma, t_\sigma h\rangle \neq 0 \Leftrightarrow h \in S_\sigma$. So $Supp(t_\sigma t_\sigma^*) = S_\sigma$. Thus $Supp(t_\sigma t_\sigma^* t_\tau t_\tau^*) = S_\sigma S_\tau$, and since $Supp(t_\tau t_\tau^*) \subseteq H$ and H is central, $(t_\sigma t_\tau)(t_\sigma t_\tau)^* = t_\sigma t_\tau t_\tau^* t_\sigma^* = t_\sigma t_\sigma^* t_\tau t_\tau^*$. So

$$Supp\left((t_\sigma t_\tau)(t_\sigma t_\tau)^*\right) = S_\sigma S_\tau.$$

Now, since $(t_\sigma//H) \cdot (t_\tau//H) = t_{\sigma\tau}//H, t_\sigma t_\tau = \sum_{h\in H} \beta_h t_{\sigma\tau}h$ with at least one $\beta_h > 0$. So $S_{\sigma\tau} = Supp(t_{\sigma\tau}t_{\sigma\tau}^*) \subseteq Supp\left((t_\sigma t_\tau)(t_\sigma t_\tau)^*\right) = S_\sigma S_\tau$.

We now show that there exists a factor set α satisfying the claimed congruence. Since $Supp\left((t_\sigma t_\tau)(t_\sigma t_\tau)^*\right) = S_\sigma S_\tau$, for each h_1, h_2 with $t_{\sigma\tau}h_1, t_{\sigma\tau}h_2 \in Supp(t_\sigma t_\tau)$, $Supp\left(t_{\sigma\tau}t_{\sigma\tau}^* h_1 h_2^{-1}\right) \subseteq S_\sigma S_\tau$, so $h_1 h_2^{-1} \in S_\sigma S_\tau$ since $1 \in Supp\left(t_{\sigma\tau}t_{\sigma\tau}^*\right)$. So for all h_1, h_2 with $t_{\sigma\tau}h_1, t_{\sigma\tau}h_2 \in Supp(t_\sigma t_\tau), h_1 \equiv h_2 \bmod S_\sigma S_\tau$. Thus there exists some $\alpha(\sigma,\tau) \in H$ with $t_\sigma t_\tau = \sum_{h\in S_\sigma S_\tau} \beta_h t_{\sigma\tau}\alpha(\sigma,\tau)h$. Note that for any $\sigma, \tau \in F$, $\alpha(\sigma,\tau)$ is

only determined up to congruence modulo $S_\sigma S_\tau$ since replacing $\alpha(\sigma,\tau)$ with $\alpha(\sigma,\tau)h$ for $h \in S_\sigma S_\tau$ gives $t_\sigma t_\tau h = t_\sigma t_\tau$.

Now, for any $h \in S_\sigma S_\tau$, $\beta_h = \dfrac{\langle t_\sigma t_\tau, t_{\sigma\tau}\alpha(\sigma,\tau)h\rangle}{\delta(t_{\sigma\tau})} = \dfrac{\langle t_\sigma t_\tau h^{-1}, t_{\sigma\tau}\alpha(\sigma,\tau)\rangle}{\delta(t_{\sigma\tau})} = \dfrac{1}{\delta(t_{\sigma\tau})}\langle t_\sigma t_\tau, t_{\sigma\tau}\alpha(\sigma,\tau)\rangle$. So β_h does not actually depend on h, so all β_h are equal. And since $t_{\sigma\tau}\alpha(\sigma,\tau)h_1 = t_{\sigma\tau}\alpha(\sigma,\tau)h_2$ if $h_1 \equiv h_2 \bmod S_{\sigma\tau}$, we can write

$$t_\sigma t_\tau = \sum_{\substack{h \text{ coset} \\ \text{reps of } S_{\sigma\tau} \\ \text{in } S_\sigma S_\tau}} \beta t_{\sigma\tau}\alpha(\sigma,\tau)h = \frac{\beta}{|S_{\sigma\tau}|}\sum_{h\in S_\sigma S_\tau} t_{\sigma\tau}\alpha(\sigma,\tau)h.$$

We now determine the value of β. Since B is standard, $\delta(t_\sigma) = \langle t_\sigma, t_\sigma\rangle = \langle t_\sigma, t_\sigma h\rangle = \langle t_\sigma t_\sigma^*, h\rangle$ for any $h \in S_\sigma$. So $t_\sigma t_\sigma^* = \delta(t_\sigma)\sum_{h\in S_\sigma} h$, and therefore

$$\delta(t_\sigma t_\sigma^*) = \delta\left(\sum_{h\in S_\sigma}\delta(t_\sigma)h\right) = \delta(t_\sigma)\sum_{h\in S_\sigma}\delta(h) = \delta(t_\sigma)|S_\sigma|$$

$$\Rightarrow \delta(t_\sigma)^2 = \delta(t_\sigma)|S_\sigma| \Rightarrow \delta(t_\sigma) = |S_\sigma|.$$

Calculating $\delta(t_\sigma t_\tau)$ and setting it equal to $|S_\sigma||S_\tau|$ now gives $\beta = \dfrac{|S_\sigma||S_\tau|}{|S_\sigma S_\tau|} = |S_\sigma \cap S_\tau|$. Thus (A, B) is integral.

We now have

$$(t_\sigma h_1)(t_\tau h_2) = \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|}\sum_{h\in S_\sigma S_\tau} t_{\sigma\tau}\alpha(\sigma,\tau)hh_1h_2. \qquad (*)$$

We now show that $\alpha(\sigma,\tau\rho)\alpha(\tau,\rho) \equiv \alpha(\sigma\tau,\rho)\alpha(\sigma,\tau) \bmod S_\sigma S_\tau S_\rho$. This is a result of the associativity of the algebra.

$$\begin{aligned}
(t_\sigma t_\tau)t_\rho &= \left(\frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|}\sum_{h\in S_\sigma S_\tau} t_{\sigma\tau}\alpha(\sigma,\tau)h\right)t_\rho \\
&= \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|}\sum_{h\in S_\sigma S_\tau} t_{\sigma\tau}t_\rho\alpha(\sigma,\tau)h \\
&= \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|}\sum_{h\in S_\sigma S_\tau}\left(\frac{|S_{\sigma\tau} \cap S_\rho|}{|S_{\sigma\tau\rho}|}\sum_{k\in S_{\sigma\tau}S_\rho} t_{\sigma\tau\rho}\alpha(\sigma\tau,\rho)k\right)\alpha(\sigma,\tau)h \\
&= \frac{|S_\sigma \cap S_\tau||S_{\sigma\tau} \cap S_\rho|}{|S_{\sigma\tau}||S_{\sigma\tau\rho}|}\sum_{h\in S_\sigma S_\tau}\sum_{k\in S_{\sigma\tau}S_\rho} t_{\sigma\tau\rho}\alpha(\sigma\tau,\rho)\alpha(\sigma,\tau)hk.
\end{aligned}$$

Similarly,

$$t_\sigma(t_\tau t_\rho) = \frac{|S_\tau \cap S_\rho||S_\sigma \cap S_{\tau\rho}|}{|S_{\tau\rho}||S_{\sigma\tau\rho}|}\sum_{h\in S_\tau S_\rho}\sum_{k\in S_\sigma S_{\tau\rho}} t_{\sigma\tau\rho}\alpha(\sigma,\tau\rho)\alpha(\tau,\rho)hk.$$

The same basis elements must appear in each of these, so

$$\begin{aligned}
&\{t_{\sigma\tau\rho}\alpha(\sigma\tau,\rho)\alpha(\sigma,\tau)hk : h\in S_\sigma S_\tau, k\in S_{\sigma\tau}S_\rho\} \\
= \;&\{t_{\sigma\tau\rho}\alpha(\sigma,\tau\rho)\alpha(\tau,\rho)hk : h\in S_\tau S_\rho, k\in S_\sigma S_{\tau\rho}\}.
\end{aligned}$$

So let $h \in S_\sigma S_\tau$ and $k \in S_{\sigma\tau}S_\rho$. Then there exists $h' \in S_\tau S_\rho$ and $k' \in S_\sigma S_{\tau\rho}$ such that

$$t_{\sigma\tau\rho}\alpha(\sigma\tau,\rho)\alpha(\sigma,\tau)hk = t_{\sigma\tau\rho}\alpha(\sigma,\tau\rho)\alpha(\tau,\rho)h'k'.$$

Then since $S_{\sigma\tau\rho} \subseteq S_\sigma S_\tau S_\rho$,

$\alpha(\sigma\tau,\rho)\alpha(\sigma,\tau)hk \equiv \alpha(\sigma,\tau\rho)\alpha(\tau,\rho)h'k' \bmod S_{\sigma\tau\rho} \Rightarrow$

$\alpha(\sigma,\tau\rho)\alpha(\tau,\rho)h'k'h^{-1}k^{-1} \equiv \alpha(\sigma\tau,\rho)\alpha(\sigma,\tau) \bmod S_{\sigma\tau\rho} \Rightarrow$

$\alpha(\sigma, \tau\rho)\alpha(\tau, \rho) \equiv \alpha(\sigma\tau, \rho)\alpha(\sigma, \tau) \bmod S_\sigma S_\tau S_\rho$ since $h'k'h^{-1}k^{-1} \in S_\sigma S_\tau S_\rho$.

For the other direction, let H, F, α, and $\{S_\sigma : \sigma \in F\}$ satisfy the given conditions. Let $B = \{t_\sigma h : \sigma \in F, h \in H\}$, where $t_\sigma h_1 = t_\tau h_2 \Leftrightarrow \sigma = \tau$ and $h_1 \equiv h_2 \bmod S_\sigma (= S_\tau)$. Let $t_1 1 = 1$; we then identify $t_1 h$ with h and $t_\sigma 1$ with t_σ. Note that this means $t_\sigma h = t_\sigma \Leftrightarrow h \in S_\sigma$. We give the elements of B the multiplication

$$(t_\sigma h_1)(t_\tau h_2) = \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \sum_{h \in S_\sigma S_\tau} t_{\sigma\tau}\alpha(\sigma, \tau)hh_1h_2.$$

We now show that this multiplication is associative.

$$(t_\sigma h_1)(t_\tau h_2 t_\rho h_3) = t_\sigma h_1 \left(\frac{|S_\tau \cap S_\rho|}{|S_{\tau\rho}|} \sum_{h \in S_\tau S_\rho} t_{\tau\rho}\alpha(\tau, \rho)h(h_2h_3) \right)$$

$$= \frac{|S_\tau \cap S_\rho|}{|S_{\tau\rho}|} \left(\sum_{h \in S_\tau S_\rho} \left(\frac{|S_\sigma \cap S_{\tau\rho}|}{|S_{\sigma\tau\rho}|} \sum_{k \in S_\sigma S_{\tau\rho}} t_{\sigma\tau\rho}\alpha(\sigma, \tau\rho)k\alpha(\tau, \rho)h(h_1h_2h_3) \right) \right)$$

$$= \frac{|S_\tau \cap S_\rho||S_\sigma \cap S_{\tau\rho}|}{|S_{\tau\rho}||S_{\sigma\tau\rho}|} \sum_{\substack{h \in S_\tau S_\rho, \\ k \in S_\sigma S_{\tau\rho}}} t_{\sigma\tau\rho}\alpha(\sigma, \tau\rho)\alpha(\tau, \rho)hk(h_1h_2h_3).$$

Now, $S_\tau S_\rho S_\sigma S_{\tau\rho} = S_\sigma S_\tau S_\rho$. In order to equate the above sum to $(t_\sigma h_1 t_\tau h_2)(t_\rho h_3)$, we need to sum over only the distinct elements of $S_\sigma S_\tau S_\rho$. Since

$$|S_\sigma S_\tau S_\rho| = \frac{|S_\tau S_\rho||S_\sigma S_{\tau\rho}|}{|S_\tau S_\rho \cap S_\sigma S_{\tau\rho}|},$$

for each $x \in S_\sigma S_\tau S_\rho$, there are $|S_\tau S_\rho \cap S_\sigma S_{\tau\rho}|$ pairs $h \in S_\tau S_\rho, k \in S_\sigma S_{\tau\rho}$ such that $hk = x$. So:

$(t_\sigma h_1)(t_\tau h_2 t_\rho h_3) =$

$$\frac{|S_\tau \cap S_\rho||S_\sigma \cap S_{\tau\rho}||S_\tau S_\rho \cap S_\sigma S_{\tau\rho}|}{|S_{\tau\rho}||S_{\sigma\tau\rho}|} \sum_{j \in S_\sigma S_\tau S_\rho} t_{\sigma\tau\rho}\alpha(\sigma, \tau\rho)\alpha(\tau, \rho)j(h_1h_2h_3). \quad (1)$$

Similarly,

$(t_\sigma h_1 t_\tau h_2)(t_\rho h_3) =$

$$\frac{|S_\sigma \cap S_\tau||S_{\sigma\tau} \cap S_\rho||S_\sigma S_\tau \cap S_{\sigma\tau} S_\rho|}{|S_{\sigma\tau}||S_{\sigma\tau\rho}|} \sum_{j \in S_\sigma S_\tau S_\rho} t_{\sigma\tau\rho}\alpha(\sigma\tau, \rho)\alpha(\sigma, \tau)j(h_1h_2h_3). \quad (2)$$

By the assumption $\alpha(\sigma, \tau\rho)\alpha(\tau, \rho) \equiv \alpha(\sigma\tau, \rho)\alpha(\sigma, \tau) \bmod S_\sigma S_\tau S_\rho$, the summands in (1) and (2) are equal. The coefficients are equal as well, because of the following:

$$\frac{|S_\tau \cap S_\rho||S_\sigma \cap S_{\tau\rho}||S_\tau S_\rho \cap S_\sigma S_{\tau\rho}|}{|S_{\tau\rho}||S_{\sigma\tau\rho}|} \quad (3)$$

$$= \frac{|S_\tau||S_\rho|}{|S_\tau S_\rho|} \cdot \frac{|S_\sigma||S_{\tau\rho}|}{|S_\sigma S_{\tau\rho}|} \cdot \frac{|S_\tau S_\rho||S_\sigma S_{\tau\rho}|}{|S_\tau S_\rho S_\sigma S_{\tau\rho}|} \cdot \frac{1}{|S_{\tau\rho}||S_{\sigma\tau\rho}|}$$

$$= \frac{|S_\tau||S_\rho||S_\sigma|}{|S_\sigma S_\tau S_\rho||S_{\sigma\tau\rho}|}. \quad (4)$$

The coefficient in (2) is exactly the same as (3) with σ and ρ switched, and (4) is symmetric in σ and ρ; so the coefficients are equal. Thus (1)=(2) and associativity holds.

The argument above that culminates in equation $(*)$ shows that this multiplication is unique.

We define the anti-automorphism of $(A, B) = (\mathbb{C}B, B)$ by

$$(t_\sigma h)^* = t_{\sigma^{-1}} h^{-1} \alpha(\sigma, \sigma^{-1})^{-1},$$

extended linearly. We now show that this map is in fact an anti-automorphism. In the following calculation, we will use $\alpha(\sigma, 1) = \alpha(1, \sigma) = 1$ for each $\sigma \in F$. This does not result in a loss of generality since $t_\sigma t_1 = t_\sigma = t_1 t_\sigma$ implies $\alpha(\sigma, 1)$ and $\alpha(1, \sigma)$ may be set equal to any element of S_σ.

$$\begin{aligned}
(t_\sigma h_1 t_\tau h_2)^* &= \left(\frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \sum_{h \in S_\sigma S_\tau} t_{\sigma\tau} \alpha(\sigma, \tau) h(h_1 h_2) \right)^* \\
&= \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \sum_{h \in S_\sigma S_\tau} t_{(\sigma\tau)^{-1}} (\alpha(\sigma, \tau) h(h_1 h_2))^{-1} \alpha(\sigma\tau, (\sigma\tau)^{-1})^{-1} \\
&= \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \sum_{h \in S_\sigma S_\tau} t_{(\sigma\tau)^{-1}} \alpha(\sigma, \tau)^{-1} h^{-1} h_1^{-1} h_2^{-1} \alpha(\sigma\tau, (\sigma\tau)^{-1})^{-1}.
\end{aligned}$$

And

$$\begin{aligned}
(t_\tau h_2)^* (t_\sigma h_1)^* &= \left(t_{\tau^{-1}} h_2^{-1} \alpha(\tau, \tau^{-1})^{-1} \right) \left(t_{\sigma^{-1}} h_1^{-1} \alpha(\sigma, \sigma^{-1})^{-1} \right) \\
&= \frac{|S_{\tau^{-1}} \cap S_{\sigma^{-1}}|}{|S_{\tau^{-1}\sigma^{-1}}|} \sum_{h \in S_{\tau^{-1}} S_{\sigma^{-1}}} t_{(\sigma\tau)^{-1}} \alpha(\tau^{-1}, \sigma^{-1}) h \left(h_2 \alpha(\tau, \tau^{-1}) h_1 \alpha(\sigma, \sigma^{-1}) \right)^{-1} \\
&= \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \sum_{h \in S_\sigma S_\tau} t_{(\sigma\tau)^{-1}} \alpha(\tau^{-1}, \sigma^{-1}) h^{-1} h_1^{-1} h_2^{-1} \alpha(\tau, \tau^{-1})^{-1} \alpha(\sigma, \sigma^{-1})^{-1}.
\end{aligned}$$

These are equal by the following argument.

$\alpha(\sigma, \tau)\alpha(\sigma\tau, (\sigma\tau)^{-1}) \equiv \alpha(\tau, (\sigma\tau)^{-1})\alpha(\sigma, \tau(\sigma\tau)^{-1}) \bmod S_\sigma S_\tau S_{(\sigma\tau)^{-1}} = S_\sigma S_\tau$

$\Rightarrow \alpha(\sigma, \tau)\alpha(\sigma\tau, (\sigma\tau)^{-1})\alpha(\tau^{-1}, \sigma^{-1}) \equiv \alpha(\tau, \tau^{-1}\sigma^{-1})\alpha(\sigma, \sigma^{-1})\alpha(\tau^{-1}, \sigma^{-1}) \bmod S_\sigma S_\tau.$

And $\alpha(\tau,\tau^{-1}\sigma^{-1})\alpha(\tau^{-1},\sigma^{-1}) \equiv \alpha(\tau\tau^{-1},\sigma^{-1})\alpha(\tau,\tau^{-1}) \bmod S_\tau S_{\tau^{-1}} S_{\sigma^{-1}} = S_\sigma S_\tau$. Since $\alpha(1,\sigma^{-1}) = 1$, we now have

$$\alpha(\sigma,\tau)\alpha(\sigma\tau,(\sigma\tau)^{-1})\alpha(\tau^{-1},\sigma^{-1}) \equiv \alpha(\sigma,\sigma^{-1})\alpha(\tau,\tau^{-1}) \bmod S_\sigma S_\tau.$$

Thus

$$\alpha(\tau^{-1},\sigma^{-1})\alpha(\sigma,\sigma^{-1})^{-1}\alpha(\tau,\tau^{-1})^{-1} \equiv \alpha(\sigma,\tau)^{-1}\alpha(\sigma\tau,(\sigma\tau)^{-1})^{-1} \bmod S_\sigma S_\tau.$$

So $(t_\sigma h_1 t_\tau h_2)^* = (t_\tau h_2)^*(t_\sigma h_1)^*$.

We now show that the structure constant $\beta_{ij0} = 0$ unless $i = j^*$. Let $b_i = t_\sigma h_1, b_j = t_\tau h_2$. Then

$$b_i b_j = \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \sum_{h \in S_\sigma S_\tau} t_{\sigma\tau}\alpha(\sigma,\tau)hh_1h_2.$$

Suppose $t_1 1 = b_0$ appears in this sum. Then $\tau = \sigma^{-1}$, and for some $h' \in S_\sigma S_\tau = S_\sigma S_{\sigma^{-1}} = S_\sigma$,

$$\begin{aligned}
t_{\sigma\tau}\alpha(\sigma,\tau)h'(h_1h_2) &= t_1\alpha(\sigma,\sigma^{-1})h'(h_1h_2) = t_1 1 \\
\Rightarrow \alpha(\sigma,\sigma^{-1})h'(h_1h_2) &\equiv 1 \bmod S_1 \\
\Rightarrow \alpha(\sigma,\sigma^{-1})h'(h_1h_2) &= 1 \\
\Rightarrow h_2 &= (\alpha(\sigma,\sigma^{-1})h'h_1)^{-1} \\
&= \alpha(\sigma,\sigma^{-1})^{-1}h_1^{-1}h'^{-1}.
\end{aligned}$$

So $b_i = t_\sigma h_1$ and $b_j = t_{\sigma^{-1}}\alpha(\sigma,\sigma^{-1})^{-1}h_1^{-1}h'^{-1} = t_{\sigma^{-1}}\alpha(\sigma,\sigma^{-1})^{-1}h_1^{-1}$ since $h'^{-1} \in S_\sigma = S_{\sigma^{-1}}$. Thus $b_j = (t_\sigma h_1)^* = b_i^*$.

Furthermore, $\beta_{ii^*0} \neq 0$ because if $b_i = t_\sigma h_1$,

$$\begin{aligned} b_i b_i^* &= (t_\sigma h_1)(t_\sigma h_1)^* = (t_\sigma h_1)(t_{\sigma^{-1}} \alpha(\sigma, \sigma^{-1})^{-1} h_1^{-1}) \\ &= \frac{|S_\sigma \cap S_{\sigma^{-1}}|}{|S_{\sigma\sigma^{-1}}|} \sum_{h \in S_\sigma} t_1 \alpha(\sigma, \sigma^{-1}) h (h_1 \alpha(\sigma, \sigma^{-1})^{-1} h_1^{-1}) = |S_\sigma| \sum_{h \in S_\sigma} t_1 h. \end{aligned}$$

So for $h = 1$, b_0 shows up with coefficient $|S_\sigma|$. Note that this also shows that $t_\sigma t_\sigma^* = |S_\sigma| \sum_{h \in S_\sigma} h$.

We now define the degree map to be $\delta(t_\sigma h) = |S_\sigma|$. This is an algebra homomorphism, since

$$\begin{aligned} \delta(t_\sigma h_1 t_\tau h_2) &= \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \sum_{h \in S_\sigma S_\tau} \delta(t_{\sigma\tau} \alpha(\sigma, \tau) h h_1 h_2) \\ &= \frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|} \cdot |S_\sigma S_\tau| \delta(t_{\sigma\tau}) \\ &= \frac{|S_\sigma \cap S_\tau||S_\sigma S_\tau||S_{\sigma\tau}|}{|S_{\sigma\tau}|} = |S_\sigma||S_\tau| = \delta(t_\sigma h_1)\delta(t_\tau h_2). \end{aligned}$$

Thus (A, B) is standard, and since the structure constants have already been shown to be integers, we have now shown that (A, B) is a standard, integral table algebra.

It remains to show that $B//H \cong F$. The isomorphism is $\phi(\sigma) = t_\sigma//H$. This is clearly a bijection. To show that it is an isomorphism, first note that $t_\sigma//H =$

$\frac{(t_\sigma H)^+}{|H|} = \frac{t_\sigma H^+}{|H||S_\sigma|}$ since $t_\sigma h_1 = t_\sigma h_2$ whenever $h_1 \equiv h_2 \bmod S_\sigma$. Thus, noting that $t_\sigma h // H = t_\sigma // H$ for all $h \in H$, we have

$$\begin{aligned}
\phi(\sigma)\phi(\tau) &= \frac{1}{o(H)|S_\sigma|}\sum_{h\in H} t_\sigma h \frac{1}{o(H)|S_\tau|}\sum_{k\in H} t_\tau k \\
&= \frac{1}{o(H)|S_\sigma|}\frac{1}{o(H)|S_\tau|}\sum_{h,k\in H} t_\sigma h t_\tau k \\
&= \frac{1}{o(H)^2|S_\sigma||S_\tau|}\sum_{h,k\in H}\frac{|S_\sigma \cap S_\tau|}{|S_{\sigma\tau}|}\sum_{m\in S_\sigma S_\tau} t_{\sigma\tau}\alpha(\sigma,\tau)m(hk) \\
&= \frac{|S_\sigma \cap S_\tau|}{o(H)|S_\sigma||S_\tau|}\sum_{\substack{h\in H \\ m\in S_\sigma S_\tau}}\frac{1}{o(H)|S_{\sigma\tau}|}\sum_{k\in H} t_{\sigma\tau}\alpha(\sigma,\tau)m(hk) \\
&= \frac{|S_\sigma \cap S_\tau|}{o(H)|S_\sigma||S_\tau|}\sum_{h\in H}\sum_{m\in S_\sigma S_\tau} t_{\sigma\tau}//H \\
&= \frac{|S_\sigma \cap S_\tau||S_\sigma S_\tau|}{|S_\sigma||S_\tau|}\cdot(t_{\sigma\tau}//H) = t_{\sigma\tau}//H = \phi(\sigma\tau).
\end{aligned}$$

□

Remark 3.1. As mentioned in the above proof, $\alpha(\sigma,\tau)$ is only determined up to congruence modulo $S_\sigma S_\tau$. Two factor sets that differ only by multiplication by an element of $S_\sigma S_\tau$ will yield exactly isomorphic algebras. With this in mind, we state the following theorem. Note the slight difference from Theorem 2.3.

Theorem 3.2. *The algebra described in Theorem 3.1 arises as the adjacency algebra of an association scheme if and only if there is a choice of factor set α such that $\alpha(\sigma,\tau\rho)\alpha(\tau,\rho) \equiv \alpha(\sigma\tau,\rho)\alpha(\sigma,\tau) \bmod S_\sigma S_\tau$ for all $\sigma,\tau,\rho \in F$.*

Proof. For the first direction, suppose that the algebra is the adjacency algebra of an association scheme. Since B is the set of adjacency matrices for this scheme, we will index the relations of the scheme by elements of B, R_b. We will calculate the relations for this scheme and then show that the factor set congruence follows. The

underlying set S for this scheme has size $|F||H|$ since $|S| = o(B)$ (as discussed after Definition 2.9), and $B//H \cong F \Rightarrow o(B)/o(H) = o(F) \Rightarrow o(B) = |F||H|$. So we will label the elements of the underlying set with ordered pairs (σ, h) for $\sigma \in F, h \in H$. H induces the equivalence relation $(\sigma, h_1) \sim (\tau, h_2) \Leftrightarrow \sigma = \tau$ on the underlying set, and the scheme given by the adjacency algebra $B//H$ has the set of these equivalence classes as its underlying set. (See [5] or [12] for a thorough explanation of quotient schemes.) We therefore label these elements by (σ, H) for $\sigma \in F$.

Now, H is the basis of a subalgebra of A, and thus gives the adjacency algebra of a subscheme of the scheme given by B. It is, in fact, the scheme given by any one of the equivalence classes described above, so its underlying set is $\{(\sigma, h) : h \in H\}$ for any $\sigma \in F$; other choices of σ will simply yield copies of the same scheme. (Again, see [5] or [12] for a thorough explanation of subschemes.) Since H is a group, this scheme is thin, so the adjacency matrices form a group isomorphic to H. This forces $((\sigma, h_1), (\sigma, h_2)) \in R_{h_1 h_2^{-1}}$.

To see what relation $((\sigma, h_1), (\tau, h_2))$ is in when $\sigma \neq \tau$, note that since F is a group, it also gives a thin scheme, with $(\sigma, \tau) \in R_{\sigma\tau^{-1}}$. Thus the quotient scheme given by $B//H$ is also a thin scheme, and it is natural to label the elements of its underlying set (σ, H) for $\sigma \in F$, with $((\sigma, H), (\tau, H)) \in R_{(t_{\sigma\tau^{-1}}//H)}$. This means that the matrix $(t_{\sigma\tau^{-1}}H)^+$ has ones in the entries indexed by $((\sigma, h_1), (\tau, h_2))$ for every $h_1, h_2 \in H$. Thus $((\sigma, h_1), (\tau, h_2)) \in R_{t_{\sigma\tau^{-1}}h}$ for some $h \in H$.

Since this h is undetermined by $B//H \cong F$, we may choose it arbitrarily. Different choices will produce isomorphic schemes since they only differ in how we choose to label the elements of the underlying set. We now show that, given an appropriate labeling of elements of S, we have $h = \alpha(\sigma, \tau^{-1})\alpha(\tau^{-1}, \tau)^{-1}h_1 h_2^{-1} k$ for some $k \in S_\sigma S_\tau$.

We first choose an element of S to label as $(1,1)$. We then choose the element $s \in S$ with $(s,(1,1)) \in R_{t_\sigma h}$ for each $h \in H, \sigma \in F$. Since we have already chosen to label the elements of S so that $((\sigma,h_1),(\tau,h_2)) \in R_{t_{\sigma\tau^{-1}}h}$ for some $h \in H$, the first component of s must be σ. We let $s = (\sigma,h)$ so that $((\sigma,h),(1,1)) \in R_{t_\sigma h}$. This choice determines how the rest of S must be labeled. Using the facts that $((\sigma,h_1),(\tau,h_2)) \in R_b \Rightarrow ((\tau,h_2),(\sigma,h_1)) \in R_{b^*}$ and $((\sigma,h_1),(\tau,h_2)) \in R_{b_1}, ((\tau,h_2),(\pi,h_3)) \in R_{b_2} \Rightarrow ((\sigma,h_1),(\pi,h_3)) \in R_b$ for some $b \in b_1b_2$, we have for any $h_1,h_2 \in H, \sigma,\tau \in F$,

$$((1,1),(\tau,h_2)) \in R_{(t_\tau h_2)^*} = R_{t_{\tau^{-1}}\alpha(\tau,\tau^{-1})^{-1}h_2^{-1}},$$

so

$$((\sigma,h_1),(\tau,h_2)) \in R_b \text{ for some } b \in (t_\sigma h_1)(t_{\tau^{-1}}\alpha(\tau,\tau^{-1})^{-1}h_2^{-1}),$$

so

$$((\sigma,h_1),(\tau,h_2)) \in R_{t_{\sigma\tau^{-1}}\alpha(\sigma,\tau^{-1})\alpha(\tau,\tau^{-1})^{-1}h_1h_2^{-1}k}$$

for some $k \in S_\sigma S_{\tau^{-1}} = S_\sigma S_\tau$.

We now show that the k only depends on σ and τ, not on h_1 and h_2. Suppose $h_3,h_4 \in H$. Then $((\sigma,h_3),(\sigma,h_1)) \in R_{t_1h_3h_1^{-1}}$, so

$$((\sigma,h_3),(\tau,h_2)) \in R_{(t_1h_3h_1^{-1})(t_{\sigma\tau^{-1}}\alpha(\sigma,\tau^{-1})\alpha(\tau,\tau^{-1})^{-1}h_1h_2^{-1}k)} = R_{t_{\sigma\tau^{-1}}\alpha(\sigma,\tau^{-1})\alpha(\tau,\tau^{-1})^{-1}h_3h_2^{-1}k}.$$

And since $((\tau,h_2),(\tau,h_4)) \in R_{t_1h_2h_4^{-1}}$,

$$((\sigma,h_3),(\tau,h_4)) \in R_{(t_{\sigma\tau^{-1}}\alpha(\sigma,\tau^{-1})\alpha(\tau,\tau^{-1})^{-1}h_3h_2^{-1}k)(t_1h_2h_4^{-1})} = R_{t_{\sigma\tau^{-1}}\alpha(\sigma,\tau^{-1})\alpha(\tau,\tau^{-1})^{-1}h_3h_4^{-1}k}.$$

So the k remains the same when h_1 and h_2 are changed. We therefore label k as $k_{\sigma,\tau}$. We now make choices for the various $\alpha(\sigma,\tau)$ that simplify the relations.

Recall that $\alpha(\sigma,\tau)$ is only determined modulo $S_\sigma S_\tau$, and that we have already chosen $\alpha(1,\sigma)=\alpha(\sigma,1)=1$. Now choose $\alpha(\sigma^{-1},\sigma)=\alpha(\sigma,\sigma^{-1})$ for all $\sigma\in F$. This is allowable since for $a=\sigma^{-1}, b=\sigma, c=\sigma^{-1}$,

$$\begin{aligned}
\alpha(b,c)\alpha(a,bc) &\equiv \alpha(a,b)\alpha(ab,c) \bmod S_aS_bS_c \Rightarrow \\
\alpha(\sigma,\sigma^{-1})\alpha(\sigma^{-1},1) &\equiv \alpha(\sigma^{-1},\sigma)\alpha(1,\sigma^{-1}) \bmod S_\sigma \Rightarrow \\
\alpha(\sigma,\sigma^{-1}) &\equiv \alpha(\sigma^{-1},\sigma) \bmod S_\sigma,
\end{aligned}$$

and $\alpha(\sigma,\sigma^{-1}), \alpha(\sigma^{-1},\sigma)$ are only determined modulo S_σ. Now, choose a set of values $\alpha(\sigma,\tau)$ that satisfy the conditions of Theorem 3.1 and have $\alpha(\sigma,1)=\alpha(1,\sigma)=1$ and $\alpha(\sigma,\sigma^{-1})=\alpha(\sigma^{-1},\sigma)$. We will modify that choice to simplify the relations. We have shown that

$$\begin{aligned}
((\sigma,h_1),(\tau,h_2)) &\in R_{t_{\sigma\tau^{-1}}\alpha(\sigma,\tau^{-1})\alpha(\tau,\tau^{-1})^{-1}h_1h_2^{-1}k_{\sigma,\tau}} \\
&= R_{t_{\sigma\tau^{-1}}\alpha(\sigma,\tau^{-1})\alpha(\tau^{-1},\tau)^{-1}h_1h_2^{-1}k_{\sigma,\tau}}
\end{aligned}$$

for some $k_{\sigma,\tau}\in S_\sigma S_\tau$. We know that $\alpha(\sigma\tau^{-1},\tau)\alpha(\sigma,\tau^{-1}) \equiv \alpha(\tau^{-1},\tau)\alpha(\sigma,1) \bmod S_\sigma S_{\tau^{-1}}$, so $\alpha(\sigma,\tau^{-1})\alpha(\tau^{-1},\tau)^{-1} \equiv \alpha(\sigma\tau^{-1},\tau)^{-1} \bmod S_\sigma S_{\tau^{-1}}$. Say $\alpha(\sigma,\tau^{-1})\alpha(\tau^{-1},\tau)^{-1}$ $= \alpha(\sigma\tau^{-1},\tau)^{-1}l_{\sigma,\tau}$, where $l_{\sigma,\tau}\in S_\sigma S_{\tau^{-1}}$. Therefore

$$\alpha(\sigma,\tau^{-1})\alpha(\tau^{-1},\tau)^{-1}k_{\sigma,\tau} = \alpha(\sigma\tau^{-1},\tau)^{-1}l_{\sigma,\tau}k_{\sigma,\tau}$$

$$\Rightarrow ((\sigma,h_1),(\tau,h_2)) \in R_{t_{\sigma\tau^{-1}}\alpha(\sigma\tau^{-1},\tau)^{-1}h_1h_2^{-1}l_{\sigma,\tau}k_{\sigma,\tau}}.$$

So for any $\rho \neq 1, \tau^{-1}$, choose

$$\alpha'(\rho, \tau) = \alpha(\rho, \tau) l^{-1}_{\rho\tau,\tau} k^{-1}_{\rho\tau,\tau}.$$

Then for $\rho = \sigma\tau^{-1}$, we have

$$\alpha'(\sigma\tau^{-1}, \tau) = \alpha(\sigma\tau^{-1}, \tau) l^{-1}_{\sigma,\tau} k^{-1}_{\sigma,\tau}$$

$$\Rightarrow \alpha'(\sigma\tau^{-1}, \tau)^{-1} = \alpha(\sigma\tau^{-1}, \tau)^{-1} l_{\sigma,\tau} k_{\sigma,\tau}.$$

This gives

$$((\sigma, h_1), (\tau, h_2)) \in R_{t_{\sigma\tau^{-1}} \alpha'(\sigma\tau^{-1},\tau)^{-1} h_1 h_2^{-1}}.$$

For the remainder of the proof, we omit the prime. The association scheme relations are then given for all $\sigma, \tau \in F, h_1, h_2 \in H$ by

$$((\sigma, h_1), (\tau, h_2)) \in R_{t_{\sigma\tau^{-1}} \alpha(\sigma\tau^{-1},\tau)^{-1} h_1 h_2^{-1}}.$$

Now let $\sigma, \tau, \rho \in F$. Let $\pi = \tau\rho$ and $\beta = \sigma\tau\rho = \sigma\pi$. Then for any $h_1, h_2 \in H$,

$$\begin{aligned}
((\beta, h_1), (\pi, h)) &\in R_{t_{\beta\pi^{-1}} \alpha(\beta\pi^{-1},\pi)^{-1} h_1 h^{-1}}, \\
((\pi, h), (\rho, h_2)) &\in R_{t_{\pi\rho^{-1}} \alpha(\pi\rho^{-1},\rho)^{-1} h h_2^{-1}}, \text{ and} \\
((\beta, h_1), (\rho, h_2)) &\in R_{t_{\beta\rho^{-1}} \alpha(\beta\rho^{-1},\rho)^{-1} h_1 h_2^{-1}}.
\end{aligned}$$

Therefore $t_{\beta\rho^{-1}}\alpha(\beta\rho^{-1},\rho)^{-1}h_1h_2^{-1}$ is in

$$Supp\left[\left(t_{\beta\pi^{-1}}\alpha(\beta\pi^{-1},\pi)^{-1}h_1h^{-1}\right)\cdot\left(t_{\pi\rho^{-1}}\alpha(\pi\rho^{-1},\rho)^{-1}hh_2^{-1}\right)\right],$$

hence

$$t_{\beta\rho^{-1}}\alpha(\beta\rho^{-1},\rho)^{-1}h_1h_2^{-1}=t_{\beta\rho^{-1}}\alpha(\beta\pi^{-1},\pi\rho^{-1})\alpha(\beta\pi^{-1},\pi)^{-1}\alpha(\pi\rho^{-1},\rho)^{-1}h_1h_2^{-1}w$$

for some $w\in S_{\beta\pi^{-1}}S_{\pi\rho^{-1}}$. So
$\alpha(\beta\rho^{-1},\rho)^{-1}\equiv\alpha(\beta\pi^{-1},\pi)^{-1}\alpha(\pi\rho^{-1},\rho)^{-1}\alpha(\beta\pi^{-1},\pi\rho^{-1})w \bmod S_{\beta\rho^{-1}}$
$\Rightarrow\alpha(\beta\pi^{-1},\pi)\alpha(\pi\rho^{-1},\rho)\equiv\alpha(\beta\rho^{-1},\rho)\alpha(\beta\pi^{-1},\pi\rho^{-1}) \bmod S_{\beta\rho^{-1}}S_{\beta\pi^{-1}}S_{\pi\rho^{-1}}$.
Converting this to an expression in σ,τ, and ρ, we have

$$\alpha(\sigma,\tau\rho)\alpha(\tau,\rho)\equiv\alpha(\sigma\tau,\rho)\alpha(\sigma,\tau) \bmod S_{\sigma\tau}S_\sigma S_\tau=S_\sigma S_\tau.$$

For the other direction, assume that $\alpha(\sigma,\tau\rho)\alpha(\tau,\rho)\equiv\alpha(\sigma\tau,\rho)\alpha(\sigma,\tau) \bmod S_\sigma S_\tau$ holds; call this congruence (*). Let the underlying set be $F\times H$ and the relations be defined by $((\sigma,h_1),(\tau,h_2))\in R_b\Leftrightarrow b=t_{\sigma\tau^{-1}}\alpha(\sigma\tau^{-1},\tau)^{-1}h_1h_2^{-1}$. It is clear that these relations partition $(F\times H)\times(F\times H)$ and that R_{t_11} is the diagonal relation.

We now show that if $((\sigma,h_1),(\tau,h_2))\in R_b$, then $((\tau,h_2),(\sigma,h_1))\in R_{b^*}$. As discussed earlier, the anti-automorphism is given by $(t_\sigma h)^*=t_{\sigma^{-1}}\alpha(\sigma,\sigma^{-1})^{-1}h^{-1}$. Since
$((\sigma,h_1),(\tau,h_2))\in R_{t_{\sigma\tau^{-1}}\alpha(\sigma\tau^{-1},\tau)^{-1}h_1h_2^{-1}}$ and $((\tau,h_2),(\sigma,h_1))\in R_{t_{\tau\sigma^{-1}}\alpha(\tau\sigma^{-1},\sigma)^{-1}h_2h_1^{-1}}$, we need to show that

$$\begin{aligned}t_{\tau\sigma^{-1}}\alpha(\tau\sigma^{-1},\sigma)^{-1}h_2h_1^{-1} &= (t_{\sigma\tau^{-1}}\alpha(\sigma\tau^{-1},\tau)^{-1}h_1h_2^{-1})^*\\ &= t_{\tau\sigma^{-1}}\alpha(\sigma\tau^{-1},\tau\sigma^{-1})^{-1}\alpha(\sigma\tau^{-1},\tau)h_2h_1^{-1}.\end{aligned}$$

We've assumed that $\alpha(\sigma,\tau\rho)\alpha(\tau,\rho) \equiv \alpha(\sigma\tau,\rho)\alpha(\sigma,\tau) \bmod S_\sigma S_\tau$. So:

$$\begin{aligned} \alpha(\sigma\tau^{-1},\tau\sigma^{-1}) &= \alpha(\sigma\tau^{-1},\tau\sigma^{-1})\alpha(1,\sigma) \\ &\equiv \alpha(\sigma\tau^{-1},\tau\sigma^{-1}\sigma)\alpha(\tau\sigma^{-1},\sigma) \bmod S_{\sigma\tau^{-1}}S_{\tau\sigma^{-1}} = S_{\sigma\tau^{-1}} \\ \Rightarrow \alpha(\tau\sigma^{-1},\sigma)^{-1} &\equiv \alpha(\sigma\tau^{-1},\tau\sigma^{-1})^{-1}\alpha(\sigma\tau^{-1},\tau) \bmod S_{\sigma\tau^{-1}}. \end{aligned}$$

Therefore $t_{\tau\sigma^{-1}}\alpha(\sigma\tau^{-1},\tau\sigma^{-1})^{-1}\alpha(\sigma\tau^{-1},\tau)h_2h_1^{-1} = t_{\tau\sigma^{-1}}\alpha(\tau\sigma^{-1},\sigma)^{-1}h_2h_1^{-1}$.

We now show that the intersection numbers p_{rst} depend only on r, s, and t, and that these are exactly the structure constants of the algebra described in Theorem 3.1. Let $((\sigma,h_1),(\tau,h_2)) \in R_{b_t}$. If (ρ,h_3) has the property that $((\sigma,h_1),(\rho,h_3)) \in R_{b_r}$ and $((\rho,h_3),(\tau,h_2)) \in R_{b_s}$, then we say that (ρ,h_3) has property P with respect to σ,h_1,τ,h_2. If (ρ,h_3) has property P with respect to σ',τ',h_1',h_2' for some other pair $((\sigma',h_1'),(\tau'h_2')) \in R_{b_t}$, we will say that (ρ,h_3) has property P'. We show that the number of (ρ,h_3) with property P is the same as the number of (ρ,h_3) with property P'.

Let $((\sigma,h_1),(\tau,h_2)) \in R_{b_t}$ and suppose (ρ,h_3) has property P. Let $((\sigma',h_1'),(\tau',h_2')) \in R_{b_t}$. We first show that there exists (ρ',h_3') with property P'. Since

$$b_t = t_{\sigma\tau^{-1}}\alpha(\sigma\tau^{-1},\tau)^{-1}h_1h_2^{-1} = t_{\sigma'\tau'^{-1}}\alpha(\sigma'\tau'^{-1},\tau')^{-1}h_1'h_2'^{-1},$$

we know that $\sigma\tau^{-1} = \sigma'\tau'^{-1}$. Thus $\sigma^{-1}\sigma' = \tau^{-1}\tau' \Rightarrow \rho\sigma^{-1}\sigma' = \rho\tau^{-1}\tau'$. Let $\rho' = \rho\sigma^{-1}\sigma' = \rho\tau^{-1}\tau'$. Since $\alpha(\sigma\tau^{-1},\tau)^{-1}h_1h_2^{-1} \equiv \alpha(\sigma'\tau'^{-1},\tau')^{-1}h_1'h_2'^{-1} \bmod S_{\sigma\tau^{-1}}$, we have

$$\alpha(\sigma\tau^{-1},\tau)\alpha(\sigma\rho^{-1},\rho\tau^{-1})h_1^{-1}h_2 \equiv \alpha(\sigma'\tau'^{-1},\tau')\alpha(\sigma'\rho'^{-1},\rho'\tau'^{-1})h_1'^{-1}h_2' \bmod S_{\sigma\tau^{-1}}$$

because $\sigma\rho^{-1} = \sigma'\rho'^{-1}$ and $\rho\tau^{-1} = \rho'\tau'^{-1}$. Since $S_{\sigma\tau^{-1}} \subseteq S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}$, this congruence holds modulo $S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}$. Furthermore, $\alpha(ab,c)\alpha(a,b) \equiv \alpha(a,bc)\alpha(b,c) \bmod S_aS_b$ with $a = \sigma\rho^{-1}, b = \rho\tau^{-1}$, and $c = \tau$ gives

$$\alpha(\sigma\tau^{-1},\tau)\alpha(\sigma\rho^{-1},\rho\tau^{-1}) \equiv \alpha(\sigma\rho^{-1},\rho)\alpha(\rho\tau^{-1},\tau) \bmod S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}. \tag{3.1}$$

Therefore

$\alpha(\sigma\tau^{-1},\tau)\alpha(\sigma\rho^{-1},\rho\tau^{-1})h_1^{-1}h_2 \equiv \alpha(\sigma'\tau'^{-1},\tau')\alpha(\sigma'\rho'^{-1},\rho'\tau'^{-1})h_1'^{-1}h_2' \bmod S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}$

$\Rightarrow \alpha(\sigma\rho^{-1},\rho)\alpha(\rho\tau^{-1},\tau)h_1^{-1}h_2 \equiv \alpha(\sigma'\rho'^{-1},\rho')\alpha(\rho'\tau'^{-1},\tau')h_1'^{-1}h_2' \bmod S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}$

$\Rightarrow \alpha(\sigma'\rho'^{-1},\rho')^{-1}\alpha(\sigma\rho^{-1},\rho)h_1'h_1^{-1}h_3 \equiv \alpha(\rho'\tau'^{-1},\tau')\alpha(\rho\tau^{-1},\tau)^{-1}h_2'h_2^{-1}h_3$

$\bmod S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}$. So let $h_3' \in H$ with

$$h_3' \equiv \alpha(\sigma'\rho'^{-1},\rho')^{-1}\alpha(\sigma\rho^{-1},\rho)h_1'h_1^{-1}h_3 \bmod S_{\sigma\rho^{-1}} \text{ and}$$

$$h_3' \equiv \alpha(\rho'\tau'^{-1},\tau')\alpha(\rho\tau^{-1},\tau)^{-1}h_2'h_2^{-1}h_3 \bmod S_{\rho\tau^{-1}}.$$

Then

$$\begin{aligned}
((\sigma',h_1'),(\rho',h_3')) &\in R_{t_{\sigma'\rho'^{-1}}\alpha(\sigma'\rho'^{-1},\rho')^{-1}h_1'h_3'^{-1}} \\
&= R_{t_{\sigma\rho^{-1}}\alpha(\sigma'\rho'^{-1},\rho')^{-1}h_1'\alpha(\sigma'\rho'^{-1},\rho')\alpha(\sigma\rho^{-1},\rho)^{-1}h_1'^{-1}h_1h_3^{-1}} \\
&= R_{t_{\sigma\rho^{-1}}\alpha(\sigma\rho^{-1},\rho)^{-1}h_1h_3^{-1}} \text{ and} \\
((\rho',h_3'),(\tau',h_2')) &\in R_{t_{\rho'\tau'^{-1}}\alpha(\rho'\tau'^{-1},\tau')^{-1}h_3'h_2'^{-1}} \\
&= R_{t_{\rho\tau^{-1}}\alpha(\rho'\tau'^{-1},\tau')^{-1}\alpha(\rho'\tau'^{-1},\tau')\alpha(\rho\tau^{-1},\tau)^{-1}h_2'h_2^{-1}h_3h_2'^{-1}} \\
&= R_{t_{\rho\tau^{-1}}\alpha(\rho\tau^{-1},\tau)^{-1}h_3h_2^{-1}}.
\end{aligned}$$

So (ρ', h_3') has property P'. Thus the existence of (ρ, h_3) with property P implies the existence of at least one (ρ', h_3') with property P'. This shows that whether $p_{rst} = 0$ is independent of choice of σ, τ, h_1, and h_2.

Now, suppose $b_r = t_{\sigma\rho^{-1}}\alpha(\sigma\rho^{-1}, \rho)^{-1}h_1h_3^{-1}$ and $b_s = t_{\rho\tau^{-1}}\alpha(\rho\tau^{-1}, \tau)^{-1}h_3h_2^{-1}$. Then

$$Supp(b_rb_s) = t_{\sigma\tau^{-1}}\alpha(\sigma\rho^{-1}, \rho\tau^{-1})\alpha(\sigma\rho^{-1}, \rho)^{-1}\alpha(\rho\tau^{-1}, \tau)^{-1}S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}h_1h_2^{-1}.$$

Suppose $x \in S_{\sigma\rho^{-1}}S_{\rho\tau^{-1}}$ with

$$\alpha(\sigma\tau^{-1}, \tau)\alpha(\sigma\rho^{-1}, \rho\tau^{-1}) = \alpha(\sigma\rho^{-1}, \rho)\alpha(\rho\tau^{-1}, \tau)x$$

as in equation (3.1). Then $b_t \in Supp(b_rb_s) \Leftrightarrow$ there exist $u \in S_{\sigma\rho^{-1}}, v \in S_{\rho\tau^{-1}}$ with

$$b_t = t_{\sigma\tau^{-1}}\alpha(\sigma\rho^{-1}, \rho\tau^{-1})\alpha(\sigma\rho^{-1}, \rho)^{-1}\alpha(\rho\tau^{-1}, \tau)^{-1}h_1h_2^{-1}x^{-1}uv \Leftrightarrow$$

$$\begin{aligned}
((\sigma, h_1u), (\rho, h_3)) &\in R_{t_{\sigma\rho^{-1}}\alpha(\sigma\rho^{-1}, \rho)^{-1}h_1uh_3^{-1}} \\
&= R_{b_r}, \\
((\rho, h_3), (\tau, h_2v^{-1})) &\in R_{t_{\rho\tau^{-1}}\alpha(\rho\tau^{-1}, \tau)^{-1}h_3h_2^{-1}v} \\
&= R_{b_s}, \text{ and} \\
((\sigma, h_1u), (\tau, h_2v^{-1})) &\in R_{t_{\sigma\tau^{-1}}\alpha(\sigma\tau^{-1}, \tau)^{-1}h_1uh_2^{-1}v} \\
&= R_{t_{\sigma\tau^{-1}}\alpha(\sigma\rho^{-1}, \rho\tau^{-1})\alpha(\sigma\rho^{-1}, \rho)^{-1}\alpha(\rho\tau^{-1}, \tau)^{-1}h_1h_2^{-1}x^{-1}uv} \\
&= b_t.
\end{aligned}$$

Therefore $b_t \in Supp(b_r b_s)$ if and only if there exists a triple $\{(\sigma, h_1 u), (\tau, h_2 v^{-1}), (\rho, h_3)\}$ so that $p_{rst} \neq 0$. Therefore the coefficient of b_t in the product $b_r b_s$ is nonzero exactly when p_{rst} is nonzero.

Suppose there exists (ρ, h_3) with property P. Another pair (π, h) has property P only if $\pi\sigma^{-1} = \rho\sigma^{-1}$, so only if $\pi = \rho$. So the number of pairs with property P is the number of $h \in H$ such that (ρ, h) has property P for some fixed ρ.

Now, (ρ, h) has property P

$$\begin{aligned}
&\Leftrightarrow \quad t_{\sigma\rho^{-1}}\alpha(\sigma\rho^{-1}, \rho)^{-1} h_1 h_3^{-1} = t_{\sigma\rho^{-1}}\alpha(\sigma\rho^{-1}, \rho)^{-1} h_1 h^{-1} \text{ and} \\
&\qquad\quad t_{\rho\tau^{-1}}\alpha(\rho\tau^{-1}, \tau)^{-1} h_3 h_2^{-1} = t_{\rho\tau^{-1}}\alpha(\rho\tau^{-1}, \tau)^{-1} h h_2^{-1} \\
&\Leftrightarrow \quad h_3^{-1} \equiv h^{-1} \bmod S_{\sigma\rho^{-1}} \text{ and } h_3 \equiv h \bmod S_{\rho\tau^{-1}} \\
&\Leftrightarrow \quad h \in h_3 S_{\sigma\rho^{-1}} \cap h_3 S_{\rho\tau^{-1}}.
\end{aligned}$$

Thus the number of (ρ, h) with property P is $|h_3 S_{\sigma\rho^{-1}} \cap h_3 S_{\rho\tau^{-1}}| = |h_3(S_{\sigma\rho^{-1}} \cap S_{\rho\tau^{-1}})| = |S_{\sigma\rho^{-1}} \cap S_{\rho\tau^{-1}}|$. Similarly, the number of (ρ', h') with property P' is $|S_{\sigma'\rho'^{-1}} \cap S_{\rho'\tau'^{-1}}|$. Since $\sigma'\rho'^{-1} = \sigma\rho^{-1}$ and $\rho'\tau'^{-1} = \rho\tau^{-1}$, these numbers are the same. So the value of p_{rst} is independent of choice of σ, τ, h_1, and h_2; and by Theorem 3.1, $|S_{\sigma\rho^{-1}} \cap S_{\rho\tau^{-1}}|$ is exactly the coefficient of b_t in the product $b_r b_s$.

□

CHAPTER 4

EXTENSIONS OF TABLE ALGEBRAS BY GROUP ALGEBRAS

We now move to the case where B is a commutative, standard, class three nilpotent table algebra. This means that $L^{(3)}(B) = B$, i.e. that $B//L^{(2)}(B)$ is a group. Since $L^{(2)}(B)$ is the preimage in B of $L(B//L(B))$, and $(B//C)//(D//C) = B//D$ for any closed subsets C, D of B with $C \subseteq D$, this means that $(B//L(B))//(L^{(2)}(B)//L(B)) = (B//L(B))//L(B//L(B))$ is a group. So if $F = B//L(B)$, F is class two nilpotent. Hence B is an extension of the class two nilpotent table algebra F by the group $L(B)$.

This case is more complicated than the case where B is class two nilpotent because F is not a group, so for $\sigma, \tau \in F$, $\sigma\tau$ is no longer a single element of F. $B//L(B) \cong F$ now implies that if $\{t_\sigma : \sigma \in F\}$ is a set of coset representatives for $L(B)$ in B, $t_\sigma t_\tau = \sum_{\rho \in \sigma\tau} \sum_{h \in L(B)} \lambda_{\sigma\tau\rho h} t_\rho h$, and it is difficult to find the coefficients, or even to say which coefficients are nonzero. We therefore look at the case where $o(B) = p^3$. This is the simplest case because it implies that $B//L^{(2)}(B), L^{(2)}(B)//L(B)$, and $L(B)$ are all isomorphic to $\mathbb{Z}_p$. The main theorem is as follows:

Theorem 4.1. *Suppose p is a prime; $H = \langle h \rangle$ is a cyclic group of order p; $r = 1 + 2\sum_{i \in R} h^i \in \mathbb{Z}H$, where R is the set of non-zero quadratic residues modulo p; and $s = 1 + 2\sum_{i \in S} h^i \in \mathbb{Z}H$, where S is the set of non-residues modulo p. Let (A, B) be a class three nilpotent SITA of order p^3. Then $o\left(L^{(2)}(B)\right) = p^2$ and*

$L(B) \cong B//L^{(2)}(B) \cong \mathbb{Z}_p$. Let $L(B) = L(X) = H$. Up to exact isomorphism of table algebras, B is either the wreath product $\left(B//L^{(2)}(B)\right) \wr L^{(2)}(B)$, or there exists a set of coset representatives $t_i, 0 \leq i \leq p-1$, for $L^{(2)}(B)$ in B such that $t_0 = 1$; for $1 \leq i \leq \frac{p-1}{2}, t_i^* = t_{p-i}$; if $p \neq 2, 3$, then $t_1 t_1 = r t_2$; if $p = 3$, then $t_1 t_1 = (r h^m) t_2$ for some m; for $2 \leq i \leq \frac{p-3}{2}$,

$$t_1 t_i = r\, t_{i+1} \quad \text{or} \quad t_1 t_i = s\, t_{i+1};$$

$$t_1 t_{\frac{p-1}{2}} = (r h^m) t_{\frac{p+1}{2}} \quad \text{or} \quad t_1 t_{\frac{p-1}{2}} = (s h^m) t_{\frac{p+1}{2}} \text{ for some } m;$$

and these conditions uniquely determine the linear decomposition of all products $t_i t_j$.

Conversely, let X be a class two nilpotent SITA of order p^2, $H \cong \mathbb{Z}_p$, and $B = X \cup \{t_i h^k : 1 \leq i \leq p-1, 0 \leq k \leq p-1\}$ as a formal set. Define products $t_1 t_i$ as above for $i \leq \frac{p-1}{2}$. Then this multiplication extends uniquely to $\mathbb{C}B$ in such a way that $(\mathbb{C}B, B)$ is a class three nilpotent SITA of order p^3 with $X = L^{(2)}(B), t_i^* = t_{p-i}$ for all i, and $B \neq \left(B//L^{(2)}(B)\right) \wr L^{(2)}(B)$.

In other words, the class three nilpotent SITAs of order p^3 are parameterized by the choices of r, s, and m for $\lambda_{1j}, 2 \leq j \leq \frac{p-1}{2}$, where $t_1 t_j = \lambda_{1j} t_{1+j}$. Different choices for these λ_{1j} may produce exactly isomorphic algebras, and this redundancy is dealt with in Proposition 4.2.

Note that $p = 2$ is a special case. There is only one coset representative $t_1 \in B \setminus L^{(2)}(B)$, and $t_1 = t_1^*$, which is why we do not assume $t_1 t_1 = r t_2$. There are no t_i for $2 \leq i \leq \frac{p-3}{2}$, so there is no choice of r's and s's to be made, and consequently there is only one algebra of this kind up to exact isomorphism. In the proof of Theorem 4.1 we will find formulas for $t_i t_i^*$ and $t_i s_j$ for $s_j \in L^{(2)}(B) \setminus L(B)$, and these

entirely describe the algebra. Also note that if $p = 3$, then $\frac{p-1}{2} = 1$, so again we do not assume $\lambda_{11} = r$; it may be that $\lambda_{11} = rh^m$ for some nonzero m.

Lastly, note that algebras as described in this theorem achieve the lower bound on the cardinality of supports of products of basis elements given in Theorem 1.7 of [7].

Much of the proof of this theorem hinges on finding the solutions to a system of $p + 1$ equations in p variables.

4.1 System of Equations

In this section, we find all solutions over $\mathbb{Z}$ to the system of equations $\sum_{k\in\mathbb{Z}_p} x_k = 0$, $\sum_{k\in\mathbb{Z}_p} x_k^2 = p - 1$, and $\sum_{k\in\mathbb{Z}_p} x_k x_{k+n} = -1$ for each $0 \neq n \in \mathbb{Z}_p$. In order to solve this sytem, we first need a lemma.

Lemma 4.1. *Let p be an odd prime and $v = (v_0, v_1, \ldots, v_{p-1}) \in \mathbb{Z}^p$. Let P be the permutation matrix with $P(v) = (v_{p-1}, v_0, \ldots, v_{p-2})$. Suppose the usual dot product $P^i(v)\cdot P^j(v) \equiv 0 \ mod\, p^2$ for all i and j. If $(P-I)^2(v) \equiv 0 \ mod\, p$, then $(P-I)(v) \equiv 0 \ mod\, p$ (that is, each coordinate is congruent modulo p).*

Proof. Suppose $P^i(v) \cdot P^j(v) \equiv 0 \bmod p^2$ for all i and j and $(P - I)^2(v) \equiv 0 \bmod p$. Then $(P - I)^2(v) \equiv 0 \bmod p \Rightarrow v \equiv 2P(v) - P^2(v) \bmod p$. Therefore

$$v_0 \equiv 2v_{p-1} - v_{p-2},$$

$$v_1 \equiv 2v_0 - v_{p-1} \equiv 2(2v_{p-1} - v_{p-2}) - v_{p-1} \equiv 3v_{p-1} - 2v_{p-2},$$

$$v_2 \equiv 2v_1 - v_0 \equiv 2(3v_{p-1} - 2v_{p-2}) - 2v_{p-1} + v_{p-2} \equiv 4v_{p-1} - 3v_{p-2},$$

$$\vdots$$

$v_{p-4} \equiv (p-2)v_{p-1} - (p-3)v_{p-2}$,

$v_{p-3} \equiv (p-1)v_{p-1} - (p-2)v_{p-2}$.

Therefore

$v = (2v_{p-1} - v_{p-2} + x_0 p, 3v_{p-1} - 2v_{p-2} + x_1 p, \ldots, (j+1)v_{p-1} - jv_{p-2} + x_{j-1}p, \ldots, (p-1)v_{p-1} - (p-2)v_{p-2} + x_{p-3}p, v_{p-2}, v_{p-1})$ for some set of integers $x_0, x_1, \ldots, x_{p-3}$.

So $(P-I)(v) = (v_{p-2} - v_{p-1} - px_0, v_{p-2} - v_{p-1} + p(x_0 - x_1), \ldots, v_{p-2} - v_{p-1} + p(x_{p-4} - x_{p-3}), (p-1)(v_{p-1} - v_{p-2}) + px_{p-3}, v_{p-2} - v_{p-1})$.

Letting $b = v_{p-2} - v_{p-1}$, we now have:

$$\begin{aligned}
(P-I)(v) \cdot (P-I)(v) &= b^2 - 2pbx_0 + p^2x_0^2 \\
&\quad + b^2 + 2pb(x_0 - x_1) + p^2(x_0 - x_1)^2 \\
&\quad + b^2 + 2pb(x_1 - x_2) + p^2(x_1 - x_2)^2 \\
&\quad \vdots \\
&\quad + b^2 + 2pb(x_{p-4} - x_{p-3}) + p^2(x_{p-4} - x_{p-3})^2 \\
&\quad + (p-1)^2b^2 - 2pb(p-1)x_{p-3} + p^2x_{p-3}^2 + b^2 \\
&= ((p-1) + (p-1)^2)b^2 - 2pbpx_{p-3} + p^2\left[x_0^2 + (x_0 - x_1)^2\right. \\
&\quad \left. + \cdots + (x_{p-4} - x_{p-3})^2 + x_{p-3}^2\right] \\
&= p(p-1)b^2 + p^2N \text{ for some } N \in \mathbb{Z}.
\end{aligned}$$

Since we assumed $P^i(v) \cdot P^j(v) \equiv 0 \bmod p^2$ for all i and j, $(P-I)(v) \cdot (P-I)(v) \equiv 0 \bmod p^2$. So we have $p(p-1)b^2 \equiv 0 \bmod p^2$, and hence $b^2 \equiv 0 \bmod p$. Thus $v_{p-2} - v_{p-1} = b \equiv 0 \bmod p$, so $v_{p-2} \equiv v_{p-1} \bmod p$. The congruences at the beginning of the proof then yield that all v_i are congruent mod p. □

Corollary 4.1. *Let p be an odd prime and $v = (v_0, v_1, \ldots, v_{p-1}) \in \mathbb{Z}^p$. Let P be the permutation matrix with $P(v) = (v_{p-1}, v_0, \ldots, v_{p-2})$ and suppose $P^i(v) \cdot P^j(v) \equiv 0$ mod p^2 for all i and j. Then all v_i are congruent modulo p.*

Proof. Since $P^p = I, (P^p - I)(v) = 0$, so $(P - I)^p(v) \equiv 0 \bmod p$.

Suppose $(P - I)^n(v) \equiv 0 \bmod p$ for some $2 < n \leq p$. Then $(P - I)^2((P - I)^{n-2}(v)) \equiv 0 \bmod p$. For any integers i and j, $P^i\left((P - I)^{n-2}(v)\right) \cdot P^j\left((P - I)^{n-2}(v)\right)$ is a $\mathbb{Z}-$linear combination of $P^s(v) \cdot P^t(v)$ for various s and t. Thus $P^i(P-I)^{n-2}(v) \cdot P^j(P - I)^{n-2}(v) \equiv 0 \bmod p^2$ for all i and j. So by Lemma 4.1, $(P - I)^{n-1}(v) = (P - I)((P - I)^{n-2}(v)) \equiv 0 \bmod p$. By induction downward on n, $(P - I)(v) \equiv 0 \bmod p$, so all v_i are congruent mod p. □

Lemma 4.2. *Suppose $v_0, v_1, \ldots, v_{p-1} \in \mathbb{R}^p$ and for $1 = (1, 1, \ldots, 1)$ and all $i \neq j$,*

$$\begin{aligned} v_i \cdot 1 &= 0, \\ v_i \cdot v_i &= p - 1, \\ v_i \cdot v_j &= -1. \end{aligned}$$

Then the v_i span a subspace of $\mathbb{R}^p$ of dimension $p - 1$, namely $1^\perp$, and the only dependence relations among the v_i are scalar multiples of $v_0 + v_1 + \cdots + v_{p-1} = 0$.

Proof. Clearly $\langle \{v_i : 0 \leq i \leq p - 1\} \rangle \subseteq 1^\perp$, which has dimension $p - 1$. Suppose $\sum_{i=0}^{p-1} \alpha_i v_i = 0$ for some scalars α_i. Then for all j,

$$0 = 0 \cdot v_j = \sum_{i=0}^{p-1} \alpha_i (v_i \cdot v_j) = (p - 1)\alpha_j + \sum_{\substack{i=0, \\ i \neq j}}^{p-1} (-1)\alpha_i,$$

so

$$\sum_{\substack{i=0,\\ i\neq j}}^{p-1} \alpha_i = (p-1)\alpha_j.$$

Therefore for any i and j,

$$\begin{aligned} \alpha_0 + \cdots + \alpha_{i-1} + \alpha_{i+1} + \cdots + \alpha_{p-1} &= (p-1)\alpha_i \\ \alpha_0 + \cdots + \alpha_{j-1} + \alpha_{j+1} + \cdots + \alpha_{p-1} &= (p-1)\alpha_j \\ \Rightarrow\ \alpha_i - \alpha_j = (p-1)(\alpha_j - \alpha_i) \Rightarrow\ \alpha_j &= \alpha_i. \end{aligned}$$

□

Definition 4.1. The *Legendre symbol of a mod p*, denoted $\left(\frac{a}{p}\right)$, is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a non-zero quadratic residue modulo } p \\ -1 & \text{if } a \text{ is not a quadratic residue modulo } p \\ 0 & \text{if } a \equiv 0 \text{ modulo } p. \end{cases}$$

We now find the solutions to the system of equations stated earlier. In this paper, 0 is not considered a quadratic residue.

Proposition 4.1. *The only solutions over the integers to the system of equations*

$$\begin{aligned} (1) &: \sum_{k\in\mathbb{Z}_p} x_k = 0, \\ (2) &: \sum_{k\in\mathbb{Z}_p} x_k^2 = p-1, \ \textit{and} \\ (3) &: \sum_{k\in\mathbb{Z}_p} x_k x_{k+n} = -1 \ \textit{for each } 0 \neq n \in \mathbb{Z}_p \end{aligned}$$

are $x_k = \left(\frac{k+m}{p}\right)$ *and* $x_k = -\left(\frac{k+m}{p}\right)$ *for fixed* $0 \leq m \leq p-1$.

Proof. We first show that $x_k = \left(\frac{k}{p}\right)$ and $x_k = -\left(\frac{k}{p}\right)$ satisfy the system. Since there are $\frac{p-1}{2}$ quadratic residues mod p and $\frac{p-1}{2}$ non-residues, it is clear that equations (1) and (2) are satisfied. In order to show that the remaining equations are satisfied, we introduce some notation. If $k, k+n \in \mathbb{Z}_p$ are both nonzero quadratic residues, we will call $(k, k+n)$ an RR pair; if both are nonresidues, we will call $(k, k+n)$ an NN pair; in either case, we will call the pair a *matching pair*. If k is a quadratic residue and $k+n$ is a nonresidue, we will call $(k, k+n)$ an RN pair; if k is a nonresidue and $k+n$ is a residue, we will call $(k, k+n)$ an NR pair; in either case we will call the pair a *nonmatching pair*. We show that for any nonzero $n \in \mathbb{Z}_p$, there are $\frac{p-1}{2} - 1$ matching pairs and $\frac{p-1}{2}$ nonmatching pairs. This will imply that $\sum_{k \in \mathbb{Z}_p} x_k x_{k+n} = -1$ for each n because each matching pair contributes a 1 to that sum, and each nonmatching pair contributes a -1.

It is well known that this holds for $n = 1$. For $p \equiv 1 \bmod 4$, there are $\frac{p-5}{4}$ consecutive RR pairs, $\frac{p-1}{4}$ consecutive NN pairs, $\frac{p-1}{4}$ consecutive NR pairs, and $\frac{p-1}{4}$ consecutive RN pairs. For $p \equiv 3 \bmod 4$, there are $\frac{p-3}{4}$ consecutive RR pairs, $\frac{p-3}{4}$ consecutive NN pairs, $\frac{p-3}{4}$ consecutive NR pairs, and $\frac{p+1}{4}$ consecutive RN pairs. Thus there are $\frac{p-1}{2} - 1$ consecutive matching pairs and $\frac{p-1}{2}$ consecutive nonmatching pairs. A proof of this can be found in [1], pages 128-131. We show that these numbers are independent of n.

The number of RR pairs $(k, k+n)$ for a given n is the number of k that satisfy the equations $k = x^2, k+n = y^2, k \neq 0, k+n \neq 0$ for some x and y. Each set of four solutions $\{(x,y), (-x,y), (x,-y), (-x,-y)\}$ gives one such k. So the number

of RR pairs for a given n is one quarter the number of solutions to these equations. Furthermore,

$$k = x^2, k + n = y^2 \Leftrightarrow x^2 + n = y^2 \Leftrightarrow y^2 - x^2 = n,$$

and thus the number of RR pairs is one quarter the number of solutions in x and y of $y^2 - x^2 = n, x \neq 0, y \neq 0$.

Let v be a nonresidue. All other nonresidues can be written as vx for some residue x, since a residue times a nonresidue is a nonresidue. The number of NN pairs $(k, k + n)$ for a given n is the number of k that satisfy $k = vx^2, k + n = vy^2$ for some nonzero x and y. So, as before, the number of NN pairs for a given n is one quarter the number of nonzero solutions to $vy^2 - vx^2 = n$.

Recalling that $n \neq 0$, if n is a quadratic residue mod $p, (x_0, y_0)$ is a solution of $y^2 - x^2 = n \Leftrightarrow ((\sqrt{n})^{-1}x_0, (\sqrt{n})^{-1}y_0)$ is a solution of $y^2 - x^2 = 1$. So if n is a residue, the number of RR pairs n apart is the same as the number of RR pairs 1 apart.

If n is a nonresidue, the number of nonzero solutions to $y^2 - x^2 = n$ is the same as the number of nonzero solutions to $n^{-1}y^2 - n^{-1}x^2 = 1$, which is the number of NN pairs 1 apart, since n being a nonresidue implies n^{-1} is a nonresidue. So if n is a nonresidue, the number of RR pairs n apart is the same as the number of NN pairs 1 apart.

If v is a nonresidue, the number of solutions to $vy^2 - vx^2 = n$ is the same as the number of solutions to $y^2 - x^2 = v^{-1}n$. So the number of NN pairs n apart is the same as the number of RR pairs $v^{-1}n$ apart, which, as shown above, is the same as the number of RR pairs 1 apart if n is a non-residue and is the same as the number of NN pairs 1 apart if n is a residue.

Putting this all together, if n is a residue, then the number of RR pairs n apart is the number of RR pairs 1 apart, and the number of NN pairs n apart is the number of NN pairs 1 apart; so the number of matching pairs n apart is the same as the number of matching pairs 1 apart. If n is a non-residue, then the number of RR pairs n apart is the number of NN pairs 1 apart, and the number of NN pairs n apart is the number of RR pairs 1 apart. So the number of matching pairs n apart is again the number of matching pairs 1 apart.

Therefore the number of matching pairs n apart for arbitrary n equals the number of matching pairs 1 apart. It follows that for each n there are $\frac{p-3}{2}$ matching pairs. Since there are $p-2$ total pairs without 0 in the pair, the number of nonmatching pairs must be $p-2-\frac{p-3}{2}=\frac{p-1}{2}$. Thus equation (3) is satisfied by $x_k=\left(\frac{k}{p}\right)$ for all k and by $x_k=-\left(\frac{k}{p}\right)$ for all k.

Now let $x=(x_0,x_1,\ldots,x_{p-1})$, and again let P be the permutation operator with $P(x)=(x_{p-1},x_0,\ldots,x_{p-2})$. If x satisfies the system of equations, so will $P^i(x)$ for every i since replacing x_k with x_{k+i} for some $i\in\mathbb{Z}_p$ will not change equations (1) and (2), and will yield the $p-1$ equations described by (3) in a different order. Thus $x_k=\left(\frac{k+m}{p}\right)$ and $x_k=-\left(\frac{k+m}{p}\right)$ are also solutions for each $m\in\mathbb{Z}_p$.

We now show that these are the only solutions. Let $x_k=\left(\frac{k}{p}\right)$ and $x=(x_0,x_1,\ldots,x_{p-1})$. Suppose $y=(y_0,y_1,\ldots,y_{p-1})$ is another solution. Then for all $i\neq j$,

$$P^i(x)\cdot 1=P^i(y)\cdot 1=0 \text{ by equation (1);}$$
$$P^i(x)\cdot P^i(x)=P^i(y)\cdot P^i(y)=p-1 \text{ by equation (2); and}$$
$$P^i(x)\cdot P^j(x)=P^i(y)\cdot P^j(y)=-1 \text{ by equation (3).}$$

Thus by Lemma 4.2, both $\{1, P^i(x) : 0 \leq i \leq p-2\}$ and $\{1, P^i(y) : 0 \leq i \leq p-2\}$ form bases of $\mathbb{R}^p$, and $P^{p-1}(x) = -(P^0(x) + \cdots + P^{p-2}(x)), P^{p-1}(y) = -(P^0(y) + \cdots + P^{p-2}(y))$. Thus there exists an orthogonal linear transformation, call it T, with $T(1) = 1$ and $T(P^i(x)) = P^i(y)$ for each i.

T also commutes with the permutations P^i since $T(P^i(x)) = P^i(y) = P^i(T(x))$ and of course $T(P^i(1)) = 1 = P^i(T(1))$. Thus if

$$T = \begin{bmatrix} b_0^0 & b_1^0 & \cdots & b_{p-1}^0 \\ b_0^1 & b_1^1 & \cdots & b_{p-1}^1 \\ & & \vdots & \\ b_0^{p-1} & b_1^{p-1} & \cdots & b_{p-1}^{p-1} \end{bmatrix},$$

then

$$T \cdot P = \begin{bmatrix} b_1^0 & b_2^0 & \cdots & b_{p-1}^0 & b_0^0 \\ b_1^1 & b_2^1 & \cdots & b_{p-1}^1 & b_0^1 \\ & & \vdots & & \\ b_1^{p-1} & b_2^{p-1} & \cdots & b_{p-1}^{p-1} & b_0^{p-1} \end{bmatrix} = P \cdot T = \begin{bmatrix} b_0^{p-1} & b_1^{p-1} & \cdots & b_{p-1}^{p-1} \\ b_0^0 & b_1^0 & \cdots & b_{p-1}^0 \\ & & \vdots & \\ b_0^{p-2} & b_1^{p-2} & \cdots & b_{p-1}^{p-2} \end{bmatrix}.$$

So

$$(T \cdot P)_{ij} = b_{j+1}^i = (P \cdot T)_{ij} = b_j^{i-1},$$

hence $T_{i(j+1)} = T_{(i-1)j}$. Thus T is a circulant matrix.

Let $T = Circ(b_0, b_1, \ldots, b_{p-1})$, where $||(b_0, b_1, \ldots, b_{p-1})|| = 1$ and $P^i(b_0, b_1, \ldots, b_{p-1}) \cdot P^j(b_0, b_1, \ldots, b_{p-1}) = 0$ for all $i \neq j$. Then we have:

$$T(x) = y \Rightarrow \begin{bmatrix} b_0 & b_1 & \cdots & b_{p-1} \\ b_{p-1} & b_0 & \cdots & b_{p-2} \\ & & \vdots & \\ b_1 & b_2 & \cdots & b_0 \end{bmatrix} \begin{bmatrix} \left(\frac{0}{p}\right) \\ \left(\frac{1}{p}\right) \\ \vdots \\ \left(\frac{p-1}{p}\right) \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{p-1} \end{bmatrix}$$

$$\Rightarrow y_0 = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) b_i, \quad y_1 = \sum_{i=0}^{p-1} \left(\frac{i+1}{p}\right) b_i, \quad \ldots \quad , \quad y_{p-1} = \sum_{i=0}^{p-1} \left(\frac{i+(p-1)}{p}\right) b_i.$$

In other words,

$$y_k = \sum_{i=0}^{p-1} \left(\frac{i+k}{p}\right) b_i \text{ for } 0 \leq k \leq p-1.$$

Since we are solving the system of equations over $\mathbb{Z}$, all of the y_k are integers. We now show that $p \cdot b_i \in \mathbb{Z}$ for each i.

Let R be the set of non-zero quadratic residues modulo p, and S the set of non-residues. For each $0 \leq i \leq p-1$, we compute $\sum_{i+k \in R} y_k - \sum_{i+k \in S} y_k$; in other words, we add together the y_k in which b_i has a coefficient of 1 and subtract the y_k in which b_i has a coefficient of -1. We find the coefficients of the various b_n.

Coefficient of b_i: $i + k$ is a quadratic residue for $\frac{p-1}{2}$ values of k, and is a non-residue for $\frac{p-1}{2}$ values of k. So the coefficient of b_i is $\frac{p-1}{2} - \left(-\frac{p-1}{2}\right) = p - 1$.

Coefficient of $b_n, n \neq i$: We add a b_n whenever $i+k, n+k \in R$ (so that y_k is being added *and* b_n has a coefficient of 1 in y_k). We also add a b_n whenever $i+k, n+k \in S$

(so that y_k is being subtracted *and* b_n has a coefficient of -1). In other words, we add a b_n whenever $(i+k, n+k)$ is a matching pair. As shown earlier, this occurs for $\frac{p-3}{2}$ values of k, regardless of the value of n.

Similarly, we subtract a b_n whenever $(i+k, n+k)$ is a non-matching pair. This occurs for $\frac{p-1}{2}$ values of k. So the coefficient of b_n for $n \neq i$ is $\frac{p-3}{2} - \frac{p-1}{2} = -1$. Thus for $0 \leq i \leq p-1$,

$$\sum_{i+k \in R} y_k - \sum_{i+k \in S} y_k = (p-1)b_i - \sum_{n \neq i} b_n.$$

Now, $\sum_{n=0}^{p-1} b_n$ is an eigenvalue of T (with eigenvector $(1, 1, \ldots, 1)$). Since T is orthogonal, $\left\| \sum_{n=0}^{p-1} b_n \right\| = 1$; and the b_i are real, so $\sum_{n=0}^{p-1} b_n = \pm 1$. So for $0 \leq i \leq p-1$,

$$\begin{aligned} \text{all } y_k \in \mathbb{Z} \;&\Rightarrow\; (p-1)b_i - \sum_{n \neq i} b_n \in \mathbb{Z} \;\Rightarrow\; (p-1)b_i - (\pm 1 - b_i) \in \mathbb{Z} \\ &\Rightarrow\; p \cdot b_i \mp 1 \in \mathbb{Z} \;\Rightarrow\; p \cdot b_i \in \mathbb{Z}. \end{aligned}$$

We write $T = Circ\left(\frac{a_0}{p}, \frac{a_1}{p}, \ldots, \frac{a_{p-1}}{p}\right)$ for $a_i \in \mathbb{Z}$. Since $\left\| \left(\frac{a_0}{p}, \frac{a_1}{p}, \ldots, \frac{a_{p-1}}{p}\right) \right\| = 1$, we also know that $-p \leq a_i \leq p$ for each i.

Let $a = (a_0, a_1, \ldots, a_{p-1})$. The vectors $P^i(a)$ are mutually orthogonal, and $\sum_{i=0}^{p-1} b_i^2 = 1 \Rightarrow \sum_{i=0}^{p-1} a_i^2 = p^2$. In particular, $P^i(a) \cdot P^j(a) \equiv 0 \mod p^2$ for every i and j. So by Corollary 4.1, all a_i are congruent modulo p.

Applying a cyclic shift if necessary, assume a_0 is non-zero. Since $-p \leq a_i \leq p$ for all i, if $a_0 > 0$, either $a_i = a_0$ or $a_i = a_0 - p$ for each i; if $a_0 < 0$, then either $a_i = a_0$ or $a_i = a_0 + p$ for each i. Suppose $a_0 > 0$. Since $\sum_{i=0}^{p-1} b_i = \pm 1, \sum_{i=0}^{p-1} a_i = \pm p$; and, as mentioned above, $\sum_{i=0}^{p-1} a_i^2 = p^2$. Suppose m of the a_i are equal to a_0, and n are equal to $a_0 - p$. Then:

$$m + n = p$$

$$ma_0 + n(a_0 - p) = \pm p$$

$$ma_0^2 + n(a_0 - p)^2 = p^2$$

$\Rightarrow$

$$ma_0 + (p - m)(a_0 - p) = \pm p$$

$$ma_0^2 + (p - m)(a_0 - p)^2 = p^2$$

$\Rightarrow$

$$ma_0 + pa_0 - p^2 - ma_0 + mp = \pm p$$

$$ma_0^2 + pa_0^2 - 2a_0p^2 + p^3 - ma_0^2 + 2ma_0p - mp^2 = p^2$$

$\Rightarrow$

$$a_0 = \pm 1 + p - m$$

$$a_0^2 - 2a_0p + p^2 + 2ma_0 - mp = p$$

$$\Rightarrow (\pm 1 + p - m)^2 - 2p(\pm 1 + p - m) + p^2 + 2m(\pm 1 + p - m) - mp = p$$

$$\Rightarrow 1 - m^2 + mp = p$$

$$\Rightarrow m^2 - pm + (p - 1) = 0$$

$$\Rightarrow m = 1, p - 1.$$

So $a = (a_0, a_0 - p, a_0 - p, \ldots, a_0 - p)$, $(a_0, a_0, \ldots, a_0 - p)$, or a cyclic permutation of one of those (since only one entry is different from the others, any permutation is a cyclic permutation). Similarly, if $a_0 < 0, a = (a_0, a_0 + p, a_0 + p, \ldots, a_0 + p)$, $(a_0, a_0, \ldots, a_0 + p)$, or a cyclic permutation of one of those. In other words,

$$a = (a_0, a_0 \pm p, a_0 \pm p, \ldots, a_0 \pm p) \text{ or a cyclic permutation of that.}$$

Since $\sum_{i=0}^{p-1} a_i = \pm p$, we have $pa_0 \pm (p-1)p = \pm p \Rightarrow pa_0 \pm (p^2-p) = \pm p \Rightarrow a_0 \pm (p-1) = \pm 1$, where the two $\pm$ are independent of each other. So $a_0 = \pm p, \pm(p-2)$. Thus

$$a = \pm(p, 0, 0, \ldots, 0) \text{ or } \pm (p-2, -2, -2, \ldots, -2),$$

or a cyclic permutation of one of those. Let $b = \left(\frac{2-p}{p}, \frac{2}{p}, \frac{2}{p}, \ldots, \frac{2}{p}\right)$. So

$$T = Circ(P^i(\pm(1, 0, 0, \ldots, 0))) = \pm P^i \text{ or } Circ(P^i(\pm b)) \text{ for some i.}$$

Obviously, if $T = \pm P^i$, then $T(P^k(x)) = \pm P^{i+k}(x)$. If $T = Circ(b)$, then

$$y_k = \frac{1}{p} \sum_{i \in \mathbb{Z}_p \setminus \{k\}} \left(\frac{i}{p}\right) \cdot 2 + \left(\frac{k}{p}\right)(2-p)$$

$$= \frac{1}{p} \begin{cases} (\frac{p-1}{2} \cdot 2 - \frac{p-1}{2} \cdot 2) & \text{if } k = 0 \\ ((\frac{p-1}{2} - 1) \cdot 2 - (\frac{p-1}{2}) \cdot 2) + (2-p) & \text{if } k \in R \\ ((\frac{p-1}{2}) \cdot 2 - (\frac{p-1}{2} - 1) \cdot 2 - (2-p) & \text{if } k \in S \end{cases}$$

$$= \begin{cases} 0 & \text{if } k = 0 \\ -1 & \text{if } k \in R \\ 1 & \text{if } k \in S \end{cases}$$

$$= -\left(\frac{k}{p}\right) = -x_k.$$

So $T(x) = -x$, and hence $T(P^i(x)) = P^i(T(x)) = P^i(-x) = -P^i(x)$. Thus if $T = Circ(P^j(b))$, then $T(x) = Circ(P^j(b))(x) = P^j(Circ(b)(x)) = P^j(-x)$. So $T(P^i(x)) = -P^{i+j}(x)$.

We now see that in every case, $y = \pm P^i(x)$ for some i. Thus the only solutions to the system of equations are $x_k = \left(\frac{k}{p}\right), x_k = -\left(\frac{k}{p}\right)$, and cyclic permutations of those, i.e. $x_k = \left(\frac{k+m}{p}\right)$ or $x_k = -\left(\frac{k+m}{p}\right)$ for $0 \leq m \leq p-1$. □

4.2 Proof of Main Theorem

We can now prove the main theorem.

Proof of Theorem 4.1: For the first direction: Since $o(B//C) = o(B)/o(C)$ for any closed subset C,

$$o(B) = o(B//L^{(2)}(B)) \cdot o(L^{(2)}(B)//L(B)) \cdot o(L(B)).$$

Since $L^{(i)}(B)//L^{(i-1)}(B)$ is a group for every $i \geq 1$, the factors in the above product are all integers. Since B is class three nilpotent, none of them is 1, so since $o(B) = p^3$, all are equal to p. Thus $L(B) \cong B//L^{(2)}(B) \cong \mathbb{Z}_p$ and therefore $o(L^{(2)}(B)) = p^2$.

Suppose $B \neq \left(B//L^{(2)}(B)\right) \wr L^{(2)}(B)$. We first find how elements of B multiply. Since $L^{(2)}(B)//L(B) \cong \mathbb{Z}_p$, we may write

$$L^{(2)}(B)//L(B) = \{s_0//L(B) = 1//L(B), s_1//L(B), \ldots, s_{p-1}//L(B)\}$$

where, reading the indices modulo p,

$$(s_i//L(B))(s_j//L(B)) = s_{i+j}//L(B).$$

Now, for $b \in B$, let $Stab(b) = \{h^k \in L(B) : bh^k = b\}$. Since $L^{(2)}(B)$ forms the basis of a class two nilpotent table algebra, we know by Theorem 3.1 that for $b \in L^{(2)}(B)$,

$$bb^* = |Stab(b)| \sum_{h^k \in Stab(b)} h^k.$$

Thus for $b \in L^{(2)}(B) \setminus L(B)$, $Stab(b) \neq \{1\}$. Since $L(B) \cong \mathbb{Z}_p$, the only other possibility is $Stab(b) = L(B)$. So

$$L^{(2)}(B) \setminus L(B) = \{s_1, s_2, \ldots, s_{p-1}\},$$

and for $i \neq -j$,

$$s_i s_j = \sum_{k=0}^{p-1} \gamma_{ijk} s_{i+j} h^k = \gamma_{ij} s_{i+j}$$

for some $\gamma_{ij} \in \mathbb{Z}$. Since for each $k, \delta(s_k) = |Stab(s_k)| = p$ by Theorem 3.1, $\delta(s_i s_j) = \gamma_{ij}\delta(s_{i+j}) \Rightarrow \gamma_{ij} = p$. So for $i \neq -j$,

$$s_i s_j = p \cdot s_{i+j}.$$

Since $1 \in Supp(s_i s_i^*)$, it must be that $s_i^* = s_{p-i}$ for each i, and

$$s_i s_i^* = p \cdot H^+.$$

Similarly, since $|B//L^{(2)}(B)| = p, B//L^{(2)}(B)$ may be written

$$\left\{t_0//L^{(2)}(B) = 1//L^{(2)}(B), t_1//L^{(2)}(B), \ldots, t_{p-1}//L^{(2)}(B)\right\},$$

where the t_i are coset representatives for $L^{(2)}(B)$ in B and, reading the indices modulo p,

$$(t_i//L^{(2)}(B))(t_j//L^{(2)}(B)) = t_{i+j}//L^{(2)}(B). \tag{4.1}$$

For the remainder of this proof, all indices will be read modulo p unless otherwise indicated. By the comments preceding the theorem, $B//L(B)$ is a class two nilpotent SITA; and by the same argument as for $L^{(2)}(B)$, this means that for $b \notin L^{(2)}(B)$,

$$Stab(b//L(B)) = L(B//L(B)) = L^{(2)}(B)//L(B).$$

Thus for all i and j,

$$(t_i//L(B))(s_j//L(B)) = t_i//L(B).$$

So

$$t_i s_j = \sum_{k=0}^{p-1} \lambda_{ijk} t_i h^k.$$

And since $t_i s_j h^m = t_i s_j$ for any m, permuting the λ_{ijk} does not change this sum; thus all λ_{ijk} are equal and $t_i s_j = \lambda \sum_{k=0}^{p-1} t_i h^k$. Applying the degree map to both sides yields $\delta(t_i) \cdot p = \lambda \cdot p \cdot \delta(t_i)$, so $\lambda = 1$. Thus

$$t_i s_j = \sum_{k=0}^{p-1} t_i h^k. \tag{4.2}$$

This implies that

$$B \setminus L^{(2)}(B) = \{t_i h^k : 1 \leq i \leq p-1, 0 \leq k \leq p-1\}.$$

Note that depending on the stabilizers of the t_i, these may not all be distinct.

Since $1 \in Supp(t_i t_i^*)$, it must be that $t_i^* = t_{p-i}h^k$ for some k. Since $i \neq p-i$ for any i and there is no danger of ending up with $t_i^* = t_i$, we may choose $k = 0$, giving $t_i^* = t_{p-i}$.

By Theorem 3.1, for $b \notin L^{(2)}(B)$,

$$|Stab(b//L(B))| = p \Rightarrow \delta(b//L(B)) = |Stab(b//L(B))| = p.$$

Thus

$$p = \delta(b//L(B)) = \frac{\delta((bL(B))^+)}{p} = \frac{\delta(b \cdot L(B)^+)}{|Stab(b)| \cdot p} = \frac{\delta(b)}{|Stab(b)|}.$$

So

$$\delta(b) = \begin{cases} p & \text{if } |Stab(b)| = 1 \\ p^2 & \text{if } |Stab(b)| = p. \end{cases}$$

Now, equations (4.1) and (4.2) $\Rightarrow Supp(t_i t_j) \subseteq \{t_{i+j}h^k : 0 \leq k \leq p-1\}$ if $j \neq p-i$. Thus for some set of $\lambda_{ijk} \in \mathbb{Z}_{\geq 0}$, we have

$$t_i t_j = \sum_{k=0}^{p-1} \lambda_{ijk} t_{i+j} h^k \tag{4.3}$$

for $j \neq p-i$.

Finally, for any n,

$$t_n t_n^* \subseteq L^{(2)}(B) \Rightarrow t_n t_n^* = \sum_{j=1}^{p-1} \lambda_j s_j + \sum_{k=0}^{p-1} \lambda_k h^k$$

for some set of $\lambda_j, \lambda_k \in \mathbb{Z}_{\geq 0}$. Suppose $Stab(t_n) = \{1\}$. Since $\delta(t_n) = p$,

$$\langle t_n t_n^*, h^k \rangle = \langle t_n, t_n h^k \rangle = \begin{cases} p & \text{if } h^k = 1 \\ 0 & \text{otherwise.} \end{cases}$$

So $t_n t_n^* = \sum_{j=1}^{p-1} \lambda_j s_j + p \cdot 1$. And by equation (4.2), for any $s_j \in L^{(2)}(B) \setminus L(B)$,

$$\langle t_n t_n^*, s_j \rangle = \langle t_n, t_n s_j \rangle = \left\langle t_n, \sum_{k=0}^{p-1} t_n h^k \right\rangle = \langle t_n, t_n \rangle = p.$$

Since $\delta(s_j) = p$, we now have

$$t_n t_n^* = \sum_{j=1}^{p-1} s_j + p \cdot 1 \text{ for each } n \text{ with } Stab(t_n) = \{1\}.$$

Putting this all together, the multiplication on B is given by the following:

$$\begin{aligned}
s_i s_j &= p \cdot s_{i+j} \text{ for } i \neq -j \\
s_i s_{-i} &= p \cdot \sum_{k=0}^{p-1} h^k \\
t_i s_j &= \sum_{k=0}^{p-1} t_i h^k \\
t_i t_j &= \sum_{k=0}^{p-1} \lambda_{ijk} t_{i+j} h^k \text{ for } i \neq -j \\
t_i t_{-i} &= \sum_{j=1}^{p-1} s_j + p \cdot 1 \text{ if } Stab(t_i) = \{1\}.
\end{aligned}$$

We now show that if $Stab(t_1) = \{1\}$, then $Stab(b) = \{1\}$ for all $b \in B \setminus L^{(2)}(B)$. Suppose $Stab(t_1) = Stab(t_2) = \cdots = Stab(t_{i-1}) = \{1\}$ and $Stab(t_i) = L(B)$. Then $t_1 t_{i-1} = \sum_{k=0}^{p-1} \lambda_{1(i-1)k} t_i h^k = \lambda t_i$ for some $\lambda \in \mathbb{Z}_{\geq 0}$. Thus $p^2 = \delta(t_1)\delta(t_{i-1}) = \delta(t_1 t_{i-1}) = \lambda \delta(t_i) = \lambda p^2 \Rightarrow \lambda = 1$. So $t_1 t_{i-1} = t_i$ and thus

$$\langle t_1 t_{i-1}, t_1 t_{i-1} \rangle = \langle t_i, t_i \rangle = p^2.$$

On the other hand, we have

$$\begin{aligned}\left\langle t_1 t_1^*, t_{i-1} t_{i-1}^* \right\rangle &= \left\langle \sum_{j=1}^{p-1} s_j + p \cdot 1, \sum_{j=1}^{p-1} s_j + p \cdot 1 \right\rangle \\ &= \sum_{j=1}^{p-1} \langle s_j, s_j \rangle + p^2 \langle 1, 1 \rangle \\ &= (p-1)p + p^2 = 2p^2 - p.\end{aligned}$$

Since $2p^2 - p \neq p^2$, we now have $\langle t_1 t_{i-1}, t_1 t_{i-1} \rangle \neq \left\langle t_1 t_1^*, t_{i-1} t_{i-1}^* \right\rangle$, a contradiction. Therefore if $Stab(t_1) = \{1\}$, then $Stab(t_i) = \{1\}$ for all i. Since the choice of which coset representative we label as t_1 is arbitrary, this means that if $Stab(t_j) = \{1\}$ for any j, then $Stab(t_i) = \{1\}$ for all i. Therefore all stabilizers of elements in $B \backslash L^{(2)}(B)$ are equal, and since $B \neq \left(B // L^{(2)}(B)\right) \wr L^{(2)}(B)$, this implies that $Stab(t_i) = \{1\}$ for each i.

We've already shown that if $i \neq p - j$,

$$t_i t_j = \sum_{k=0}^{p-1} \lambda_{ijk} t_{i+j} h^k$$

for some set of $\lambda_{ijk} \in \mathbb{Z}_{\geq 0}$. We now show that for each i, j, and k with $i \neq -j$, $\sum_{k=0}^{p-1} \lambda_{ijk} h^k = r h^n$ or $s h^n$ for some n which depends on i and j.

First of all, for $i \neq -j$,

$$\delta(t_i t_j) = \sum_{k=0}^{p-1} \lambda_{ijk} \delta(t_{i+j}) \Rightarrow p^2 = p \cdot \sum_{k=0}^{p-1} \lambda_{ijk}.$$

So

$$\sum_{k=0}^{p-1} \lambda_{ijk} = p. \tag{4.4}$$

Second,

$$\delta(t_{i+j})\lambda_{ijk} = \langle t_i t_j, t_{i+j} h^k \rangle = \langle t_i h^{-k}, t_{i+j} t_j^* \rangle = \langle t_i h^{-k}, t_{i+j} t_{-j} \rangle = \delta(t_i)\lambda_{(i+j)(-j)(-k)}.$$

So

$$\lambda_{ijk} = \lambda_{(i+j)(-j)(-k)}. \tag{4.5}$$

And lastly,

$$(t_i t_j)t_{-j} \;=\; t_i(t_j t_{-j})$$

$$\Rightarrow \sum_{k=0}^{p-1} \lambda_{ijk} t_{i+j} h^k t_{-j} \;=\; t_i \left(\sum_{n=1}^{p-1} s_n + p \cdot 1 \right)$$

$$\begin{aligned} \Rightarrow \sum_{k=0}^{p-1} \sum_{m=0}^{p-1} \lambda_{ijk}\lambda_{(i+j)(-j)m} t_i h^m h^k \;&= \sum_{n=1}^{p-1} t_i s_n + p \cdot t_i \\ &= \sum_{n=1}^{p-1} \sum_{k=0}^{p-1} t_i h^k + p \cdot t_i \\ &= (p-1) \sum_{k=0}^{p-1} t_i h^k + p \cdot t_i. \end{aligned}$$

On the left-hand side, the coefficient of $t_i h^n$ is

$$\sum_{m+k=n} \lambda_{ijk}\lambda_{(i+j)(-j)m} = \sum_{k=0}^{p-1} \lambda_{ijk}\lambda_{(i+j)(-j)(n-k)}.$$

On the right-hand side, the coefficient of $t_i h^n$ is $p-1$ if $n \neq 0$ and $p-1+p = 2p-1$ if $n = 0$. So

$$\sum_{k=0}^{p-1} \lambda_{ijk}\lambda_{(i+j)(-j)(n-k)} = p-1 \text{ for } 1 \leq n \leq p-1 \text{ and}$$
$$\sum_{k=0}^{p-1} \lambda_{ijk}\lambda_{(i+j)(-j)(-k)} = 2p-1.$$

By (4.5), we now have:

$$\sum_{k=0}^{p-1} \lambda_{ijk}\lambda_{ij(k-n)} = p-1 \text{ for } 1 \leq n \leq p-1 \tag{4.6}$$

and

$$\sum_{k=0}^{p-1} \lambda_{ijk}^2 = 2p-1. \tag{4.7}$$

Now, letting $x_k = \lambda_{ijk} - 1$ and noting that $\sum_{k=0}^{p-1} \lambda_{ijk}\lambda_{ij(k-n)} = \sum_{k=0}^{p-1} \lambda_{ijk}\lambda_{ij(k+n)}$, equations (4.4), (4.6), and (4.7) give the system of equations solved in Proposition 4.1. Therefore we must have $\lambda_{ijk} - 1 = \left(\frac{k+m}{p}\right)$ or $\lambda_{ijk} - 1 = -\left(\frac{k+m}{p}\right)$ for some $0 \leq m \leq p-1$. Thus $\lambda_{ijk} = \left(\frac{k+m}{p}\right) + 1$ or $-\left(\frac{k+m}{p}\right) + 1$ for some $0 \leq m \leq p-1$, so for each i and j with $i \neq -j$,

$$t_i t_j = (rh^m)t_{i+j} \quad \text{or} \quad t_i t_j = (sh^m)t_{i+j},$$

where the m depends on i and j.

Let $\lambda_{ij} = \sum_{k=0}^{p-1} \lambda_{ijk} h^k$; so $t_i t_j = \lambda_{ij} t_{i+j}$ for $i \neq -j$. We've just shown that for some $0 \leq m \leq p-1$, and each i and j with $i \neq -j, \lambda_{ij} = (rh^m)$ or sh^m, where the m depends on i and j. Note that since $\left(\sum_{k=0}^{p-1} \lambda_{ijk} h^k\right)^* = \sum_{k=0}^{p-1} \lambda_{ij(-k)} h^k$,

$$\lambda_{ij}^* = \sum_{k=0}^{p-1} \lambda_{ij(-k)} h^k.$$

Since $t_i t_j = (t_{-i} t_{-j})^*$, we have

$$\lambda_{ij} = \lambda_{(-i)(-j)}^*.$$

By equation (4.5), $\lambda_{1ik} = \lambda_{i1k} = \lambda_{(1+i)(-1)(-k)}$, so

$$\lambda_{1i} = \lambda_{(1+i)(-1)}^* = \lambda_{1(-i-1)}. \tag{4.8}$$

Next, we show that rh^k and sh^k are invertible elements of $\mathbb{R}H$. There exists $\sum_{k=0}^{p-1} \alpha_k h^k \in \mathbb{R}H$ with $\left(\sum_{k=0}^{p-1} \lambda_{ijk} h^k\right)\left(\sum_{k=0}^{p-1} \alpha_k h^k\right) = 1$ if and only if

$$\begin{bmatrix} \lambda_{ij0} & \lambda_{ij1} & \cdots & \lambda_{ij(p-1)} \\ \lambda_{ij(p-1)} & \lambda_{ij0} & \cdots & \lambda_{ij(p-2)} \\ & & \vdots & \\ \lambda_{ij1} & \lambda_{ij2} & \cdots & \lambda_{ij0} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_{p-1} \\ \alpha_{p-2} \\ \vdots \\ \alpha_1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

has a solution in the α_i, which occurs if the left-most matrix is invertible. Let $\lambda_{ij} = r$. Then $\begin{bmatrix} \lambda_{ij0} & \lambda_{ij1} & \cdots & \lambda_{ij(p-1)} \\ \lambda_{ij(p-1)} & \lambda_{ij0} & \cdots & \lambda_{ij(p-2)} \\ & & \vdots & \\ \lambda_{ij1} & \lambda_{ij2} & \cdots & \lambda_{ij0} \end{bmatrix}$ is the circulant matrix $Circ\left(\left(\frac{0}{p}\right)+1, \left(\frac{1}{p}\right)+1, \ldots, \left(\frac{p-1}{p}\right)+1\right)$. The eigenvalues of a circulant matrix $Circ(c_0, \ldots, c_{p-1})$ are $\psi_\omega = \sum_{k=0}^{p-1} c_k \omega^k$, where ω is a p^{th} root of unity. (For more information on the eigenvalues of a circulant matrix, see chapter 3 in [10].) Since $\sum_{k=0}^{p-1} \left(\left(\frac{k}{p}\right)+1\right)\omega^k \neq 0$ for any ω, this matrix is invertible. So r has an inverse. Similarly, s has an inverse and hence rh^k and sh^k are invertible for all k.

Now, since (A, B) is associative, $(t_a t_b)t_c = t_a(t_b t_c)$ for all $a, b, c \Rightarrow \lambda_{ab}\lambda_{(a+b)c} = \lambda_{bc}\lambda_{a(b+c)}$ for all a, b, c with $a, b, c, a+b, b+c, a+b+c \neq 0$. For $a = 1, b = i-1, c = j$, this gives

$$\lambda_{1(i-1)}\lambda_{ij} = \lambda_{(i-1)j}\lambda_{1(i+j-1)}$$

for $j \neq 0, i \neq 0, 1, -j, -j+1$. So for these i and j,

$$\lambda_{ij} = \lambda_{(i-1)j}\lambda_{1(i+j-1)}\lambda^{-1}_{1(i-1)}.$$

For the following argument, to avoid complications we will not read indices modulo p; all indices will be integers between 1 and $p-1$. Suppose $i \neq 1, i+j \leq p-1$. Then

$$\begin{aligned}
\lambda_{ij} &= \lambda_{(i-1)j}\lambda_{1(i+j-1)}\lambda_{1(i-1)}^{-1} \\
\lambda_{(i-1)j} &= \lambda_{(i-2)j}\lambda_{1(i+j-2)}\lambda_{1(i-2)}^{-1} \\
&\vdots \\
\lambda_{3j} &= \lambda_{2j}\lambda_{1(j+2)}\lambda_{12}^{-1} \\
\lambda_{2j} &= \lambda_{1j}\lambda_{1(j+1)}\lambda_{11}^{-1}
\end{aligned}$$

since $\lambda_{1j}, \lambda_{(p-j)j}, \lambda_{(p-j+1)j}$ do not appear on the left-hand side of this list. Thus for $1 \leq i, j$ with $i + j \leq p - 1$,

$$\lambda_{ij} = (\lambda_{1j}\lambda_{1(j+1)} \dots \lambda_{1(i+j-1)})(\lambda_{11}\lambda_{12} \dots \lambda_{1(i-1)})^{-1}. \tag{4.9}$$

Also,

$$\lambda_{(p-i)(p-j)} = \lambda_{ij}^* = \left((\lambda_{1j}\lambda_{1(j+1)} \dots \lambda_{1(i+j-1)})(\lambda_{11}\lambda_{12} \dots \lambda_{1(p-i-1)})^{-1}\right)^*.$$

From this and equation (4.8), it follows that for all i and j with $i + j \neq p, \lambda_{ij}$ is uniquely determined by $\{\lambda_{1j} : 1 \leq j \leq \frac{p-1}{2}\}$.

Now suppose that for $1 \leq i \leq \frac{p-3}{2}, \lambda_{1i} = x_i h^{n_i}$, where $x_i = r$ or s for each i. Define

$$t_1' = t_1 \text{ and } t_i' = h^{n_1+n_2+\dots+n_{i-1}} t_i \text{ for all } 2 \leq i \leq \frac{p-3}{2}.$$

Then $t_1't_1' = \lambda_{11}t_2 = x_1h^{n_1}t_2 = x_1t_2'$, and for $2 \leq i \leq \frac{p-3}{2}$,

$$\begin{aligned} t_1't_i' &= t_1h^{n_1+n_2+\cdots n_{i-1}}t_i = h^{n_1+n_2+\cdots n_{i-1}}x_ih^{n_i}t_{i+1} \\ &= x_ih^{n_1+n_2+\cdots n_{i-1}+n_i}t_{i+1} = x_it_{i+1}'. \end{aligned}$$

Thus replacing

$$t_1, t_2, \ldots, t_{\frac{p-3}{2}}, t_{\frac{p-1}{2}}, t^*_{\frac{p-1}{2}}, t^*_{\frac{p-3}{2}}, \ldots, t_1^* \text{ with}$$
$$t_1', t_2', \ldots, t'_{\frac{p-3}{2}}, t_{\frac{p-1}{2}}, t^*_{\frac{p-1}{2}}, t'^*_{\frac{p-3}{2}}, \ldots, t_1'^*$$

yields a set of coset representatives for $L^{(2)}(B)$ in B that satisfies the conditions of the theorem.

For the other direction: Suppose $(\mathbb{C}X, X)$ is a class 2 nilpotent table algebra of order p^2 and $L(X) = H = \langle h \rangle \cong \mathbb{Z}_p$. Let $B = X \cup \{t_ih^k : 1 \leq i \leq p-1, 0 \leq k \leq p-1\}$ as a formal basis for a $\mathbb{C}-$vector space. We define the multiplication on B as follows.

For $x \in X \setminus L(X), xx^* \neq 1$, so $Stab(x) \neq \{1\}$, so $Stab(x) = H$. By Theorem 3.1, $xx^* = |Stab(x)| \sum_{h^k \in Stab(x)} h^k$ for each $x \in X$. Also by Theorem 3.1, $\delta(x) = |Stab(x)|$ for each x, so $\delta(x) = p$ for $x \in X \setminus L(X)$, and therefore $p \cdot |X \setminus L(X)| = o(X \setminus L(X)) = o(X) - o(L(X)) = p^2 - p$. Thus $|X \setminus L(X)| = p - 1$. We write $X = H \cup \{s_i : 1 \leq i \leq p-1\}$. Let $h^kt_i = t_ih^k$,

$$s_jt_i = t_is_j = t_i \sum_{k=0}^{p-1} h^k,$$

and

$$t_it_{p-i} = \sum_{j=1}^{p-1} s_j + p \cdot 1.$$

Let * be the existing anti-automorphism of X. Extend * to B via $(t_ih^k)^* = t_{p-i}h^{-k}$ for each i and k. Note that $r^* = r$ if $p \equiv 1 \bmod 4$ and $r^* = s$ if $p \equiv 3 \bmod$

4, since -1 is a quadratic residue if $p \equiv 1 \bmod 4$ and is a non-residue if $p \equiv 3 \bmod 4$. Similarly, $s^* = s$ if $p \equiv 1 \bmod 4$ and $s^* = r$ if $p \equiv 3 \bmod 4$. Also, recall from the first direction that rh^k and sh^k are invertible elements of $\mathbb{R}H$ for all k.

We now define the products $t_i t_j$ for $j \not\equiv -i$ by setting $t_i t_j = \lambda_{ij} t_{i+j}$ and specifying below the $\lambda_{ij} \in \mathbb{Z}H$. For the following argument, note that whenever ambiguity is possible, indices are not read modulo p and we ensure that they are between 1 and $p-1$.

Let $\lambda_{11} = r$.

For $2 \leq j \leq \frac{p-3}{2}$, let $\lambda_{1j} = r$ or s.

Let $\lambda_{1\left(\frac{p-1}{2}\right)} = rh^m$ or sh^m for some $0 \leq m \leq p-1$.

For $\frac{p-1}{2} < j \leq p-2$, let $\lambda_{1j} = \lambda_{1(p-j-1)}$.

For $i + j \leq p-1$, let $\lambda_{ij} = (\lambda_{1j}\lambda_{1(j+1)} \dots \lambda_{1(i+j-1)})(\lambda_{11}\lambda_{12} \dots \lambda_{1(i-1)})^{-1}$.

For $i + j \geq p+1$, let $\lambda_{ij} = \lambda^*_{(p-i)(p-j)}$.

In the fifth line above, note that the inverted factor contains nothing if $i = 1$. We now show that B is a class three nilpotent SITA of order p^3. We first show that $*$ is an automorphism. For $t_i \in B \setminus X, s_j \in X$, since we already know that $(t_m h^k)^* = t^*_m (h^k)^*$, we have

$$(s_j t_i)^* = (t_i s_j)^* = \left(t_i \sum_{k=0}^{p-1} h^k \right)^* = t_{p-i} \sum_{k=0}^{p-1} h^k = t_{p-i} s_{p-j} = t^*_i s^*_j = s^*_j t^*_i.$$

Suppose $i + j \leq p-1$. Then $p - i + p - j \geq p+1$, so $\lambda_{(p-i)(p-j)} = \lambda^*_{ij}$, and therefore $\lambda^*_{(p-i)(p-j)} = \lambda_{ij}$. If $i + j \geq p+1, \lambda_{ij} = \lambda^*_{(p-i)(p-j)}$ by definition. Thus

$$(t_i t_j)^* = (\lambda_{ij} t_{i+j})^* = \lambda^*_{ij} t_{p-i+p-j} = \lambda_{(p-i)(p-j)} t_{p-i+p-j} = t_{p-i} t_{p-j} = t^*_i t^*_j.$$

We now show that B is commutative. Suppose $i+j \leq p-1$, and suppose WLOG that $i < j$. Then:

$$\begin{aligned}\lambda_{ji} &= (\lambda_{1i}\lambda_{1(i+1)}\dots\lambda_{1j}\dots\lambda_{1(i+j-1)})(\lambda_{11}\lambda_{12}\dots\lambda_{1i}\dots\lambda_{1(j-1)})^{-1} \\ &= (\lambda_{1j}\dots\lambda_{1(i+j-1)})(\lambda_{11}\dots\lambda_{1(i-1)})^{-1} \\ &= \lambda_{ij}.\end{aligned}$$

If $i+j \geq p+1$, then $p-i+p-j \leq p-1$, so $\lambda_{ij} = \lambda^*_{(p-i)(p-j)} = \lambda^*_{(p-j)(p-i)} = \lambda_{ji}$.

We now define the degree map δ. Define δ on X to be the existing degree map on X. For $t_ih^k \in B \setminus X$, let $\delta(t_ih^k) = p$, and extend δ linearly to $\mathbb{C}B$. We show that δ is a homomorphism.

$$\delta(t_is_j) = \delta\left(t_i\sum_{k=0}^{p-1}h^k\right) = \sum_{k=0}^{p-1}\delta(t_ih^k) = p^2 = \delta(t_i)\delta(s_j)$$

for $t_i \in B \setminus X, s_j \in X \setminus H$.

Now, δ is a homomorphism from $\mathbb{C}X$ to $\mathbb{C}, \mathbb{C}H \subseteq \mathbb{C}X$, and $\delta(h^k) = 1$ for all k. Thus $\delta(r) = \delta\left(1 + 2\sum_{i\in R}h^i\right) = p$, and similarly, $\delta(s) = p$. Since $\lambda_{1j} = rh^k$ or sh^k for all j, this gives $\delta(\lambda_{1j}) = p$ for all j. If $i+j \leq p-1$, then

$$\delta(\lambda_{ij}) = \delta(\lambda_{1j}\dots\lambda_{1(i+j-1)})\delta(\lambda_{11}\dots\lambda_{1(i-1)})^{-1} = p^ip^{-(i-1)} = p.$$

Since $r^* = r$ or s and $s^* = s$ or r, $(h^k)^* = h^{-k}$, and $\lambda^*_{(p-i)(p-j)} = \lambda^*_{ij}$ for $i+j \leq p-1$, it follows that $\delta(\lambda_{(p-i)(p-j)}) = p$ as well.

Now $\lambda_{ij} \in \mathbb{Z}H$ implies that $\delta(\lambda_{ij}t_n) = \delta(\lambda_{ij})\delta(t_n)$ for all i, j, and n. So for $i \not\equiv -j$,

$$\delta(t_it_j) = \delta(\lambda_{ij}t_{i+j}) = p^2 = \delta(t_i)\delta(t_j).$$

Also,

$$\delta(t_i t_{p-i}) = \delta\left(\sum_{j=1}^{p-1} s_j + p \cdot 1\right) = (p-1)p + p = p^2 = \delta(t_i)\delta(t_{p-i}).$$

Since it is clear from the multiplication that $1 \in Supp(b_1 b_2) \Leftrightarrow b_2 = b_1^*$, all that remains is to show that the multiplication is associative.

Let $s_i, s_j \in X \setminus L(X), t_m, t_n \in B \setminus X$ with $i + j, m + n \neq 0$. Then

$$\begin{aligned} s_i(s_j t_m) &= s_i \cdot \sum_{k=0}^{p-1} t_m h^k = \sum_{k,l=0}^{p-1} t_m h^k h^l = p \sum_{k=0}^{p-1} t_m h^k \text{ and} \\ (s_i s_j)t_m &= p s_{i+j} \cdot t_m = p \sum_{k=0}^{p-1} t_m h^k; \end{aligned}$$

$$\begin{aligned} s_i(t_m t_n) &= s_i \cdot \lambda_{mn} t_{m+n} = \lambda_{mn} \cdot \sum_{k=0}^{p-1} t_{m+n} h^k \text{ and} \\ (s_i t_m)t_n &= \sum_{k=0}^{p-1} t_m h^k \cdot t_n = \sum_{k=0}^{p-1} \lambda_{mn} t_{m+n} h^k; \end{aligned}$$

$$\begin{aligned} s_i(s_i^* t_m) &= s_i(s_{-i} t_m) = s_i \cdot \sum_{k=0}^{p-1} t_m h^k = \sum_{k,l=0}^{p-1} t_m h^k h^l = p \sum_{k=0}^{p-1} t_m h^k \text{ and} \\ (s_i s_i^*)t_m &= p \sum_{k=0}^{p-1} h^k \cdot t_m; \end{aligned}$$

$$\begin{aligned} s_i(t_m t_m^*) &= s_i \left(\sum_{k=1}^{p-1} s_k + p \cdot 1\right) = \sum_{k=1}^{p-1} s_i s_k + p \cdot s_i \\ &= \sum_{\substack{k \in \mathbb{Z}_p \\ k \neq 0, -i}} p s_{i+k} + p \sum_{k=0}^{p-1} h^k + p s_i = p \sum_{x \in X} x \quad \text{and} \end{aligned}$$

$$\begin{aligned}(s_i t_m)t_m^* &= \sum_{k=0}^{p-1} t_m h^k \cdot t_m^* = \sum_{k=0}^{p-1}\left(\sum_{l=1}^{p-1} s_l + p\cdot 1\right)h^k \\ &= p\sum_{l=1}^{p-1} s_l + p\sum_{k=0}^{p-1} h^k = p\sum_{x\in X} x.\end{aligned}$$

Now, $\lambda_{mn} = \sum_{k=0}^{p-1} \lambda_{mnk} h^k$ where $\{\lambda_{mnk} + 1 : 0 \leq k \leq p-1\}$ satisfies the system of equations in Proposition 4.1. Thus

$$\sum_{k=0}^{p-1} \lambda_{ijk} = p, \sum_{k=0}^{p-1} \lambda_{ijk}^2 = 2p-1, \text{ and } \sum_{k=0}^{p-1} \lambda_{ijk}\lambda_{ij(k+m)} = p-1 \text{ for } m \neq 0.$$

We now show that $\lambda_{ij} = \lambda_{(p-i-j)j}$ (or, if $i+j \geq p+1$, $\lambda_{(2p-i-j)j}$). Suppose $i+j \leq p-1$. Then $0 < p-i-j < p$ and $(p-i-j)+j = p-i \leq p-1$. Hence

$$\begin{aligned}\lambda_{ij} &= (\lambda_{1j}\ldots\lambda_{1(i+j-1)})(\lambda_{11}\ldots\lambda_{1(i-1)})^{-1} \text{ and} \\ \lambda_{(p-i-j)j} &= (\lambda_{1j}\ldots\lambda_{1p-i-j+j-1})(\lambda_{11}\ldots\lambda_{1(p-i-j-1)})^{-1} \\ &= (\lambda_{1j}\ldots\lambda_{1p-i-1})(\lambda_{11}\ldots\lambda_{1(p-i-j-1)})^{-1}.\end{aligned}$$

If $p-i-j < i$, then $p-i \leq i+j-1$ and $p-i-j \leq i-1$. Since $\lambda_{1k} = \lambda_{1(p-k-1)}$ for all $k \neq p-1$, we have:

$$\begin{aligned}\lambda_{ij} &= (\lambda_{1j}\lambda_{1(j+1)}\ldots\lambda_{1(p-i-1)}\lambda_{1(p-i)}\ldots\lambda_{1(i+j-1)})(\lambda_{11}\lambda_{12}\ldots\lambda_{1(p-i-j)}\ldots\lambda_{1(i-1)})^{-1} \\ &= (\lambda_{1j}\ldots\lambda_{1(p-i-1)}\cdot\lambda_{1(i-1)}\lambda_{1(i-2)}\ldots\lambda_{1(p-i-j)})(\lambda_{11}\ldots\lambda_{1(p-i-j)}\ldots\lambda_{1(i-1)})^{-1} \\ &= (\lambda_{1j}\ldots\lambda_{1(p-i-1)})(\lambda_{11}\ldots\lambda_{1(p-i-j-1)})^{-1} \\ &= \lambda_{(p-i-j)j}.\end{aligned}$$

A similar argument shows that if $p-i-j > i$, the result still holds.

Suppose $i+j \geq p+1$. Then $p-i+p-j \leq p-1$ and

$$\lambda_{ij} = \lambda^*_{(p-i)(p-j)} = \lambda^*_{(p-(p-i)-(p-j))(p-j)} = \lambda_{(2p-i-j)j}.$$

Therefore

$$\lambda_{ij} = \lambda_{(-i-j)j} = \lambda^*_{(i+j)(-j)} \tag{4.10}$$

for all i and j.

We now have

$$\begin{aligned} t_m(t_n t_n^*) &= t_m\left(\sum_{l=1}^{p-1} s_l + p\cdot 1\right) = \sum_{l=1}^{p-1}\sum_{k=0}^{p-1}(t_m h^k) + p\cdot t_m \\ &= (p-1)\sum_{k=0}^{p-1} t_m h^k + p\cdot t_m = (p-1)\sum_{k=1}^{p-1} t_m h^k + (2p-1)t_m, \end{aligned}$$

and by (4.10)

$$\begin{aligned} (t_m t_n)t_n^* &= \lambda_{mn} t_{m+n}\cdot t_{-n} = \lambda_{mn}\lambda_{(m+n)(p-n)} t_m = \lambda_{mn}\lambda^*_{mn} t_m \\ &= \left(\sum_{k=0}^{p-1}\lambda_{mnk}h^k\right)\left(\sum_{l=0}^{p-1}\lambda_{mnl}h^l\right)^* t_m = \sum_{k,l=0}^{p-1}\lambda_{mnk}\lambda_{mnl}h^{k-l}t_m \\ &= \sum_{k-l=0}\lambda_{mnk}\lambda_{mnl}h^{k-l}t_m + \sum_{q=1}^{p-1}\sum_{k-l=q}\lambda_{mnk}\lambda_{mnl}h^{k-l}t_m \\ &= \left(\sum_{k=0}^{p-1}\lambda^2_{mnk}\right)t_m + \sum_{q=1}^{p-1}\left(\sum_{l=0}^{p-1}\lambda_{mn(q+l)}\lambda_{mnl}\right)h^q t_m \\ &= (2p-1)t_m + (p-1)\sum_{q=1}^{p-1} t_m h^q. \end{aligned}$$

Since for $s_k \in X\setminus L(X), h^l \in L(X), s_k\cdot rh^l = s_k\cdot sh^l = p\cdot s_k$, we now have

$$\begin{aligned} t^*_{m+n}(t_m t_n) &= t^*_{m+n}\cdot\lambda_{mn}t_{m+n} = \sum_{k=1}^{p-1} s_k\lambda_{mn} + p\cdot\lambda_{mn} \\ &= p\sum_{k=1}^{p-1} s_k + p\cdot\lambda_{mn} \text{ and} \end{aligned}$$

$$\begin{aligned}(t^*_{m+n}t_m)t_n &= \lambda_{(-m-n)m}t_{-n}\cdot t_n = \sum_{k=1}^{p-1} s_k\lambda_{(-m-n)m} + p\cdot\lambda_{(-m-n)m}\\ &= p\cdot\sum_{k=1}^{p-1} s_k + p\cdot\lambda_{(-m-n)m} = p\cdot\sum_{k=1}^{p-1} s_k + p\cdot\lambda_{nm}\\ &= p\cdot\sum_{k=1}^{p-1} s_k + p\cdot\lambda_{mn}.\end{aligned}$$

Finally, let $t_i, t_j, t_k \in B\setminus X$ with $i+j, j+k, i+j+k \not\equiv 0$. Note that since $s = 2H^+ - r$,

$$s^2 = (2H^+ - r)^2 = 4H^+H^+ - 4H^+r + r^2 = 4pH^+ - 4pH^+ + r^2 = r^2.$$

Suppose $i+j+1 \le p-1$. Then $i+j \le p-2$, so

$$\begin{aligned}\lambda_{1i}\lambda_{(1+i)j} &= \lambda_{ij}\lambda_{1(i+j)}\\ \Leftrightarrow \lambda_{1i}(\lambda_{1j}\dots\lambda_{1(i+j)})(\lambda_{11}\dots\lambda_{1i})^{-1} &= \lambda_{1(i+j)}(\lambda_{1j}\dots\lambda_{1(i+j-1)})(\lambda_{11}\dots\lambda_{1(i-1)})^{-1},\end{aligned}$$

which is clearly true.

Suppose $i \ne p-1$ and $i+j+1 \ge p+1$. Then $i+j \ge p+1$ since $i+j \ne p$, so $(p-(1+i))+(p-j) \le p-1$ and $(p-i)+(p-j) \le p-1$. So

$$\begin{aligned}&\lambda_{1i}\lambda_{(1+i)j} = \lambda_{ij}\lambda_{1(i+j)}\\ &\Leftrightarrow \lambda_{1(p-i-1)}\lambda^*_{(p-(1+i))(p-j)} = \lambda^*_{(p-i)(p-j)}\lambda_{1(2p-i-j-1)}\\ &\Leftrightarrow \lambda_{1(p-i-1)}\left[(\lambda_{1(p-j)}\dots\lambda_{1(2p-i-j-2)})(\lambda_{11}\dots\lambda_{1(p-i-2)})^{-1}\right]^*\\ &\quad = \lambda_{1(2p-i-j-1)}\left[(\lambda_{1(p-j)}\dots\lambda_{1(2p-i-j-1)})(\lambda_{11}\dots\lambda_{1(p-i-1)})^{-1}\right]^*\\ &\Leftrightarrow (\lambda_{1(p-j)}\dots\lambda_{1(2p-i-j-2)})(\lambda_{11}\dots\lambda_{1(p-i-2)})^{-1}\\ &\quad = \left(\lambda_{1(p-j)}\cdots\lambda_{1(2p-i-j-1)}\cdot\lambda^*_{1(2p-i-j-1)}\right)\left(\lambda_{11}\cdots\lambda_{1(p-i-1)}\cdot\lambda^*_{1(p-i-1)}\right)^{-1}\\ &\Leftrightarrow 1 = \left(\lambda_{1(2p-i-j-1)}\cdot\lambda^*_{1(2p-i-j-1)}\right)\left(\lambda_{1(p-i-1)}\cdot\lambda^*_{1(p-i-1)}\right)^{-1},\end{aligned}$$

which is true if $p \equiv 1 \bmod 4$ because $r^2 = s^2$, and if $p \equiv 3 \bmod 4$ because $rs = sr$.

So $\lambda_{1i}\lambda_{(1+i)j} = \lambda_{ij}\lambda_{1(i+j)}$ for $i, i+j \neq p-1$. Therefore

$$t_1(t_it_j) = t_1 \cdot \lambda_{ij}t_{i+j} = \lambda_{ij}\lambda_{1(i+j)}t_{i+j+1} = \lambda_{1i}\lambda_{(1+i)j}t_{i+j+1} = (t_1t_i)t_j.$$

We may now use the notation t_1^i for the product of i copies of t_1. Since the λ_{ij} are invertible elements of $\mathbb{R}H$, we have:

$$\begin{aligned}
&t_1^2 = \lambda_{11}t_2 \Longrightarrow t_2 = \lambda_{11}^{-1}t_1^2 \\
&t_1^3 = (\lambda_{11}t_2)t_1 = \lambda_{11}\lambda_{12}t_3 \Longrightarrow t_3 = (\lambda_{11}\lambda_{12})^{-1}t_1^3 \\
&\vdots \\
&t_i = (\lambda_{11}\ldots\lambda_{1(i-1)})^{-1}t_1^i \text{ for } i = 1, 2, \ldots, p-1.
\end{aligned}$$

We write $t_i = v_it_1^i$. Reading the i, j, and k modulo p, for $i+j, j+k, i+j+k \not\equiv 0$,

$$t_i(t_jt_k) = (v_it_1^i)(v_jt_1^jv_kt_1^k) = (v_iv_jv_k)t_1^{i+j+k} = (t_it_j)t_k.$$

So the multiplication is associative. Thus $(\mathbb{C}B, B)$ is a commutative, associative algebra with $1 \in B$, an (anti)-automorphism * permuting B, and structure constants and degrees in $\mathbb{Z}_{\geq 0}$. Since $t_it_i^* = \sum_{j=1}^{p-1} s_k + p \cdot 1, \delta(t_i)$ is the coefficient of 1 in $t_it_i^*$. We have now shown that $(\mathbb{C}B, B)$ is a commutative, standard SITA.

Finally,

$$o(B) = o(B \setminus X) + o(X \setminus H) + o(H) = (p-1) \cdot p \cdot p + (p-1) \cdot p + p = p^3.$$

And $L(B) = H, L^{(2)}(B) = \{b : bb^* \subseteq L(B)\} = X$, and $L^{(3)}(B) = \{b : bb^* \subseteq L^{(2)}(B)\} = B$. Therefore B is class three nilpotent of order p^3. $\square$

4.3 Isomorphic Redundancy

Theorem 4.1 and its proof show that if (A, B) is a class three nilpotent SITA of order p^3, then there is a set of coset representatives $\{t_i : 1 \leq i \leq p-1\}$ for $L^{(2)}(B)$ in B with $t_i^* = t_{p-i}$ and $t_i t_j = \lambda_{ij} t_{i+j}$ for $i \neq -j$, where $\lambda_{ij} = rh^{k_{ij}}$ or $sh^{k_{ij}}$ for each i and j; and the set $\{\lambda_{1j} : 1 \leq j \leq p-2\}$ uniquely determines the algebra up to exact isomorphism. Since two different sets of these λ_{1j} can yield isomorphic algebras, we now investigate this redundancy. For the remainder of this section, when the word "algebra" is used, we will mean a class three nilpotent SITA of order p^3 for an odd prime p that is not a wreath product. We will use the notation (A, p) to denote such an algebra whenever the prime needs to be stated explicitly.

Call $(\lambda_{11}, \lambda_{12}, \ldots, \lambda_{1(p-2)})$ a t_1 *string* for (A, p). Let m be a primitive root modulo p, and call $(\lambda_{11}, \lambda_{mm}, \lambda_{m^2m^2}, \ldots, \lambda_{m^{p-2}m^{p-2}})$ the corresponding *squares string* for (A, p). We will approach the problem of isomorphic redundancy from the viewpoint of squares strings rather than t_1 strings.

Theorem 4.1 also shows that the t_i can be chosen so that $k_{1j} = 0$ if $j \neq \frac{p-1}{2}$. In this case, we will show that the corresponding squares string has a specific format, and that it uniquely determines the algebra up to exact isomorphism as well. The next definition deals with these cases.

Definition 4.2. We will call a t_1 string $(\lambda_{11}, \lambda_{12}, \ldots, \lambda_{1(p-2)})$ *special* if it has the property that $\lambda_{1j} = r$ or s for $j \neq \frac{p-1}{2}$. We will call a squares string $(\lambda_{11}, \lambda_{mm}, \ldots, \lambda_{m^{p-2}m^{p-2}})$ *special* if it has the property that

$$\lambda_{ii} = \begin{cases} rh^k \text{ or } sh^k & \text{if } \frac{p+1}{4} \leq i \leq \frac{p-1}{2} \\ rh^{-k} \text{ or } sh^{-k} & \text{if } p - \frac{p-1}{2} \leq i \leq p - \frac{p+1}{4} \\ r \text{ or } s & \text{otherwise.} \end{cases}$$

We will denote a squares string of this form by s_k; so s_0 gives the pattern of r's and s's that appear in the string, and two strings s_k and s_n have the same patterns of r's and s's and only differ in the power of h that appears. Let s_0^{op} have an r wherever s_0 has an s, and an s wherever s_0 has an r. Thus the strings s_k and s_n^{op} each have an r wherever the other has an s, and h^k appears in the first, whereas h^n appears in the second.

Lemma 4.3. *Suppose (A, p) and (A', p) are algebras and $\phi : A' \to A$ is an exact table algebra isomorphism. Then there exist $1 \leq a, b, c \leq p-1$ so that for each i,*

$$\begin{aligned} &\phi((h')^i) = h^{ai}, \\ &\phi(s_i') = s_{bi}, \text{ and} \\ &\phi(t_i') = t_{ci}h^{d_i} \text{ for some } 0 \leq d_i \leq p-1. \end{aligned}$$

Proof. Clearly $\phi\left(L^{(i)}(B')\right) = L^{(i)}(B)$ for each i. Since $L(B') \cong L(B) \cong \mathbb{Z}_p$, for some $1 \leq a \leq p-1$ we have $\phi((h')^i) = h^{ai}$ for each i.

Since $L^{(2)}(B')//L(B') \cong L^{(2)}(B)//L(B) \cong \mathbb{Z}_p$, we have for some $1 \leq b \leq p-1$

$$\phi\left(s_i'//L(B')\right) = s_{bi}//L(B)$$

for each i. So

$$\phi\left(\frac{s_i'}{p}\right) = \frac{s_{bi}}{p} \Rightarrow \phi(s_i') = s_{bi}.$$

Finally, since $B'//L^{(2)}(B') \cong B//L^{(2)}(B) \cong \mathbb{Z}_p$, we have for some $1 \leq c \leq p-1$

$$\phi\left(t_i'//L^{(2)}(B)\right) = t_{ci}//L^{(2)}(B) \text{ for each } i$$

$$\Rightarrow \phi\left(\frac{(t_i'L^{(2)}(B'))^+}{|L^{(2)}(B')|}\right) = \frac{(t_{ci}L^{(2)}(B))^+}{|L^{(2)}(B)|}$$

$$\Rightarrow \phi\left(\sum_{k=0}^{p-1} t_i'h^k\right) = \sum_{k=0}^{p-1} t_{ci}h^k$$

$$\Rightarrow \phi(t_i') = t_{ci}h^{d_i} \text{ for some } d_i.$$

□

By equation (4.2) in the proof of Theorem 4.1, we have $t_i s_j = \sum_{k=0}^{p-1} t_i h^k$ for every j. Since this is the same for every s_j, an isomorphism $\phi : A' \to A$ that simply sends s_i' to s_{bi} can have no effect on the strings that determine either algebra; so henceforth we will simply assume that $b = 1$.

Proposition 4.2. *Let m be a primitive root modulo p. If the t_1 string determining an algebra (A, p) is special, then so is its corresponding squares string, and in this case the squares string uniquely determines the algebra up to exact isomorphism. Suppose (A, p) is determined by the special squares string s_q, and (A', p) is deter-*

mined by the special squares string s'_n. If $\phi : A' \to A$ is is an exact table algebra isomorphism as in Lemma 4.3, then

$$s'_0 = \begin{cases} P^k(s_0) & \text{if } a \in R \\ P^k(s_0^{op}) & \text{if } a \in S, \end{cases}$$

and

$$n = \begin{cases} ca^{-1}q \text{ if } c \leq \frac{p-1}{2}, \\ -ca^{-1}q \text{ if } c > \frac{p-1}{2}, \end{cases}$$

where $c = m^k$ and P is the permutation operator as in Lemma 4.1.

Proof. Let m be a primitive root modulo p. Suppose λ_{ii} is known for each i. For $i < \frac{p-1}{2}$, by equation (4.9) in Theorem 4.1 we have

$$\begin{aligned} \lambda_{ii} = \lambda_{(i+1)(i+1)}h^k \text{ for some } k \quad &\Leftrightarrow \quad \lambda_{1i}\lambda_{1(i+1)} \dots \lambda_{1(2i-1)}\lambda_{11}^{-1}\lambda_{12}^{-1} \dots \lambda_{1(i-1)}^{-1} \\ &\qquad = \lambda_{1(i+1)}\lambda_{1(i+2)} \dots \lambda_{1(2i+1)}\lambda_{11}^{-1}\lambda_{12}^{-1} \dots \lambda_{1i}^{-1}h^k \\ &\Leftrightarrow \quad \lambda_{1i} = \lambda_{1(2i)}\lambda_{1(2i+1)}\lambda_{1i}^{-1}h^k \\ &\Leftrightarrow \quad \lambda_{1i}^2 = \lambda_{1(2i)}\lambda_{1(2i+1)}h^k \\ &\Leftrightarrow \quad \lambda_{1(2i)} = \lambda_{1(2i+1)}h^n \end{aligned}$$

for some n since $r^2 = s^2$ and $rh^q \neq s$ for any q. So for every even j, the squares string determines whether there exists n_j with $\lambda_{1j} = \lambda_{1(j+1)}h^{n_j}$.

Furthermore, by equation (4.8) in Theorem 4.1, $\lambda_{1(2i)} = \lambda_{1(p-2i-1)}$ and $\lambda_{1(2i+1)} = \lambda_{1(p-(2i+1)-1)} = \lambda_{1(p-2i-2)}$. So the squares string determines whether there exists n with $\lambda_{1(p-2i-2)}h^n = \lambda_{1(p-2i-1)}$ as well; since $p-2i-2$ is odd, this means it determines whether there exists n_j with $\lambda_{1j} = \lambda_{1(j+1)}h^{n_j}$ for each odd j as well. Since $rh^q \neq s$

for any q, this shows that the squares string determines whether $\lambda_{1j} = rh^{n_j}$ or sh^{n_j} for each j. For $j \neq \frac{p-1}{2}$, we know that $n_j = 0; n_{\frac{p-1}{2}}$ is the only remaining ambiguity.

Let A be determined by the special t_1 string $(\lambda_{11}, \ldots, \lambda_{1(p-2)})$, where $\lambda_{1\left(\frac{p-1}{2}\right)} = rh^q$ or sh^q for some $0 \leq q \leq p-1$. For $i \leq \frac{p-1}{2}$,

$$\lambda_{ii} = (\lambda_{1i} \ldots \lambda_{1(2i-1)})(\lambda_{11} \ldots \lambda_{1(i-1)})^{-1}.$$

Now, $\lambda_{1\left(\frac{p-1}{2}\right)}$ appears once in this product if and only if $i \leq \frac{p-1}{2} \leq 2i-1$, i.e. if and only if $\frac{p+1}{4} \leq i \leq \frac{p-1}{2}$; otherwise it does not appear at all. So, since $\lambda_{ii} = \left(\lambda_{(-i)(-i)}\right)^*$,

$$\lambda_{ii} = \begin{cases} rh^q \text{ or } sh^q & \text{if } \frac{p+1}{4} \leq i \leq \frac{p-1}{2} \\ rh^{-q} \text{ or } sh^{-q} & \text{if } p - \frac{p-1}{2} \leq i \leq p - \frac{p+1}{4} \\ r \text{ or } s & \text{otherwise.} \end{cases}$$

In other words, A is determined by the special squares string s_q, and the power of h that appears in λ_{ii} for $\frac{p+1}{4} \leq i \leq \frac{p-1}{2}$ is equal to $n_{\frac{p-1}{2}}$. Thus the squares string determines $n_{\frac{p-1}{2}}$, and therefore determines $\{\lambda_{1j} : 1 \leq j \leq p-2\}$, which determines the entire algebra.

Let m be a primitive root mod p. For A determined by the special squares string s_q and A' determined by the special squares string s'_n, suppose $\phi : A' \to A$ is an arbitrary exact table algebra isomorphism with $\phi(s'_i) = s_i$ for each i. Then by Lemma 4.3, there exist $1 \leq c, a \leq p-1$ such that for each i,

$$\phi(t'_i) = t_{ci}h^{d_i}, \phi((h')^i) = h^{ai}$$

for some $0 \leq d_i \leq p-1$. So there exist algebras A'' and A''', and isomorphisms ϕ_1, ϕ_2, ϕ_3 such that:

$$\begin{array}{lcll} A' & \cong & A'' & \text{via} \quad \phi_1((h')^i) = (h'')^i, \quad \phi_1(t_i') = t_i''(h'')^{d_i}, \\ A'' & \cong & A''' & \text{via} \quad \phi_2((h'')^i) = (h''')^i, \quad \phi_2(t_i'') = t_{ci}''', \text{ and} \\ A''' & \cong & A & \text{via} \quad \phi_3((h''')^i) = h^{ai}, \quad \phi_3(t_i''') = t_i, \end{array}$$

and thus $\phi = \phi_3 \circ \phi_2 \circ \phi_1$.

For each i,

$$t_i t_i = \phi_3(t_i''' t_i''') = \phi_3(\lambda_{ii}''' t_{2i}''') = \phi_3(\lambda_{ii}''') t_{2i},$$

so $\lambda_{ii} = \phi_3(\lambda_{ii}''')$. If $a \in R$, then $\phi_3(r'''(h''')^i) = rh^{ai}, \phi_3(s'''(h''')^i) = sh^{ai}$; so $\lambda_{ii} = rh^{ak_i} \Leftrightarrow \lambda_{ii}''' = r'''(h''')^{k_i}, \lambda_{ii} = sh^{ak_i} \Leftrightarrow \lambda_{ii}''' = s'''(h''')^{k_i}$. Therefore A''' is determined by $s_{a^{-1}q}$.

If $a \in S$, then $\phi_3(r'''(h''')^i) = sh^{ai}$ and $\phi_3(s'''(h''')^i) = rh^{ai}$; so $\lambda_{ii} = rh^{ak_i} \Leftrightarrow \lambda_{ii}''' = s'''(h''')^{k_i}, \lambda_{ii} = sh^{ak_i} \Leftrightarrow \lambda_{ii}''' = r'''(h''')^{k_i}$. Thus A''' is determined by $s^{op}_{a^{-1}q}$.

So A''' is determined by $s_{a^{-1}q}$ if $a \in R$, and by $s^{op}_{a^{-1}q}$ if $a \in S$.

Suppose $c = m^k$. Then for each j,

$$t'''_{m^k m^j} t'''_{m^k m^j} = \phi_2(t''_{m^j} t''_{m^j}) = \phi_2(\lambda''_{m^j m^j} t''_{2m^j}) = \phi_2(\lambda''_{m^j m^j}) t'''_{2m^k m^j}.$$

So $\lambda'''_{(m^k m^j)(m^k m^j)} = \phi_2(\lambda''_{m^j m^j})$. So, since $\phi_2(r''(h'')^i) = r'''(h''')^i, \phi_2(s''(h'')^i) = s'''(h''')^i$ for all i,

$$\lambda''_{m^j m^j} = r''(h'')^i \Leftrightarrow \lambda'''_{m^{j+k} m^{j+k}} = r'''(h''')^i,$$

$$\lambda''_{m^j m^j} = s''(h'')^i \Leftrightarrow \lambda'''_{m^{j+k} m^{j+k}} = s'''(h''')^i.$$

So the squares string $(\lambda''_{11}, \lambda''_{mm}, \ldots, \lambda''_{m^{p-2}m^{p-2}})$ is the k^{th} cyclic permutation (to the left) of the one that determines A'''. In other words, this squares string is equal to $P^k(s_{a^{-1}q})$ if $a \in R$ and is equal to $P^k(s^{op}_{a^{-1}q})$ if $a \in S$.

Now,

$$\lambda''_{ii}t''_{2i}(h'')^{2d_i} = t''_i t''_i (h'')^{2d_i} = \phi_1(t'_i t'_i) = \phi_1(\lambda'_{ii}t'_{2i}) = \phi_1(\lambda'_{ii})t''_{2i}(h'')^{d_{2i}}.$$

So $\phi_1(\lambda'_{ii}) = \lambda''_{ii}(h'')^{2d_i - d_{2i}}$. Since $\phi_1(r'(h')^i) = r''(h'')^i$, $\phi_1(s'(h')^i) = s''(h'')^i$, and $r''(h'')^i \neq s''$ for any i, this implies that

$$\lambda'_{ii} = r'(h')^n \Leftrightarrow \lambda''_{ii} = r''(h'')^{k_i} \text{ for some } k_i \text{ and}$$

$$\lambda'_{ii} = s'(h')^n \Leftrightarrow \lambda''_{ii} = s''(h'')^{k_i} \text{ for some } k_i.$$

So $s'_0 = P^k(s_0)$ if $a \in R$, $s'_0 = P^k(s^{op}_0)$ if $a \in S$. This gives the pattern of r's and s's in the squares string for A'. We now need only determine the power of h' that appears in λ'_{ii} for $i \in \left[\frac{p+1}{4}, \frac{p-1}{2}\right]$.

Since

$$\lambda'''_{c(ci)}t'''_{c(i+1)} = t'''_c t'''_{ci} = \phi_2(t''_1 t''_i) = \phi_2(\lambda''_{1i}t''_{i+1}) = \phi_2(\lambda''_{1i})t'''_{c(i+1)},$$

we have $\lambda'''_{c(ci)} = \phi_2(\lambda''_{1i})$. So since $\phi_2(r''(h'')^i) = r'''(h''')^i, \phi_2(s''(h'')^i) = s'''(h''')^i$, we have

$$\lambda''_{1i} = r''(h'')^{n_i} \Leftrightarrow \lambda'''_{c(ci)} = r'''(h''')^{n_i} \text{ and } \lambda''_{1i} = s''(h'')^{n_i} \Leftrightarrow \lambda'''_{c(ci)} = s'''(h''')^{n_i}. \quad (4.11)$$

For the following argument, suppose ci has been reduced modulo p (so $0 \leq ci \leq p-1$) and suppose $c \leq \frac{p-1}{2}$.

Suppose $c + ci \leq p - 1$. Then

$$\lambda'''_{c(ci)} = \left(\lambda'''_{1(ci)} \dots \lambda'''_{1(c+ci-1)}\right) \left(\lambda'''_{11} \dots \lambda'''_{(c-1)}\right)^{-1}$$

by equation (4.9) in Theorem 4.1. Now, $\lambda'''_{1(\frac{p-1}{2})}$ appears in this product exactly once if $ci \leq \frac{p-1}{2} \leq c + ci - 1$ and does not appear at all otherwise. Since $c \leq \frac{p-1}{2}$, $\left(\lambda'''_{1(\frac{p-1}{2})}\right)^{-1}$ does not appear at all. So if $c \leq \frac{p-1}{2}$,

$$\lambda'''_{c(ci)} = r'''(h''')^{a^{-1}q} \text{ or } s'''(h''')^{a^{-1}q} \text{ for } ci \leq \frac{p-1}{2} \leq c + ci - 1,$$

and

$$\lambda'''_{c(ci)} = r''' \text{ or } s''' \text{ otherwise.}$$

Suppose $c + ci \geq p + 1$. Then $p - c + p - ci \leq p - 1$, so

$$\begin{aligned} \lambda'''_{c(ci)} &= \left(\lambda'''_{(p-c)(p-ci)}\right)^* = \left(\lambda'''_{(p-ci)(p-c)}\right)^* \\ &= \left[\left(\lambda'''_{1(p-c)} \dots \lambda'''_{1(p-ci+p-c-1)}\right) \left(\lambda'''_{11} \dots \lambda'''_{1(p-ci-1)}\right)^{-1}\right]^*. \end{aligned}$$

Since $p - c \geq \frac{p+1}{2}$, $\lambda'''_{1(\frac{p-1}{2})}$ does not appear in the first factor of this, and since $p - ci - 1 \leq \frac{p-3}{2}$, $\lambda'''_{1(\frac{p-1}{2})}$ does not appear in the second factor either. So $\lambda'''_{c(ci)} = r'''$ or s'''.

Thus for $c \leq \frac{p-1}{2}, \lambda'''_{c(ci)} = r'''(h''')^{a^{-1}q}$ or $s'''(h''')^{a^{-1}q}$ exactly when $ci \leq \frac{p-1}{2} \leq c + ci - 1$, and $\lambda'''_{c(ci)} = r'''$ or s''' otherwise. Furthermore,

$$ci \leq \frac{p-1}{2} \leq c + ci - 1 \Leftrightarrow 0 \leq \frac{p-1}{2} - ci \leq c - 1$$

$$\Leftrightarrow ci = \frac{p-1}{2} - (c-1), \frac{p-1}{2} - (c-2), \ldots, \frac{p-3}{2}, \frac{p-1}{2}.$$

The germane thing to notice here is that $\lambda'''_{c(ci)} = r'''(h''')^{a^{-1}q}$ or $s'''(h''')^{a^{-1}q}$ for c values of i. If $c > \frac{p-1}{2}$, this argument applies to $p-c$; so $\lambda'''_{(p-c)[(p-c)i]} = r'''(h''')^{a^{-1}q}$ or $s'''(h''')^{a^{-1}q}$ for c values of i, and therefore $\lambda'''_{c(ci)} = r'''(h''')^{-a^{-1}q}$ or $s'''(h''')^{-a^{-1}q}$ for c values of i.

So, by (4.11), the same is true of λ''_{1i}: if $c \leq \frac{p-1}{2}$, then $\lambda''_{1i} = r''(h'')^{a^{-1}q}$ or $s''(h'')^{a^{-1}q}$ for c values of i, and if $c > \frac{p-1}{2}$, then $\lambda''_{1i} = r''(h'')^{-a^{-1}q}$ or $s''(h'')^{-a^{-1}q}$ for c values of i. Since $\lambda''_{1i} = \lambda''_{(-1-i)1} = \lambda''_{1(-i-1)}$, the string is symmetric about $\lambda''_{1(\frac{p-1}{2})}$, which is its middle element. So the number of $i < \frac{p-1}{2}$ with $\lambda''_{1i} = r''(h'')^{\pm a^{-1}q}$ or $s''(h'')^{\pm a^{-1}q}$ is $\frac{c}{2}$ if c is even, and $\frac{c-1}{2}$ if c is odd; and $\lambda''_{1(\frac{p-1}{2})} = r''$ or s'' if c is even, $\lambda''_{1(\frac{p-1}{2})} = r''(h'')^{a^{-1}q}$ or $s''(h'')^{a^{-1}q}$ if $c \leq \frac{p-1}{2}$ is odd, and $\lambda''_{1(\frac{p-1}{2})} = r''(h'')^{-a^{-1}q}$ or $s''(h'')^{-a^{-1}q}$ if $c > \frac{p-1}{2}$ is odd.

We can now deduce the squares string determining A'. We have

$$\lambda''_{1i}t''_{i+1}(h'')^{d_1+d_i} = t''_1t''_i(h'')^{d_1+d_i} = \phi_1(t'_1t'_i) = \phi_1(\lambda'_{1i}t'_{i+1}) = \phi_1(\lambda'_{1i})t''_{i+1}(h'')^{d_{i+1}},$$

so

$$\lambda''_{1i}(h'')^{d_1+d_i} = \phi_1(\lambda'_{1i})(h'')^{d_{i+1}} \tag{4.12}$$

for all i.

Since the squares string s'_n is special, the t'_1 string determining A' is also special. So for $i \neq \frac{p-1}{2}, \lambda'_{1i} = r'$ or s'. Write $\lambda''_{1i} = r''(h'')^{n_i}$ or $s''(h'')^{n_i}$. Since $\phi_1(r'(h')^i) = r''(h'')^i$ and $\phi_1(s'(h')^i) = s''(h'')^i$ for all i, we have for $i \neq \frac{p-1}{2}$

$$\lambda''_{1i}(h'')^{d_1+d_i} = \phi_1(\lambda'_{1i})(h'')^{d_{i+1}}$$

$$\Rightarrow d_1 + d_i + n_i = d_{i+1}.$$

So for $i \neq \frac{p+1}{2}$,

$$d_i = id_1 + \sum_{j<i} n_j.$$

Since $t''_{p-i}(h'')^{d_{p-i}} = \phi_1(t'^*_i) = \phi_1(t'_i)^* = t''_{p-i}(h'')^{-d_i}$, we have $d_{p-i} = -d_i$. Therefore, by equation (4.12),

$$\begin{aligned}
\phi_1\left(\lambda'_{1\left(\frac{p-1}{2}\right)}\right) &= \lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{d_1+d_{\frac{p-1}{2}}-d_{\frac{p+1}{2}}} \\
&= \lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{d_1+2d_{\frac{p-1}{2}}} \\
&= \lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{d_1+2\left(\frac{p-1}{2}\right)d_1+2\sum_{j<\frac{p-1}{2}} n_j} \\
&= \lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{2\sum_{j<\frac{p-1}{2}} n_j} \\
&= \begin{cases}
\lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{2\left(\frac{c}{2}\right)a^{-1}q} & \text{if } c \text{ is even and } c \leq \frac{p-1}{2}, \\
\lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{2\left(\frac{c}{2}\right)(-a^{-1}q)} & \text{if } c \text{ is even and } c > \frac{p-1}{2}, \\
\lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{2\left(\frac{c-1}{2}\right)a^{-1}q} & \text{if } c \text{ is odd and } c \leq \frac{p-1}{2}, \\
\lambda''_{1\left(\frac{p-1}{2}\right)}(h'')^{2\left(\frac{c-1}{2}\right)(-a^{-1}q)} & \text{if } c \text{ is odd and } c > \frac{p-1}{2}.
\end{cases}
\end{aligned}$$

So, recalling that

$$\lambda''_{1\left(\frac{p-1}{2}\right)} = \begin{cases}
r'' \text{ or } s'' & \text{if } c \text{ is even ,} \\
r''(h'')^{a^{-1}q} \text{ or } s''(h'')^{a^{-1}q} & \text{if } c \text{ is odd and } c \leq \frac{p-1}{2}, \\
r''(h'')^{-a^{-1}q} \text{ or } s''(h'')^{-a^{-1}q} & \text{if } c \text{ is odd and } c > \frac{p-1}{2},
\end{cases}$$

we have

$$\phi_1\left(\lambda'_{1\left(\frac{p-1}{2}\right)}\right) = \begin{cases} r''(h'')^{ca^{-1}q} \text{ or } s''(h'')^{ca^{-1}q} & \text{if } c \leq \frac{p-1}{2}, \\ r''(h'')^{-ca^{-1}q} \text{ or } s''(h'')^{-ca^{-1}q} & \text{if } c > \frac{p-1}{2}, \end{cases}$$

regardless of whether c is even or odd. Thus

$$\lambda'_{1\left(\frac{p-1}{2}\right)} = \begin{cases} r'(h')^{ca^{-1}q} \text{ or } s'(h')^{ca^{-1}q} & \text{if } c \leq \frac{p-1}{2}, \\ r'(h')^{-ca^{-1}q} \text{ or } s'(h')^{-ca^{-1}q} & \text{if } c > \frac{p-1}{2}. \end{cases}$$

So if A is determined by s_q and $\phi : A' \to A$ is as described in Lemma 4.3, then s'_n, the squares string determining A', is described by the following:

$$s'_0 = \begin{cases} P^k(s_0) & \text{if } a \in R \\ P^k(s_0^{op}) & \text{if } a \in S, \end{cases}$$

and

$$n = \begin{cases} ca^{-1}q \text{ if } c \leq \frac{p-1}{2}, \\ -ca^{-1}q \text{ if } c > \frac{p-1}{2}. \end{cases}$$

This establishes the result. □

REFERENCES

[1] George E. Andrews, *Number Theory*, Courier Dover Publications, 2012.

[2] Zvi Arad and Harvey I. Blau, *On table algebras and applications to finite group theory*, Journal of Algebra, Volume 138, Issue 1, April 1991, Pages 137-185.

[3] Zvi Arad, Elsa Fisman, and Mikhail Muzychuk, *Generalized table algebras*, Israel Journal of Mathematics, Volume 114, Issue 1, December 1999, Pages 29-60.

[4] Zvi Arad and Mikhail Muzychuk, *Standard Integral Table Algebras Generated by a Non-real Element of Small Degree*, Lecture Notes in Mathematics Vol. 1773, Springer, Berlin, 2002.

[5] Sejeong Bang and Mitsugu Hirasaka, *Construction of association schemes from difference sets*, European Journal of Combinatorics, Volume 26, Issue 1, January 2005, Pages 59-74.

[6] Harvey I. Blau, *Table Algebras*, European Journal of Combinatorics, Volume 30, Issue 6, August 2009, Pages 1426-1455.

[7] Harvey I. Blau *Decomposition of products in nilpotent table algebras*, Journal of Algebra, Volume 323, Issue 5, March 2010, Pages 1581-1592.

[8] Harvey I. Blau and Bangteng Xu, *Irreducible characters of wreath products in reality-based algebras and applications to association schemes*, Journal of Algebra, Volume 412, August 2014, Pages 155-172.

[9] Harvey I. Blau and Bangteng Xu, unpublished manuscript.

[10] Robert M. Gray, *Toeplitz and Circulant Matrices: A Review*, Now Publishers Inc., 2006.

[11] Akihide Hanaki and Izumi Miyamoto, *Classification of association schemes with small vertices*, December 2012, retrieved from http://kissme.shinshu-u.ac.jp/as/

[12] Paul-Hermann Zieschang, *Theory of Association Schemes*, Springer, New York, 2005.